KASPERSKY LAB

Kaspersky Anti-Virus 5.6 for Linux Mail Server

GUIDE DE L'ADMINISTRATEUR

KASPERSKY ANTI-VIRUS 5.6 FOR LINUX MAIL SERVER

Guide de l'administrateur

http://www.kaspersky.com

Date de révision : November, 2008

Table des matières

CHAPITRE 1. INTRODUCTION

Kaspersky Anti-Virus® 5.6 for Linux Mail Server (désigné par la suite par *Kaspersky Anti-Virus* ou par l'*application*) est conçu pour le traitement antivirus du trafic de courrier et des systèmes de fichiers de serveurs sous systèmes d'exploitation Linux ou FreeBSD, utilisant les logiciels de messagerie Sendmail, Postfix, qmail, Exim MTA.

Cette application offre les fonctionnalités suivantes :

- Recherche de menaces sur tous les systèmes de fichiers serveurs ainsi que des messages entrants et sortants.
- Détection des fichiers infectés, suspects, endommagés et protégés par mot de passe, y compris les fichiers qui ne peuvent être analysés.
- Neutralisation de menaces découvertes dans les fichiers ou les messages de courrier. Désinfection d'objets infectés.
- Sauvegarde de sécurité des messages électroniques avant traitement et filtrage antivirus.
- Traitement du trafic des messages conformément à des règles prédéfinies pour des groupes d'expéditeurs ou de destinataires.
- Assure le filtrage par contenu du trafic de courrier par nom et type de pièce jointe, et fait appel à des règles de traitement individuelles sur les objets filtrés.
- Informe l'administrateur, les expéditeurs et les destinataires de la détection de messages contenant des objets infectés, suspects ou protégés par mot de passe, ou de messages qu'il n'est pas possible d'analyser.
- Génération de statistiques et de rapports sur l'activité de l'application.
- Mise à jour des bases antivirus, de manière planifiée ou à la demande, en téléchargeant les mises à jour depuis les serveurs spécialisés de Kaspersky Lab.

  La base antivirus est utilisée pour rechercher et nettoyer les objets infectés. Pendant l'analyse, chaque fichier est analysé à la recherche de menaces, en comparant son code avec le code typique de différentes menaces.
- Configuration et administration de Kaspersky Anti-Virus à la fois en local (avec les moyens standard du S.E., comprenant l'utilisation d'options en ligne de commande, de signaux et la modification du fichier de

configuration de l'application) et à distance grâce à l'interface Web fournie par le programme Webmin.

- Utilisation de SNMP pour l'obtention d'informations sur la configuration et les statistiques d'activité du produit, et configuration de l'application pour générer des pièges SNMP quand des événements spécifiés se produisent.

1.1. Nouveautés

La version 5.6 de **Kaspersky Anti-Virus for Linux Mail Server** combine les caractéristiques de Kaspersky Anti-Virus 5.5 for Linux Mail Server et FreeBSD et de Kaspersky Anti-Virus 5.6 pour Sendmail avec l'API Milter, auxquelles s'ajoutent les améliorations suivantes :

- L'intégration de la file d'attente en amont et en aval est prise en charge pour Exim. Dans le cas de l'intégration en amont de la file d'attente, le message est transféré pour analyse avant d'être ajouté à la file d'attente du système de messagerie, tandis que l'intégration en aval signifie que les messages sont analysés après leur ajout à la file d'attente. L'intégration automatique par un script de configuration de l'application est désormais disponible. Voir Chapitre 4 à la p. 30 pour plus de détails sur la procédure d'intégration.

- Les possibilités de configuration des fonctions d'analyse du courrier ont été améliorées : deux méthodes d'analyse sont maintenant disponibles. Un message peut être analysé en tant qu'objet simple ou par une approche combinée – d'abord comme un simple objet puis comme la collection de ses parties. Ces méthodes diffèrent quant au niveau de protection assuré. Reportez-vous à la section 5.2 à la p. 50 pour plus de détails.

- La configuration de l'application a changé. La configuration séparée de groupes d'expéditeurs et de destinataires est maintenant prise en charge. Reportez-vous à la section 5.1 à la p.48 pour plus de détails sur la configuration de groupes.

- La liste des actions applicables aux messages a été enrichie. Ajout d'un nouveau type d'actions, dépendant du logiciel malveillant découvert. Reportez-vous à la section 5.4 à la p. 54 pour plus de détails.

- Les prestations de filtrage par contenu ont été améliorées par l'ajout de critères de filtrage par taille de pièce jointe. Reportez-vous à la section 5.3.2 à la p. 53 pour plus de détails.

- La bibliothèque de modèles de notifications a été enrichie par de nouveaux modèles administrateurs. Les modèles sont désormais conservés dans un répertoire séparé.
- La possibilité de placer les objets infectés dans une zone de sauvegarde n'est plus implémentée.
- Les fonctions de sauvegarde ont été améliorées – des fichiers d'information peuvent être créés pour chacune des entrées de sauvegarde. Reportez-vous à la section 5.6 à la p.59 pour plus de détails.
- La génération de rapports a été améliorée en augmentant les niveaux de consignations. Reportez-vous à la section 9.1 à la p.91 pour plus de détails.
- Les fonctions statistiques ont été étendues par l'ajout de statistiques par message. Reportez-vous à la section 9.2 à la p.94 pour plus de détails.
- Des requêtes SNMP sur la configuration, des statistiques et des indicateurs d'état de l'application sont désormais pris en charge. Des pièges SNMP sont également prises en charge. Reportez-vous à la section 10.1 à la p. 98 pour plus de détails.
- Un outil d'administration sur la ligne de commande est compris dans le paquet de l'application. Il est capable de gérer plusieurs aspects du fonctionnement de l'application. Reportez-vous à la section 10.3 à la p. 105 pour plus de détails.

1.2. Spécifications requises

Les spécifications système pour Kaspersky Anti-Virus sont :

- Spécifications matérielles pour un serveur de messagerie avec un trafic journalier d'environ 200 mo :
  - Intel Pentium IV, processeur 3 GHz ou supérieur ;
  - 1 Go RAM ;
  - 200 mo d'espace disque disponible (non compris l'espace nécessaire à la conservation des copies de sauvegarde des messages).
- Configuration logicielle :
  - L'un des systèmes d'exploitation 32 bits suivants :
    - Red Hat Enterprise Linux Server 5.2 ;
    - Fedora 9 ;

- SUSE Linux Enterprise Server 10 SP2 ;
- openSUSE 11.0 ;
- Debian GNU/Linux 4.0 r4 ;
- Mandriva Corporate Server 4.0 ;
- Ubuntu 8.04.1 Server Edition ;
- FreeBSD 6.3, 7.0.

- L'un des systèmes d'exploitation 64 bits suivants :
  - Red Hat Enterprise Linux Server 5.2 ;
  - Fedora 9 ;
  - SUSE Linux Enterprise Server 10 SP2 ;
  - openSUSE Linux 11.0.
- L'un des systèmes de messagerie suivants : Sendmail 8.12.x ou supérieur, qmail 1.03, Postfix 2.x, Exim 4.x ;
- Facultatif – le logiciel Webmin (www.webmin.com) pour l'administration à distance de Kaspersky Anti-Virus ;
- Perl version 5.0 ou supérieur (www.perl.org).

1.3. Services aux utilisateurs enregistrés

Kaspersky Lab offre à ses utilisateurs légalement enregistrés un éventail de prestations complémentaires leur permettant d'utiliser plus efficacement le logiciel Kaspersky Anti-Virus.

En vous enregistrant, vous devenez utilisateur agréé du programme et durant toute la période de validité de votre souscription, vous bénéficiez des prestations suivantes :

- mises à niveau du logiciel d'application ;
- assistance téléphonique et par messagerie sur l'installation, la configuration et l'utilisation de ce logiciel antivirus ;
- communications sur les nouveaux produits de Kaspersky Lab, et les nouvelles attaques virales. Ce service est offert aux utilisateurs ayant souscrit un abonnement à la liste de diffusion de Kaspersky Lab.

Remarque :

Kaspersky Lab n'assure pas de service sur le fonctionnement ou l'utilisation de votre système d'exploitation, de logiciels d'autres fabricants ou d'autres technologies.

CHAPITRE 2. STRUCTURE ET ALGORITHME DE FONCTIONNEMENT DE L'APPLICATION

Kaspersky Anti-Virus comprend les composants suivants :

- Filtre – le service de connexion au système de messagerie, c'est un programme séparé qui assure l'interaction entre Kaspersky Anti-Virus et un agent de transfert de messages (MTA, message transfer agent) spécifique. Le paquet de distribution comprend des modules pour chaque système de messagerie pris en charge :
  - *kav4lms-milter* – service Milter pour la connexion avec Sendmail et Postfix via l'API Milter.
  - *kav4lms-filter* – service SMTP pour la connexion à Postfix et Exim.
  - *kav4lms-qmail* – gestionnaire de file d'attente de messages pour qmail.
- *kavmd* – service central de l'application, à l'écoute des requêtes de filtre et implémentant les fonctions antivirus de l'application protégeant le trafic de messagerie.
- *kav4lms-kavscanner* – assure la protection antivirus des systèmes de fichiers serveurs.
- *kav4lms-keepup2date* – assure la mise à jour de la base antivirus en téléchargeant les nouvelles données depuis les serveurs de mises à jour de Kaspersky Lab ou d'un répertoire local.
- *kav4lms-licensemanager* – composant gestionnaire des clés de produit : installation, suppression, affichage d'informations statistiques.
- *kav4lms.wbm* – complément logiciel pour Webmin pour la gestion à distance de l'application à travers une interface Web (optionnelle), qui permet de configurer et de lancer la mise à jour de la base antivirus, d'afficher des informations statistiques, de définir des actions sur les objets en fonction de leur état, et de surveiller les données d'activité des applications.

- *kav4lms-cmd* – utilitaire de gestion de l'antivirus depuis la ligne de commande.

L'application utilise l'algorithme suivant pour contrôler les messages :

1. Le filtre reçoit un message depuis l'agent de transfert de messages ou MTA. Si le filtre et le service central s'exécutent sur le même ordinateur, ce sont les noms des fichiers de messages qui sont transmis pour analyse, au lieu des messages réels.

2. Le filtre détermine les groupes auxquels le message appartient, sélectionne celui avec la priorité la plus haute (section 5.1 à la p. 48) puis transmet pour analyse le message au service central de l'application. Si le groupe n'existe pas, l'application applique au message les règles du groupe **Default** compris dans le paquet de distribution.

   Le service central examine le message en fonction des paramètres précisés par le fichier de configuration du groupe. En fonction de la méthode définie par la **stratégie**, l'application peut analyser le message comme un seul objet compact ou utiliser une approche combinée, en analysant d'abord l'objet comme un tout, puis ses parties individuellement (section 5.2 à la p. 50).

   L'analyse combinée est plus approfondie et assure un meilleur degré de protection, au prix de performances un peu inférieures, par la vérification du message dans son ensemble ou par celle du message et de chacune de ses parties (stratégie combinée).

3. Si l'analyse antivirus du courrier est activée (section 5.3 à la p. 50), le service central vérifie un message en tant qu'objet simple. Conformément à l'état attribué après cette vérification (section 5.3.1 à la p. 51) le service central peut interdire la réception du message, le refuser ou l'autoriser, le remplacer par un avertissement ou modifier ses en-têtes (section 5.4 à la p. 54). Si un traitement spécial est défini pour certains types de logiciels malveillants individuels (option **VirusNameList**), les actions spécifiées sont exécutées quand les types en question sont détectées(option **VirusNameAction**). L'ordre de traitement des messages est précisé dans le fichier de configuration du groupe.

   L'application crée une copie de sauvegarde du message original avant de lui appliquer un traitement, si cette opération est activée dans les paramètres de groupe.

4. Après l'analyse antivirus du message, l'application exécute le filtrage, si cette opération est activée dans les paramètres de groupe.

   Le filtrage peut être exécuté en fonction du nom, du type ou de la taille de la pièce jointe (section 5.3.2 à la p. 53). L'examen se traduit par

l'application des actions définies par les paramètres de filtrage du fichier de configuration du groupe. Parmi les objets traités, ceux qui correspondent aux critères de filtrage sont transmis pour analyse avancée pièce par pièce, si la méthode d'analyse combinée est activée dans les paramètres du groupe.

5. Pendant l'inspection pièce par pièce du courrier, l'application décompose sa structure MIME et traite les composants du message.

   Dans le message, les objets sont traités conformément à l'état qui leur est attribué individuellement, sans tenir compte de l'état attribué au message dans son ensemble.

   Si un message considéré comme un objet simple est identifié comme étant infecté, mais qu'aucune menace n'est trouvée après l'examen de ses parties, l'application applique à l'ensemble du message l'action définie pour un courrier infecté (option **InfectedAction**). Si le nombre d'imbrications d'un objet en pièce jointe, dans un message non infecté, dépasse la limite spécifiée dans les paramètres du groupe (option **MaxScanDepth**), l'application applique au message dans son ensemble l'action définie pour les messages qui provoquent une erreur au cours de leur analyse (option **ErrorAction**).

   Pendant son traitement des objets dans les messages, le service central peut renommer, supprimer ou remplacer un objet par un avertissement, ajouter des en-têtes d'information ou autoriser la transmission du message (section 5.4 à la p. 54). Les messages infectés sont réparés. L'application crée une copie de sauvegarde du message original dans son ensemble avant d'appliquer un traitement à son objet (sauf si c'est déjà fait), si cette opération est activée dans les paramètres de groupe.

6. Après analyse et traitement du message, le service central renvoie de nouveau le message vers le filtre. Le message traité, accompagné de notifications sur le résultat de l'analyse et de la désinfection, est transmis au MTA, qui délivre à son tour le message aux utilisateurs locaux, ou le redirige vers d'autres serveurs de messagerie.

CHAPITRE 3. INSTALLATION ET DESINSTALLATION DE L'APPLICATION

Avant d'installer Kaspersky Anti-Virus, nous vous recommandons de préparer votre système de la manière suivante :

- Assurez-vous que votre système est conforme aux spécifications matérielles et logicielles minimales requises, décrites dans la section 1.2 à la page 9.
- Réalisez des copies de sauvegardes des fichiers de configuration du système de messagerie installé sur votre serveur.
- Configurez votre connexion Internet.
- Connectez-vous au système avec des droits d'accès **root**, ou sous tout autre compte disposant des privilèges d'un super-utilisateur.

Attention !

Nous vous conseillons d'installer l'application pendant les heures de faible trafic, lorsque le trafic de courrier est au plus bas.

3.1. Installation de l'application sur un serveur Linux

Pour les serveurs exploités sous Linux, Kaspersky Anti-Virus est distribué dans *deux paquets d'installation différents,* en fonction du type de votre distribution Linux.

Pour installer l'application sous Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise Server, openSUSE et Mandriva Linux, utilisez le paquet *rpm*.

Pour démarrer l'installation de Kaspersky Anti-Virus à partir du paquet .rpm, tapez ce qui suit sur la ligne de commande :

```
# rpm -i <package_name>
```

Attention !

Après avoir installé l'application à partir du paquet rpm, vous devez exécuter le script *postinstall.pl* pour la configuration post-installation. L'emplacement par défaut des scripts *postinstall.pl* se trouve dans le répertoire */opt/kaspersky/kav4lms/lib/bin/setup/* (sous Linux) et dans le répertoire */usr/local/libexec/kaspersky/kav4lms/setup/* (sous FreeBSD) !

Pour les versions Debian GNU/Linux et Ubuntu, l'installation est assurée par un paquet .deb.

Pour démarrer l'installation de Kaspersky Anti-Virus à partir du paquet .deb, tapez ce qui suit sur la ligne de commande :

```
# dpkg -i <package_name>
```

Après envoi de cette commande, l'application sera installée automatiquement. Une fois installation terminée, des informations sur la configuration de post-installation sont affichées (section 3.4 à la p. 21).

Attention !

La procédure d'installation de l'application pour les distributions Mandriva présente quelques particularités.

Pour permettre le démarrage correct de Kaspersky Anti-Virus après son installation, vous devez vous assurer que le répertoire /root/tmp/ est bien utilisé pour stocker les fichiers temporaires du système d'exploitation et que le compte utilisé pour lancer l'application (kluser, par défaut) possède des droits d'écriture dans le répertoire.

Vous devrez peut-être modifier les droits d'accès du répertoire, redéfinir ou supprimer les variables d'environnement **TMP** et **TEMP**, pour permettre au système d'utiliser un autre répertoire (tel que /tmp/) avec les droits nécessaire pour le fonctionnement de l'application.

3.2. Installation de l'application sur un serveur FreeBSD

Le fichier de distribution pour l'installation de Kaspersky Anti-Virus sur des serveurs sous S.O. FreeBSD est fourni sus la forme d'un paquet *pkg*.

Pour démarrer l'installation de Kaspersky Anti-Virus à partir du paquet pkg, tapez ce qui suit sur la ligne de commande :

```
# pkg_add <package_name>
```

Après envoi de cette commande, l'application sera installée automatiquement. Une fois installation terminée, des informations sur la configuration de post-installation sont affichées (section 3.4 à la p. 21).

3.3. Emplacement des fichiers de l'application

Pendant l'installation de Kaspersky Anti-Virus, l'installateur du produit recopie les fichiers d'application dans les répertoires du programme, sur le serveur.

Attention !

Pour que les pages du manuel de l'application soient disponibles par une commande man <nom_de_page_man>, les opérations suivantes sont nécessaires :

- pour les distributions Debian Linux, Ubuntu Linux, SUSE Linux, ajoutez la ligne suivante au fichier */etc/manpath.config* :

  `MANDATORY_MANPATH /opt/kaspersky/kav4lms/share/man`

- pour les distributions Red Hat Linux et Mandriva Linux, ajoutez la ligne suivante au fichier */etc/man.config* :

  `MANPATH /opt/kaspersky/kav4lms/share/man`

- pour les distributions FreeBSD distributions, ajoutez la ligne suivante au fichier /etc/manpath.config :

  `MANDATORY_MANPATH /usr/local/man`

Si votre système utilise la variable **MANPATH**, ajoutez à sa liste de valeurs le chemin du répertoire contenant les pages du manuel de l'application, en exécutant la commande suivante :

```
# export MANPATH=$MANPATH:<chemin du répertoire des pages du manuel>
```

3.3.1. Emplacement des fichiers sur un serveur Linux

Les emplacements par défaut des fichiers Kaspersky Anti-Virus sur un serveur exploité sous Linux sont les suivants :

/etc/opt/kaspersky/kav4lms.conf – fichier de configuration principal de l'application ;

/etc/opt/kaspersky/kav4lms/ – répertoire des fichiers de configuration de Kaspersky Anti-Virus :

groups.d/ – répertoire des fichiers de configuration des groupes ;

default.conf – fichier de configuration, avec les paramètres du groupe par défaut ;

locale.d/strings.en – fichier de chaînes, utilisées par l'application ;

profiles/ – répertoire de profils de configuration prédéfinis :

default_recommandé/ – répertoire des fichiers de configuration par défaut ;

high_overall_security/ – répertoire des fichiers de configuration du profil de sécurité maximum ;

high_scan_speed/ répertoire des fichiers de configuration du profil de vitesse maximum ;

modèles/ – répertoire des modèles de notifications ;

templates-admin/ – répertoire des modèles de notifications pour l'administrateur ;

kav4lms.conf – le fichier de configuration principal de l'application ;

/opt/kaspersky/kav4lms/ – répertoire principal de Kaspersky Anti-Virus, contenant :

bin/ – répertoire des fichiers exécutables de tous les composants de Kaspersky Anti-Virus :

kav4lms-cmd – fichier exécutable de l'outil de ligne de commande ;

kav4lms-setup.sh – script d'installation de l'application ;

kav4lms-kavscanner – fichier exécutable du composant analyseur du système de fichiers ;

kav4lms-licensemanager – fichier exécutable du composant gestionnaire des clés ;

kav4lms-keepup2date – fichier exécutable du composant d'actualisation ;

sbin/ – répertoire contenant les fichiers exécutables des services de l'application ;

lib/ – répertoire des fichiers de bibliothèque de Kaspersky Anti-Virus ;

bin/avbasestest – outil de validation des mises à jour de bases antivirus téléchargées, utilisé par le composant *kav4lms-keepup2date* ;

share/doc/ – répertoire contenant l'accord de licence et la documentation de déploiement ;

share/man/ – répertoire contenant les fichiers du manuel ;

share/scripts/ – répertoire des scripts d'application ;

share/snmp-mibs/ – répertoire de Kaspersky Anti-Virus MIB ;

share/webmin/ – répertoire du complément logiciel pour Webmin ;

/etc/init.d/ – répertoire des scripts de contrôle des services de l'application :

kav4lms – script de contrôle du service central de l'application ;

kav4lms-filters – script de contrôle pour le filtre Kaspersky Anti-Virus ;

/var/opt/kaspersky/kav4lms/ – répertoire contenant des données variables de Kaspersky Anti-Virus :

backup/ – répertoire des copies de sauvegarde des messages et des fichiers d'information ;

bases/ – répertoire des bases antivirus ;

bases.backup/ – répertoire des copies de sauvegarde des bases antivirus ;

licenses/ – répertoire des fichiers de clés ;

nqueue/ – répertoire des files d'attente de messages ;

patches/ – répertoire des correctifs des modules d'application ;

stats/ – répertoire des fichiers de statistiques ;

updater/ – répertoire du fichier d'informations de la mise à jour précédente.

Attention !

La spécification Linux des chemins d'accès est utilisée dans la suite de ce document.

3.3.2. Emplacement des fichiers sur un serveur FreeBSD

Les emplacements par défaut des fichiers Kaspersky Anti-Virus sur un serveur exploité sous FreeBSD sont les suivants :

/usr/local/etc/kaspersky/kav4lms.conf – fichier de configuration principal de l'application ;

/usr/local/etc/kaspersky/kav4lms/ – répertoire des fichiers de configuration de Kaspersky Anti-Virus :

groups.d/ – répertoire des fichiers de configuration des groupes ;

default.conf – fichier de configuration, avec les paramètres du groupe par défaut ;

locale.d/strings.en – fichier de chaînes utilisées par l'application ;

profiles/ – répertoire de profils de configuration prédéfinis :

default_recommandé/ – répertoire des fichiers de configuration par défaut ;

high_overall_security/ – répertoire des fichiers de configuration du profil de sécurité maximum ;

high_scan_speed/ – répertoire des fichiers de configuration du profil de vitesse maximum ;

modèles/ – répertoire des modèles de notifications ;

templates-admin/ – répertoire des modèles de notifications pour l'administrateur ;

kav4lms.conf – le fichier de configuration principal de l'application.

/usr/local/bin/ – répertoire des fichiers exécutables de tous les composants de Kaspersky Anti-Virus :

kav4lms-cmd – fichier exécutable de l'outil de ligne de commande ;

kav4lms-setup.sh - script d'installation de l'application ;

kav4lms-kavscanner – fichier exécutable du composant analyseur du système de fichiers ;

kav4lms-licensemanager – fichier exécutable du composant gestionnaire des clés ;

kav4lms-keepup2date – fichier exécutable du composant d'actualisation ;

/usr/local/sbin/ – répertoire des fichiers exécutables des services de l'application ;

/usr/local/etc/rc.d/ – répertoire des scripts de contrôle pour les services de l'application :

kav4lms.sh – script de contrôle du service central de l'application ;

kav4lms-filters.sh – script de contrôle pour le filtre Kaspersky Anti-Virus ;

/usr/local/lib/kaspersky/kav4lms/ – répertoire des fichiers de bibliothèque de Kaspersky Anti-Virus ;

/usr/local/libexec/kaspersky/kav4lms/avbasestest – outil de validation des mises à jour de bases antivirus téléchargées, utilisé par le composant *kav4lms-keepup2date* ;

/usr/local/share/doc/kav4lms/ – répertoire contenant l'accord de licence et la documentation de déploiement ;

/usr/local/man/ – répertoire des fichiers du manuel ;

/usr/local/share/kav4lms/scripts/ – répertoire de scripts de l'application ;

/usr/local/share/kav4lms/snmp-mibs/ – répertoire des fichiers MIB pour Kaspersky Anti-Virus ;

/usr/local/share/kav4lms/webmin/ – répertoire du complément logiciel pour l'application Webmin ;

/var/db/kaspersky/kav4lms/ – répertoire contenant des données variables de Kaspersky Anti-Virus :

backup/ – répertoire des copies de sauvegarde des messages et des fichiers d'information ;

bases/ – répertoire des bases antivirus ;

bases.backup/ – répertoire des copies de sauvegarde des bases antivirus ;

licenses/ – répertoire des fichiers de clés ;

nqueue/ – répertoire des files d'attente de messages ;

patches/ – répertoire des correctifs des modules d'application ;

stats/ – répertoire des fichiers de statistiques ;

updater/ – répertoire du fichier d'informations de la mise à jour précédente.

3.4. Configuration postérieure à l'installation

Immédiatement après avoir recopié les fichiers d'application dans le serveur, le processus de configuration du système démarre. La procédure de configuration démarre automatiquement ou bien, si le gestionnaire de paquets (*rpm*, par exemple) ne permet pas l'usage de scripts interactifs, vous devez la lancer manuellement.

Pour lancer la configuration du produit manuellement, tapez ce qui suit sur l'invite de commande :

Sous Linux :

```
# /opt/kaspersky/kav4lms/lib/bin/setup/postinstall.pl
```

Sous FreeBSD :

```
# /usr/local/libexec/kaspersky/kav4lms/setup/postinstall.pl
```

Une invite vous présente au choix les opérations suivantes :

1. Si des fichiers de configuration de Kaspersky Anti-Virus 5.5 for Linux Mail Server ou de Kaspersky Anti-Virus 5.6 for Sendmail avec l'API Milter sont retrouvés dans l'ordinateur, l'application propose à cette étape de choisir le fichier à convertir et à enregistrer dans le format de la version courante du produit. En sélectionnant l'un des fichiers, vous aurez la possibilité de remplacer le fichier de configuration par défaut compris dans le paquet de distribution par le fichier restauré et converti.

   Pour remplacer le fichier de configuration du paquet de distribution par le fichier restauré, tapez la réponse **yes**. Pour annuler le remplacement, tapez **no**.

   Par défaut, les fichiers de configuration convertis sont enregistrés dans les répertoires suivants :

```
kav4mailservers -
/etc/opt/kaspersky/kav4lms/profiles/kav4mailservers5.
5-converted
kavmilter -
/etc/opt/kaspersky/kav4lms/profiles/kavmilter5.6-
converted
```

2. Spécifiez le chemin au fichier clé.

   Notez que si la clé du produit n'est pas installée, l'antivirus ne fera pas la mise à jour des bases de données et ne créera pas la liste des domaines protégés au cours de l'installation. Dans ce cas, vous devrez réaliser ces étapes manuellement après l'installation d'une clé.

3. Spécifiez les paramètres du serveur proxy utilisé pour la connexion à Internet avec la mise en forme suivante :

   ```
   http://<IP-proxy_server_address>:<port>
   ```

   ou

   ```
   http://<user_name>:<password>@<proxy_server_IP_addres
   s>:<port>
   ```

   if the proxy server requires authentication.

   Si aucun serveur proxy n'est utilisé pour se connecter à Internet, tapez la réponse **no**.

   Le composant *kav4lms-keepup2date* pour la mise à jour utilise cette valeur pour se connecter à la source des mises à jours.

4. Mettre à jour les bases antivirus. Pour ce faire, tapez la réponse **yes**. Pour ignorer les mises à jour pendant cette étape, tapez **no**. Vous pourrez exécuter la procédure de mise à jour par la suite à l'aide du composant *kav4lms-keepup2date* (section 7.2 à la p. 83 pour plus de détails).

   Remarque :

   Les bases antivirus ne peuvent être mises à jour que si une clé de produit est installée.

5. Configurez les mises à jour automatiques des bases antivirus. Pour ce faire, tapez la réponse **yes**. Pour ignorer la configuration des les mises à jour automatiques pendant cette étape, tapez **no**. Vous pourrez configurer les mises à jour plus tard, à l'aide du composant *kav4lms-setup* (section 7.1 à la p. 82) ou manuellement (section 10.2 à la p. 102 pour plus de détails).

Attention !

Dans le cas de l'intégration du produit avec qmail, il convient de configurer les mises à jour automatiques comme ceci :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh      \
--install-cron=updater --user=root
```

6. Installez le module Webmin afin de pouvoir gérer Kaspersky Anti-Virus à l'intérieur de l'interface Web de l'outil Webmin.

   Le complément logiciel du gestionnaire à distance ne sera installé que si Webmin est installé dans le répertoire par défaut. Après l'installation du plug-in, des instructions appropriées s'afficheront pour configurer l'interaction avec l'application.

   Tapez **yes** pour installer le module Webmin ou **no** pour annuler son installation.

7. Déterminez la liste des domaines dont le trafic de messagerie doit être protégé contre les virus. La valeur par défaut est **localhost, localhost.localdomain**. Pour l'utiliser, tapez **Entrée**.

   Pour préciser la liste des domaines manuellement, entrez-les sur la ligne de commande. Vous pouvez définir plusieurs valeurs séparées pas des virgules ; les caractères génériques et les expressions régulières sont également acceptées. Les points doivent être précédés par un caractère barre-inversée.

   Par exemple :

   ```
   re:.*\.example\.com
   ```

8. Intégration de Kaspersky Anti-Virus avec MTA. Vous pouvez accepter la méthode suggérée par défaut pour l'intégration avec le MTA localisé sur l'ordinateur ou annuler et effectuer manuellement l'intégration. Reportez-vous à Chapitre 4 à la p. 30 pour une description détaillée de l'intégration avec MTA.

   Par défaut, l'intégration aval de la file d'attente avec Exim fait appel à la modification du routage (section 4.1.1 à la p. 31).

Attention !

Pendant l'intégration automatique avec Sendmail, le script essaie toujours de modifier le fichier *.mc* parce que les mises à jours postérieures ne détruiront pas les modifications introduites. Si le fichier *.mc* contient des adressages “include” faisant référence à des fichiers *.mc* qui n'existent pas, il n'est pas alors possible d'utiliser ce fichier pour l'intégration de Kaspersky Anti-Virus. Dans ce cas, installez le paquet **sendmail-cf** pour faire l'intégration à partir du fichier *.cf*.

Si le fichier *.mc* ne peut pas être utilisé, l'intégration de l'application fait alors appel au fichier *.cf*.

3.5. Configuration des règles d'accès dans les systèmes SELinux et AppArmor

Pour créer un module SELinux contenant les règles nécessaires au fonctionnement de Kaspersky Anti-Virus, effectuez les étapes suivantes après l'installation et l'intégration de l'application avec le système de messagerie :

1. Basculez SELinux en mode permissif :

   ```
   # setenforce Permissive
   ```

2. Envoyez un ou plusieurs messages de test et assurez-vous qu'il sont passés par l'analyseur antivirus et ont été remis à leurs destinataires.

3. Créez un module de règles, à partir des enregistrements sur les blocages appliqués :

   Pour Fedora :

   ```
   # audit2allow -l –M kav4lms -i /var/log/messages
   ```

   Pour RHEL :

   ```
   # audit2allow -l -M kav4lms –i\
   /var/log/audit/audit.log
   ```

4. Chargez le module de règles ainsi obtenu :

   ```
   # semodule -i kav4lms.pp
   ```

5. Basculez SELinux en mode restrictif :

   ```
   # setenforce Enforcing
   ```

Si de nouveaux messages d'audit appartenant à Kaspersky Anti-Virus apparaissent, il convient de mettre à jour le fichier module des règles :

Pour Fedora :

```
# audit2allow -l –M kav4lms -i /var/log/messages
# semodule –u kav4lms.pp
```

Pour RHEL :

```
# audit2allow -l –M kav4lms -i /var/log/audit/audit.log
# semodule –u kav4lms.pp
```

Pour des informations complémentaires, reportez-vous à :

- **RedHat Enterprise Linux**: “Red Hat Enterprise Linux Deployment Guide”, chapitre 44 “Security and SELinux”.
- **Fedora**: Fedora SELinux Project Pages.
- **Debian GNU/Linux**: manuel « Configuring the SELinux Policy » du paquet selinux-doc « Documentation for Security Enhanced Linux ».

Pour mettre à jour les profils AppArmor nécessaires au fonctionnement de Kaspersky Anti-Virus, effectuez les étapes suivantes après l'installation et l'intégration de l'application avec le système de messagerie :

1. Basculez toutes les règles d'application en mode audit (“complain”) :

   ```
   # aa-complain /etc/apparmor.d/*
   # /etc/init.d/apparmor reload
   ```

2. Redémarrez le système de messagerie :

   ```
   # /etc/init.d/postfix restart
   ```

3. Redémarrez kav4lms et kav4lms-filters :

   ```
   # /etc/init.d/kav4lms restart
   # /etc/init.d/kav4lms-filters restart
   ```

4. Envoyez un ou plusieurs messages de test et assurez-vous qu'il sont passés par l'analyseur antivirus et ont été remis à leurs destinataires.

5. Lancez l'outil de mise à jour des profils :

   ```
   # aa-logprof
   ```

6. Rechargez les règles pour AppArmor :

   ```
   # /etc/init.d/apparmor reload
   ```

7. Basculez toutes les règles d'application en mode restrictif :

```
# aa-enforce /etc/apparmor.d/*
# /etc/init.d/apparmor reload
```

Si de nouveaux messages d'audit appartenant à Kaspersky Anti-Virus apparaissent, les étapes 5 et 6 doivent être répétées.

Pour des informations complémentaires, reportez-vous à :

- **OpenSUSE** et **SUSE Linux Enterprise Server**: “Novell AppArmor Quick Start”, “Novell AppArmor Administration Guide”.
- **Ubuntu**: “Ubuntu Server Guide”, chapitre 8, “Security”.

3.6. Installation du module Webmin pour gérer Kaspersky Anti-Virus

Il est possible de contrôler à distance l'activité de Kaspersky Anti-Virus depuis un navigateur Web browser utilisant Webmin.

Webmin est un programme qui simplifie l'administration des systèmes Linux/Unix. Le logiciel possède une structure modulaire, prenant en charge les connexions de nouveaux modules ou de modules personnalisés. Vous trouverez des informations complémentaires sur Webmin et ses paquets distribution téléchargeables depuis le site Web officiel du logiciel, à l'adresse : www.webmin.com.

Le paquet de distribution de Kaspersky Anti-Virus contient un module pour Webmin qu'il est possible de connecter soit à l'étape de configuration postérieure à l'installation de l'application (section 3.4 à la p. 21) si le système est déjà équipé de Webmin, soit à tout moment après l'installation de Webmin.

La partie suivante de ce manuel décrit en détail la procédure requise pour connecter le module Webmin afin d'administrer Kaspersky Anti-Virus.

Si les paramètres par défaut ont été sélectionnés lors de l'installation de Webmin, vous pouvez alors accéder au logiciel après avoir configuré un navigateur Web pour se connecter au port 10000 via HTTP/HTTPS.

Pour installer le module Webmin pour la gestion de Kaspersky Anti-Virus :

1. Utilisez votre navigateur Web pour accéder à Webmin avec des privilèges d'administrateur.
2. Sélectionnez l'onglet **Webmin Configuration** dans le menu puis dirigez-vous à la section **Webmin modules**.

3. Sélectionnez l'option **From Local File** dans la section **Install module** puis cliquez sur (Figure 1).

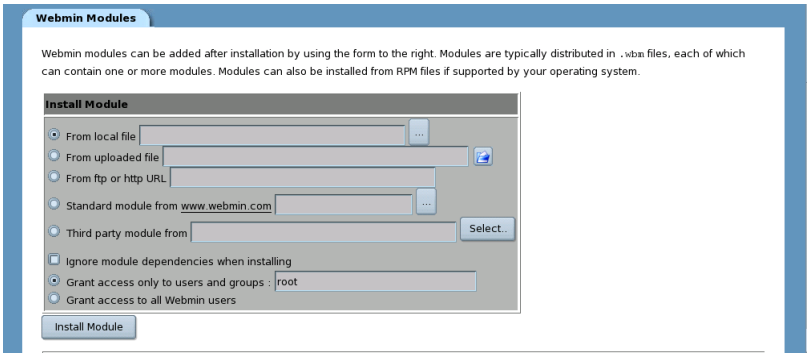

Figure 1. Section **Install Module**

4. Sélectionnez le chemin du module Webmin du produit et cliquez sur **OK**.

Remarque :

Le module Webmin est le fichier *mailgw.wbm*, installé par défaut dans le répertoire */opt/kaspersky/kav4lms/share/webmin/* (pour les distributions Linux), ou */usr/local/share/kav4lms/webmin/* (pour les distributions FreeBSD).

Un message confirmera à l'écran l'installation réussie du module Webmin.

Pour accéder aux paramètres de Kaspersky Anti-Virus, vous pouvez cliquer sur son icône, dans l'onglet **Others** (Figure 2).

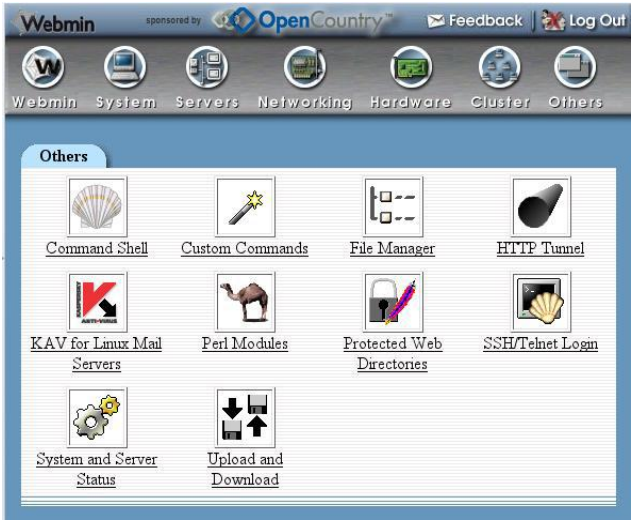

Figure 2. L'icône de Kaspersky Anti-Virus dans l'onglet **Others**

3.7. Suppression de l'application

La suppression de Kaspersky Anti-Virus dans le serveur exige des privilèges de super-utilisateur (**root**). Si vous ne disposez pas de ces privilèges au moment de la désinstallation, vous devez d'abord ouvrir une session en tant qu'utilisateur **root**.

Attention !

La procédure de suppression arrête l'application sans autre intervention de l'utilisateur !

Pendant la désinstallation, l'application est arrêtée, les fichiers et les répertoires créés lors de l'installation du produit sont supprimés. Cependant, les fichiers et répertoires créés ou modifiés par l'administrateur (fichier de configuration de l'application, fichiers de configuration des groupes, fichiers modèle de notification, répertoires de sauvegarde, fichier clé) seront conservés.

Il est possible de lancer la procédure de suppression de l'application par différentes méthodes, en fonction du gestionnaire de paquets du système. Nous allons examiner ces méthodes de plus près.

Pour supprimer une installation de Kaspersky Anti-Virus réalisée à partir d'un paquet rpm, tapez le texte suivant dans une ligne de commande :

```
# rpm -e <package_name>
```

Pour supprimer une installation de Kaspersky Anti-Virus réalisée à partir d'un deb, tapez ce qui suit sur la ligne de commande :

```
# dpkg -P <package_name>
```

si vous souhaitez supprimer l'application en même temps que ses fichiers de configuration, ou bien :

```
# dpkg -r <package_name>
```

si vous souhaitez désinstaller l'application mais en gardant ses fichiers de configuration.

Pour supprimer une installation de Kaspersky Anti-Virus réalisée à partir d'un pkg, tapez ce qui suit sur la ligne de commande :

```
# pkg_delete <package_name>
```

Un message confirmera à l'écran la suppression réussie de l'application.

Si un complément logiciel est installé pour la gestion à distance de l'application (module Webmin), il doit être supprimé manuellement à l'aide des outils standard de Webmin.

CHAPITRE 4. INTEGRATION AVEC MTA

Après son installation, l'antivirus doit être intégré au système de messagerie de l'hôte. Pour ce faire, les paramètres des fichiers de configuration de l'application et du MTA doivent être modifiés. L'intégration peut se faire avec le script de configuration du produit compris dans le paquet de distribution (section 3.4 à la p. 21 et 10.2 à la p. 102), ou en modifiant les fichiers de configuration de Kaspersky Anti-Virus et du MTA manuellement.

Pour Exim et Postfix, l'antivirus prend en charge l'intégration aussi bien en amont qu'en aval de la file d'attente. Dans le cas de l'intégration en amont de la file d'attente, les messages sont transférés pour analyse avant d'être ajoutés à la file d'attente MTA, tandis que l'intégration en aval signifie qu'ils sont contrôlés après leur ajout à la file d'attente des messages.

Remarque :

Le MTA ne permet pas le rejet des messages en cas d'intégration en aval de la file d'attente. Cependant, si l'action de **rejet** des objets est sélectionnée dans les paramètres de Kaspersky Anti-Virus, l'expéditeur recevra une notification sur le rejet du message. Le texte de la notification est défini par l'option **RejectReply** dans la section **[kav4lms: groups. <group_name>.settings]** du fichier de configuration du groupe.

Les sockets utilisés pour l'échange des données entre le MTA, le filtre et le service central de Kaspersky Anti-Virus sont attribués d'après les règles suivantes :

- `inet:<port>@<adresse_ip>` – pour un socket réseau
- `local:<socket_path>` – pour un socket local.

Attention !

Deux règles sont à respecter pour utiliser un socket :

- Le numéro du port, qui fait partie de la définition du socket réseau, doit être supérieur à 1024.
- Le service de filtrage et le service central doivent avoir des privilèges d'accès suffisants au socket local utilisé.

4.1. Intégration avec Exim

L'antivirus peut suivre deux méthodes pour son intégration avec Exim :

- **intégration aval de la file d'attente par la modification des routages**: tout le trafic de messagerie qui traverse le serveur protégé est alors transféré pour analyse après avoir été ajouté à la file d'attente du MTA (filtrage en aval).
- **intégration amont de la file d'attente moyennant le chargement de bibliothèques dynamiques**: les messages seront transférés pour analyse avant qu'ils ne soient ajoutés à la file d'attente du MTA queue (filtrage en amont).

4.1.1. Intégration aval de la file d'attente en modifiant les routages

L'intégration par modification des routages implique que les messages vont être envoyés pour analyse dans le cas de tous les transferts de courrier. Pour ce faire, **kav4lms_filter** doit figurer en tant que valeur de l'option **pass_router** de chaque routage Exim.

Dans le cas d'une intégration aval de la file d'attente correcte, le courrier est transféré vers l'antivirus et son retour au MTA exige que soient respectées les conditions suivantes :

1. Le filtre doit être configuré pour intercepter les messages provenant du MTA. L'extrémité de la connexion “filtre – MTA” est le socket défini par l'option **FilterSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.
2. Le filtre doit transmettre les messages au service central de l'application, pour analyse. L'extrémité de la connexion “filtre – service central” est le socket défini par l'option **ServiceSocket** dans la section **[kav4lms:server.settings]** du fichier de configuration de l'application principale.

   Attention !

   Dans le cas d'une intégration du filtre avec Exim (en tant que filtre intermédiaire) les options **FilterSocket**, **ServiceSocket** et **ForwardSocket** doivent pointer sur le socket réseau.

3. Le filtre doit renvoyer les messages vers le MTA. L'extrémité de la connexion “application – MTA” est le socket défini par l'option

ForwardSocket dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.

Pour intégrer Kaspersky Anti-Virus avec Exim avec le script de configuration de l'application :

exécutez la commande suivante :

Sous Linux :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim
```

Sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=exim
```

Pour intégrer l'application avec Exim manuellement :

1. Faites une sauvegarde des fichiers de configuration Exim.
2. Ajoutez les lignes suivantes à la section **main configuration settings** du fichier de configuration Exim :

   ```
   #kav4lms-filter-begin-1
   local_interfaces=0.0.0.0.25:<forward_socket_ip>.\
   <forward_socket_port_number>
   #kav4lms-filter-end-1
   ```

   où `<forward_socket_ip>.<forward_socket_port_number>` est l'adresse IP et le port du socket vers lequel le courrier est rerouté par l'application, après analyse.
3. Ajoutez les lignes suivantes à la section **routers** du fichier de configuration Exim :

   ```
   #kav4lms-filter-begin-2
   kav4lms_dnslookup:
     driver = dnslookup
     domains = ! +local_domains
     ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
     verify_only
     pass_router = kav4lms_filter
     no_more

   kav4lms_system_aliases:
     driver = redirect
   ```

```
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/aliases}}
  verify_only
  pass_router = kav4lms_filter

kav4lms_localuser:
  driver = accept
  check_local_user
  verify_only
  pass_router = kav4lms_filter

failed_address_router:
  driver = redirect
  verify_only
  condition = "{0}"
  allow_fail
  data = :fail: Failed to deliver to address
  no_more

kav4lms_filter:
  driver = manualroute
  condition = "${if or {{eq {$interface_port}\
{<forward_socket_port_number>}} \
      {eq {$received_protocol}{spam-scanned}} \
      }{0}{1}}"
  transport = kav4lms_filter
  route_list = "* localhost byname"
  self = send
#kav4lms-filter-end-2
```

où `<forward_socket_port_number>` est le numéro de port vers lequel le courrier est rerouté par l'application après analyse.

4. Ajoutez les lignes suivantes à la section de définition des transports pour Exim :

```
#kav4lms-filter-begin-3
kav4lms_filter:
```

```
  driver = smtp
  port = <filter_socket_port_number>
  delay_after_cutoff = false
  allow_localhost
#kav4lms-filter-end-3
```

où `<filter_socket_port_number>` est le numéro du port, sur lequel le service de filtrage de l'application est à l'écoute.

5. Renseignez le paramètre **ForwardSocket** avec la `<forward_socket_ip>.<forward_socket_port_number>` valeur définie à l'étape 2. Le paramètre **ForwardSocket** se trouve dans la section **[kav4lms:filter.settings]** du fichier de configuration *kav4lms.conf*.
6. Arrêtez le service *kav4lms-filter*.
7. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) file :

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

8. Lancez le service *kav4lms-filter*.
9. Redémarrez Exim :

4.1.2. Intégration amont par chargement d'une bibliothèque dynamique

Le filtre doit transmettre les messages au service central de l'application, pour analyse. L'extrémité de la connexion “filtre – service central” est le socket défini par l'option **ServiceSocket** dans la section **[kav4lms:server.settings]** du fichier de configuration du produit principal.

Pour intégrer Kaspersky Anti-Virus avec Exim avec le script de configuration de l'application :

exécutez la commande suivante :

sous Linux:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim-dlfunc
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=exim-dlfunc
```

Pour intégrer Kaspersky Anti-Virus avec Exim manuellement :

1. Assurez-vous qu'Exim prend en charge la fonction dlfunc, chargée du filtrage par contenu. Pour ce faire, exécutez la commande suivante :

   ```
   exim -bV
   ```

   Une réponse positive ressemble à ceci :

   ```
   Expand_dlfunc
   ```

2. Faites une sauvegarde des fichiers de configuration Exim.

3. Ajoutez les lignes suivantes à la section **main configuration settings** du fichier de configuration Exim :

   ```
   #kav4lms-filter-begin
   acl_smtp_data = acl_check_data
   #kav4lms-filter-end
   ```

4. Ajoutez les lignes suivantes à la section **ACL** du fichier de configuration Exim :

   ```
   acl_check_data:
   #kav4lms-dlfunc-begin
   warn set acl_m0 = \
   ${dlfunc{<libkavexim.so>}{kav}{<socket>} \
   {/var/tmp//.kav4lms-exim}}
   accept condition = ${if match{$acl_m0}{\N^kav4lms: \
   continue\N}{yes}{no}}
   logwrite = kav4lms returned continue
   deny condition = ${if match{$acl_m0}{\N^kav4lms: \
   reject.*\N}{yes}{no}}
   logwrite = kav4lms returned reject
   message = Kaspersky Anti-Virus rejected the mail
   discard condition = ${if match{$acl_m0}\
   {\N^kav4lms: drop.*\N}{yes}{no}}
   logwrite = kav4lms returned drop
   message = Kaspersky Anti-Virus dropped the mail
   defer condition = ${if match{$acl_m0}\
   {\N^kav4lms: temporary failure.*\N}{yes}{no}}
   logwrite = kav4lms returned temporary failure
   ```

```
message = Kaspersky Anti-Virus returned \
temporary failure
accept
#kav4lms-dlfunc-end
```

où <socket> correspond au socket utilisé pour les communications entre le filtre et le service central de Kaspersky Anti-Virus défini par l'option **FilterSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration principal de Kaspersky Anti-Virus; `<libkavexim.so>` - le chemin de la bibliothèque *libkavexim.so* :

pour les distributions Linux pour 32 bits :

```
/opt/kaspersky/kav4lms/lib/libkavexim.so
```

pour les distributions Linux pour 64 bits :

```
/opt/kaspersky/kav4lms/lib64/libkavexim.so
```

sous FreeBSD:

```
/usr/local/lib/kaspersky/kav4lms/libkavexim.so
```

5. Arrêtez le service *kav4lms-filter*.
6. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   sous Linux :

   ```
   FILTER_SERVICE=false
   FILTER_PROGRAM=/opt/kaspersky/kav4lms/lib/libkavexim\
   .so
   ```

   in FreeBSD:

   ```
   FILTER_SERVICE=false
   FILTER_PROGRAM=/usr/local/lib/kaspersky/kav4lms/\
   libkavexim.so
   ```

7. Redémarrez Exim.

4.2. Intégration avec Postfix

Il est possible de suivre trois méthodes pour intégrer l'antivirus avec Exim :

- **intégration en aval** : tout le trafic de courrier qui passe à travers le serveur protégé est transféré pour analyse après avoir été ajouté à la file d'attente du système de messagerie;
- **intégration en amont** : le courrier est transféré pour analyse avant qu'il ne soit ajouté à la file d'attente du système de messagerie;
- **intégration avec l'API Milter** : les messages sont transférés pour analyse moyennant l'interfacce de programmation Milter.

4.2.1. Intégration en aval de la file d'attente

Pour que le transfert des messages vers l'antivirus et leur retour vers le MTA se fasse correctement, les conditions suivantes doivent être respectées :

1. Le filtre doit être configuré pour intercepter les messages provenant du MTA. L'extrémité de la connexion “filtre – MTA” est le socket défini par l'option **FilterSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.
2. Le filtre doit transmettre les messages au service central de l'application, pour analyse. L'extrémité de la connexion “filtre – service central” est le socket défini par l'option **ServiceSocket** dans la section **[kav4lms:server.settings]** du fichier de configuration de l'application principale.

   Attention !

   Dans le cas d'une intégration avec Postfix, les options **FilterSocket**, **ServiceSocket** et **ForwardSocket** peuvent pointer sur un socket réseau ou local.

3. Le filtre doit renvoyer les messages vers le MTA. L'extrémité de la connexion “application – MTA” est le socket défini par l'option **ForwardSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.

Remarque :

Quand vous recopiez des lignes du manuel vers le fichier de configuration, supprimez les caractères "\" suivis de retours à la ligne.

Pour intégrer Kaspersky Anti-Virus avec Postfix avec le script de configuration de l'application :

exécutez la commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix
```

Pour intégrer l'application avec Postfix manuellement :

1. Ajoutez les lignes suivantes au fichier *master.cf* :

```
#kav4lms-filter-begin
kav4lms_filter         unix    -         -         n\
        -      10      smtp
    -o smtp_send_xforward_command=yes
<forward_socket_ip_address>:<forward_socket_port>\
        inet    n         -         n         -
10\
     smtpd
    -o content_filter=
    -o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

Remarque :

Si des sockets locaux sont utilisés avec Postfix 2.3 ou supérieur, ajoutez également la ligne précédente à l'option “no_milters”, comme ceci :

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters
```

```
    -o smtpd_helo_restrictions=
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
```

```
    -o smtpd_recipient_restrictions=\
permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8,[::1]/128
    -o smtpd_authorized_xforward_hosts=\
127.0.0.0/8,[::1]/128
#kav4lms-filter-end
```

où `<forward_socket_ip_address>:<forward_socket_port>` est l'adresse et le port du socket vers lequel le courrier est rerouté par l'application, après analyse.

2. Ajoutez les lignes suivantes au fichier *main.cf* :

```
#kav4lms-filter-begin
content_filter = \
kav4lms_filter:<filter_socket_ip_address>:\
<filter_socket_port>
#kav4lms-filter-end
```

où `<filter_socket_ip_address>:<filter_socket_port>` est l'adresse et le port du socket, où le processus du filtre est à l'écoute.

3. Arrêtez le service *kav4lms-filter*.
4. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

5. Lancez le service *kav4lms-filter*.
6. Redémarrez Postfix.

4.2.2. Pre-queue integration

Pour que le transfert des messages vers l'antivirus et leur retour vers le MTA se fasse correctement, les conditions suivantes doivent être respectées :

1. Le filtre doit être configuré pour intercepter les messages provenant du MTA. L'extrémité de la connexion “filtre – MTA” est le socket défini par l'option **FilterSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.
2. Le filtre doit transmettre les messages au service central de l'application, pour analyse. L'extrémité de la connexion “filtre – service central” est le socket défini par l'option **ServiceSocket** dans la section

[kav4lms:server.settings] du fichier de configuration de l'application principale.

> **Attention !**
>
> Dans le cas d'une intégration avec Postfix, les options **FilterSocket**, **ServiceSocket** et **ForwardSocket** peuvent pointer sur un socket réseau ou local.

3. Le filtre doit renvoyer les messages vers le MTA. L'extrémité de la connexion “application – MTA” est le socket défini par l'option **ForwardSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.

> **Remarque :**
>
> Quand vous recopiez des lignes du manuel vers le fichier de configuration, supprimez les caractères "\" suivis de retours à la ligne.

Pour intégrer Kaspersky Anti-Virus avec Postfix avec le script de configuration de l'application :

exécutez la commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix-prequeue
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix-prequeue
```

Pour intégrer l'application avec Postfix manuellement :

1. Ajoutez les lignes suivantes au fichier *master.cf* :

```
#kav4lms-filter-begin
kav4lms_filter        unix    -        -        n\
        -     10     smtp
    -o smtp_send_xforward_command=yes
<forward_socket_ip_address>:<forward_socket_port>\
       inet    n        -        n        -
10\
     smtpd
    -o content_filter=
    -o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

Remarque :

Si des sockets locaux sont utilisés avec Postfix 2.3 ou supérieur, ajoutez également la ligne précédente à l'option “no_milters”, comme ceci :

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters
```

```
    -o smtpd_helo_restrictions=
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=\
permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8,[::1]/128
    -o smtpd_authorized_xforward_hosts=\
127.0.0.0/8,[::1]/128
#kav4lms-prequeue-end
```

où `<forward_socket_ip_address>:<forward_socket_port>` est l'adresse et le port du socket vers lequel le courrier est rerouté par l'application, après analyse.

2. Ajoutez les lignes suivantes au fichier *master.cf* :

   ```
   smtp inet n - n - 20 smtpd
   ```

   Ajoutez le paramètre :

   ```
   #kav4lms-prequeue-begin
   -o smtpd_proxy_filter=:<filter_socket_port>
   #kav4lms-prequeue-end
   ```

3. Arrêtez le service *kav4lms-filter*.

4. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   ```
   FILTER_SERVICE=true
   FILTER_PROGRAM=kav4lms-filter
   ```

5. Lancez le service *kav4lms-filter*.

6. Redémarrez Postfix.

4.2.3. Integration avec Milter

Pour que le transfert des messages vers l'antivirus et leur retour vers le MTA se fasse correctement, les conditions suivantes doivent être respectées :

1. Le filtre doit être configuré pour intercepter les messages provenant du MTA. L'extrémité de la connexion “filtre – MTA” est le socket défini par l'option **FilterSocket** dans la section **[kav4lms:filter.settings]** du fichier de configuration de l'application principale.
2. Le filtre doit transmettre les messages au service central de l'application, pour analyse. L'extrémité de la connexion “filtre – service central” est le socket défini par l'option **ServiceSocket** dans la section **[kav4lms:server.settings]** du fichier de configuration de l'application principale.

Attention !

Dans le cas d'une intégration avec Postfix, les options **FilterSocket**, **ServiceSocket** peuvent pointer sur un socket réseau ou local.

Remarque :

Quand vous recopiez des lignes du manuel vers le fichier de configuration, supprimez les caractères "\" suivis de retours à la ligne.

Pour intégrer Kaspersky Anti-Virus avec Postfix avec le script de configuration de l'application :

exécutez la commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix-milter
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix-milter
```

Pour intégrer l'application avec Postfix manuellement :

1. Ajoutez les lignes suivantes au fichier *main.cf* :

```
smtpd_milters = inet:127.0.0.1:10025,
#kav4lms-milter-begin
milter_connect_macros = j _ {daemon_name} {if_name} \
{if_addr}
```

```
milter_helo_macros = {tls_version} {cipher} \
{cipher_bits} {cert_subject} {cert_issuer}
milter_mail_macros = i {auth_type} {auth_authen} \
{auth_ssf} {auth_author} {mail_mailer} {mail_host} \
{mail_addr}
milter_rcpt_macros = {rcpt_mailer} {rcpt_host} \
{rcpt_addr}
milter_default_action = tempfail
milter_protocol = 3
milter_connect_timeout=180
milter_command_timeout=180
milter_content_timeout=600
#kav4lms-milter-end
```

2. Arrêtez le service *kav4lms-milter*.
3. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   ```
   FILTER_SERVICE=true
   FILTER_PROGRAM=kav4lms-milter
   ```

4. Lancez le service *kav4lms-milter*.
5. Redémarrez Postfix.

4.3. Intégration avec qmail

The MTA de qmail n'offre pas de prise en charge pour des extensions de filtrage. Le filtrage est implémenté par l'exécutable */opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail* (*/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail* pour FreeBSD), fourni avec l'application, et qui remplace l'exécutable *qmail-queue* originaire. Le fichier de remplacement implémente le filtrage et transfère le trafic de messagerie au binaire original *qmail-queue* pour distribution. Les messages sont transférés pour analyse avant d'être ajoutés à la file d'attente du MTA (filtrage amont de la file d'attente).

Attention !

Dans le cas d'une intégration avec qmail, l'option **ServiceSocket** peut pointer sur un socket réseau ou local.

Pour intégrer Kaspersky Anti-Virus avec qmail avec le script de configuration de l'application :

exécutez la commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=qmail
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=qmail
```

Pour intégrer l'application avec qmail manuellement *:*

1. Renommez le fichier *qmail-queue* dans le répertoire */var/qmail/bin* à *qmail-queue-real*.
2. Copiez le fichier */opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail* (*/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail* for FreeBSD) dans le répertoire */var/qmail/bin* et renommez-le à *qmail-queue*.
3. Définissez les permissions suivantes pour les fichiers *qmail-queue* et *qmail-queue-real* :

   ```
   -rws—x--x 1 qmailq qmail
   ```

4. Arrêtez le service *kav4lms-filter*.
5. Changez le propriétaire et le groupe à `qmailq:qmail`, pour les répertoires suivant, y compris leurs contenus :

   - pour Linux :

   ```
   # /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
   --switch-credentials=qmailq,qmail
   ```

   - pour FreeBSD :

   ```
   # /usr/local/bin/kav4lms-setup.sh \
   --switch-credentials=qmailq,qmail
   ```

6. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   sous Linux :

   ```
   FILTER_SERVICE=false
   FILTER_PROGRAM=/opt/kaspersky/kav4lms/lib/bin\
   /kav4lms-qmail
   ```

in FreeBSD:

```
FILTER_SERVICE=false
FILTER_PROGRAM=/usr/local/libexec/kaspersky/kav4lms\
/kav4lms-qmail
```

7. Redémarrez qmail.

4.4. Intégration avec Sendmail

Sendmail offre l'API Milter pour implémenter l'intégration de filtres personnalisés. Le trafic de messagerie doit être transmis de Sendmail à Kaspersky Anti-Virus, puis être renvoyé moyennant des appels à l'interface Milter. Les messages sont transférés pour analyse avant d'être ajoutés à la file d'attente du MTA (intégration amont de la file d'attente).

En règle générale, quand le produit est intégré avec Sendmail, si des modifications sont apportées au fichier de configuration MTA au format *mc*, alors le fichier *cf* est automatiquement modifié. Si cette fonctionnalité n'est pas prise en charge, alors après la modification du fichier *mc* approprié, le fichier *cf* correspondant doit être également modifié.

Remarque :

Si vous modifiez le fichier *cf* uniquement, les modifications seront perdues quand la prochaine génération du fichier *cf* à partir du fichier *mc* se produira.

Attention !

Dans le cas d'une intégration avec Sendmail, les options **FilterSocket** et **ServiceSocket** peuvent pointer sur un socket réseau ou local.

4.4.1. Intégration avec Sendmail par un fichier *.cf*

Pour intégrer Kaspersky Anti-Virus avec Sendmail avec le script de configuration de l'application :

exécutez la commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=sendmail-milter
```

sous FreeBSD :

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=sendmail-milter
```

Pour intégrer l'application avec Sendmail manuellement *:*

1. Faites une sauvegarde du fichier *sendmail.cf*.
2. Ajoutez les chaînes suivantes au fichier *sendmail.cf* :

```
#kav4lms-milter-begin-filter
O InputMailFilters=kav4lms_filter
O Milter.macros.connect=j, _, {daemon_name}, \
{if_name}, {if_addr}
O Milter.macros.helo={tls_version}, {cipher}, \
{cipher_bits}, {cert_subject}, {cert_issuer}
O Milter.macros.envfrom=i, {auth_type}, \
{auth_authen}, {auth_ssf}, {auth_author}, \
{mail_mailer}, {mail_host}, {mail_addr}
O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, \
{rcpt_addr}
#kav4lms-milter-end-filter
```

3. Ajoutez les lignes suivantes au fichier *sendmail.cf* :

   a) si l'intégration se fait via un socket réseau :

```
#kav4lms-milter-begin-socket
Xkav4lms_filter,
S=inet:<filter_port>@<filter_address>,F=T,\
T=S:3m;R:5m;E:10m
#kav4lms-milter-end-socket
```

   où `<filter_port>` est le numéro du port du socket réseau, sur lequel le service de filtrage est à l'écoute, et `<filter_address>` est le nom ou l'adresse IP du serveur sur lequel est exécuté le service de filtrage.

   b) Si le socket local est nécessaire pour la connexion, modifiez la section de définition du socket comme ceci :

```
#kav4lms-milter-begin-socket
Xkav4lms_filter,
S=unix:<filter_socket_file_path>,F=T,T=S:3m;\
R:5m;E:10m
#kav4lms-milter-end-socket
```

   où `<socket_file_path>` est le chemin d'accès au socket local.

4. Arrêt du service *kav4lms-milter*.
5. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   ```
   FILTER_SERVICE=true
   FILTER_PROGRAM=kav4lms-milter
   ```

6. Démarrage du service *kav4lms-milter*.
7. Redémarrez Sendmail.

4.4.2. Intégration avec Sendmail par un fichier *.mc*

Pour intégrer l'application avec Sendmail *via le fichier .mc :*

1. Faites une sauvegarde du fichier *.mc*.
2. Ajoutez les chaînes suivantes au fichier *.mc* :

   ```
   dnl kav4lms-milter-begin dnl
   define(`_FFR_MILTER', `true')dnl
   INPUT_MAIL_FILTER(`kav4lms_filter',\
   `S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
   dnl kav4lms-milter-end dnl
   ```

3. Compilez le fichier *.cf* configuration suivant la procédure de votre système d'exploitation.
4. Arrêtez le service *kav4lms-filter*.
5. Ajoutez la ligne suivante à la section **[1043]** du fichier de configuration */var/opt/kaspersky/applications.setup* (sous Linux) */var/db/kaspersky/applications.setup* (sous FreeBSD) :

   ```
   FILTER_SERVICE=true
   FILTER_PROGRAM=kav4lms-milter
   ```

6. Lancez le service *kav4lms-filter*.
7. Redémarrez Sendmail.

CHAPITRE 5. PROTECTION ANTIVIRUS DE LA MESSAGERIE

5.1. Configuration de groupes

Un group consiste en plusieurs adresses d'expéditeurs et de destinataires dont les messages sont traités en fonction des mêmes paramètres de Kaspersky Anti-Virus.

Il est possible d'utiliser des paramètres personnalisés d'analyse des messages pour chaque groupe défini, par exemple :

- Méthode d'analyse du courrier (section 5.2 à la p. 50).
- Mode d'analyse du courrier (section 5.3 à la p. 51).
- Actions sur les messages et leurs objets (section 5.4 à la p. 54).
- Copie de sauvegarde des messages avant leur traitement (section 5.6 à la p. 59).
- Notifications sur les objets trouvés (section 5.7 à la p. 60).

Chaque groupe de paramètres est conservé dans un fichier de configuration séparé (section A.2 à la p. 137). Tous les fichiers de configuration des groupes doivent être spécifiés par une directive `_include` dans la section **[kav4lms:groups]** du fichier de configuration principal de l'application *kav4lms.conf*. Il est possible d'inclure les configurations de groupes en indiquant le nom d'un fichier de configuration, ou d'un répertoire contenant tous les fichiers de configuration de groupes.

Par défaut, les fichiers de configuration de groupes doivent se trouver dans le répertoire */etc/opt/kaspersky/kav4lms/groups.d/*.

Le paquet de distribution du produit inclut le fichier de configuration du groupe **Default**, *–default.conf*. Après l'installation du produit, il figure dans le répertoire */etc/opt/kaspersky/kav4lms/groups.d/*. Les valeurs définies dans ce fichier sont utilisées par défaut, à moins d'être spécifiées dans le fichier de configuration du groupe correspondant. Les paramètres du fichier de configuration du groupe **Default** sont utilisés en l'absence de groupe.

L'antivirus analyse un message en fonction de paramètres du groupe auquel appartiennent son expéditeur ou son destinataire (d'après les commandes MAIL FROM et RCPT TO). Si l'expéditeur et tous les destinataires appartiennent à des groupes différents, l'application sélectionne le groupe avec la *priorité* la plus haute. Si aucun groupe n'a pu être trouvé, les messages seront traités en appliquant les paramètres spécifiés dans le fichier de configuration du groupe **Default**, qui possède la priorité la plus basse de **0**. Par conséquent, il est recommandé de spécifier un niveau de protection plus élevé pour les groupes de plus grande priorité.

La priorité est un identificateur de groupe unique. Il est défini par l'option **Priority** de la section **[kav4lms:groups.<group_name>.definition]** du fichier de configuration du groupe.

Les expéditeurs et destinataires sont définis par les options **Expéditeurs** et **Destinataires** de la section **[kav4lms:groups.<group_name>.definition]** d'un fichier de configuration de groupe.

Pour créer un nouveau groupe,

1. Créez un fichier de configuration du groupe dans le répertoire spécifié dans la section **[kav4lms:groups]** du fichier de configuration du produit principal. Le répertoire par défaut est **/etc/opt/kaspersky/kav4lms/groups.d/**

   Remarque :

   Il est conseillé d'utiliser le fichier *default.conf* comme modèle pour la création d'un fichier de configuration de groupe. Exécutez les commandes suivantes pour remplacer rapidement le nom de groupe :

   ```
   # cd /etc/opt/kaspersky/kav4lms/groups.d
   #     sed     's|groups.default|groups.<group_name>|'
   default.conf > <group_name>.conf
   ```

2. Définissez la priorité du groupe dans ses fichiers de configuration avec l'option **Priority** dans la section **[kav4lms:groups.<group_name>.definition]**. Tous les nombres naturels sont admis. Les groupes avec la même priorité ou avec une priorité **0** ne sont pas autorisés.

3. Définissez les adresses des expéditeurs et destinataires dans le fichier de configuration du groupe avec les options **Expéditeurs** et **Destinataires** dans la section **[kav4lms:groups.<group_name>.definition]**.

   Les caractères génériques "*" et "?" sont acceptés pour créer des masques, ainsi que les expressions régulières préfixées avec "re:". Pour spécifier plusieurs adresses (ou masques d'adresses), chaque nouvel enregistrement doit commencer sur une nouvelle ligne :

```
Senders=reporter@*.mydomain.com
Recipients=re:office\d+@central\.mydomain\.com
```

Au moins une des options **Destinataires** ou **Expéditeurs** doit être définie. Si l'option **Destinataires** ou **Expéditeurs** manque dans la définition du groupe, l'application la renseigne avec la valeur par défaut spécifiée dans *default.conf* – **"*@*"** (toutes adresses)**.**

> **Attention !**
>
> Les expressions régulières ne sont pas sensibles à la casse.

4. Si nécessaire, spécifiez les options d'analyse du courrier dans les sections correspondantes du fichier de configuration du groupe (section A.2 à la p. 137 pour plus de détails). Si une option n'est pas définie dans le fichier de configuration du groupe, l'application utilise la valeur correspondante spécifiée dans le fichier de configuration du groupe **Default** – *default.conf.*

5.2. Définition d'une stratégie d'analyse du courrier

L'antivirus prend en charge les méthodes d'analyse du courrier suivantes :

- Analyse de l'ensemble du message comme un seul objet simple – les en-têtes et le corps du message sont analysés comme un tout.
- Approche combinée – l'application analyse d'abord un message en tant qu'objet simple, puis le décompose en parties (corps du message, pièces jointes, etc.) et analyse chacune d'elles séparément. Cette méthode offre un meilleur niveau de protection et une plus grande fiabilité.

> **Remarque :**
>
> Si une action applicable à une partie du message est choisie pour s'appliquer à l'ensemble du message (section 5.4 à la p. 54), alors ce message sera examiné partie par partie, sans tenir compte de la méthode d'analyse choisie.

La méthode d'analyse du courrier est déterminée par la stratégie et définie par l'option **ScanPolicy** de la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe.

Pour analyser des messages en tant qu'objets simples,

définissez l'option **ScanPolicy** à **message**.

Pour utiliser l'approche combinée lors de l'analyse des messages,

définissez l'option **ScanPolicy** à **combined**.

5.3. Mode d'analyse du courrier

L'étape suivante de la configuration du groupe est la sélection du mode d'analyse du courrier. Kaspersky Anti-Virus offre les modes d'analyse suivants :

- Analyse de la présence de logiciels malveillants.
- Filtrage du contenu.

La spécification du mode d'analyse pour un groupe se fait avec l'option **Check** de la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe. Il est possible d'utiliser les valeurs suivantes :

- **antivirus** – exécute une analyse antivirus du courrier ;
- **content-filter** – filtrage par nom, par type et par taille de pièce jointe ;
- **all** – exécute à la fois un examen antivirus et un filtrage par contenu ;
- **none** – désactive l'analyse du courrier.

Si les deux fonctions d'analyse antivirus et de filtrage par contenu son activées, l'analyse est exécutée dans l'ordre suivant :

1. analyse antivirus d'un message considéré comme un tout ;
2. filtrage des pièces jointes ;
3. analyse des messages pièce par pièce (si la méthode d'analyse combinée est sélectionnée avec **ScanPolicy**=**combined**).

5.3.1. Analyse antivirus

L'analyse antivirus est activée en renseignant l'option **Check** dans la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe, avec la valeur **antivirus** ou **all**.

Suite à l'analyse antivirus d'un objet, l'application attribue un certain état au message ou à ses objets :

- **clean** – le message ne contient pas de code malveillant ;
- **infected** – le message (ou l'une de ses parties) contient des objets malveillants ;

- **suspicious** – le message (ou l'une de ses parties) contient un objet suspect (attribué uniquement quand un analyseur heuristique est activé) ;
- **protected** – le message (ou l'une de ses parties) est protégé par un mot de passe ou chiffré ;
- **error** – le message est endommagé ou le processus d'analyse a généré une erreur.

L'état attribué après l'analyse est utilisée pour dans le traitement postérieur des messages et de leurs objets (section 5.4 à la p. 54).

Pour des messages infectés (**infected**), il est possible de définir une procédure de traitement spécifique, en fonction du nom de la menace détectée (option **VirusNameAction** dans la section **[kav4lms:groups.<group_name>.actions]** du fichier de configuration du groupe). Kaspersky Anti-Virus renvoie les noms des menaces identifiées, en utilisant la notation de Kaspersky Lab décrite sur www.viruslist.com. La liste des noms de virus qui sont passibles d'actions est précisée par le paramètre **VirusNameList** dans la section **[kav4lms:groups.<group_name>.contentfiltering]**. Ce paramètre reconnaît les noms de virus notés littéralement ou par une expression régulière (standard POSIX).

Il est possible de personnaliser les possibilités d'analyse de l'application pour augmenter la précision ou la vitesse de l'analyse. Les paramètres liés à la performance du moteur d'analyse se trouvent dans la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe. Ces paramètres indiquent :

- s'il faut analyser les archives (paramètre **ScanArchives**) ;
- s'il faut analyser les exécutables comprimés (paramètre **ScanPacked**) ;
- s'il faut effectuer une analyse heuristique (paramètre **UseCodeAnalyzer**) ;

  Remarque :

  La valeur **yes** de ce paramètre active le verdict **suspicious**, qui n'est pas disponible autrement.

- le temps maximum autorisé pour l'analyse d'un message ou d'un de ses objets (paramètre **MaxScanTime**). Si la durée d'analyse dépasse la limite spécifiée, l'analyse conclut sur le verdict **error** ;
- si l'application doit décoder les objets MIME qui ne sont pas conformes aux normes RFC, au moyen d'algorithmes heuristiques (option **MIMEEncodingHeuristics**) ;

- quels types de logiciels malveillants sont détectés (paramètre **UseAVBasesSet** dans la section **[kav4lms:server.settings]** du fichier de configuration *kav4lms.conf*).

5.3.2. Filtrage du contenu

Le service de filtrage par contenu est activé en renseignant le paramètre **Check** dans la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe avec les valeurs **content-filter** ou **all**.

L'antivirus peut utiliser les critères suivants pour le filtrage par contenu :

- type MIME des pièces jointes (s'applique aux en-têtes “Content-Type”) ;

  Attention !

  Dans certaines situations, le contenu réel ne correspond pas au type MIME déclaré. L'application n'effectue pas une identification du contenu.

- nom de pièce jointe (s'applique aux noms et aux extensions des pièces jointes) ;
- taille de la pièce jointe (s'applique à la taille des parties du message, calculée après décompression de chaque pièce jointes).

Remarque :

Si les deux fonctions d'analyse antivirus et de filtrage par contenu son activées, le filtrage par contenu précède l'analyse.

Les critères de filtrage sont définis dans la section **[kav4lms:groups.<group_name>.contentfiltering]**du fichier de configuration du groupe.

Chaque critère peut être associé à deux règles :

- Règle d'inclusion. Cette règle spécifie que les objets sont soumis au filtre et sa description utilise les paramètres suivants :
  - **IncludeMime** – spécifie la liste des types MIME ;
  - **IncludeName** – spécifie la liste des noms de pièces jointes ;
  - **IncludeSize** – spécifie la liste de tailles des objets.
- Règle d'exclusion. Cette règle spécifie que les objets ne sont pas soumis au filtre et sa description utilise les paramètres suivants :
  - **ExcludeMime** – spécifie la liste des types MIME ;

- **ExcludeName** – spécifie la liste des noms de pièces jointes ;
- **ExcludeSize** – spécifie la liste de tailles des objets.

Attention !

Si la règle d'inclusion est vide, mais pas la règle d'exclusion, alors tous les objets qui ne vérifient pas la règle d'exclusion sont inclus dans le filtrage.

Si les deux règles sont vides, le filtrage par contenus n'est pas exécuté, quelle que soit la valeur du paramètre **Check**.

Les règles de filtrage des types MIME et des noms de pièces jointes doivent être précisées comme une liste de :

- chaînes ;
- caractères génériques (normalisés UNIX) ;
- expressions régulières (au standard POSIX).

Attention !

Les expressions régulières ne sont pas sensibles à la casse ; elles doivent commencer par le préfixe "re:".

Les règles pour la taille des objets doivent être précisées comme :

- le nombre d'octets ;
- des nombres avec indicateur de taille ('KB' ou 'MB' en anglais) ;
- des signes de comparaison.

5.4. Actions sur les objets

Suite à l'analyse et au filtrage des contenus, Kaspersky Anti-Virus exécute des actions spécifiques sur les messages et leurs parties. Certaines actions sont applicables aux messages dans leur ensemble, tandis que d'autres ne s'appliquent qu'aux parties des messages. Les paramètres qui déterminent les actions de l'application peuvent avoir les valeurs suivantes :

- **warn** – le message est complètement remplacé par un texte d'avertissement sur la présence d'un objet dangereux ;
- **drop** – le message est accepté, mais écarté sans plus, sans le remettre au destinataire ;
- **reject** – la délivrance du message est rejetée (cette action n'est pas effectuée quand l'application est utilisée avec Postfix (intégration aval

de la file d'attente) ou avec Exim (l'action bounce se produit dans ce cas). Si cette action est choisie. l'expéditeur reçoit une notification définie par l'option **RejectReply** ;

- **skip** – le message ou sa partie est autorisée à passer sans modification, le résultat de l'analyse est consigné dans le registre de l'application ;
- **cure** (disponible uniquement après l'analyse antivirus des parties du message) – l'application tente de réparer les objets infectés. Si la réparation échoue, l'action **delete** est appliquée ;
- **rename** (disponible uniquement pour le filtrage par contenus des parties du message) – l'application ajoute au nom de la pièce jointe la valeur du paramètre **RenameTo**. Si la valeur définit une extension (`.vir`, par exemple), alors cette valeur est ajoutée au nom de la pièce jointe. Autrement, cette valeur est interprétée comme le nom complet, de sorte que le nom tout entier de la pièce jointe est remplacé ;
- **delete** – la partie du message est supprimée et (si le paramètre **UsePlaceholderNotice** est défini à **yes**) remplacé par une notification. Le texte de la notification est pris dans un fichier modèle appelé *part_<action>*.

Les actions réalisées après l'analyse antivirus sont spécifiées par les paramètres **InfectedAction**, **SuspiciousAction**, **ProtectedAction**, **ErrorAction** et **VirusNameAction**. Les actions réalisées après le filtrage sont spécifiées par les paramètres **FilteredMimeAction**, **FilteredNameAction** et **FilteredSizeAction**.

Les paramètres liés aux actions sont disponibles dans la section **[kav4lms:groups.<group_name>.actions]** du fichier de configuration du groupe.

Attention !

Le fait que le filtrage par contenus intervienne avant l'analyse peut conduire à une situation dans laquelle le résultat d'une analyse du message correspond au verdict **infected**, alors que l'analyse pièce par pièce indique qu'aucune partie n'est infectée. Ceci peut se produire si l'action **delete** est choisie en réponse au filtrage des contenus, et la partie du message est supprimée après le filtrage.

5.5. Profils de sécurité prédéfinis

Le paquet de distribution de Kaspersky Anti-Virus est fourni avec des profils de configuration prédéfinis pour différents niveaux de protection du courrier :

- **recommandé** – sauvegardé dans le répertoire *default_recommended* (section 5.5.1 à la p. 56 pour plus de détails) ;
- **protection maximum** – sauvegardé dans le répertoire *high_overall_security* (section 5.5.2 à la p. 57 pour plus de détails) ;
- **performance maximum** – sauvegardé dans le répertoire *high_scan_speed* (section 5.5.3 à la p. 58 pour plus de détails).

Chaque profil consiste en deux fichiers de configuration: *kav4lms.conf* et *default.conf* (placé dans le sous-répertoire *groups.d*). Les profils sont conservés dans les sous-répertoires du même nom, sous le répertoire */etc/opt/kaspersky/kav4lms/profiles.*

Vous pouvez sélectionner l'un des profils prédéfinis ou configurer manuellement les paramètres de protection du courrier dans les fichiers de configuration de l'application.

Pour utiliser un profil prédéfini :

1. Sauvegardez les fichiers de configuration de l'application (*kav4lms.conf* et *groups.d/default.conf*).
2. Copiez le contenu du répertoire du profil requis vers le répertoire */etc/opt/kaspersky/kav4lms*.
3. Appliquez la nouvelle configuration en exécutant la commande suivante :

   ```
   /etc/init.d/kav4lms reload
   ```

5.5.1. *Profil Recommandé*

Ce profil offre un équilibre optimum entre le degré de protection antivirus et la vitesse d'analyse. Les caractéristiques du profil sont les suivantes :

- Les messages sont analysés conformément à la stratégie d'analyse par **message** : chaque message considéré comme un tout est analysé à la recherche de virus.
- Des bases antivirus étendues sont utilisées pour l'analyse.
- Le nombre d'imbrications d'objets MIME autorisé est de 10 maximum par message.
- Une copie de sauvegarde et un fichier d'informations sont créés pour chaque message soumis à un traitement antivirus.
- Les messages infectés sont réparés.

- Le filtrage des pièces jointes par type MIME est activé. L'application élimine des messages les liens aux objets externes (type *message/external-body*) et les pièces jointes avec des extensions *.pif*, *.com*, *.bat* et *.exe*.
- Des avertissements sont émis pour tous les messages identifiés comme suspects, protégés par un mot de passe, erronés, filtrés par leur type MIME et par le nom de pièce jointe. Si une menace spécifique est découverte, le message est écarté.
- L'application ajoute à l'en-tête et au corps du message des informations sur le résultat du traitement.
- L'application envoie des notifications sur le traitement du message à ses destinataires. Aucune notification n'est délivrée à l'expéditeur ni à l'administrateur.
- Tous les messages de l'application (à l'exception des informations de mise au point) sont consignés dans le rapport.
- Des statistiques sont collectées sur tous les aspects opérationnels de l'application.

5.5.2. *Profil de sécurité maximum*

Ce profil offre la protection la plus complète du trafic de courrier. Le profil dispose des fonctions suivantes :

- Le courrier électronique est analysé conformément à une stratégie d'analyse **combinée** : chaque message est d'abord analysé comme un tout puis chaque objet du message est analysé séparément, que des objets infectés soient trouvés ou pas.
- L'application interprète les messages non conformes aux normes RFC à l'aide d'algorithmes heuristiques ; les messages sont renvoyés pour analyse après un décodage réussi.
- Des bases antivirus étendues sont utilisées pour l'analyse.
- Les messages sont filtrés par type MIME. L'application filtre les messages contenant des références à des objets de type externe (*message/external-body*) et les supprime. En outre, les pièces jointes *.pif*, *.com*, *.bat* et *.exe* sont supprimées.
- Le nombre d'imbrications par message est illimité.
- Un fichier d'informations est créé pour chaque message soumis à un traitement antivirus ou à un filtrage.

- Les objets infectés sont réparés.
- L'application supprime tous les objets suspects, protégés ou filtrés dans les messages. Les messages contenant des menaces recensées dans une liste spécifiée sont écartés.
- Si un message contient des objets ayant causé une erreur lors de l'analyse, son contenu est remplacé par une notification.
- L'application envoie des notifications sur le traitement du message à ses destinataires. Aucune notification n'est délivrée à l'expéditeur ni à l'administrateur.
- Tous les messages de l'application (à l'exception des informations de mise au point) sont consignés dans le rapport.
- Les statistiques ne sont pas préservées.

5.5.3. *Profil de performance maximum*

Ce profil offre une performance maximum de l'application, en échange d'une certaine perte de fiabilité dans la protection antivirus. Les caractéristiques du profil sont les suivantes :

- Les messages sont analysés conformément à la stratégie d'analyse par **message** : chaque message considéré comme un tout est analysé à la recherche de virus.
- Le filtrage des objets dans le message est désactivé.
- L'application enregistre une copie de sauvegarde pour chaque message qui se trouve écarté ou génère un avertissement suite à une action. Aucun fichier d'informations n'est créé.
- Des avertissements sont émis pour tous les objets infectés, suspects, protégé et erronés dans les messages de courrier. Si une menace recensée dans la liste spécifiée est découverte, le message est écarté.
- L'application ajoute à l'en-tête les informations sur le résultat du traitement.
- L'application envoie des notifications sur le traitement du message à ses destinataires. Aucune notification n'est délivrée à l'expéditeur ni à l'administrateur.
- L'application consigne des informations dans le rapport d'activité sur tous les aspects de son fonctionnement ; niveau de détail : erreurs fatales ou autres, ainsi que les messages d'information importants.
- Des statistiques sont collectées sur les virus détectés.

- Le nombre maximum de pétitions client adressées au service central est doublé, par rapport aux profils recommandé et de protection maximale. Le nombre maximum de pétitions d'analyses simultanées est illimité.

5.6. Copies de sauvegarde

L'application prend en charge la copie de sauvegarde des messages avant leur traitement. Les paramètres de sauvegarde sont spécifiés dans la section **[kav4lms:groups.<group_name>.backup]** du fichier de configuration du groupe.

Le mode de sauvegarde du courrier est déterminé par l'option Policy, qui peut prendre les valeurs suivantes :

- **message** – seule une copie du message est créée ;
- **info** – le fichier d'informations est créé en même temps que la copie du message. Ce fichier contient les informations suivantes :
  - adresse IP (ou hôte si disponible) du client MTA ;
  - adresse IP (ou hôte si disponible) du connecteur MTA ;
  - l'expéditeur du message, indiqué par le connecteur MTA ;
  - l'adresse du serveur de traitement ;
  - le nom du groupe correspondant, sous lequel le message a été analysé ;
  - la liste des destinataires du message, indiquée par le connecteur MTA ;
  - la cause de l'action de sauvegarde (réparé, supprimé, rejeté, filtré, etc.) ;
  - le chemin vers le fichier d'origine, relativement à la cible de la sauvegarde ;
  - informations sur l'instance de l'application (process id et thread id).
- **none** – pas de sauvegarde du message.

Le paramètre **Options** spécifie l'activité de l'application qui est la cause de la sauvegarde :

- **cured** – quand l'objet du message original a été réparé ;
- **deleted** – quand l'objet du message original a été supprimé ;

- **rejected** – quand le message original a été rejeté (le client MTA reçoit le code d'erreur), mais l'administrateur a décidé de sauvegarder le message infecté ;
- **dropped** – quand le message original a été écarté ;
- **warning** – quand le message original a été remplacé par un avertissement ;
- **renamed** – quand le message contient au moins un objet (partie MIME) qui a vérifié les règles de filtrage et qui a été renommé ;
- **all** – toutes les options mentionnées ci-dessus.

Le paramètre **Options** peut prendre une des valeurs précédentes ou une liste de ces valeurs, séparées par des virgules.

Les sauvegardes de messages et les fichiers d'information sont conservés sous un répertoire spécifié par le paramètre **Destination**.

5.7. Notifications

Une notification est un message électronique contenant un message traité et transmis à son destinataire, à l'expéditeur ou à l'administrateur du serveur.

Outre le texte de la notice proprement dite, une notification contient également la description des objets qui ont été supprimés du message pour une raison ou pour une autre.

L'application se charge également d'annexer le message d'origine à la notification. Cependant, ceci n'est possible que pour des notifications adressées au destinataire. Dans le cas des administrateurs et des expéditeurs, l'application génère de nouveaux messages ne contenant que le texte de la notification.

5.7.1. Configuration des notifications

Les paramètres de l'application associés aux notifications sont conservés :

- dans la section **[kav4lms:server.notifications]** du fichier de configuration *kav4lms.conf* de l'application ;
- dans la section **[kav4lms:groups.<group_name>.notifications]** de chacun des fichiers de configuration de groupe.

La mise en place des notifications se fait en deux étapes.

Etape 1. Qui doit recevoir la notification ?

Les destinataires de notifications peuvent être :

- l'expéditeur du message (paramètre **NotifySender** dans le fichier de configuration du groupe) ;
- les destinataires du message (paramètre **NotifyRecipients** dans le fichier de configuration du groupe) ;
- les administrateurs de la sécurité (paramètre **NotifyAdmin** dans la configuration du groupe). La liste des adresses électroniques des administrateurs de la sécurité est spécifiée par le paramètre **AdminAdresses** dans la configuration du groupe ;
- les administrateurs du produit (définis par le paramètre **ProductNotify** du fichier *kav4lms.conf*). La liste des adresses des administrateurs du produit est spécifiée par le paramètre **ProductAdmins** dans le fichier *kav4lms.conf*.

Les notifications à l'expéditeur du message sont activées en renseignant ces paramètres avec une valeur différente de **none**. Autrement, les notifications sont désactivées.

Etape 2. Quel doit être le sujet de la notification ?

Les expéditeurs et destinataires du message et les administrateurs de la sécurité peuvent recevoir une notification sur :

- la valeur **InfectedAction** (section 5.4 à la p. 54 pour plus de détails) appliquée (au moins un objet était infecté). Ce type de notification est activé en renseignant le paramètre obligatoire avec la valeur **infected** ;
- la valeur **ProtectedAction** (section 5.4 à la p. 54 pour plus de détails) appliquée (au moins un objet était protégé). Ce type de notification est activé en renseignant le paramètre obligatoire avec la valeur **protected** ;
- la valeur **ErrorAction** (section 5.4 à la p. 54 pour plus de détails) appliquée (au moins un objet était erroné). Ce type de notification est activé en renseignant le paramètre obligatoire avec la valeur **error** ;
- la vérification d'un règle de filtrage (section 5.3.2 à la p. 53 pour plus de détails). Ce type de notification est activé en renseignant le paramètre obligatoire avec la valeur **filtered** ;
- toutes les options mentionnées. Ce type de notification est activé en renseignant le paramètre obligatoire avec la valeur **all**.

Les administrateurs du produit peuvent recevoir une notification sur :

- le téléchargement d'une nouvelle mise à jour des bases antivirus. Ce type de notification est activé en renseignant le paramètre **ProductNotify** avec la valeur **update** ;
- une défaillance critique de l'application (récupérable ou pas). Ce type de notification est activé en renseignant le paramètre **ProductNotify** avec la valeur **fault** ;
- des notifications liées à la gestion des licences. Ce type de notification est activé en renseignant le paramètre **ProductNotify** avec la valeur **license** ;
- toutes les options mentionnées. Ce type de notification est activé en renseignant le paramètre **ProductNotify** avec la valeur **all**.

Les notifications associées à la licence sont des cas exceptionnel qui ne peuvent être exclus de la liste. Ces sortes de notifications sont toujours émises et quand les notifications sont désactivées, elles sont consignées dans les registres.

Les notifications sur la licence sont envoyées en cas de :

- expiration de la clé – la première notification est émise 14 jours avant la date d'expiration, puis quotidiennement jusqu'à cette dernière. Le jour suivant, une notification sur l'expiration de la clé est émise ;
- violation des restrictions de licence – en cas de dépassement du nombre d'utilisateurs ou du trafic autorisé par la clé.

5.7.2. Modèles de notifications

Les modèles suivants peuvent être utilisés pour créer des notifications (les modèles sont stockés dans le répertoire définit par le paramètre **Templates** dans le fichier de configuration de l'application) :

- **Modèles de notifications sur des objets supprimés** – texte ajouté au message original si l'une de ses parties a été supprimée pendant le traitement antivirus ou par filtrage. Ce texte peut inclure une macro décrivant les raisons de la suppression. Les modèles suivants sont disponibles :
  - *part_infected* – texte de remplacement de l'objet supprimé après une tentative échouée de désinfection ;
  - *part_filtered* – texte de remplacement de l'objet MIME supprimé suite au filtrage des objets MIME ;

- *part_suspicious* – texte de remplacement de l'objet identifié comme suspect et supprimé ;
- *part_filtered* – notice remplaçant objet de courrier original, renommé après le filtrage ;
- *part_protected* – notice remplaçant objet protégé, qui a été supprimé car il ne pouvait être soumis à l'analyse antivirus ;
- *part_error* – texte de remplacement de l'objet supprimé pour avoir généré une erreur d'analyse.

- **Modèle standard de notification** – texte de la notification envoyée à l'expéditeur, au destinataire et à l'administrateur à travers le filtre ou nouveau message automatique envoyé par le composant SMTP. Ce texte peut inclure une macro décrivant les raisons de la suppression. Les modèles suivants sont disponibles :
  - *notify_common* – texte envoyé par défaut au destinataire, à l'expéditeur et aux administrateurs au sujet des actions appliquées au message ;
  - *notify_infected* – notice remplaçant le message infecté ;
  - *notify_suspicious* – notice remplaçant le message contenant des objets suspects ;
  - *notify_filtered* – notice remplaçant le message exclu par le filtre ;
  - *notify_error* – notice remplaçant message ayant généré une erreur d'analyse ;
  - *notify_protected* – notice remplaçant message protégé contre l'analyse ;
  - *disclaimer* – texte ajouté à tous les messages traités ou automatiques. Par défaut, ce modèle inclut une notice en anglais indiquant que le message a été analysé par Kaspersky Anti-Virus, signifiant : “Ce message a été analysé par Kaspersky Anti-Virus. Pour plus d'informations sur la sécurité des données, visitez http://www.kaspersky.com et http://www.viruslist.com".
- **Modèle de notification détaillée** – texte d'information adressé à une personne désireuse d'en savoir plus sur le traitement antivirus d'un message de courrier. Il existe des modèles de notifications séparés pour le destinataire, l'expéditeur et l'administrateur. Définissez le paramètre **UseCustomTemplates** à **yes** pour pouvoir utiliser ces modèles. Les modèles suivants sont disponibles :

- notifications pour l'expéditeur :
  - *notify_ sender_common* – texte de la notification envoyée au l'expéditeur sur les actions appliquées au message original ;
  - *notify_sender_infected* – notice remplaçant le message infecté ;
  - *notify_sender_suspicious* – notice remplaçant le message contenant des objets suspects ;
  - *notify_sender_filtered* – notice remplaçant le message exclu par le filtre ;
  - *notify_sender_error* – notice remplaçant message ayant généré une erreur d'analyse ;
  - *notify_sender_protected* – notice remplaçant message protégé contre l'analyse ;
- notifications aux destinataires :
  - *notify_recipients_common* – texte de la notification envoyée au destinataire sur les actions appliquées au message original ;
  - *notify_recipients_infected* – notice remplaçant le message infecté ;
  - *notify_recipients_suspicious* – notice remplaçant le message contenant des objets suspects ;
  - *notify_recipients_filtered* – notice remplaçant le message exclu par le filtre ;
  - *notify_recipients_error* – notice remplaçant message ayant généré une erreur d'analyse ;
  - *notify_recipients_protected* – notice remplaçant message protégé contre l'analyse ;
- notifications pour administrateurs :
  - *notify_admin_common* – texte de la notification envoyée au l'administrateur sur les actions appliquées au message original ;
  - *notify_admin_infected* – notice remplaçant le message infecté ;
  - *notify_admin_suspicious* – notice remplaçant le message contenant des objets suspects ;
  - *notify_admin_filtered* – notice remplaçant le message exclu par le filtre ;

- *notify_admin_error* – notice remplaçant message ayant généré une erreur d'analyse ;
- *notify_admin_protected* – notice remplaçant message protégé contre l'analyse.

- **Modèle de notification spéciale pour l'administrateur** – texte ajouté aux notifications spécialisées, envoyé en cas d'événements graves qui exigent l'attention particulière de l'administrateur. Les modèles des administrateurs sont conservés dans un répertoire spécifié par le paramètre **Templates** dans la section **[kav4lms:server.notifications]** du fichier de configuration de l'application. Les modèles suivants sont disponibles :
  - *product_update* – texte informant l'administrateur de la réception des mises à jour des bases antivirus de l'application ;
  - *product_fault* – notification pour l'administrateur qu'une erreur critique s'est produite pendant l'exécution de Kaspersky Anti-Virus ;
  - *product_license* – notification à l'administrateur d'une violation de l'accord de licence ou de la fin de la période de validité.

Attention !

Quand l'application est lancée, la présence de tous les modèles ci-dessus est vérifiée. Il suffit qu'un seul de ces modèles soit absent pour que l'application retourne une erreur.

L'application vérifie également que la taille de chaque modèle ne dépasse pas 8 Ko.

5.7.3. Personnalisation des modèles de notification

Kaspersky Anti-Virus est suffisamment flexible pour permettre aux utilisateurs de personnaliser les modèles de notification envoyés aux administrateurs, aux expéditeurs et aux destinataires. La personnalisation des modèles fait appel à un langage spécialisé pour les notifications.

Le langage des modèles est un ensemble d'instructions de contrôle et de macros.

Nous présentons ci-après les règles du langage, sa syntaxe et des exemples d'utilisation détaillés.

Attention !

La première ligne d'un modèle ne doit pas contenir le signe ":", qui est interprété comme une en-tête. Vous pouvez commencer par un saut de ligne (appuyez sur **Entrée**) pour éviter que ce caractère ne soit interprété par erreur comme une en-tête de notification.

5.7.3.1. Macros

Une macro est un élément de substitution utilisé dans les modèles de notification par courrier. Dans le texte d'une notice créée à partir d'un modèle, la macro est remplacée par une certaine valeur.

La syntaxe des macros est `%macro_name%`.

Si un nom de macro contient le signe "%", celui-ci doit être précédé d'un caractère d'échappement (section 5.7.3.5 à la page 70).

Plusieurs valeurs peuvent être associées à une macro. Dans ce cas, la simple interprétation de "`%macro_name%`" renverra la dernière valeur attribuée.

Pour attribuer plusieurs valeurs à une même macro, utilisez des *instructions itératives*.

5.7.3.2. Constructions itératives

Une construction itérative (CI) est l'élément central du langage des modèles.

La syntaxe d'une instruction itérative est :

<FOR INAME **IOP** IVALUE**>**BODY**</FOR>**

où :

- `<FOR` – début de la définition de la CI. Un symbole "<", s'il n'ouvre pas sur la définition d'une CI, doit être échappé (section 5.7.3.5 à la page 70).
- `INAME` – nom de la CI sous la forme **1*(nchar)*(nchar)**; la longueur maximale est de 64 octets.
- `IOP` – opération de comparaison sous la forme **== | !=**; la longueur maximale est de 2 octets.
- `IVALUE` – valeur de la CI sous la forme **1*(vchar)*(vchar)**; la longueur maximale est de 4096 octets. Les valeurs de CI ne sont acceptées qu'entre guillemets. Pour des comparaisons avec une valeur contenant elle-même des guillemets, faites précéder ceux-ci du caractère d'échappement (section 5.7.3.5 à la page 70). Exemple :

  `<FOR` ***_macro_name_parent_*** **== "\"** **value 1\""**>

`>` – fin de la définition de la CI et début du corps de l'itération. Un caractère `<`, s'il n'est pas la fin de la définition d'une CI, doit être précédé d'un caractère d'échappement (section 5.7.3.5 à la page 70).

`BODY` – corps de l'itération sous la forme ***(char)**.

`</FOR>` – fin de la définition du corps de l'itération. Le caractère `<` qui n'est pas le caractère final de la définition du corps de l'itération doit être précédé d'un caractère d'échappement (section 5.7.3.5 à la page 70).

`...` – séparateur sous la forme ***( )*(\t)**

`nchar` – caractères appartenant à l'ensemble a-z, A-Z, 0-9, -, _

`vchar` – caractères appartenant à l'ensemble nchar, *, ?

`char` – caractères appartenant à la plage de valeurs 32 – 255

Exemple de construction itérative :

```
<FOR _macro_name_ == "*">%_macro_name_%</FOR>
```

Quand il exécute la construction, l'analyseur syntactique (le “parseur”) transforme la commande ci-dessus en structures conditionnelles :

```
<FOR _macro_name_ == "_value_1">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_2">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_3">%_macro_name_%</FOR>
<FOR _macro_name_ == "_value_N">%_macro_name_%</FOR>
```

Ces structures conditionnelles sont interprétées de manière séquentielle.

De cette manière, les constructions itératives sont capables de différencier une macro avec une valeur unique et la même macro, avec des valeurs multiples.

Par exemple, si la macro `%FILTERNAME%` possède les valeurs `KAVFilter1`, `KAVFilter2`, `KAVFilter3` et `SimpleFilter`, alors

la construction :

```
<FOR FILTERNAME == "KAVFilter1">%FILTERNAME%</FOR>
```

produira le texte :

```
KAVFilter1
```

la construction :

```
<FOR FILTERNAME = "KAVFilter?">%FILTERNAME%, </FOR>
```

produira le texte :

```
KAVFilter1, KAVFilter2, KAVFilter3
```

la construction :

```
<FOR FILTERNAME != "KAVFilter2">%FILTERNAME%, </FOR>
```

produira le texte :

```
KAVFilter1, KAVFilter3, SimpleFilter
```

la construction :

```
<FOR FILTERNAME != "KAV*">%FILTERNAME%, </FOR>
```

produira le texte :

```
SimpleFilter
```

5.7.3.3. Limites de visibilité d'une instruction itérative

Une construction itérative peut contenir des sous-macros, dont les valeurs ne sont accessibles (“visibles”) qu'à l'intérieur de la construction parente. Des instructions itératives peuvent être utilisées non seulement pour retourner les valeurs particulières de macros concrètes, mais aussi pour circonscrire la visibilité des sous-macros.

La visibilité d'une sous-macro est déterminée par les balises de début et de fin de la structure conditionnelle :

```
<FOR _macro_name_parent_ ==
"_value_1">%_macro_name_child_%</FOR>
```

Dans l'exemple précédent, la macro *%_macro_*name*_parent_%* est visible pour tous les sous-niveaux (entre les balises **FOR**), pour le cas où sa valeur serait modifiée.

5.7.3.4. Variables

Les variables offrent une meilleure flexibilité pour personnaliser des modèles en utilisant le langage des modèles.

Une variable peut être définie à l'intérieur de certaines limites de visibilité, de la manière suivante :

```
<DEF _var_name_ = "_const_value_"/>
```

Cette variable peut être utilisée par la suite comme une macro normale, sans aucune limitation.

La syntaxe d'une instruction de définition d'une variable est la suivante :

```
<DEF VNAME VOP VVALUE/>
```

où :

`<DEF` – début d'une instruction de définition d'une variable. Le caractère "<", s'il n'introduit pas une instruction, doit être précédé d'un caractère d'échappement (section 5.7.3.5 à la page 70) ;

`VNAME` – nom de variable sous la forme **1*(nchar)*(nchar)**; la longueur maximale est de 64 octets ;

`VOP` – opération d'affectation sous la forme =, d'une longueur de 1 octet ;

`VVALUE` – valeur de variable sous la forme **1*(vchar)*(vchar)**; la longueur maximale est de 4096 octets. La valeur n'est acceptée qu'entre guillemets. Pour des comparaisons avec une valeur contenant elle-même des guillemets, précédez ceux-ci du caractère d'échappement (section 5.7.3.5 à la page 70). Exemple :

```
<DEF _value_name_ = "\"_value_1\""/>
```

`>` – fin de l'instruction de définition d'une variable. Le caractère > qui n'est pas la fin de la définition d'une variable doit être précédé d'un caractère d'échappement (section 5.7.3.5 à la page 70). À la différence d'une instruction FOR, l'instruction DEF n'a pas de corps. Par conséquent, la balise clôturée permet d'indiquer au parseur que la balise de fin est absente.

`. . .` – séparateur sous la forme ***( )*(\t)**

`nchar` – caractères appartenant à l'ensemble a-z, A-Z, 0-9, -, _

`vchar` – caractères appartenant à l'ensemble nchar, *, ?

Si une variable est redéfinie à l'intérieur de ses limites de visibilité, elle prend une nouvelle valeur à chaque redéfinition. Par conséquent, l'instruction :

```
<DEF __NAME__= "NAME_1"/>Voici la première
valeur: %__NAME__%.
<DEF __NAME__= "_NAME__2"/>Voici la seconde
valeur: %__NAME__%.
```

aura pour sortie :

```
Voici la première valeur: NAME_1.
Voici la seconde valeur: NAME_2.
```

Il est possible de renseigner une variable avec une macro.

```
<DEF _var_name_ = "% macro_name_%"/>
```

Dans ce cas, le parseur substitue en premier lieu la macro par sa valeur puis renseigne la variable avec cette valeur, qui sera effective à l'intérieur des limites courantes de visibilité.

5.7.3.5. Syntaxe du langage

Symboles spéciaux

% signale une macro. La macro doit figurer entre deux symboles "%".
Exemple : `%VIRUSNAME%`

< crochet ouvrant d'une balise.
Exemple : `<FOR FILTERNAME == "KAVFilter1">`

> crochet fermant d'une balise.
Exemple : `<FOR FILTERNAME == "KAVFilter1">`

</ crochet ouvrant d'une balise de fermeture.
Exemple : `</FOR>`

/> crochet fermant d'une balise, dans le cas d'une structure ne possédant pas de corps.
Exemple : `<DEF __NAME __= "NAME_1"/>`

**** caractère d'échappement. Indique au parseur de traiter le caractère spécial qui le suit comme un simple caractère normal. Exemple : `\%VIRUSNAME\%`

== signe égal : coïncidence dans un masque ou dans une valeur.
Exemple : `<FOR FILTERNAME == "KAVFilter1">`
Exemple : `<FOR FILTERNAME == "KAVFilter*">`

!= signe non égal : non-coïncidence dans un masque ou dans une valeur.
Exemple : `<FOR FILTERNAME != "KAVFilter1">`
Exemple : `<FOR FILTERNAME != "KAVFilter*">`

***** Nombre illimité de caractères quelconques. Utilisé uniquement à l'intérieur d'une balise, pour des comparaison avec des modèles.
Exemple: `<FOR FILTERNAME == "KAV*">`

? Un seul caractère quelconque. Utilisé uniquement à l'intérieur d'une balise, pour des comparaison avec des modèles.
Exemple: `<FOR FILTERNAME == "KAVFilter?">`

\# Commentaire ; le parseur ignore tous les caractères qui suivent le signe "**#**" jusqu'à la fin de la ligne.

Mots-clés réservés

FOR Définition d'une construction itérative.
Exemple : `<FOR FILTERNAME = "KAVFilter1">`

DEF Définition de variable (instruction sans balise finale). Exemple : `<DEF __NAME__= "NAME_1"/>`

Macros prédéfinies

%CRLF% Retour chariot et saut de ligne (CR+LF)

%TAB% Tabulation

Le traitement est exécuté a l'intérieur d'une section globale (aucune instruction n'est nécessaire) ou a l'intérieur d'une structure conditionnelle :

```
<FOR KAV_LANGUAGE == "5.0">... </FOR>
```

Séquences d'échappement

Les séquences suivantes sont disponibles pour afficher des caractères spéciaux dans le langage des modèles :

- Pour afficher le symbole "`\`" dans le texte du modèle, tapez "`\\`".
- Si une ligne se termine sur un caractère "`\`", elle sera interprétée comme une chaîne qui se poursuit sur la ligne suivante. En outre, un symbole d'échappement à la fin d'une ligne permet d'ignorer le caractère de fin de ligne (EOL) qui autrement serait inséré dans le message généré. Une telle ligne est concaténée avec la suivante pendant le traitement avant que le parseur ne réalise d'autres actions. Cette situation est gérée indépendamment, que la séquence d'échappement figure à l'intérieur ou à l'extérieur d'une balise. Voir l'élément 1 ci-dessus si vous souhaitez placer un caractère "`\`" à la fin de la ligne.
- Pour afficher le symbole "`%`" dans le texte du modèle, utilisez "`\%`".
- Pour afficher le symbole "`/`" dans le texte du modèle, utilisez "`\/`".

- Pour afficher le symbole "<" dans le texte du modèle, utilisez "\<".
- Pour afficher le symbole ">" dans le texte du modèle, utilisez "\>".
- Pour afficher le symbole "#" dans le texte du modèle, utilisez "\#".

Remarque :

Le langage des modèles est sensible à la casse. Le nombre d'espaces ou de tabulations (qu'ils soient présents ou absents) n'est pas normalisé. Les mots-clés réservés doivent être séparés par des caractères d'espacement ou par des caractères spéciaux.

5.7.3.6. Macros de notifications pour l'application

Il est possible d'utiliser des macros dans des modèles de notifications pour gérer le message en entier ou par parties. Les macros permettent de personnaliser les notifications pour inclure des informations complémentaires sur les propriétés du message ou de l'objet d'origine, ou sur les actions qui vont leur être appliquées.

L'administrateur peut utiliser dans les notifications les macros suivantes, associées aux messages en entier :

%VERSION% – numéro de version de l'instance de Kaspersky Anti-Virus installé, utilisé pour analyser le message.

%PRODUCT% – nom complet du produit de Kaspersky Anti-Virus.

%CLIENT% – adresse IP distante du client de messagerie.

%SERVER% – adresse IP du serveur exécutant le service central de l'application.

%SENDER% – adresse de l'expéditeur.

%RECIPIENTS% – adresse du destinataire.

%HEADERS% – en-tête du message.

%MSGID% – numéro d'identification du message.

%SUBJECT% – contenu du champ **Sujet** du message d'origine.

%DATE% – date de traitement du message.

%TIME% – heure de traitement du message.

%BK_ACTION% – actions appliquées au message ayant entraîné la création d'une copie de sauvegarde (si l'application est configurée pour sauvegarder les messages).

%BK_LOCATION% – chemin complet du dossier de sauvegarde (si la zone de stockage existe).

%ACTION_LIST% – liste contenant des informations sur le message et les pièces jointes, ainsi qu'une liste d'actions appliquées. Les informations en sorties ont la forme suivante :

```
<status> <action> <information>
```

pour chaque partie traitée du message.

Dans les notifications en rapport avec les objets supprimés d'un message, la macro suivante est disponible :

%INFO% – information associées aux actions suivantes exécutées :

- liste des virus (logiciels malveillant) détectés – dans le cas d'objets infectés ;
- Description du code d'erreur – dans le cas d'objets ayant provoqué une erreur d'analyse ;
- type MIME ou nom de pièce jointe – dans le cas d'objets filtrés.

Les macros doivent être spécifiées dans le texte des modèles de notification.

CHAPITRE 6. PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS

La protection antivirus du système de fichiers est assurée par le composant *kav4lms-kavscanner* qui analyse les fichiers de l'ordinateur et traite les objets infectés ou suspects conformément à ses paramètres.

Remarque :

Tous les paramètres du composant *kav4lms-kavscanner* figurent groupés dans les options de la section **[scanner.*]** du fichier de configuration de l'application.

Attention !

Par défaut, uniquement les utilisateurs **root** et **kluser** peuvent lancer une analyse à la demande.

Vous pouvez analyser le système de fichiers complet ou seulement un répertoire ou fichier individuels. Tous les paramètres de protection peuvent être divisés en groupes qui définissent :

- La couverture de l'analyse (section 6.1 à la p. 75).
- Comment les objets vont être analysés et désinfectés (section 6.2 à la p. 76).
- Les actions à exécuter sur les objets (section 6.3 à la p. 77).

L'analyse du système de fichiers de votre ordinateur peut être lancée :

- Comme une tâche exécutée une seule fois depuis la ligne de commande (section 6.4 à la p. 78).
- En fonction d'une planification programmée avec l'application **cron** (section 6.5 à la p. 79).

Attention !

Une analyse antivirus de l'ordinateur tout entier est un processus qui mobilise des ressources considérables. Il convient de noter qu'après avoir démarré la tâche, le rendement de votre ordinateur se réduira : c'est pourquoi nous conseillons de ne pas exécuter une autre application lourde pendant le même temps. Pour contourner cet inconvénient, nous vous conseillons à la place de lancer l'analyse sur des catalogues sélectionnés individuels.

6.1. Couverture de l'analyse

La couverture de l'analyse se décompose grossièrement en deux parties :

- *chemin de l'analyse* – la liste des répertoires et des objets dans lesquels l'analyse exécute sa recherche antivirus ;
- *objets de l'analyse* – types des objets sur lesquels s'exécute l'analyse antivirus (comprimés, etc.).

Par défaut tous les objets de tous les systèmes de fichiers disponibles sont analysés, en commençant par le répertoire courant.

Remarque :

Pour analyser l'ensemble du système de fichiers de l'ordinateur, remontez au répertoire racine ou, sur la ligne de commande, spécifiez la couverture d'analyse sous la forme "/".

Vous pouvez redéfinir le chemin de l'analyse avec l'une des méthodes suivantes :

- Indiquer sur la ligne de commande la liste (avec un espace séparateur) de tous les répertoires et de tous les fichiers à analyser, avec des chemins absolus ou relatifs (relatifs au répertoire courant).
- Recenser dans un fichier texte tous les chemins d'analyse et spécifier ce fichier avec le paramètre **-@<filename>** sur le ligne de commande**.** Chaque objet dans ce fichier doit figurer sur une ligne séparée, avec un chemin d'accès absolu.

  Attention !

  Si la ligne de commande utilise les deux méthodes (chemins à analyser et fichier avec la liste d'objets), l'analyse s'effectuera uniquement sur la liste des chemins indiqués dans le fichier. Les chemins saisis directement sur la ligne de commande seront ignorés.

- Désactivez l'*analyse récursive des catalogues* (section **[scanner.options]**, option **Recursion** ou paramètre **-r** sur la ligne de commande).
- Créez un fichier de configuration alternatif et spécifiez ce fichier sur la ligne de commande, avec le paramètre **-c <filename>** au lancement du composant.

Le chemin de l'objet à analyser ne doit pas dépasser 4096 octets. Les objets situés à des niveaux d'imbrications plus profonds ne seront pas analysés.

Les objets à vérifier par défaut sont définis dans le fichier de configuration *kav4lms.conf* (section **[scanner.options]**) et peuvent être redéfinis :

- directement dans ce fichier ;
- par des paramètres de ligne de commande au démarrage du composant ;
- en utilisant un fichier de configuration alternatif.

6.2. Mode d'analyse et de réparation des objets

Les paramètres de ce mode sont très importants, car ils déterminent si l'application devra réparer les fichiers infectés qui seront découverts.

Par défaut, la réparation est désactivée : le comportement par défaut est d'analyser les objets et d'alerter de la présence de virus détectés et d'autres fichiers suspects ou endommagés par l'écriture de messages à l'écran et dans le rapport.

Suite à l'analyse antivirus, chaque objet se voit attribuer un indicateur d'état, parmi la liste suivante :

- **Clean** – aucun virus détecté (l'objet n'est pas infecté).
- **Infected** – l'objet est infecté.
- **Warning** – le code de l'objet ressemble à celui d'un virus connu.
- **Suspicious** – l'objet est suspecté d'être infecté par un virus inconnu (non attribué si l'option **UseCodeAnalyzer=no**).
- **Corrupted** – l'objet est endommagé.
- **Protected** – l'objet ne peut être analysé car il est chiffré (ou protégé par mot de passe).

- **Error** – une erreur est survenue pendant l'analyse de l'objet.

En activant le mode de réparation (section **[scanner.options]**, paramètre **Cure=yes**) seuls les fichiers avec l'état **Infected** sont envoyés pour réparation. Après traitement, l'objet se voit attribuer un indicateur d'état, parmi la liste suivante :

- **Cured** – réparation réussie de l'objet.
- **CureFailed** – l'objet n'a pas pu être réparé. Les fichiers avec cet état seront traités conformément aux règles spécifiées pour les fichiers infectés.

6.3. Actions à exécuter sur les objets

Les actions à réaliser sur un objet dépendent de l'état de l'objet. L'action par défaut est uniquement d'informer de la détection d'objets infectés ou d'objets suspects. Cependant, dans le cas d'objets avec l'état **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** et **Corrupted**, il est possible de configurer des réponses supplémentaires, y compris :

- *déplacement vers un répertoire* – déplacement d'objets avec l'état indiqué vers un répertoire (des déplacements *simples* et *récursifs* sont pris en charge) ;
- *suppression de objet* du système de fichiers ;
- *exécution d'une commande* – les fichiers sont traités par des fichiers de script au standard Unix ou similaire.

Il convient de noter que Kaspersky Anti-Virus fait la différence entre les objets simples (un fichier) et les conteneurs (composés de plusieurs objets, un fichier comprimé, par exemple). Les actions effectuées sur ces objets sont également différenciées ; dans les fichiers de configuration ces actions sont placées dans différentes sections, la section **[scanner.object]** pour les objets simples et la section **[scanner.container]** pour les conteneurs.

Attention !

Les actions exécutées sur des archives auto-extractibles peuvent être différentes : si le fichier d'archive est lui-même infecté, il sera considéré comme un objet simple, mais si ce sont les objets qui se trouvent à l'intérieur de l'archive qui sont infectés, le fichier d'archive sera alors considéré comme un conteneur. Par conséquent les actions à réaliser sur les archives seront déterminées, selon le cas, par des paramètres spécifiés dans des sections différentes du fichier de configuration.

Pour sélectionner les actions à réaliser sur un objet, vous pouvez employer plusieurs méthodes comme les suivantes :

- Définir ces actions dans le fichier de configuration *kav4lms.conf*, si elles seront utilisées comme actions par défaut (sections **[scanner.object]** et **[scanner.container]**).
- Spécifier les actions dans un fichier de configuration alternatif que vous indiquez lors du lancement du composant.

  Remarque :

  Si au lancement du composant, aucun fichier de configuration n'est spécifié sur la ligne de commande, alors les paramètres d'opération sont lus dans le fichier *kav4lms.conf.* Il n'est pas nécessaire de préciser ce fichier au lancement.

- Spécifier les actions applicables pendant la session courante en utilisant des paramètres de ligne de commande lors du lancement du composant *kav4lms-kavscanner*.

Les actions effectuées à la fois sur des objets simples et conteneurs utilisent la même syntaxe (sections **[scanner.object]** et **[scanner.container]**).

6.4. Analyse à la demande d'un répertoire individuel

L'une des tâches les plus communes implémentée par Kaspersky Anti-Virus est l'analyse antivirus et réparation d'un répertoire individuel.

Exécuter une analyse antivirus avec les conditions suivantes :

1. Analyse antivirus du répertoire /tmp avec réparation automatique de tous les objets infectés. Suppression de tous les objets qui ne peuvent être réparés.

2. Création des fichiers **infected.lst**, **suspicion.lst**, **corrupted.lst** et **warning.lst** pour enregistrer les noms de tous les objets infectés, suspects ou endommagés, pendant l'analyse.

3. Le résultat du fonctionnement de l'opération du composant (date de démarrage, informations sur tous les fichiers à l'exception des fichiers sains) sera consigné dans le rapport kavscanner-date_courante-pid.log créé dans le répertoire courant.

Pour mettre en œuvre cette tâche, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-kavscanner -\
rlq -pi/tmp/infected.lst -ps/tmp/suspicion.lst -\
pc/tmp/corrupted.lst -pw/tmp/warning.lst -o /tmp/ \
kav4lms-kavscanner-`date "+%Y-%m-%d-$$"`.log -i3 \
```

6.5. Planification de l'analyse

Les tâches de Kaspersky Anti-Virus peuvent être programmées à l'aide de l'application **cron**.

*Exécuter une analyse antivirus du répertoire **/home** tous les jours à 0:00, avec les paramètres d'analyse spécifiés dans le fichier de configuration **/etc/kav/scanhome.conf**. Pour exécuter cette tâche, procédez comme ceci :*

1. Créez le fichier de configuration */etc/kav/scanhome.conf* et spécifiez les paramètres d'analyse requis dans ce fichier.

2. Modifiez le fichier qui définit les règles de fonctionnement du processus cron **(crontab -e)** en tapant la ligne suivante :

```
0 0 * * *    /opt/kaspersky/kav4lms/bin/kav4lms-\
kavscanner -c /etc/kav/scanhome.conf /home
```

6.6. Notifications émises vers l'administrateur

Les outils standard d'Unix vous permettent de spécifier que les notifications doivent être envoyées à l'administrateur en cas de détection d'objets infectés, suspects ou endommagés dans les systèmes de fichiers de l'ordinateur.

Configurer la notification adressée à l'administrateur sur la détection de fichiers ou d'archives infectés pendant l'analyse des systèmes de fichiers, avec les paramètres spécifiés dans le fichier de configuration kav4lms.conf.

Attention !

Cet exemple est pour un Linux !

Pour exécuter cette tâche, procédez comme ceci :

Spécifiez les règles suivantes pour le traitement d'objets simples ou d'objets conteneurs dans le fichier de configuration *kav4lms.conf* :

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is \
infected by %VIRUSNAME% |
mail -s kav4lms-kavscanner admin@localhost
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% \
is infected, viruses list is in the attached file \
%LIST% | mail -s kav4lms-kavscanner -a %LIST% \
admin@localhost
```

Attention !

Avant de lancer cet exemple, assurez-vous que l'outil **mail** se trouve sur le chemin d'installation standard dans le système d'exploitation.

CHAPITRE 7. MISE A JOUR DES BASES ANTIVIRUS

La mise à jour de la base antivirus, exécutée par le composant *kav4lms-keepup2date*, joue un rôle essentiel pour une protection antivirus complètement efficace. Les serveurs de mises à jour de Kaspersky Lab sont la source par défaut utilisée pour le téléchargement des bases antivirus. La liste de ces serveurs comprend :

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

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

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

La liste des liens URL sur lesquels vous pouvez télécharger les mises à jour figure dans le fichier *updcfg.xml*, compris dans le kit de distribution de l'application. Pour consulter cette liste de serveurs de mises à jour, tapez ce qui suit sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -s
```

Au cours de la mise à jour, le composant *kav4lms-keepup2date* sélectionne la première adresse de cette liste et tente de télécharger les bases antivirus à partir du serveur correspondant. L'emplacement courant de l'ordinateur (correspondant au code du pays avec deux lettres, conformément à la norme ISO 3166-1) peut être précisé avec le paramètre **RegionSettings** dans la section **[updater.options]** du fichier de configuration de l'application. Dans ce cas, le composant *kav4lms-keepup2date* choisit en premier les serveurs de mises à jour appartenant à la région spécifiée. Si la mise à jour à partir de l'adresse sélectionnée échoue, le composant essaie à nouveau à partir de l'adresse URL suivante.

Remarque :

Des mises à jour des bases antivirus sont mises à disposition sur les serveurs de Kaspersky Lab toutes les heures.

Après une mise à jour réussie, la commande indiquée par le paramètre **PostUpdateCmd** dans la section **[updater.options]** du fichier de configuration est exécutée. Par défaut, cette commande recharge automatiquement la base antivirus. Si une modification invalide est faite sur ce paramètre, l'utilisation par l'application de la base mise à jour peut échouer ou fonctionner incorrectement.

Remarque :

Tous les paramètres du composant *kav4lms-keepup2date* sont regroupés dans les options de la section **[updater.*]** du fichier de configuration.

Si la structure de votre réseau local est plutôt complexe, nous vous recommandons de télécharger d'heure en heure les mises à jour de la base antivirus depuis les serveurs de mises à jour, de les placer dans un répertoire partagé, puis de configurer les autres ordinateurs du réseau local pour qu'ils utilisent ce répertoire comme leur source de mises à jour. Pour plus détails sur la création d'un répertoire réseau, reportez-vous à la section 7.3 à la p. 84.

La mise à jour peut être programmée à l'aide de l'outil **cron** (section 7.1 à la p. 82) ou exécutée à la demande par l'administrateur, en lançant manuellement cette tâche depuis la ligne de commande (section 7.2 à la p. 83).

7.1. Mise à jour automatique de la base antivirus

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

Configurer la mise à jour automatique de la base antivirus toutes les heures. Seules les erreurs de l'application doivent être consignées dans le journal système. Gérer un journal général de toutes les tâches démarrées, sans imprimer d'informations sur l'écran. Pour exécuter cette tâche, procédez comme ceci :

1. Spécifiez ces valeurs dans le fichier de configuration de l'application, par exemple :

   ```
   [updater.options]
   KeepSilent=yes
   [updater.report]
   Append=yes
   ReportLevel=1
   ```

2. Modifiez le fichier de configuration du processus cron (crontab -e) en tapant la ligne suivante :

   ```
   0 0-23/1 * * * /opt/kaspersky/kav4lms/bin/kav4lms-\
   keepup2date -e
   ```

Configurer le composant kav4lms-keepup2date pour sélectionner automatiquement dans la liste fournie par l'application l'adresse URL du serveur de mises à jour. Pour exécuter cette tâche, procédez comme ceci :

Affectez la valeur **No** au paramètre **UseUpdateServerUrl** dans la section **[updater.options]** du fichier de configuration de l'application.

Configurer le composant keepup2date pour télécharger les mises à jour depuis l'adresse URL spécifiée par l'administrateur. Si le téléchargement ne peut pas se faire à partir de cette adresse URL, interrompre le processus de téléchargement. Pour exécuter cette tâche, procédez comme ceci :

Affectez la valeur **Yes** à la fois aux paramètres **UseUpdateServerUrl** et **UseUpdateServerUrlOnly** de la section **[updater.options]**. En outre, le paramètre **UpdateServerUrl** doit contenir l'adresse URL du serveur de mises à jour.

Configurer le composant keepup2date pour télécharger les mises à jour depuis une adresse URL spécifiée. Si le téléchargement ne peut pas se faire à partir de cette adresse URL, mettre à jour la base antivirus depuis les adresses URL spécifiée par la liste comprise dans le composant keepup2date*. Pour exécuter cette tâche, procédez comme ceci :*

Affectez la valeur **Yes** au paramètre **UseUpdateServerUrl** de la section **[updater.options]**, et la valeur **No** au paramètre **UseUpdateServerUrlOnly**. En outre, le paramètre **UpdateServerUrl** doit contenir l'adresse URL du serveur de mises à jour.

7.2. Mise à jour à la demande de la base antivirus

Vous pouvez démarrer la mise à jour de la base antivirus depuis la ligne de commande à tout moment. Pour ce faire, tapez la commande suivante :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date
```

Lancer la mise à jour de la base antivirus et enregistrez les résultats dans le fichier /tmp/updatesreport.log. Pour implémenter cette tâche, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -l \
/tmp/updatesreport.log
```

La manière la plus appropriée de mettre à jour la base antivirus sur plusieurs ordinateurs est de télécharger une seule fois les mises à jour depuis les serveurs de mises à jour, de les placer dans un répertoire du réseau, puis de configurer les autres ordinateurs pour qu'ils utilisent ce répertoire comme leur source de mises à jour.

Organiser la mise à jour de la base antivirus depuis un répertoire réseau ftp://10.10.10.1/home/bases et uniquement si ce répertoire n'est pas disponible, ou s'il est vide, faire la mise à jour de la base à partir des serveurs de mises à jour de Kaspersky Lab. Consigner les résultats dans le fichier ***report.txt****.*

Pour exécuter cette tâche, procédez comme ceci :

1. Spécifiez les valeurs des paramètres correspondants dans le fichier de configuration de l'application :

   ```
   [updater.options]
   UpdateServerUrl=ftp://10.10.10.1/home/bases
   UseUpdateServerUrl=yes
   UseUpdateServerUrlOnly=no
   ```

2. Tapez à la ligne de commande :

   ```
   # /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -l \
   /tmp/report.txt
   ```

7.3. Création d'un répertoire réseau pour entreposer les mises à jour

Pour s'assurer que la base antivirus est correctement mise à jour depuis le répertoire réseau, ce dernier doit reproduire à l'identique la structure de fichiers des serveurs de mises à jour de Kaspersky Lab. Voici une description détaillée de cette tâche.

Créer un répertoire réseau depuis lequel les ordinateurs du réseau local peuvent recopier les mises à jour de la base antivirus. Pour exécuter cette tâche, procédez comme ceci :

1. Créez un répertoire local.
2. Lancez le composant *kav4lms-keepup2date* comme ceci :

   ```
   # /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -u
   <dir>
   ```

   où `<dir>` est le chemin complet au répertoire local.

3. Autorisez l'accès en lecture seule des ordinateurs réseau à ce catalogue.

Configurer la mise à jour de la base antivirus pour qu'elle s'exécute via un serveur proxy. Pour exécuter cette tâche, procédez comme ceci :

1. Affectez la valeur **Yes** au paramètre **UseProxy** de la section **[updater.options]**.
2. Vérifiez que le paramètre **ProxyAddress** de la section **[updater.options]** du fichier de configuration contient l'adresse URL du serveur proxy. L'adresse doit être indiquée sous la forme **http://nom_utilisateur:mot_de_passe@adresse_ip:port**. Les valeurs **adresse_ip** et **port** sont obligatoires, tandis que **nom_utilisateur** et **mot_de_passe** ne sont nécessaires que lorsque le proxy requiert une authentification.

ou :

1. Renseignez avec la valeur **Yes** le paramètre **UseProxy** de la section **[updater.options]**.
2. Spécifiez la variable d'environnement **http_proxy** sous la forme **http://nom_utilisateur:mot_de_passe@adresse_ip:port**. Notez que la variable d'environnement ne sera prise en compte que si le paramètre UseProxy de la section **[updater.options]** est absent ou s'il possède la valeur Yes.

CHAPITRE 8. GESTION DES CLES DE LICENCE

Le fichier-clé vous donne l'autorisation d'utiliser l'application, e contient toutes les informations relatives à la licence que vous avez achetée, y compris le schéma de licence, la date de péremption de la clé et les détails du distributeur.

Outre le droit d'utiliser l'application, pendant la période d'activité de la licence vous bénéficiez de :

- service d'assistance technique 24/7 ;
- nouvelles mises à jour de la base antivirus heure toutes les heures ;
- mises à jour de l'application (correctifs) ;
- réception de nouvelles versions de l'application (mises à niveau) ;
- dernières informations récentes sur les nouveaux virus.

L'expiration de la clé vous fait perdre automatiquement le bénéfice des services précédents. Kaspersky Anti-Virus continue de réaliser les traitements antivirus mais il n'utilise que la base antivirus dans l'état où elle se trouvait à la date d'expiration de la clé. La fonction de mise à jour de la base antivirus ne sera plus disponible. Si la base antivirus est mise à jour manuellement, sa date de renouvellement sera sans doute postérieure à la date d'expiration de la clé. Dans ce cas, l'application perdra ses fonctionnalités antivirus et une notification correspondante est émise.

Par conséquent, il est extrêmement important d'examiner avec régularité les fichiers de rapport contenant les détails de la licence et de surveiller la date de péremption de la clé.

L'application prend en charge plusieurs schémas de licence :

- **par trafic**.

  Ce schéma de licence assure la protection d'un certain volume de trafic journalier spécifié par la clé. Seul le trafic traité, dont l'état est **clean** ou **notchecked**, est pris en compte. Si le trafic quotidien dépasse les limites de licence, la notification pour l'administrateur est émise pour tous les messages à compter du premier qui dépasse cette limite.

- **par adresses**.

  Ce schéma de licence assure la protection d'un certain nombre d'adresses de messagerie. Ceci s'applique à la liste des domaines

spécifiée par le paramètre **LicensedUsersDomains** dans la section **[kav4lms:server.settings]** du fichier de configuration *kav4lms.conf*, et aux adresses du serveur sur lequel l'application s'exécute.

Les noms de domaines sous licence peuvent être précisés :

- en tant que chaîne littérale
- par des expressions avec caractères génériques (syntaxe UNIX)
- par des expressions régulières (syntaxe POSIX).

> **Attention !**
>
> Les expressions régulières ne sont pas sensibles à la casse.

Si le nombre d'adresses de messagerie dans un domaine dépasse les limites de licence, l'administrateur sera invité à acquérir une clé pour la quantité de trafic supplémentaire.

8.1. Affichage des détails de la clé

En outre, Kaspersky Anti-Virus incorpore un composant spécial, le composant *kav4lms-licensemanager*, qui permet non seulement d'afficher des informations complètes sur les clés, mais de recevoir également des informations analytiques.

Toutes les informations seront imprimées à l'écran.

Pour afficher des informations sur toutes les clés, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager -s
```

Des informations similaires aux suivantes seront imprimées à l'écran :

```
Kaspersky license manager for Linux. Version
5.6/RELEASE #68
Copyright © Kaspersky Lab, 1997-2007.
Portions Copyright © Lan Crypto


License info:
Product name: Kaspersky Anti-Virus BO for SendMail /
Qmail / Postfix Milter API International Edition. 10-
14 MailAddress 1 month Beta Licence
Expiration date: 01-09-2007, expires in 28 days
```

```
Active key info:
Key file:         00BEA0DB.key
Install date:     02-08-2007
Product name:     Kaspersky Anti-Virus BO for SendMail
/ Qmail / Postfix Milter API International Edition.
10-14 MailAddress 1 month Beta Licence
Creation date:     02-02-2007
Expiration date: 03-03-2008
Serial:          0038-000413-00BEA0DB
Type:             Beta
Count:             10
Lifespan:         30
Objs:             7:10
```

Le paramètre `Objs` représente l'objet de licence. Sa valeur est composée des parties `<type_of_objects>:<number_of_objects>`. La partie `<type_of_objects>` peut avoir les valeurs suivantes :

- 3 – représente le trafic journalier ;
- 7 – représente les adresses de courrier.

La partie `<number_of_objects>` possède la même valeur que le paramètre `Count`.

Pour afficher des informations sur une clé en particulier, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\
 -k <key filename>
```

où `<key filename>` est le nom du fichier-clé, par exemple, `0003D3EA.key`.

Les informations suivantes seront imprimées à l'écran :

```
Kaspersky license manager for Linux. Version
5.6/RELEASE #68
Copyright © Kaspersky Lab, 1997-2007.
Portions Copyright © Lan Crypto
Product name:     Kaspersky Anti-Virus BO for SendMail
/ Qmail / Postfix Milter API International Edition.
10-14 MailAddress 1 month Beta Licence
Creation date:     02-02-2007
Expiration date: 03-03-2008
```

```
Serial:          0038-000413-00BEA0DB
Type:             Beta
Count:             10
Lifespan:         30
Objs:             7:10
```

8.2. Renouvellement de la clé

Le renouvellement de votre clé vous donne le droit de restaurer les fonctionnalités complètes de l'application : c'est à dire. de mettre à jour la base antivirus et de réactiver les services supplémentaires énumérés à la section 1.3 à la p. 10.

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

Pour renouveler votre clé :

Contactez la société qui vous a vendu l'application et achetez un renouvellement de la licence d'utilisation de Kaspersky Anti-Virus.

ou :

Renouvelez directement la clé sur le site de Kaspersky Labs, par une commande directe à notre Département commercial (sales@kaspersky.com), ou en remplissant un formulaire sur notre site Web (http://www.kaspersky.com), section **eStore -> Renewal**. Après réception de votre paiement, vous recevrez une nouvelle clé à l'adresse de messagerie précisée sur votre commande.

Remarque :

Kaspersky Lab Ltd. réalise régulièrement des promotions qui vous permettent d'obtenir des réductions considérables lors du renouvellement de la licence de nos produits. Pour être informé sur nos offres, visitez le site de la société Kaspersky Lab et suivez les liens **Products → Sales and special offers** (Produits, Ventes et offres spéciales).

Vous devez installer la clé que vous avez achetée.

Pour installer votre nouvelle clé, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\
 -a <key filename>
```

Après ceci, nous vous conseillons de mettre à jour votre base antivirus (section Chapitre 7 à la p. 81).

Pour supprimer une clé, tapez sur l'invite de commande :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\
 -da
```

pour supprimer la clé active,

ou

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\
 -dr
```

pour supprimer la clé supplémentaire.

CHAPITRE 9. GENERATION DE RAPPORTS ET DE STATISTIQUES

9.1. Fichier-journal de l'application

Remarque :

L'application peut consigner des informations sur l'activité de ses deux composants : le serveur et le filtre. Les options de consignation figurent respectivement dans les sections **[kav4lms:server.log]** et **[kav4lms:filter.log]** du fichier de configuration kav4lms.conf.

Les résultats de l'activité des composants de l'application sont conservés soit dans le journal du système, soit dans un fichier journal propre. La destination est précisée par le paramètre **Destination**. La syntaxe de la destination est :

- `syslog:<name>@<facility>` – s'inscrit en tant qu'application `<name>`, dans la catégorie `<facility>`
- `file:<log_file_path>` – les messages sont enregistrés dans le fichier indiqué.

Attention !

N'utilisez pas le même fichier destination pour le journal du serveur et pour celui du filtre – un seul processus peut accéder à la fois au fichier journal.

Le type et la précision des informations consignées sont spécifiées par le paramètre **Options**. Le paramètre **Options** est la liste des options de consignation. L'option de consignation est divisée en deux parties, séparées par un point :

1. Module de journalisation. Cette partie représente le module des fonctionnalités de l'application, dont l'activité est consignée. Les valeurs acceptées sont :
    - **all** – inclut tous les groupes ;
    - **config** – messages en rapport à la configuration ;
    - **app** – événements liés à la logique commerciale du produit ;

- **scan** – état de l'analyse, actions ;
- **cfilter** – état du filtrage des contenus, actions ;
- **backup** – message lié aux copies de sauvegarde ;
- **notif** – messages provenant du système de notifications ;
- **admin** – événements liés aux caractéristiques administratives (par exemple : SNMP, commandes) ;
- **smtp** – dialogue SMTP d'information entre le MTA et l'application.

2. Niveau d'information des rapports. Cette partie décrit l'importance des informations consignées. Il peut être spécifié par nom, par un lettre ou par un nombre. Voir le tableau des options disponibles avec leurs descriptions.

Symbole de niveau	Nom du niveau	Description
0, F	**fatal**	Erreurs critiques uniquement. Par exemple, le composant est infecté ou une erreur s'est produite pendant une vérification ou lors du chargement de la base de données ou des clés de licence. Les informations liées aux erreurs critiques sont signalées par un caractère "F" dans le fichier journal.
1, E	**error**	Autres erreurs, y compris celles qui provoquent la fermeture du composant : par exemple, informations sur l'erreur d'analyse d'un objet. Les informations non critiques sont signalées par un caractère "E" dans le fichier journal.
2, W	**warning**	Erreur pouvant causer la fermeture de l'application : par exemple, espace disque insuffisant ou expiration de la clé. Ces messages sont signalés par un caractère "W" dans le fichier journal.

Symbole de niveau	Nom du niveau	Description
3, I	**info**	Message important : par exemple, pour indiquer si le composant est en exécution, le chemin du fichier de configuration, la couverture d'analyse, des informations sur la base antivirus, les clés de licence et des informations statistiques sur les résultats. Les messages d'information sont signalés par un caractère "I" dans le fichier journal.
4, A	**activity**	Messages sur l'activité courante des applications (par exemple, le nom de l'objet analysé). Ces messages sont signalés par un caractère "A" dans le fichier journal.
9, D	**debug**	Messages de débogage ou mise au point. Ces messages sont signalés par un caractère "D" dans le fichier journal.

Les options de consignation peuvent être spécifiées des manières suivantes :

- une combinaison du groupe et du niveau (par exemple, **scan.info**) ;
- une combinaison niveau-groupe précédée par "-" détermine l'exclusion de l'option spécifiée.

Exemple :

```
[kav4lms:server.log]
Options = backup.all, config.error, scan.all, -scan.debug
Options = backup.all, config.E, scan.all, -scan.9
```

Ceci active tous les messages de sauvegarde, tous les messages de configuration et tous les messages d'analyse, à l'exception des messages de mise au point. Le second exemple est identique au premier et montre comment utiliser les options de sélection du niveau.

Attention !

Les niveaux de reporting ne contiennent pas les niveaux inférieurs. Pour sélectionner plusieurs niveaux, tous doivent être recensés ou les niveaux non souhaités doivent être exclus.

Les fichiers journaux peuvent grandir très rapidement, mais il est possible de limiter leur taille en activant la rotation des journaux. Cette caractéristique est activée en renseignant les paramètres **RotateSize** et **RotateRounds** avec des valeurs non-nulles.

Si la rotation des journaux est activée, un fichier journal grandit jusqu'à ce qu'il atteigne la taille spécifiée par **RotateSize**. Il est alors renommé en lui ajoutant le suffixe ".1". Si un fichier avec ce suffixe existe déjà, des fichiers avec suffixes ".2", ".3", etc. sont créés, jusqu'à ce que leur nombre (en suffixe) atteigne la valeur **RotateRounds**. Si cette valeur est atteinte, un fichier avec suffixe ".1" est utilisé de nouveau.

9.2. Statistiques d'application

Remarque :

Les options de collecte des statistiques d'application figurent dans la section **[kav4lms:server.statistics]** du fichier de configuration principal.

Pendant l'exécution de l'application, des statistiques de deux sortes sont collectées :

- **Statistiques générales** collectées de temps en temps, qui reflètent l'activité d'ensemble de l'application.
- **Statistiques détaillées** collectées à partir chaque message traité.

Le type des statistiques conservées est précisé par le paramètre **Options**. La liste des valeurs disponibles est donnée par le tableau ci-après.

Catégorie statistique	Valeur des options	Informations collectées
Messages	**messages**	Nombre de messages entrants, nombre de messages analysés, nombre de messages protégés, nombre de messages infectés, nombre de messages erronés (endommagés), moyenne des tailles de tous les message (en octets), durée moyenne investie dans la vérification d'un (en millisecondes)

Catégorie statistique	Valeur des options	Informations collectées
Ressources système	**resources**	Durée en secondes depuis la dernière requête de statistiques, la taille totale du trafic (en kilo-octets), usage total de l'UC par utilisateur, usage total de l'UC par le système
Menaces détectées	**virus**	10 derniers virus détectés, 10 premières adresses IP qui envoient le plus grand nombre de virus
Filtrage du contenu	**filters**	Nombre de messages filtrés par type MIME, nombre de messages filtrés par pièce jointe, nombre de messages filtrés par taille, nombre de messages filtrés par nom de virus
Tout	**all**	Toutes les options ci-dessus
Statistiques par message	**raw**	Statistiques complètes (brutes) par message
Sans statistiques	**none**	Sans de collecte statistique

La valeur du paramètre **Options** est la liste des valeurs mentionnées, séparées par des virgules.

Exemples :

```
Options = all
```

Collecte uniquement des données récapitulatives (messages, ressources, virus, filtres)

```
Options = all, raw
```

Collecte également les statistiques par message.

```
Options = none, raw
```

Collecte uniquement des données par message, sans récapitulatifs.

Pour activer la collecte de statistiques, renseignez le paramètre **Options** avec unevaleur différente de **none**.

Attention !

Renseigner le paramètre **Options** avec la valeur **all** ne permet pas d'activer les statistiques brutes (raw) ! Ce type de statistiques doit être explicitement défini.

Échantillon d'enregistrement du fichier de statistiques brutes :

```
1210247100     1208    from@exmaple.com
rcpt@example.com infected        EICAR-Test-File 127.0.0.1
1Ju4YW-000Du9-0U Default
```

où :

- 1210247100 – heure de traitement du message (au format UNIX) ;
- 1208 – taille du message ;
- from@example.com – adresse de l'expéditeur du message ;
- rcpt@example.com – adresse du destinataire du message ;
- infected – état attribué au message après analyse ;
- EICAR-Test-File – nom de la menace détectée dans le message ;
- 127.0.0.1 – adresse IP utilisée pour l'envoi du message ;
- 1Ju4YW-000Du9-0U – Id. du message dans la file d'attente du système de messagerie ;
- Default – nom du groupe associé aux paramètres utilisés pour le traitement du message.

Pour écrire des statistiques dans un fichier, exécutez la commande suivante :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \
write
```

Cette commande écrase également le fichier de statistiques existantes avec de nouvelles informations.

Pour réinitialiser les compteurs statistiques internes, exécutez la commande suivante :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \
reset
```

Remarque :

Le fichier de statistiques doit être écrasé pour refléter les modifications après la réinitialisation des compteurs.

Les paramètres de fonctionnement des statistiques sont regroupés dans la section **[kav4lms:server.statistics]** du fichier de configuration *kav4lms.conf*.

Il existe deux types de statistiques :

- **récapitulatives** – accumulées dans le temps, pour refléter l'activité générale du produit ;
- **par message** – écrites pour chaque message traité, affichant des informations détaillées sur son traitement ; elles sont également désignées statistiques **brutes** (raw).

Les statistiques récapitulatives sont conservées dans un fichier spécifié par le paramètre **Destination**. Les statistiques brutes sont conservées dans le fichier spécifié par le paramètre **RawDestination**.

Attention !

Quand un message contient plusieurs types d'objets avec différents verdicts d'analyse, le même message est comptabilisé par chacun des compteurs correspondants. Par conséquent, les compteurs ne sont pas cumulatifs, c'est à dire que leur somme ne correspond pas forcément au total des messages analysés.

Prenons par exemple un même message avec trois pièces jointes : l'une est infectée, une autre est protégée par un mot de passe et la dernière est du type `application/msword`. Il peut être comptabilisé (selon la configuration) par :

- **total_messages** – il fait partie des messages transférés ;
- **scanned_messages** – il a été analysé ;
- **protected_messages** – une partie est protégée ;
- **infected_messages** – une partie est infectée ;
- **filtered_mime** – il possède un type MIME énuméré.

Les statistiques peuvent être collectées en 2 formats :

- **fichier txt**
- **fichier xml**.

Le format du fichier de statistiques est précisé par le paramètre **Format**.

CHAPITRE 10. CONFIGURATION AVANCEE

10.1. Surveillance de l'état de la protection via SNMP

À partir de la version 5.6, l'application offre un accès en lecture seule aux informations suivantes via le protocole SNMP :

- *configuration du produit* – paramètres de toutes les sections des fichiers de configuration de l'application, y compris les fichiers de configuration de groupes ;
- *statistiques de fonctionnement* – statistiques complètes sur le fonctionnement de l'application.

Remarque :

L'application fonctionne avec des agent qui prennent en charge le protocole SNMP, v1, v2 et v3. Il convient de noter que le produit envoie des pièges v2, il faut donc configurer en conséquence le récepteur de pièges (“trap sink”).

Les information accessible par SNMP sont déterminées par le paramètre **SNMPServices**, placé dans la section **[kav4lms:server.snmp]** du fichier de configuration *kav4lms.conf*. Ce paramètre peut prendre les valeurs suivantes :

- **config** – informations configuration de l'application ;
- **statistics** – statistiques de fonctionnement (section 9.2 à la p. 94 pour plus de détails sur les statistiques publiées) ;
- **admin** – informations administratives contenant :
  - **Status.StartedOn** – la date de lancement de l'application, au format ISO 8601 ;
  - **Status.UpTime** – temps (en secondes) écoulé depuis le démarrage de l'application ;
- **update** – informations de mise à jour de l'application, comprenant :
  - **Last.Checked** – date de la dernière recherche de mise à jour, au format ISO 8601 ;

- **Last.Result** – état de la dernière mise à jour, qui peut être :
  - **updated** – mise à jour réussie, de nouvelles bases antivirus ont été installées ;
  - **not-needed** – mise à jour terminée correctement, mais aucun fichier n'était nécessaire ;
  - **error** – échec du processus de mise à jour ;
  - **rolled-back** – mise à jour réussie mais la base antivirus était endommagée, et un retour à l'état antérieur a donc été effectué ;
  - **unknown** – l'état de la dernière mise à jour n'a pas pu être déterminé.
- **Current.Loaded** – date de la dernière mise à jour réussie, au format ISO 8601 ;
- **Current.Records** – nombre de signatures actuellement en cours dans la base antivirus ;
- **Current.Released** – date au format ISO 8601 de publication de la dernière mise à jour.

- **all** – toutes les information décrites ci-dessus ;
- **none** – pas de publication d'informations par SNMP.

Kaspersky Anti-Virus fait appel à un sous-agent SNMP pour interagir avec l'agent principal SNMP via le protocole *AgentX*. Les paramètres du protocole AgentX sont les suivants :

- **Socket** – socket de communication ; vous pouvez utiliser un fichier local ou un socket réseau comme dans l'exemple :

  ```
  Socket=local:/var/agentx/master
  ```

  ou

  ```
  Socket=inet:705@127.0.0.1
  ```

Attention !

Si vous utilisez un socket Unix local, assurez-vous que le sous-agent et l'agent principal y ont accès. Ceci peut impliquer la modification des paramètres **RunAsUser** et **RunAsGroup**, ainsi que des droits d'accès du socket et des fichiers de donnée utilisés par le service (et pas le service central, si tous deux se trouvent sur la même machine).

- **Timeout** – délai (en secondes) d'une requête AgentX. La valeur par défaut est **5**.

- **Retries** – nombre de tentatives de requête AgentX. La valeur par défaut est **10**. Si ce paramètre n'est pas défini, l'application utilise la valeur **5**.

> **Attention !**
>
> Le nombre réel de tentatives peut être différent de la valeur spécifiée pour **Retries**. Ceci s'explique en raison de l'action de l'horloge de surveillance ("*watchdog*") et ne pose pas de problème.

- **PingInterval** – intervalle de temps (en secondes) entre deux tentatives du sous-agent pour se connecter à l'agent principal, en cas de déconnexion.

Vous pouvez utiliser n'importe quel agent SNMP prenant en charge le protocole AgentX en tant qu'agent principal. La section suivante présente un exemple de configuration d'un agent *NET-SNMP*, dans lequel l'application sous-agent utilise un socket local pour se connecter au NET-SNMP.

> **Attention !**
>
> Il est conseillé d'utiliser NET-SNMP version 5.1.2 ou supérieur, qui implémente correctement le protocole AgentX.

Pour configurer l'agent principal, suivez ces étapes :

1. Ajoutez les lignes suivantes au fichier de configuration *snmpd.conf* :

```
master agentx
AgentXSocket /var/agentx/master
AgentXPerms 770 770 root klusers
rocommunity public localhost
trapsink localhost
```

   ou, si un a socket réseau est employé, modifiez la seconde ligne par :

```
AgentXSocket tcp:127.0.0.1:705
```

2. Ajoutez les lignes suivantes au fichier de configuration *snmp.conf* :

Sous Linux:

```
mibdirs +/opt/kaspersky/kav4lms/share/snmp-mibs
mibs all
```

Sous FreeBSD:

```
mibdirs +/usr/local/share/kav4lms/snmp-mibs/
mibs all
```

où le chemin */opt/kaspersky/kav4lms/share/snmp-mibs* spécifie le répertoire par défaut de l'emplacement des fichiers MIB pour Kaspersky

Anti-Virus. Si l'application est installée dans un autre répertoire, modifiez le chemin correspondant.

3. Redémarrez *NET-SNMP*.

Remarque :

Vous trouverez d'autres informations sur *NET-SNMP* sur le site http://www.net-snmp.org/. Pour plus d'informations sur les fichiers de configuration *snmpd.conf* et *snmp.conf*, reportez-vous aux pages correspondantes du manuel.

Les OID produit sont disponibles sous la branche suivante :

.1.3.6.1.4.1.23668.1043

ou, sous forme symbolique :

iso.org.dod.internet.private.enterprises.kaspersky.kav4lms

Cette entrée contient les groupes suivants :

- **config** – paramètres de configuration de l'application, y compris la configuration de groupes, divisés en sections comme dans les fichiers de configuration ;
- **statistics** – informations statistiques sur les messages traités, les resources utilisées et les virus découverts ;
- **update** – informations de mise à jour de l'application ;
- **admin** – informations administratives (heure de démarrage de l'application, erreurs, etc.).

Attention !

Pour obtenir les valeurs des paramètres des objet de la section **config.Groups**, utilisez la méthode *Walk* au lieu de la méthode *Get*.

L'administrateur peut également configurer l'application pour émettre des pièges SNMP dans le cas d'événements spécifiques. Le paramètre **SNMPTraps**, dans la section **[kav4lms:server.snmp]** du fichier de configuration *kav4lms.conf* détermine les événements devant déclencher l'envoi de pièges SNMP par l'application. Les valeurs acceptées sont :

- **config** – un piège SNMP est émis quand la configuration ou les bases sont rechargées (*ConfigReloaded trap* et *BasesReloaded trap*) ;
- **admin** – un piège SNMP est émis quand l'application démarre ou s'arrête (*ProductStart trap*, *ProductStop trap*) ou présent une erreur fatale (*ProductError trap*). En outre, si la valeur du paramètre *AlertThreshold* n'est pas définie à zéro, un piège SNMP est envoyé quand le pourcentage de messages infectés détectés pendant la

dernière heure dépasse la valeur spécifiée (*AlertThreshold*). Un *AlertThreshold trap* est envoyé toutes les heures après que le seuil ait été dépassé, jusqu'à ce que le pourcentage de messages infectés retombe en dessous de la limite définie.

Remarque :

Il existe un piège **ConfigReloaded** qui correspond au rechargement de l'application. Cependant, les pièges **ProductStart**, **ProductStop** et **BasesReloaded** sont également émis dans ce cas. Ceci se produit parce que le watchdog provoque un redémarrage à chaud de l'application.

- **update** – piège SNMP émis en cas de mise à jour de l'application (*UpdateStatus trap*) ou quand la base antivirus date de plus de cinq jours (*ObsoleteBases trap*) ;
- **all** – piège SNMP envoyé quand n'importe lequel des événements ci-dessus se produit ;
- **none** – pas d'émission de pièges SNMP.

Attention !

Si vous utilisez l'agent principal NET-SNMP, vous devez démarrer le démon *snmptrapd* pour pouvoir recevoir les pièges.

10.2. Utilisation du script d'installation de l'application

Kaspersky Anti-Virus offre un script spécial permettant de gérer l'application après son installation.

L'utilisation du script d'installation est la suivante :

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh <option>
```

Les options disponibles sont :

- `--install-services` – inscrire les services central et de filtrage dans le système ;
- `--remove-services` – désinscription de tous les services (ils ne seront pas lancés ou arrêtés par le système) ;
- `--check-services` – vérifie si les services de l'application sont bien inscrits ;

- `--install-filter=<MTA>` – inscrit le filtre spécifié dans la configuration du MTA. Notez que ceci l'inscrit également en tant que service (si applicable) ;
- `--remove-filter=<MTA>` – désinscription du service de filtrage du MTA spécifié ;
- `--remove-filters` – supprime tous les filtres activés dans la ou dans les configurations du MTA ;
- `--check-filter=<MTA>` – vérifie si les changements d'inscription avec le MTA ont été faits ;
- `--filter-options=<options>` – définit des options de filtrage spécifiques. Cette option n'est utilisée qu'avec l'option `--install-filter`, afin de préciser les paramètres de filtrage spécifiques. Pour Sendmail les options suivantes sont disponibles : **tempfail**, **reject**, **pass** ;
- `--install-cron=<component_name>` – installe une tâche cron pour le composant spécifié ;
- `--remove-cron=<component_name>` – supprime un tâche cron pour le composant spécifié ;
- `--check-cron=<component_name>` – vérifie si une tâche cron est inscrite pour le composant ;
- `--user=<user_name>` – précise le nom de l'utilisateur utilisé pour exécuter le service central et le filtre de l'application. Cette option, utilisé en même temps que les paramètres `--install-cron` et `--remove-cron`, définit le compte utilisateur auquel on associe la planification.

  Par exemple :

  ```
  # /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
  --install-cron=updater --user=root
  ```

  ou

  ```
  # /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
  --install-cron=updater --user=qmailq
  ```

- `--add-composants-info` – ajoute des options spécifiques au fichier *applications.setup* ;
- `--del-composants-info` – supprime des options spécifiques des composants du registre de l'application ;
- `--check-composants-info` – vérifie si les options des composants du produit son présentes ;

- `--install-webmin-module` – ajoute un module d'administration Web à l'outil Webmin ;
- `--remove-webmin-module` – supprime le module de Webmin ;
- `--check-webmin-module` – vérifie si le module pour Webmin est installé ;
- `--register-key=key-id` – inscrit une clé avec son chemin complet ou son Identifiant relativement au répertoire *licenses* ;
- `--group=<group_name>` – spécifie le groupe utilisé pour exécuter Kaspersky Anti-Virus ; l'option modifie la valeur **Group** dans la section **[options]** du fichier de configuration de l'application ;
- `--switch-credentials=<user_name>[,<group_name>]` – spécifie l'utilisateur et (si précisé) le groupe utilisés pour démarrer le service central et le filtre de l'application. L'option modifie les valeurs **RunAsUser** et (si précisé) **RunAsGroup** dans les sections **[kav4lms:server.settings]** et **[kav4lms:filter.settings]** du fichier de configuration de l'application. Si cette option est utilisée, le service central et le filtre de l'application seront redémarrés.

Le paramètre `<MTA>` spécifie le MTA avec lequel est faite l'intégration. Les valeurs disponibles sont :

- **exim** – intégration aval de la file d'attente avec Exim ;
- **exim-dlfunc** – intégration en amont de la file d'attente avec Exim, par chargement d'une bibliothèque dynamique ;
- **postfix** – intégration aval de la file d'attente avec Postfix ;
- **qmail** – intégration avec qmail ;
- **sendmail-milter** – intégration avec Sendmail.

Le paramètre `<component_name>` spécifie le nom du composant de l'application. L'option disponible est **updater**.

Remarque :

Toutes les options terminées par "**--check**" s'exécutent en arrière-plan et renvoient 0 si l'élément vérifié est présent, ou une valeur différente de 0 dans le cas contraire.

10.3. Gestion de l'application depuis la ligne de commande

Kaspersky Anti-Virus propose l'utilitaire *kav4lms-cmd* de gestion depuis la ligne de commande, situé sous le répertoire */opt/kaspersky/kav4lms/bin*.

Attention !

L'outil *ka4lms-cmd* requiert que le service central de l'application soit en exécution.

Les options de ligne de commande de cet outil sont divisées en deux catégories :

1. Options générales de l'application. Ce sont :
   - `-v` ou `--version` – affiche la version du programme
   - `-h` ou `--help` – affiche un message d'aide sur la ligne
   - `-m` ou `--module<argument>` – sélectionne un module spécifique pour les prochaines commandes ; les options disponibles pour les modules sont : `config`, `filter`, `kavmd`, `statistiques`, `update`
   - `-c` ou `--config<argument>` – spécifie un autre fichier de configuration que celui par défaut
   - `-l` ou `--list` – affiche la liste des modules disponibles
2. Options spécifiques aux modules.
   a) **Config**. Ce module modifie les fichiers de configuration de l'application en exécutant des requêtes et en définissant les clés de configuration :
      - `-q <key>` – requête de valeur d'une clé de configuration. , e.g.`-q Path.TempPath ;`

   b) **Filter**. Ce module gère le composant de filtrage. L'option disponible est :
      - `-x <command>` – invoque une commande du composant de filtrage ; les options acceptées sont : `start`, `stop`, `restart`, `reload`, `status`, `test-service`.

   c) **Central service (kavmd)**. Ce module gère le service central de l'application. L'option disponible est :

- `-x <service-command>` – invoque une commande du service central ; les options acceptées sont : `start`, `stop`, `restart`, `reload`, `status`, `test-service`.

d) **Statistics**. Ce module gère les statistiques de l'application. Les options disponibles sont :

- `-x <stats-command>` – invoque une commande statistique ; les options acceptées sont : `write`, `reset`.

e) **Update**. Ce module gère le composant *kav4lms-keepup2date :*

- `-e <event-name>` – indique la génération d'un certain événement, les options sont : `OnUpdated`, `OnNotNeeded`, `OnError`, `OnRolledback`, `OnUnknown`.

10.4. Champs d'information supplémentaires dans les messages

L'application permet d'ajouter certaines informations supplémentaires aux messages sous forme de champs d'en-tête, en utilisant l'une des deux méthodes suivantes :

- Ajout d'un champ d'en-tête étendu au message.

  Les informations peuvent indiquer la version de l'application, la date de la dernière mise à jour de la base antivirus, l'heure et le résultat de l'analyse du message (déterminé par le paramètre **AddXHeaders** dans la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe).

  Format de l'en-tête :

  ```
  X-Anti-Virus: <product name and version>, bases: <date of the last update to anti-virus databases in YYYYMMDDTHHMMSS format> #<the number of records in AV databases>, check: <scan date in YYYYMMDD format> <scanning status or notchecked>
  ```

  où :

  `YYYY` correspond à l'année au format de quatre chiffres ;

  `MM` – mois ;

  `DD` – date ;

`HH` – heure ;

`MM` – minute ;

`SS` – second.

Par exemple :

```
X-Anti-Virus: Kaspersky Anti-Virus for Linux Mail
Server 5.6.17/RELEASE build 4,
bases: 20080415 #705877, check: 20080415 clean
```

- Ajout d'un texte de décharge dans le corps du message.

  Les informations sont ajoutés au format de texte simple ; elles peuvent contenir des instructions générées en accord avec la stratégie de sécurité (ou avec d'autres règles) d'une organisation donnée, et elles sont spécifiées par le paramètre **AddDisclaimer** dans la section **[kav4lms:groups.<group_name>.settings]**. Le texte par défaut du message informe que le message a été traité par Kaspersky Anti-Virus. À la demande de l'administrateur, l'application peut modifier le format des informations (par exemple, générer le message de décharge au format de texte HTML).

- Remplacement des parties supprimées du message.

  Pendant le traitement, des parties du message peuvent être supprimées suite aux actions sélectionnées. Les parties supprimées peuvent être remplacées par une notice qui en donne les raisons. Pour ce faire, définissez le paramètre **UsePlaceholderNotice** (dans la section **[kav4lms:groups.<group_name>.settings]** du fichier de configuration du groupe) à **yes**. Si la valeur du paramètre **UsePlaceholderNotice** est **no**, alors les parties du message correspondantes seront complètement supprimées, comme si elles n'avaient jamais existé.

  Le texte de la notice est pris dans un fichier modèle appelé *part_<action_taken>*, qui admet également des macros de notification (section 5.7 à la p. 60 pour plus de détails).

10.5. Affichage régional de la date et de l'heure

Pendant son fonctionnement, Kaspersky Anti-Virus produit des rapports pour chaque composant et génère diverses notifications à l'intention des utilisateurs et des administrateurs. Ces informations portent toujours la date et l'heure de sortie.

Par défaut, Kaspersky Anti-Virus utilise la mise en forme de la date et de l'heure correspondant au standard strftime :

%H:%M:%S – format de sortie de l'heure (**hh.mm.ss**).

%d-%m-%y – format de sortie de la date (**dd.mm.yy**).

L'administrateur peut modifier la mise en forme de la date et de l'heure. Cette mise en forme est effectuée conformément à la section **[locale]** du fichier de configuration *kav4lms.conf*. Vous pouvez définir les mises en forme suivantes :

%I:%M:%S %P – format de sortie de l'heure sur 12 heures (paramètre **TimeFormat**).

%y/%m/%d et %m/%d/%y – format de sortie de la date (paramètre **DateFormat**) (**yy.mm.dd** et **mm.dd.yy**, respectivement).

CHAPITRE 11. TEST DE L'APPLICATION

Après avoir installé et configuré Kaspersky Anti-Virus, il est conseillé de vérifier son fonctionnement correct à l'aide d'un “virus” de test et de ses modifications.

Ce “virus” a été spécialement mis au point par eicar (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 détectent comme un virus.

Attention !

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

Vous pouvez télécharger le “virus” depuis le site officiel de l'organisation **EICAR** à l'adresse http://www.eicar.org/anti_virus_test_file.htm.

Remarque :

Vous devez désactiver la protection antivirus avant de le télécharger, car autrement la solution antivirus installée dans l'ordinateur va identifier et traiter le fichier *anti_virus_test_file.htm* comme un objet infecté transmis par HTTP.

Notez que la protection antivirus doit être activée immédiatement après avoir téléchargé le “virus” de test.

Le fichier que vous aurez téléchargé depuis le site de l'organisation **EICAR** ou que vous aurez modifié vous-même contient le corps du “virus” d'essai standard. Kaspersky Anti-Virus le détecte, lui attribue l'état **Infected**non-disinfectable et applique l'action définie par l'administrateur pour le traitement des objets de ce type.

Afin de vérifier la réaction de Kaspersky Internet quand il détecte des objets d'un autre type, vous pouvez modifier le contenu du “virus” de test standard en ajoutant l'un des préfixes répertoriés dans le tableau ci-dessous. Vous pouvez modifier le texte dans n'importe quel éditeur de texte.

Remarque :

Vous pourrez vérifier le bon fonctionnement de l'application avec un “virus” EICAR modifié uniquement si la mise à jour de votre base antivirus est postérieure au 24 octobre 2003 (elle contient la mise à jour cumulée pour octobre 2003).

Tableau. Modification du “virus” de test

Préfixe	Type d'objet
Pas de préfixe, “virus” d'essai standard.	**Infecté.** L'objet n'est pas réparable.
CORR–	**Endommagé**.
SUSP–	**Suspect** (code d'un virus inconnu).
WARN–	**Suspect** (code modifié d'un virus connu).
ERRO–	**Non analysé** en raison d'une erreur.
CURE–	**Réparé.** L'objet sera réparé ; le texte dans le corps du “virus” sera remplacé par le mot “CURE”.

La première colonne du tableau contient les préfixes qu'il faut ajouter au début de la chaîne du “virus” standard.

Après avoir inséré le préfixe dans le “virus”, enregistrez celui-ci sous un autre nom de fichier, par exemple *eicar_corr.com*.

La deuxième colonne contient les types des objets tels qu'ils sont identifiés par l'application antivirus, après l'ajout du préfixe. Les actions exécutées sur chacun des types d'objet dépendent des paramètres de l'application, définis par l'administrateur.

ANNEXE A. INFORMATIONS COMPLÉMENTAIRES

A.1. Fichier de configuration de l'application *kav4lms.conf*

Le paquet Kaspersky Anti-Virus inclut le fichier de configuration *kav4lms.conf* contenant les paramètres de l'application. Cette section contient une explication détaillée des paramètres du fichier de configuration, avec les valeurs par défaut définies après l'installation du produit.

Le fichier de configuration contient des sections qui décrivent des aspects particuliers des fonctionnalités de l'application. Chaque section utilise la syntaxe suivante : la première ligne contient une en-tête de section sous la forme **[nom_section]**, suivie d'une description des paramètres de section.

Remarque :

Dans le cas de paramètres booléens renseignés avec des valeurs **true**|**false**, le fichier de configuration accepte également les équivalents : **yes**|**no**, **y**|**n** ou **1**|**0**.

La limite supérieure des paramètres numériques est **UINT_MAX=4294967295**.

Attention !

Les paramètres signalés par la description comme étant “obligatoires” sont indispensables au bon fonctionnement de l'application. Ils doivent être spécifiés ; autrement, l'antivirus ne fonctionnera pas !

A.1.1. Section *[kav4lms:server.settings]*

La section **[kav4lms:server.settings]** contient les paramètres du service central de l'application :

RunAsUser – nom du compte dont on utilise les privilèges pour exécuter le service central.

Paramètre obligatoire.

La valeur par défaut est **kluser**.

> **Remarque :**
>
> Si les services de filtrage et central sont installés sur le même ordinateur, assurez-vous que le paramètre **RunAsUser** possède la même valeur pour les deux composants, pour qu'il puisse avoir accès correctement aux fichiers partagés.

RunAsGroup – nom du groupe dont on utilise les privilèges pour exécuter le service central.

Paramètre obligatoire.

La valeur par défaut est **klusers**.

ServiceSocket=inet:<port>@<ip-address>|local:<path_to_socket> – le socket local ou réseau utilisé par service de filtrage de Kaspersky Anti-Virus pour communiquer avec le service central de l'application (extrémité de la connexion service central – filtre).

> **Attention !**
>
> Le service central de l'application doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Syntaxe :

`ServiceSocket=inet:<port>@<ip-address>` - pour un socket réseau

`ServiceSocket=local:<path_to_socket>` - pour un socket local.

où :

- **<port>**: port de communications utilisé ;
- **<ip-address>**: Adresse IP ;
- **<path_to_socket>**: chemin du socket local.

Paramètre obligatoire.

La valeur par défaut est **local:/var/run/kav4lms/kavmd.sock**.

> **Remarque :**
>
> Si un socket local est utilisé, assurez-vous que le répertoire ainsi que le fichier socket lui-même sont bien accessibles en lecture et en écriture, à la fois pour le service de filtrage et pour le service central de l'application.

ServiceSocketPerms – permissions pour **ServiceSocket** si un socket local est utilisé. Le propriétaire du socket est défini par le couple de paramètres **RunAsUser:RunAsGroup**.

La valeur par défaut est **0600** (utilisée si aucune valeur n'est spécifiée pour le paramètre).

AdminSocket – le socket local utilisé pour l'administration du service central (par exemple, via SNMP). Le service central peut être contrôlé par des commandes administratives et peut également répondre à des requêtes de service provenant du composant SNMP. Le dialogue est assuré sur ce socket spécifique.

> **Attention !**
>
> Le service central de l'application doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Paramètre obligatoire.

La valeur du paramètre par défaut est

local:/var/run/kav4lms/kavmdctl.sock.

> **Attention !**
>
> Quand ce paramètre est sélectionné, assurez-vous que le fichier et répertoire du socket sont accessibles en écriture uniquement pour le compte utilisateur utilisé pour exécuter l'application.

AdminSocketPerms – permissions pour **AdminSocket**. Le propriétaire du socket est **RunAsUser:RunAsGroup**.

La valeur par défaut est **0600**.

MaxWatchdogRetries=0...UINT_MAX – nombre maximum de tentatives de redémarrage de Kaspersky Anti-Virus avec le *watchdog*. La valeur **–1** (moins un) correspond à un nombre illimité de tentatives. La valeur **0** désactive le watchdog.

La valeur par défaut est **10**.

MaxClientRequests=0...UINT_MAX – le nombre maximum de pétitions client acceptées et traitées par le service central. Si le paramètre vaut **0**, le nombre de pétitions est illimité.

La valeur par défaut est **20**.

MaxScanRequests=0...UINT_MAX – le nombre maximum de pétitions d'analyse de messages. Si le paramètre vaut **0**, le nombre de pétitions est illimité.

La valeur par défaut est **0**.

LicensedUsersDomains – liste des domaines contenant des comptes à protéger, conformément au schéma de licence de Kaspersky Anti-Virus for Linux Mail Server. Cette option n'est disponible qui si votre clé est préparée pour un certain nombre d'adresses de messagerie. Vous pouvez spécifier plusieurs valeurs séparées par des virgules.

La valeur par défaut est **localhost**, **localhost.localdomain**.

A.1.2. Section *[kav4lms:server.log]*

La section **[kav4lms:server.log]** contient les paramètres du journal du service central :

Options=<functionality_category>.<details_level> – catégorie des événements consignés dans le journal, où :

- **<functionality_category>** peut prendre l'une des valeurs suivantes : **all**, **config**, **app**, **scan**, **cfilter**, **backup**, **notif**, **admin**, **smtp** (section 9.1 à la page 91).
- **<details_level>** peut prendre l'une des valeurs suivantes : **debug**, **activity**, **info**, **warning**, **error**, **fatal** (section 9.1 à la page 91).

Vous pouvez spécifier plusieurs niveaux, séparés par des virgules.

Par exemple :

```
Options = backup.all, config.error, \
scan.all, -scan.debug
Options = backup.all, config.E, \
scan.all, -scan.9
```

Paramètre obligatoire.

La valeur par défaut est **all,-all.debug**.

Destination=syslog:<name>@<category>|file:<path_to_file> – chemin du fichier journal destinataire des informations sur l'activité du service central de l'application :

- **syslog:<name>@<facility>**: écrit un rapport dans le journal du système ; **<name>** est le nom de l'application ; **<facility>** est la catégorie de consignation.
- **file:<path_to_file>**: écrit un rapport dans le fichier cible du chemin spécifié.

Paramètre obligatoire.

La valeur par défaut est **syslog:kavmd@mail**.

Append=yes|no – spécifie comment les informations doivent être ajoutées au fichier journal :

- **yes** – ajoute de nouvelles informations au fichier existant.
- **no** – crée un nouveau fichier journal à chaque démarrage de l'application.

La valeur par défaut est **yes**.

RotateRounds=0...UINT_MAX – nombre de fichiers de rapport créés pendant la rotation. Dès que ce nombre est atteint, l'application écrase le fichier le plus ancien. Si ce nombre est différent de zéro, la rotation est activée.

La valeur par défaut est **10**.

RotateSize=1M – taille du fichier de rapport en octets. Quand cette valeur est atteinte, un nouveau fichier de rapport est créé.

La valeur par défaut est 1M.

> **Attention !**
>
> Les paramètres **Append**, **RotateRounds** et **RotateSize** ne sont effectifs que lorsque la cible des consignations est un fichier.

A.1.3. Section *[kav4lms:server.statistics]*

La section **[kav4lms:server.statistics]** contient les paramètres des statistiques du service central :

Options=none|all|messages|resources|viruses|filters|raw – catégories de données à consigner (section 9.2 à la page 94). Vous pouvez spécifier plusieurs catégories séparées par des virgules.

Par exemple :

```
Options=none, raw
```

Paramètre obligatoire.

La valeur par défaut est **none**.

Format=xml|txt – spécifie le format du fichier de statistiques.

La valeur par défaut est **xml**.

Destination=file:<path_to_file> – destination des consignations pour le service central. La version courante de Kaspersky Anti-Virus ne prend en charge que des fichiers destination.

La valeur par défaut est:
file:/var/opt/kaspersky/kav4lms/stats/statistics.xml (sous Linux)
file:/var/db/kaspersky/kav4lms/stats/statistics.xml (sous FreeBSD).

RawDestination= file:<path_to_file> – destination des statistiques brutes (par message). La version courante de Kaspersky Anti-Virus ne prend en charge que des fichiers destination.

Paramètre obligatoire.

La valeur par défaut est:
file:/var/opt/kaspersky/kav4lms/stats/statistics.raw (sous Linux)
file:/var/db/kaspersky/kav4lms/stats/statistics.raw (sous FreeBSD).

A.1.4. Section *[kav4lms:server.snmp]*

La section **[kav4lms:server.snmp]** contient les paramètres qui définissent les communications avec l'application à travers le protocole SNMP :

SNMPServices=config|statistiques|admin|update|all|none – informations sur l'application qui peuvent être lue par SNMP :

- **config**: informations sur tous les paramètres de toutes les sections du fichier de configuration de l'application ;
- **statistiques**: informations statistiques récapitulatives sur l'activité de l'application ;
- **admin**: informations dépendantes du temps d'exécution de l'application (heure de démarrage, durée d'utilisation, etc.) ;
- **update**: informations sur la mise à jour des bases antivirus (date de dernière mise à jour, nombre d'enregistrements dans les bases de données, etc.) ;
- **all**: toutes les information et données statistiques sur la configuration de l'application ;
- **none**: l'accès aux informations à travers SNMP est désactivé.

Vous pouvez définir une liste de plusieurs valeurs, avec chaque paramètre figurant sur une ligne séparée.

Par exemple :

```
SNMPServices=config
SNMPServices=admin
```

Paramètre obligatoire.

La valeur par défaut est **none**.

SNMPTraps=config|admin|update|all|none – liste des événements qui déclenchent une notification vers l'administrateur par piégeage SNMP.

- **config**: en cas de modification de la configuration de l'application ou d'une mise à jour réussie des bases antivirus.
- **admin**: en cas de démarrage ou d'arrêt de l'application ou quand des erreurs graves se produisent en cours de fonctionnement et également en cas de détection d'objets infectés qui déclenchent la condition définie par le paramètre **AlertThreshold**.
- **update**: en cas de mise à jour des bases antivirus, quel qu'en soit le résultat ;
- **all**: quand n'importe lequel des événements ci-dessus se produit ;
- **none**: les pièges SNMP sont désactivés.

Vous pouvez définir une liste de plusieurs valeurs, avec chaque paramètre figurant sur une ligne séparée.

Par exemple :

```
SNMPTraps=config
SNMPTraps=admin
```

Paramètre obligatoire.

La valeur par défaut est **none**.

AlertThreshold=0...100 – seuil en pourcentage de messages infectés sur tous les messages analysés pendant la dernière heure, qui déclenche l'envoi d'un piège SNMP par l'application (si le paramètre **SNMPTraps** a la valeur **admin**).

La valeur par défaut est **10**.

Socket – le socket est utilisé pour communiquer avec l'agent principal ; il est possible d'utiliser un socket local ou réseau.

Syntaxe :

`inet:<port>@<ip-address>` - pour un socket réseau.

`local:<path_to_socket>` - pour un socket local.

Où :

- **<port>**: port de communication.
- **<ip-address>**: adresse IP.
- **<path_to_socket>**: chemin du socket local.

> **Remarque :**
>
> Dans le cas d'un socket local, vous devez fournir un fichier nommé "*master*", ce qui est une contrainte de nommage SNMP. Par conséquent, il faut spécifier un chemin absolu **<path_to_socket>** contenant le nom du fichier "*master*".

La valeur par défaut est –**inet:705@127.0.0.1**.

Timeout=0...UINT_MAX – délai d'attente (en secondes) des requêtes transmises à l'agent principal.

La valeur par défaut est 5.

Retries=0...UINT_MAX – nombre de tentatives des requête transmises à l'agent principal.

La valeur par défaut est **10.**

> **Attention !**
>
> Le nombre réel de tentatives peut être différent de la valeur spécifiée pour **Retries**. Ceci s'explique en raison de l'action de l'horloge de surveillance ("*watchdog*") et ne pose pas de problème.

PingInterval=0...UINT_MAX – intervalle (en secondes) entre deux tentatives de connexion du sous-agent à l'agent principal, si la connexion échoue.

La valeur par défaut est **30.**

A.1.5. Section *[kav4lms:server.notifications]*

La section **[kav4lms:server.notifications]** contient les options liées aux notifications :

ProductAdmins – adresse électronique de l'administrateur de Kaspersky Anti-Virus. Vous pouvez spécifier plusieurs adresses séparées par des virgules.

La valeur par défaut est **postmaster.**

ProductNotify=fault|update|license|all|none – informe l'administrateur de Kaspersky Anti-Virus quand les événements spécifiés se produisent :

- **fault** – erreurs critiques ;
- **update** – résultats des mises à jour de la base antivirus ;

- **license** – expiration de la clé du produit et cas de dépassement des restrictions imposées par la clé de licence du produit ;
- **all** – tous les événements ;
- **none** – les notifications sont désactivées.

Vous pouvez spécifier plusieurs valeurs séparées par des virgules.

Paramètre obligatoire.

La valeur par défaut est **all**.

Subject – en-tête de notification standard ajoutée à la zone **Sujet**.

La valeur par défaut est **Antivirus notification message**.

Charset – jeu de caractères à utiliser dans les notifications envoyées.

La valeur par défaut est **us-ascii.**

TransferEncoding – valeur de l'algorithme d'encodage de la notification. La valeur par défaut est **7bit**.

NotifierRelay – spécifie l'adresse MTA des notifications.

Syntaxe :

```
NotifierRelay=<protocol>:<host>:<port>
```

La valeur par défaut est **smtp:127.0.0.1:25**.

NotifierQueue – répertoire dans lequel le MTA des notifications place la file d'attente et les fichiers gestionnaires.

La valeur par défaut est:
/var/opt/kaspersky/kav4lms/nqueue/ (sous Linux)
/var/db/kaspersky/kav4lms/nqueue/ (sous FreeBSD).

NotifierTimeout=0...UINT_MAX – délai d'attente (en secondes) pour l'envoi des notifications. La valeur par défaut est **5**.

NotifierPersistence=yes|no – spécifie si la connexion au MTA des notifications est persistante.

Templates – répertoire contenant les modèles de notifications pour l'administrateur du produit.

La valeur par défaut est:
/etc/opt/kaspersky/kav4lms/templates-admin/en (sous Linux),
/usr/local/etc/kaspersky/kav4lms/templates-admin/en (FreeBSD).

A.1.6. Section *[kav4lms:filter.settings]*

La section **[kav4lms:filter.settings]** contient les paramètres du service de

filtrage de Kaspersky Anti-Virus :

RunAsUser nom du compte dont on utilise les privilèges pour exécuter le service de filtrage.

Paramètre obligatoire.

La valeur par défaut est **kluser**.

> **Remarque :**
>
> Si les services de filtrage et central sont installés sur le même ordinateur, assurez-vous que le paramètre **RunAsUser** possède la même valeur pour les deux composants, pour qu'il puisse avoir accès correctement aux fichiers partagés.

RunAsGroup – nom du groupe dont on utilise les privilèges pour exécuter le service de filtrage.

Paramètre obligatoire.

La valeur par défaut est **klusers**.

FilterSocket=inet:<port>@<ip-address>|local:<path_to_socket> – le socket local ou réseau utilisé par service de filtrage de Kaspersky Anti-Virus pour communiquer avec le service central de l'application (extrémité de la connexion service central – filtre).

> **Attention !**
>
> Le service de filtrage doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Syntaxe :

`FilterSocket=inet:<port>@<ip-address>` - pour un socket réseau

`FilterSocket=local:<path_to_socket>` - pour un socket local.

où :

- **<port>**: port de communications utilisé ;
- **<ip-address>**: adresse IP ;
- **<path_to_socket>**: chemin du socket local.

Paramètre obligatoire.

La valeur par défaut est **inet:10025@127.0.0.1**.

> **Remarque :**
>
> Si un socket local est utilisé, assurez-vous que le répertoire ainsi que le fichier socket lui-même sont bien accessibles en lecture et en écriture, à la fois pour le service de filtrage et pour le service central de l'application.

FilterSocketPerms – permissions pour **FilterSocket**, si un socket Unix local est utilisé. Le propriétaire du socket est **RunAsUser:RunAsGroup**.

La valeur par défaut est **0660**.

ServiceSocket=inet:<port>@<ip-address>|local:<path_to_socket> – le socket local ou réseau utilisé par service de filtrage de Kaspersky Anti-Virus pour communiquer avec le service central de l'application (extrémité de la connexion service central – filtre). Le format d'enregistrement est identique à celui de **FilterSocket**.

> **Attention !**
>
> Le service de filtrage doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Paramètre obligatoire.

La valeur par défaut est **local:/var/run/kav4lms/kavmd.sock**.

AdminSocket=local:<path_to_socket> – le socket local utilisé pour gérer le service de filtrage (par exemple, via SNMP). Le service de filtrage peut être contrôlé par des commandes administratives. Le dialogue est assuré sur ce socket spécifique.

> **Attention !**
>
> Le service de filtrage doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Paramètre obligatoire.

La valeur par défaut est **local:/var/run/kav4lms/kavmdctl.sock**.

> **Attention !**
>
> Quand ce paramètre est sélectionné, assurez-vous que le compte utilisé pour exécuter l'application possède des permissions d'accès en écriture sur le fichier et sur le répertoire du socket.

AdminSocketPerms=0600 – permissions pour **AdminSocket**. Le propriétaire du socket est **RunAsUser:RunAsGroup**.

ForwardSocket=inet:<port>@<ip-address>|local:<path_to_socket> – le socket local ou réseau utilisé par service de filtrage de Kaspersky Anti-Virus pour communiquer avec le MTA (extrémité de la connexion application – MTA).

> **Attention !**
>
> Le service de filtrage doit être stoppé avant de pouvoir modifier ce paramètre. Après la modification, redémarrez le service pour appliquer la nouvelle valeur.

Le format d'enregistrement est identique à celui de **FilterSocket**.

Paramètre obligatoire.

La valeur par défaut est **inet:10026@127.0.0.1**.

> **Remarque :**
>
> Le paramètre **ForwardSocket** est utilisé pour l'intégration avec Postfix et avec Exim.

FilterTimeout=0...UINT_MAX – délai d'attente (en secondes) des communications entre le service de filtrage et le MTA. Si aucune commande de données n'est transmise pendant la durée spécifiée ici, Kaspersky Anti-Virus ferme la connexion avec le MTA.

La valeur par défaut est **600**.

FilterThreads=0...UINT_MAX – le nombre de fils lancés par le service de filtrage pour l'écoute des requêtes du MTA.

La valeur par défaut est **10**.

MaxMilterThreads=0...UINT_MAX – nombre maximum de fils exploités simultanément par la bibliothèque Milter. La valeur 0 spécifie un nombre illimité de fils.

La valeur par défaut est **0**.

> **Attention !**
>
> Ceci ne s'applique qu'à Sendmail !

A.1.7. Section *[kav4lms:filter.log]*

La section **[kav4lms:filter.log]** contient les paramètres du journal du service de filtrage :

Options=<functionality_category>.<details_level> – catégorie des événements de filtrage consignés dans le journal, où :

- **<functionality_category>** peut prendre l'une des valeurs suivantes : **all**, **config**, **app**, **scan**, **cfilter**, **backup**, **notif**, **admin**, **smtp** (section 9.1 à la page 91).
- **<details_level>** peut prendre l'une des valeurs suivantes : **debug**, **activity**, **info**, **warning**, **error**, **fatal** (section 9.1 à la page 91).

Vous pouvez spécifier plusieurs niveaux, séparés par des virgules.

Paramètre obligatoire.

La valeur par défaut est **all,-all.debug**.

Destination=syslog:<name>@<category>|file:<path_to_file> – chemin du fichier journal destinataire des informations sur l'activité du service de filtrage :

- **syslog:<name>@<facility>**: écrit un rapport dans le journal du système ; **<name>** est le nom de l'application ; **<facility>** est la catégorie de consignation ;
- **file:<path_to_file>**: écrit un rapport dans le fichier cible du chemin spécifié.

Paramètre obligatoire.

La valeur par défaut est **syslog:kav4lms-filters@mail**.

Append=yes|no – spécifie comment les informations sur l'activité du filtre doivent être ajoutées au fichier journal :

- **yes** – ajoute de nouvelles informations au fichier existant ;
- **no** – crée un nouveau fichier journal à chaque démarrage de l'application.

La valeur par défaut est **yes**.

RotateRounds=0...UINT_MAX – nombre de fichiers de rapport créés pendant la rotation. Dès que ce nombre est atteint, l'application écrase le fichier le plus ancien. Si ce nombre est différent de zéro, la rotation est activée.

La valeur par défaut est **10**.

RotateSize=1M – taille du fichier de rapport en octets. Quand cette valeur est atteinte, un nouveau fichier de rapport est créé.

La valeur par défaut est **1M**.

Attention !

Les paramètres **Append**, **RotateRounds** et **RotateSize** ne sont effectifs que lorsque la cible des consignations est un fichier.

A.1.8. Section *[kav4lms:groups]*

La section **[kav4lms:groups]** contient des références aux fichiers de configuration de groupes :

_includes=<path_to_directory> – chemin du répertoire contenant les fichiers de configuration des groupes. Le chemin du répertoire doit être relatif à l'emplacement du fichier de configuration principal de l'application.

Paramètre obligatoire.

La valeur par défaut est **groups.d/**.

A.1.9. Section *[path]*

La section **[path]** contient la définition des chemins d'accès aux répertoires critiques.

BasesPath – chemin complet du répertoire des bases antivirus.

Paramètre obligatoire.

Valeur par défaut : **/var/opt/kaspersky/kav4lms/bases** (sous Linux) ou **/var/db/kaspersky/kav4lms/bases** (sous FreeBSD).

LicensePath – chemin complet au répertoire contenant les clés.

Valeur par défaut : **/var/opt/kaspersky/kav4lms/bases** (sous Linux) ou **/var/db/kaspersky/kav4lms/bases** (sous FreeBSD).

PidPath – chemin du fichier PID du service central de l'application.

Paramètre obligatoire.

La valeur par défaut est **/var/run/kav4lms/**.

TempPath – chemin du répertoire des fichiers temporaires. L'application crée des sous-répertoires *.kav4lms-<id>* à l'adresse spécifiée.

Paramètre obligatoire.

La valeur par défaut est **/var/tmp/**.

iCheckerDBFile – chemin des bases de données pour iChecker™.

Paramètre obligatoire.

Valeur par défaut : **/var/opt/kaspersky/kav4lms/iChecker.db** (sous Linux) ou **/var/db/kaspersky/kav4lms/iChecker.db** (sous FreeBSD).

A.1.10. Section *[locale]*

La section **[locale]** section contient des options pour l'affichage de la date et de l'heure dans les rapports et les statistiques.

DateFormat – le format de date est affiché dans le rapport.

Paramètre obligatoire.

La valeur par défaut est **%d-%m-%Y**.

TimeFormat – le format de date est affiché dans le rapport.

Paramètre obligatoire.

La valeur par défaut est **%H:%M:%S**.

> **Remarque :**
> Vous pouvez changer le format de l'heure à 12 heures (am, pm): **%I:%M:%S %P**.

Strings – chemin du fichier de constantes chaînes utilisé par l'application. Le chemin du répertoire doit être relatif à l'emplacement du fichier de configuration principal de l'application.

Paramètre obligatoire.

La valeur par défaut est **locale.d/strings.en**.

A.1.11. Section *[options]*

La section **[options]** contient différents paramètres d'application non compris dans d'autres groupes :

- **User** – compte système utilisé pour exécuter les composants de l'application.

  Paramètre obligatoire.

  La valeur par défaut est **kluser**.

- **Group** – groupe système utilisé pour exécuter les composants de l'application.

  Paramètre obligatoire.

  La valeur par défaut est **klusers**.

A.1.12. Section *[updater.path]*

La section **[updater.path]** définit les chemins aux répertoires utilisés pour les mises à jour.

BackUpPath=/var/opt/kaspersky/kav4lms/bases.backup/ – chemin complet du répertoire pour les copies de sauvegarde des bases antivirus.

A.1.13. Section *[updater.options]*

La section **[updater.options]** contient les paramètres de définition des options de mise à jour.

UpdateComponentsList – liste des composants à mettre à jour.

La valeur par défaut est **AVS, AVS_OLD, CORE, Updater, BLST**.

RetranslateComponentsList – liste des composants dont les mises à jour sont à enregistrer dans un répertoire réseau.

Si la valeur du paramètre est vide (par défaut), la valeur du paramètre **UpdateComponentsList** est utilisée.

KeepSilent=yes|no – définit si l'application doit afficher sur la console un rapport sur une mise à jour. Si renseigné à **yes**, les rapports ne sont pas envoyés à la console.

La valeur par défaut est **no**.

UseUpdateServerUrl=yes|no – définit si l'application doit utiliser l'URL du serveur de Kaspersky Lab définie par le paramètre **UpdateServerUrl** en tant que source de mises à jour.

La valeur par défaut est **no**.

UpdateServerUrl=http://url/|ftp://url/|/local_path/ – l'adresse du serveur utilisé comme source de mises à jour.

La valeur par défaut du paramètre est vide.

UseUpdateServerUrlOnly=yes|no – définit si l'application doit utiliser uniquement l'adresse URL spécifiée par **UpdateServerUrl** pour mettre à jour la base de données. Si cette option est renseignée à **no**, chaque fois qu'une mise à jour depuis l'adresse **UpdateServerUrl** échoue, l'application choisit une adresse alternative dans la liste des serveurs de mises à jour.

La valeur par défaut est **no**.

RegionSettings – définit la région cliente utilisée pour mettre à jour les bases antivirus à partir du serveur de Kaspersky Lab le plus proche.

La valeur par défaut est **ru**.

ConnectTimeout – intervalle (en secondes) dans lequel l'application tente des se connecter à la source de mises à jour.

La valeur par défaut est **30**.

ProxyAddress – adresse IP d'un serveur proxy si celui-ci est requis pour la connexion Internet.

Par défaut, la valeur n'est pas définie.

UseProxy=yes|no – utilise un serveur proxy pour se connecter à l'un des serveurs de mises à jour. Si le paramètre est **no**, the serveur proxy ne sera pas utilisé. Si le paramètre est **yes**, l'adresse du serveur proxy définie par le paramètre **ProxyAddress** est utilisée.

La valeur par défaut est **no**.

PassiveFtp=yes|no – s'il faut utiliser le mode FTP passif pour le téléchargement de mises à jour par FTP.

La valeur par défaut est **yes**.

Index=u0607g.xml – fichier contenant l'index principal du système de mises à jour utilisé pour choisir l'ensemble des mises à jour sur les serveurs de Kaspersky Lab. Il n'est pas recommandé de modifier cette valeur.

IndexRelativeServerPath=index/6 – chemin du fichier contenant l'index du système principal de mises à jour. Le chemin doit être relatif à l'emplacement fichier de configuration principal de l'application. Il n'est pas recommandé de modifier cette valeur.

A.1.14. Section *[updater.report]*

La section **[updater.report]** contient les paramètres des rapports de mises à jour.

Append=yes|no – détermine le mode de consignation de l'activité du composant *kav4lms-keepup2date* :

- **yes** – ajoute de nouvelles informations au fichier existant ;
- **no** – crée un nouveau fichier journal à chaque démarrage du composant. Ensuite, le fichier journal ne contiendra que les informations sur les résultats de la dernière mise à jour.

La valeur par défaut est **yes**.

ReportFileName – nom du fichier de rapport *kav4lms-keepup2date*.

Valeur par défaut : **/var/log/kaspersky/kav4lms/keepup2date.log**.

ReportLevel=0|1|2|3|4|9 – niveau de détail du rapport de mise à jour (**0** – Fatal,
1 – Error, **2** – Warning, **3** – Info, **4** – Activity, **9** – Debug). La valeur par défaut est: **3**.

A.1.15. Section *[updater.actions]*

La section **[updater.actions]** contient les paramètres définissant les actions appliquée en cas d'événements spécifiques pour *keepup2date*.

OnAny – spécifie la commande exécutée à chaque événement. Par défaut les autres composants de l'application sont informés de l'événement.

La valeur par défaut est **/opt/kaspersky/kav4lms/bin/kav4lms-cmd -m \ update -e %EVENT_NAME%** (sous Linux),
/usr/local/bin/kav4lms-cmd -m update -e %EVENT_NAME% (sous FreeBSD).

OnStarted – spécifie la commande exécutée quand le composant *kav4lms-keepup2date* démarre.

La valeur est vide par défaut.

OnUpdated – spécifie la commande exécutée en cas de mise à jour réussie.

La valeur par défaut redémarre l'application -

/opt/kaspersky/kav4lms/bin/kav4lms-cmd -x bases (sous Linux), **/var/db/kaspersky/kav4lms/bin/kav4lms-cmd -x bases** (sous FreeBSD).

OnRetranslated – commande exécutée après le téléchargement réussi depuis un répertoire réseau d'une mise à jour des base de données, vers le répertoire où sont placées les bases antivirus.

La valeur est vide par défaut.

OnNotUpdated – spécifie la commande exécutée si la mise à jour n'a pas été réalisée.

La valeur est vide par défaut.

OnFailed – spécifie la commande exécutée en cas d'échec de la mise à jour.

La valeur est vide par défaut.

OnRolledBack – spécifie la commande exécutée en cas de retour en arrière.

La valeur est vide par défaut.

OnBasesCheck – spécifie la commande exécutée après une mise à jour, pour valider les bases antivirus. L'outil *avbasestest* est utilisé par défaut pour vérifier l'intégrité des bases antivirus. Il vérifie les mises à jour téléchargées depuis la source et enregistrées sous un répertoire temporaire. Si les mises à jour ne sont pas endommagées, elles sont recopiées depuis leur emplacement temporaire vers le répertoire contenant les bases antivirus.

> **Remarque :**
>
> Le démarrage de l'outil *avbasestest* est automatique, il ne nécessite aucune intervention de l'utilisateur.

La valeur par défaut est /**opt/kaspersky/kav4lms/lib/bin/avbasestest %TEMP_BASES_PATH% %BASES_PATH%** (in Linux), **/usr/local/libexec/kaspersky/kav4lms/avbasestest %TEMP_BASES_PATH% %BASES_PATH%** (sous FreeBSD).

> **Remarque :**
>
> Les actions de l'outil avbasestest acceptent les macros suivantes :
>
> - %EVENT_NAME% – nom de l'événement qui a déclenché cette commande ;
> - %BASES_PATH% – si applicable, le chemin des bases existantes ;
> - %TEMP_BASES_PATH% – si applicable, le chemin du répertoire temporaire utilisé pour la mise à jour des bases ;
> - %AVS_UPDATE_DATE% – date de l'événement au format **mm:dd:yyyy hh:mm:ss**.

A.1.16. Section *[scanner.display]*

La section **[scanner.display]** contient les paramètres d'impression du rapport de *kav4lms-kavscanner* sur écran :

ShowContainerResultOnly=true|false – mode d'affichage à l'écran des résultats de l'analyse des archives. Pour afficher des résultats au format court, renseignez ce paramètre avec la valeur **true**. Le format étendu des messages est celui utilisé par défaut.

Paramètre obligatoire.

La valeur par défaut est **false**.

ShowObjectResultOnly=true|false – mode d'affichage à l'écran des résultats de l'analyse d'un objet simple. Pour afficher des résultats au format court, renseignez ce paramètre avec la valeur **true**. Le format étendu des messages est celui utilisé par défaut.

Paramètre obligatoire.

La valeur par défaut est **false**.

ShowOK=true|false – mode d'impression écran des messages sur les fichiers sains. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

ShowProgress=true|false – mode d'affichage à l'écran d'informations sur le fonctionnement du composant courant, y compris le téléchargement de la base antivirus ou sur l'analyse du fichier courant. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

A.1.17. Section *[scanner.options]*

La section **[scanner.options]** contient les paramètres du composant *kav4lms-kavscanner* :

ExcludeDirs=mask1:mask2:...:maskN – masques d'exclusion pour des répertoires exclus de la couverture d'analyse. Ils sont définis comme des masques standard du shell.

La valeur par défaut est **/dev:/udev:/proc:/sys**.

ExcludeMask=mask1:mask2:...:maskN – masques des fichiers exclus de la couverture d'analyse. Par défaut, tous les fichiers sont analysés. Les masques sont définis comme des masques standard du shell.

La valeur par défaut est **not defined**.

Packed=true|false – mode d'analyse des objets compressés. Pour désactiver l'analyse, renseignez le paramètre à **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

Archives=true|false – mode d'analyse des archives. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

Cure=true|false – mode de réparation des objets infectés. Pour activer ce mode, renseignez ce paramètre avec la valeur **true**.

Paramètre obligatoire.

La valeur par défaut est **false**.

Heuristic=true|false – mode d'utilisation de l'analyseur heuristique de code au cours de l'analyse. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

LocalFS=true|false – mode d'analyse pour le système de fichiers local uniquement. Pour activer ce mode, renseignez ce paramètre avec la valeur **true**.

Paramètre obligatoire.

La valeur par défaut est **false**.

MailBases= true|false – mode d'analyse des bases de messagerie. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

MailPlain=true|false – analyse des messages au format de texte plat. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

Packed=true|false – mode d'analyse des objets compressés. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

Recursion=true|false – mode d'analyse récursive des répertoire au cours de l'analyse antivirus . Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

SelfExtArchives=true|false – mode d'analyse des archives auto-extractibles. Pour le désactiver, renseignez ce paramètre avec la valeur **no**. Si le mode d'analyse des archives est activé **(Archives=yes)**, les fichiers auto-extractibles seront analysés même si le paramètre **SelfExtArchives** est renseigné avec la valeur **false.**

Paramètre obligatoire.

La valeur par défaut est **true**.

Ichecker=true|false – mode d'utilisation de la technologie iChecker au cours de l'analyse antivirus . Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

La valeur par défaut est **true**.

MaxLoadAvg – charge maximum de l'unité centrale. En cas de dépassement de cette valeur, le composant *kav4lms-kavscanner* stoppe ses opérations.

La valeur est vide par défaut.

UseAVbasesSet=standard|extended – ensemble de bases antivirus utilisé par l'application pendant l'analyse. L'ensemble **extended** contient, en plus des enregistrements contenus dans l'ensemble **standard**, des descriptions de logiciels à risque (riskware), tels que les logiciels publicitaires (adware) ou de contrôle à distance.

La valeur par défaut est **standard**.

FollowSymlinks=true|false – cette option contrôle la gestion des liens symboliques. Si le paramètre est renseigné à **true**, au cours de l'analyse, l'application suit les liens qui pointent vers des répertoires et vérifie les objets situés aux adresses correspondantes. Pour désactiver ce mode, utilisez la valeur **false**.

La valeur par défaut est **true**.

A.1.18. Section *[scanner.report]*

La section **[scanner.report]** contient des paramètres pour la génération de rapports avec les résultats du composant *kav4lms-kavscanner*.

Append=true|false – mode ajout nouveaux messages dans le fichier rapport avec les résultats de l'analyse antivirus du système de fichiers :

- **true** – ajoute les nouvelles informations au fichier existant.
- **false** – crée un nouveau fichier journal à chaque démarrage de l'application.

Paramètre obligatoire.

La valeur par défaut est **true**.

ReportFileName – nom du fichier de rapport où sont consignés les résultats du fonctionnement du composant.

La valeur est vide par défaut.

ReportLevel=0|1|2|3|4|9 – niveau de détail du rapport (**0** – Fatal, **1** – Error, **2** – Warning, **3** – Info, **4** – Activity, **9** – Debug).

Paramètre obligatoire.

La valeur par défaut est **4**.

ShowOK=true|false – mode de consignation dans le rapport de messages sur les fichiers sains. Pour désactiver ce mode, renseignez ce paramètre avec la valeur **false**.

Paramètre obligatoire.

La valeur par défaut est **true**.

ShowContainerResultOnly=true|false – mode d'affichage des résultats de l'analyse des archives. Pour afficher un court rapport renseignez ce paramètre avec la valeur **true**. Le format étendu des messages est celui utilisé par défaut.

Paramètre obligatoire.

La valeur par défaut est **false**.

ShowObjectResultOnly=true|false – mode d'affichage des résultats de l'analyse d'un objet simple. Pour afficher avec un format court renseignez ce paramètre avec la valeur **yes**. Le format étendu des messages est celui utilisé par défaut.

Paramètre obligatoire.

La valeur par défaut est **false**.

A.1.19. Section *[scanner.container]*

La section **[scanner.container]** inclut des paramètres qui déterminent les actions appliquées dans le cadre de la protection protection des systèmes de fichiers du serveur.

OnInfected=action – actions exécutées si un objet infecté est découvert. Si le mode de réparation des fichiers infectés est activé, l'action spécifiée est appliquée sur les objets qu'il n'est pas possible de désinfecter.

La valeur est vide par défaut.

OnSuspicion=action – actions à effectuer si l'application détecte un objet suspect qui ressemble une menace, et qui n'est pas encore connu de Kaspersky Lab.

La valeur est vide par défaut.

OnWarning=action – actions à effectuer si l'application détecte un fichier qui ressemble à une menace déjà connue.

La valeur est vide par défaut.

OnCured=action – actions à effectuer si l'application détecte un fichier infecté qu'elle parvient à réparer.

La valeur est vide par défaut.

OnProtected=action – actions à effectuer si l'application rencontre un objet protégé par un mot de passe. Ces objets ne peuvent pas être analysés.

La valeur est vide par défaut.

OnCorrupted=action – actions à effectuer si l'application détecte un fichier endommagé.

La valeur est vide par défaut.

OnError=action – actions à effectuer si une erreur système se produit au cours de l'analyse d'un objet.

La valeur est vide par défaut.

La syntaxe du paramètre **action** compte deux parties : l'action et un paramètre supplémentaire séparé par un espace. La valeurs du paramètres supplémentaire doit figurer entre guillemets.

Par exemple :

```
OnInfected=move "/tmp/infected"
```

L'action peut prendre l'une des valeurs suivantes :

- *move <directory>* – déplace le fichier vers <directory>.

- *movePath <directory>* – déplacement récursif du fichier vers <directory> (en utilisant le chemin absolu).
- *remove* – supprime le fichier.
- *exec <parameter>* – exécute une commande externe définie par la variable <*parameter*>.

Les macros suivantes sont acceptées comme paramètre complémentaire de l'action **exec** sur des conteneurs :

- %VIRUSNAME% – nom de la menace détectée ou erreur.
- %LIST% – nom du fichier ou liste de fichiers infectés, suspects ou endommagés rencontrés dans un conteneur. L'enregistrement possède le format suivant :**<virus name>\t<file name>**.
- %FULLPATH% – chemin complet du conteneur.
- %FILENAME% – nom de fichier sans spécification de répertoire.
- %CONTAINERTYPE% – type du conteneur sous forme chaîne.

A.1.20. Section *[scanner.object]*

La section **[scanner.object]** contient des paramètres qui définissent les actions à appliquer sur des objets simples avec certains types, dans le cadre de la protection antivirus du système de fichiers de l'ordinateur.

OnInfected=action – actions exécutées si un objet infecté est découvert. Si le mode de réparation des fichiers infectés est activé, l'action spécifiée est appliquée sur les objets qu'il n'est pas possible de désinfecter.

La valeur est vide par défaut.

OnSuspicion=action – actions à effectuer si l'application détecte un objet suspect qui ressemble une menace, et qui n'est pas encore connu de Kaspersky Lab.

La valeur est vide par défaut.

OnWarning=action – actions à effectuer si l'application détecte un fichier qui ressemble à une menace déjà connue.

La valeur est vide par défaut.

OnCured=action – actions à effectuer si l'application détecte un fichier infecté qu'elle parvient à réparer.

La valeur est vide par défaut.

OnProtected=action – actions à effectuer si l'application rencontre un objet protégé par un mot de passe. Ces objets ne peuvent pas être analysés.

La valeur est vide par défaut.

OnCorrupted=action – actions à effectuer si l'application détecte un fichier endommagé.

La valeur est vide par défaut.

OnError=action – actions à effectuer si une erreur système se produit au cours de l'analyse d'un objet.

La valeur est vide par défaut.

La syntaxe du paramètre **action** est la même que pour la section **[scanner.container]** (section A.1.19 à la page 134).

Les macros suivantes sont acceptées comme paramètre complémentaire de l'action **exec** sur des conteneurs :

- %VIRUSNAME% – nom de la menace détectée ou erreur.
- %LIST% – nom d'un fichier infectés, suspect ou endommagé. L'enregistrement possède le format suivant :**<virus name>\t<file name>**.
- %FULLPATH% – chemin complet du fichier.
- %FILENAME% – nom de fichier sans spécification de répertoire.

A.1.21. Section *[scanner.path]*

La section **[scanner.path]** contient les paramètres qui déterminent les chemins d'accès aux fichiers sans lesquels le composant *kav4lms-kavscanner* ne peut pas fonctionner.

BackupPath= path - chemin complet à la zone de sauvegarde des objets qui vont être analysés par le composant.

La valeur est vide par défaut.

A.2. Fichier de configuration de groupe

Cet annexe décrit de manière détaillée chacune des sections du fichier de configuration *default.conf*, qui définit pour le groupe **Default** les paramètres de traitement des messages.

Les paramètres spécifiés pour le groupe **Default** sont utilisé lorsque :

- aucun groupe n'a été créé ;
- aucun expéditeur ni destinataire du message ne figure l'un des groupes existants ;
- la valeur d'un paramètre n'est pas définie pour un certain groupe.

Attention !

Si un fichier de configuration du groupe est créé sur le modèle du fichier de configuration default.conf du groupe **Default**, pensez à modifier le nom du groupe qui figure dans les titres des sections du fichier de configuration.

A.2.1. Section *[kav4lms:groups.<group_name>.definition]*

La section **[kav4lms:groups.<group_name>.definition]** section contient les paramètres d'identification du groupe :

Priority – priorité du groupe ; si le message appartient à plusieurs groupes, en fonction de son expéditeur (ou de son destinataire), il sera traité en utilisant les règles du groupe avec la priorité la plus haute. Vous pouvez spécifier n'importe quel nombre naturel dans ce paramètre. Des groupes de même priorité ou avec une priorité **0** ne sont pas autorisés.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **0**.

Senders – liste des adresses des expéditeur du message. Chaque adresse doit être spécifiée sur une ligne séparée. Les caractères génériques et les expressions régulières sont acceptés. Si cette option n'est pas définie, la valeur est supposée être ***@*** (toutes les adresses).

Par exemple :

```
Senders=user1@mycompany.com
Senders=reporter*@mycompany.com
Senders=re:office@.*\.example\.com
```

La valeur du paramètre pour le groupe **Default** n'est pas définie.

Recipients – liste des adresses des destinataire du message. Chaque adresse doit être spécifiée sur une ligne séparée. Les caractères génériques et les expressions régulières sont acceptés. Si cette option n'est pas définie, la valeur est supposée être ***@*** (toutes les adresses).

Par exemple :

```
Recipients=user2@mycompany.com
Recipients=reporter*@mycompany.com
Recipients=re:office\d+@central\.mydomain\.com
```

La valeur du paramètre pour le groupe **Default** n'est pas définie.

Attention !

Au moins un des paramètres **Destinataires** ou **Expéditeurs** doit être spécifié.

A.2.2. Section *[kav4lms:groups.<group_name>.settings]*

La section **[kav4lms:groups.<group_name>.settings]** contient les paramètres qui définissent la stratégie d'analyse des messages et l'ajout de champs d'information spéciaux aux messages traités.

Check=antivirus|content-filter|all|none – service de sécurité pour un groupe.

Paramètre obligatoire.

Le paramètre pour le groupe **Default** est **all**.

ScanPolicy=message|combined – stratégie d'analyse du courrier qui détermine le mode d'analyse des messages.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **message**.

ScanArchives=yes|no – analyser les archives. Pour désactiver ce mode, utilisez la valeur **no**.

La valeur du paramètre pour le groupe **Default** est **yes**.

ScanPacked=yes|no – analyser les exécutables compressés. Pour désactiver ce mode, utilisez la valeur **no**.

La valeur du paramètre pour le groupe **Default** est **yes**.

UseAVBasesSet=standard|extended – ensemble de bases antivirus utilisé par l'application pendant l'analyse. L'ensemble **extended** contient, en plus des enregistrements contenus dans l'ensemble **standard**, des descriptions de logiciels à risque (riskware), tels que des logiciels publicitaires (adware), de balayage réseau et des simulateurs de virus.

La valeur du paramètre pour le groupe **Default** est **standard**.

UseCodeAnalyzer=yes|no – mode d'utilisation de l'analyseur heuristique de code pour la détection de programmes malveillants et de virus modifiés ou inconnus. Pour désactiver ce mode, utilisez la valeur **no**.

La valeur du paramètre pour le groupe **Default** est **yes**.

MaxScanTime – temps maximum, en secondes, que l'application peut prendre pour analyser un objet simple (un message ou un objet du message). En cas de dépassement de sa valeur, l'application renvoie une erreur.

La valeur du paramètre pour le groupe **Default** est **30**.

> **Remarque :**
>
> Le cas peut apparaître où le temps d'analyse total d'un message spécifique dépasse la valeur du paramètre **MaxScanTime**, mais aucune erreur n'est renvoyée. Ceci peut arriver quand le type d'analyse **combined** est sélectionné pour la stratégie d'analyse. La durée d'analyse totale du message est donc la somme des analyses du message en tant qu'objet et des parties qui le composent.

MaxScanDepth=0...UINT_MAX – Le nombre d'imbrications d'objets MIME autorisé dans un seul message. En cas de dépassement de sa valeur, l'application renvoie une erreur. La valeur **0** signifie qu'un nombre illimité d'imbrications est autorisé.

La valeur du paramètre pour le groupe **Default** est **10**.

MIMEEncodingHeuristics=yes|no – le mode d'interprétation des objets MIME qui ne sont pas conformes aux normes RFC.

Par défaut, le filtre de l'application ne transfère pour analyse que des messages conformes à la norme RFC. Si le paramètre **MIMEEncodingHeuristics** est renseigné à **yes**, un message non conforme sera interprété à l'aide d'algorithmes heuristiques puis, si le décodage réussit, transféré pour analyse. Si le décodage du message échoue ou si le paramètre **MIMEEncodingHeuristics** est défini à **no**, ces messages ne sont pas retransmis pour analyse.

La valeur du paramètre pour le groupe **Default** est **no**.

Remarque :

Quand il est activé, ce paramètre peut ralentir l'analyse.

AddXHeaders=none|message|parts|all – instruction pour ajouter des en-têtes d'information contenant le résultat d'analyse des messages (pour plus de détails reportez-vous à la section 10.4 à la page 106).

AddDisclaimer=yes|no – ajoute un texte de décharge à chaque message traité ou généré. Vous pouvez personnaliser ce texte en modifiant le modèle *disclaimer*. Le texte de décharge est ajouté sous forme de texte à la fin du message, dont le contenu original n'est en rien modifié ou affecté.

La valeur du paramètre pour le groupe **Default** est **no**.

UsePlaceholderNotice=yes|no – joint une notification sur l'objet supprimé.

La valeur du paramètre pour le groupe **Default** est **yes**.

RejectReply – en-tête de la notification sur le message refusé. L'option n'est pas utilisée dans le cas d'une intégration du produit avec qmail.

La valeur du paramètre pour le groupe **Default** est:
Message rejected because it contains malware (Message refusé en raison de contenu malveillant).

A.2.3. Section *[kav4lms:groups.<group_name>.actions]*

La section **[kav4lms:groups.<group_name>.actions]** contient des options qui déterminent comment les messages sont traités après une analyse antivirus :

InfectedAction=warn|drop|reject|cure|delete|skip – action par défaut appliquée aux objets infectés.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **skip**.

SuspiciousAction=warn|drop|reject|delete|skip – action par défaut appliquée aux objets suspects d'une infection par du code malveillant non identifié.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **skip**.

ProtectedAction=warn|drop|reject|skip|delete – action appliquée aux objets protégés par un mot de passe dans lesquels on ne peut examiner la présence de menaces.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **skip**.

ErrorAction=warn|skip|delete – action appliquée à des objets endommagés qui ne peuvent être analysés en raison d'une erreur.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **skip**.

VirusNameAction= warn|drop|reject – actions à appliquer sur un message ou sur ses objets infectés par un virus recensé par le paramètre **VirusNameList**.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **drop**.

FilteredMimeAction=skip|delete|drop|reject|warn – action à appliquer sur une pièce jointe du type MIME défini par le paramètre**IncludeMime**.

La valeur du paramètre pour le groupe **Default** est **skip**.

FilteredNameAction=skip|delete|drop|reject|rename|warn – action à appliquer sur une pièce jointe dont le nom coïncide avec le masque du paramètre **IncludeName**.

La valeur du paramètre pour le groupe **Default** est **skip**.

FilteredSizeAction=skip|delete|drop|reject|warn – action à appliquer sur une pièce jointe si sa taille correspond avec la valeur définie pour le paramètre **IncludeSize**.

La valeur du paramètre pour le groupe **Default** est **skip**.

A.2.4. Section *[kav4lms:groups.<group_name>.contentfiltering]*

La section **[kav4lms:groups.<group_name>.contentfiltering]** définit les règles de filtrage des messages :

IncludeMime – définit des masques de filtrage par type MIME. Les objets seront filtrés si leurs types MIME correspondent aux masques spécifiés mais non aux masques définissant des exclusions de l'analyse (paramètre **ExcludeMime**).

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Les caractères génériques ("*****" et "**?**") et les expressions régulières sont acceptés.

Par exemple :

```
IncludeMime=application/octet-stream
IncludeMime=application/vnd.*
IncludeMime=re:image/.*
IncludeMime=re:multipart/(encrypted|signed)
```

Si la valeur du paramètre n'est pas spécifiée ou est vide, le filtrage par type MIME n'est pas appliqué.

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

ExcludeMime – définit des masques de types MIME d'objets qui seront ignorés au cours du filtrage. Les objets seront ignorés si leurs types ne vérifient pas ces masques.

Si la liste **ExcludeMime** est précisée mais non la liste **IncludeMime**, les masque qui n'appartiennent pas à la liste **ExcludeMime** sont filtrés.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Les caractères génériques ("*****" et "**?**") et les expressions régulières sont acceptés.

Par exemple :

```
ExcludeMime=application/octet-stream
ExcludeMime=application/vnd.*
ExcludeMime=re:image/.*
ExcludeMime=re:multipart/(encrypted|signed)
```

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

IncludeName – définit des masques de filtrage par nom. L'application filtre les objets dont les noms correspondent aux masques spécifiés mais non aux masques définissant des exclusions de l'analyse (**ExcludeName** paramètre).

Si la valeur du paramètre n'est pas spécifiée ou est vide, le filtrage par nom de pièce jointe n'est pas appliqué.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Les caractères génériques ("*****" et "**?**") et les expressions régulières sont acceptés.

Par exemple :

```
IncludeName=*accounting*
IncludeName=re:.*\.(doc|xls|ppt)
IncludeName=re:.*\.(pif|com|exe)
```

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

ExcludeName – définit des masques d'objets qui seront ignorés au cours du filtrage. L'application ignore les objets qui répondent à ces masques.

Si le paramètre **ExcludeName** est précisé mais pas **IncludeName**, les masques qui ne figurent pas dans la liste **ExcludeName** sont considérés inclus dans le filtrage.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Les caractères génériques ("*****" et "**?**") et les expressions régulières sont acceptés.

Par exemple :

```
ExcludeName=re:.*\.(txt|rtf)
ExcludeName=re:.*\.(doc|xls|ppt)
ExcludeName=re:.*\.(pif|com|exe)
```

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

IncludeSize – taille des pièces jointes à inclure dans le filtrage. Vous pouvez spécifier la valeur en octets, par exemple, **3456261** ou utiliser un format court pour indiquer la grandeur de taille: **10KB**, **100MB**. Pour filtrer les valeurs vides, renseignez le paramètre à **0**.

Format d'enregistrement :

`IncludeSize=`**`attachment_size`** – l'application filtre les pièces jointes dont la taille est égale à la valeur spécifiée.

`IncludeSize=<attachment_size` - l'application filtre les pièces jointes dont la taille est inférieure à la valeur spécifiée.

`IncludeSize=<=attachment_size` - l'application filtre les pièces jointes dont la taille est inférieure ou égale à la valeur spécifiée.

`IncludeSize=>attachment_size` - l'application filtre les pièces jointes dont la taille est supérieure à la valeur spécifiée.

`IncludeSize=>=attachment_size` - l'application filtre les pièces jointes dont la taille est supérieure ou égale à la valeur spécifiée.

`IncludeSize=0` – l'application filtre toutes les pièces jointes vides.

Si la valeur du paramètre n'est pas spécifiée, le filtrage par type de pièce jointe n'est pas appliqué.

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

ExcludeSize – taille des pièces jointes à exclure du filtrage. Le format d'enregistrement est identique à celui du paramètre **IncludeSize**. Pour ignorer les pièces jointes vides, renseignez le paramètre à **0**.

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

VirusNameList – liste des menaces qui requièrent des actions spéciales définies par **VirusNameAction**, effectuées sur les objets ou messages infectés par elles. Le nom de la menace doit être spécifié tel qu'il apparaît dans l'Encyclopédie du Virus à l'adresse www.viruslist.com. Les masques et les expressions régulières sont acceptés. Pour spécifier plusieurs valeurs, séparez-les par des virgules.

Exemple :

```
VirusNameList=re:trojan.*, backdoor*
```

Si la valeur du paramètre n'est pas définie, les objets seront traités conformément à l'état qui leur a été attribué lors de l'analyse.

Dans le cas du groupe **Default**, la valeur du paramètre est vide.

RenameTo=<file_name>|.<extension> – le mode de renommage de l'objet quand l'action **rename** est appliquée :

- **RenameTo=<file_name>** – le nom de fichier sera entièrement remplacé par la valeur spécifiée.
- **RenameTo=.<extension>** – l'extension spécifiée sera ajoutée au nom de fichier.

Par exemple :

```
RenameTo=.vir
```

Le fichier *file.doc* sera renommé à *file.doc.vir*.

```
RenameTo=VIRUS-DO-NOT-OPEN
```

Le fichier *file.doc* sera renommé à *VIRUS-DO-NOT-OPEN*.

Si la valeur du paramètre n'est pas définie, l'application ne renommera pas les objets.

La valeur du paramètre pour le groupe **Default** est **.vir**.

A.2.5. Section *[kav4lms:groups.<group_name>.notifications]*

La section **[kav4lms:groups.<group_name>.notifications]** contient les options liées aux notifications :

NotifySender=all|filtered|infected|protected|suspicious|error|none – informe les expéditeurs originaux du message de la détection d'un message (ou d'objets dans le message) avec cet état.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Si une valeur vide est spécifiée, aucune notification n'est envoyée aux expéditeurs du message.

La valeur du paramètre **Default** group est **none**.

> **Remarque :**
>
> En cas de détection d'objets avec plusieurs état différents, pour que l'application envoie des notifications, vous pouvez définir plusieurs valeurs pour le paramètre **NotifySender**, par exemple :
>
> ```
> NotifySender=filtered
> NotifySender=infected
> ```
>
> Vous pouvez renseigner les paramètres **NotifyRecipients** et **NotifyAdmin** de la même manière.

NotifyRecipients=all|filtered|infected|protected|suspicious|error|none – informe les destinataires originaux du message de la détection d'un message (ou d'objets dans le message) avec cet état.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Si une valeur vide

est spécifiée, aucune notification n'est envoyée aux destinataires du message original.

Paramètre obligatoire.

La valeur du paramètre pour le groupe **Default** est **all**.

NotifyAdmin=all|filtered|infected|protected|suspicious|error|none – informe l'administrateur de la détection d'un message ou d'objets du message avec cet état.

Vous pouvez définir plusieurs valeurs sous forme de liste. Chaque paramètre doit alors figurer sur une ligne séparée. Si une valeur vide est spécifiée, aucune notification n'est envoyée à l'administrateur.

Paramètre obligatoire.

La valeur du paramètre **Default** group est **none**.

AdminAddresses – adresse électronique de l'administrateur du serveur de messagerie. Vous pouvez spécifier plusieurs adresses séparées par des virgules.

La valeur du paramètre pour le groupe **Default** est **postmaster**.

> **Remarque :**
>
> Le paramètre **AdminAdresses** fait référence à l'administrateur de la sécurité, et non à l'administrateur de Kaspersky Anti-Virus (auquel fait référence le paramètre **ProductAdmins** dans la section **[kav4lms:server.notifications]** du fichier de configuration *kav4lms.conf*.

PostmasterAddresses – adresse de remplacement de l'adresse des destinataires (champ "FROM") dans les notifications émises.

La valeur du paramètre pour le groupe **Default** est **POSTMASTER@localhost**.

Templates – répertoire où sont conservés les modèles de notification.

La valeur du paramètre pour le groupe **Default** est **/etc/opt/kaspersky/kav4lms/modèles/en** (sous Linux) **/usr/local/etc/kaspersky/kav4lms/modèles/en** (sous FreeBSD).

Subject – en-tête de notification standard ajoutée à la zone **Sujet**.

La valeur du paramètre pour le groupe **Default** est **Antivirus notification message**.

Charset – jeu de caractères à utiliser dans les notifications.

La valeur du paramètre pour le groupe **Default** est **us-ascii**.

TransferEncoding – valeur de l'algorithme d'encodage de la notification.

La valeur du paramètre pour le groupe **Default** est **7bit**.

UseCustomTemplates=yes|no – active l'utilisation de modèles personnalisés pour la génération des notifications. Pour activer ce mode, renseignez le paramètre à **yes**.

La valeur du paramètre pour le groupe **Default** est **no**.

SenderSubject – zone Sujet du message de notification à l'expéditeur.

La valeur du paramètre pour le groupe **Default** est **Antivirus notification message**.

AdminSubject – zone Sujet du message de notification à l'administrateur de la sécurité.

La valeur du paramètre pour le groupe **Default** est **Antivirus notification message**.

A.2.6. Section *[kav4lms:groups.<group_name>.backup]*

La section **[kav4lms:groups.<group_name>.backup]** contient les options qui contrôlent la création de copies de sauvegarde avant l'application d'actions aux messages :

Policy=message|info|none – définit la stratégie de sauvegardes.

La valeur du paramètre pour le groupe **Default** est **info**.

Options=cured|deleted|dropped|rejected|warning|renamed|all – type des messages dont il faut créer des copies de sauvegardes.

Vous pouvez spécifier plusieurs valeurs séparées par des virgules.

La valeur du paramètre pour le groupe **Default** est **all**.

Destination=/var/opt/kaspersky/kav4lms/backup/ – répertoire où sont conservées les copies de sauvegardes des messages.

La valeur du paramètre pour le groupe **Default** est **/var/opt/kaspersky/kav4lms/backup/** (sous Linux) **/var/db/kaspersky/kav4lms/backup/** (sous FreeBSD).

A.3. Paramètres de commande du composant *kav4lms-licensemanager*

Options d'aide :	
-h	Affiche à l'écran l'aide du composant *kav4lms-licensemanager* ;
-v	Affiche la version de l'application.
Options de gestion des clés de licence :	
-s	Affiche à l'écran des informations sur toutes les clés installées.
-c (-C) <path_to_file>	Utilise un fichier de configuration alternatif **<path_to_key_file>**.
-k <path_to_file>	Affiche à l'écran des informations sur la clé **<path_to_key_file>**.
-a <path_to_file>	Installe la clé **<path_to_key_file>**.
-d(a|r)	Supprime la clé active (option **-da**) ou supplémentaire (option **-dr**).
-i	Affiche sur la console des informations détaillées sur les objets sous licence.

A.4. Codes retour du composant *kav4lms-licensemanager*

Pendant son fonctionnement, le composant *kav4lms-licensemanager* peut retourner les codes suivants :

0	Le composant a chargé avec succès les informations de la clé et terminé son exécution.

30	Une erreur système est apparue pendant le fonctionnement du composant.
64	Les informations sur la clé sont absentes ou les clés sont introuvables sur le chemin spécifié dans le fichier de configuration.
65	Impossible de charger le fichier de configuration.
66	Option invalide du fichier de configuration.
70	Le component *kav4lms-licensemanager* est endommagé.

A.5. Paramètres de commande du composant *kav4lms-keepup2date*

Options d'aide :	
-v	Imprime à l'écran la version de l'application puis ferme le composant.
-h	Imprime à l'écran de l'aide sur les paramètres de ligne de commande reconnus par le composant, puis ferme celui-ci.

Options de fonctionnement :	
-r	Annule la dernière mise à jour et retour à la version précédente.
-s	Imprime à l'écran la liste des serveurs de mises à jour.
-k	N'exécute pas la commande **PostUpdateCmd** après la mise à jour réussie de la base antivirus.
-q	Mode de fonctionnement du composant pendant lequel aucun message système n'est affiché à l'écran.
-e	Mode de fonctionnement du composant pendant lequel seuls les messages liés à des erreurs critiques seront imprimés à l'écran.
-x <path_to_file>	Copie toutes les mises à jour de la base antivirus vers un répertoire local **<path_to_file>**.
-g <URL>	Adresse de mise à jour de la base antivirus. Quand ce paramètre est spécifié, la mise à jour se réalise à partir de cette adresse.
-d <path_to_file>	Utilise le fichier-pid du composant, situé dans un répertoire local **<path_to_file>**.

Options de génération de rapport :	
-l <path_to_file>	Consigne les résultats du fonctionnement du composant dans le fichier **<path_to_file>**.

A.6. Codes retour du composant *kav4lms-keepup2date*

Pendant son fonctionnement, le composant *kav4lms-keepup2date* peut retourner les codes suivants :

0	Il n'est pas nécessaire de mettre à jour la base antivirus.
1	Mise à jour réussie de la base antivirus.
10	Une erreur critique est apparue, le processus de mise à jour va se terminer.
11	Une erreur est apparue : une autre instance de l'application est en exécution.
12	Error apparue après l'annulation de la dernière mise à jour de la base antivirus.
30	Impossible d'exécuter la commande **PostUpdateCmd** après la mise à jour de la base antivirus.
60	Les informations sur la clé sont absentes ou la clé est introuvable sur le chemin spécifié dans le fichier de configuration.
75	Impossible de charger le fichier de configuration ou erreur de configuration.

ANNEXE B. KASPERSKY LAB

Fondée en 1997, la société 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, en Pologne et en Roumanie. Un nouveau service de la compagnie, le centre européen de recherches antivirus, 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 450 experts, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat, et deux experts senior sont des membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse complète du comportement des virus informatiques permet à la société de fournir une protection complète contre les menaces présentes et 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 assurer la plus grande des protections antivirus aussi bien aux particuliers, qu'aux clients corporatifs.

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 Anti-virus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau de Kaspersky Anti-Virus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde) et BorderWare (Canada).

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

B.1. Autres produits Kaspersky Lab

Kaspersky Lab News Agent

Le composant News Agent est conçu pour distribuer périodiquement les bulletins d'annonce de Kaspersky Lab, avec des notifications sur l'état courant d'activité virale et des nouvelles de dernière heure. L'application parcourt une liste et lit le contenu des bulletins d'informations du serveur de news de Kaspersky Lab avec une fréquence définie.

Le composant News Agent permet aux utilisateurs de ;

- Visualiser le contexte viral sur la barre système.
- S'abonner ou se désabonner aux canaux d'informations.
- Récupérer les informations des canaux sélectionnés à l'intervalle spécifié et recevoir des notifications de dernière heure.
- Lire les informations des canaux sélectionnés.
- Examiner la liste et l'état des canaux.
- Ouvrir le texte complet de l'article dans le navigateur.

Le produit News Agent est une application Microsoft Windows indépendante, qui peut être utilisée seule ou intégrée avec différentes solutions fournies par Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Le programme est un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab. Le service offre en ligne une analyse antivirus efficace de votre ordinateur. Kaspersky OnLine Scanner s'exécute directement dans votre navigateur. Les utilisateurs reçoivent ainsi des réponses rapides à leurs questions sur une infection potentielle de leurs ordinateurs. Avec ce service, les visiteurs peuvent :

- Exclure de l'analyse les fichiers compressés LHA et ICE et les bases de messagerie ;
- Choisir des bases antivirus standard ou étendues pour réaliser l'analyse.
- Enregistrer un rapport avec les résultats de l'analyse au format .txt ou .html.

Kaspersky® OnLine Scanner Pro

Le programme est un service par abonnement offert aux visiteurs du site Internet de la société Kaspersky Lab. Le service offre en ligne une analyse antivirus efficace de votre ordinateur et la neutralisation des fichiers dangereux. Kaspersky OnLine Scanner Pro s'exécute directement dans votre navigateur. Avec ce service, les visiteurs peuvent :

- Exclure de l'analyse les fichiers compressés LHA et ICE et les bases de messagerie ;
- Choisir des bases antivirus standard ou étendues pour réaliser l'analyse.
- Enregistrer un rapport avec les résultats de l'analyse au format .txt ou .html.

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 est conçu pour protéger les ordinateurs personnels contre les logiciels malveillants et offre une combinaison excellente de méthodes antivirus conventionnelles et de technologies proactives récentes.

Le programme offre une vérification antivirus complexe qui comprend :

- Analyse antivirus du trafic de messagerie au niveau des protocoles de transmission de données (POP3, IMAP et NNTP pour le courrier entrant, et SMTP pour le courrier sortant), indépendamment du client utilisé, ainsi que la réparation des bases de messagerie.
- Analyse antivirus en temps réel du trafic Internet échangé via HTTP.
- Analyse antivirus de fichiers individuels, de répertoires ou d'unités de disque. En outre, une tâche prédéfinie permet de centrer l'analyse antivirus exclusivement sur les zones critiques du système d'exploitation et sur les objets de démarrage de Microsoft Windows.

La protection proactive offre les caractéristiques suivantes :

- **Contrôle des modifications dans le système de fichiers**. Le programme permet aux utilisateurs de créer une liste d'applications qui seront contrôlées en fonction de leurs composants. Ceci permet de protéger l'intégrité des applications contre les actions de logiciels malveillants.
- **Surveillance des processus en mémoire vive**. Kaspersky Anti-Virus 7.0 informe régulièrement les utilisateurs chaque fois qu'il détecte des processus suspects ou cachés, ou quand des modifications non autorisées se produisent dans des processus actifs.
- **Surveillance des changements dans le Registre du système** grâce à un contrôle interne du Registre système.

- **Surveillance des processus cachés** qui protège contre le code malveillant dissimulé dans le système d'exploitation par des technologies de type “rootkit”.
- **Analyseur heuristique**. Au cours de l'analyse d'un logiciel, l'analyseur simule son exécution et enregistre toutes les activités suspectes, par exemple l'ouverture ou l'écriture dans un fichier, l'interception des vecteurs d'interruption, etc. En fonction de cette procédure, une décision est prise sur la possible infection du logiciel par un virus. L'émulateur travaille dans un environnement virtuel isolé qui protège contre tout risque d'infection de l'ordinateur.
- **Restauration du système** après l'attaque d'un logiciel malveillant, grâce à l'enregistrement de toutes les modifications introduites dans le Registre et les fichiers système, puis leur annulation à la demande de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution intégrale de protection des ordinateurs personnels contre les principales menaces aux données, à savoir, les virus, les pirates, le courrier indésirable et les logiciels espions. Une interface unique permet aux utilisateurs de configurer et de gérer tous les composants du logiciel.

Les caractéristiques de protection antivirus comprennent :

- **Analyse antivirus du trafic de messagerie** au niveau des protocoles de transmission de données (POP3, IMAP et NNTP pour le courrier entrant, et SMTP pour le courrier sortant), indépendamment du client utilisé. Le programme inclut des plug-ins pour les clients les plus répandus (Microsoft Office Outlook, Microsoft Outlook Express / /Windows Mail et The Bat!) et assure la réparation de leurs bases de messagerie.
- **Analyse antivirus en temps réel du trafic Internet** échangé via HTTP.
- **Protection du système de fichiers**: analyse antivirus de fichiers individuels, de répertoires ou d'unités de disque. En outre, l'application peut réaliser l'analyse antivirus centrée exclusivement sur les zones critiques du système d'exploitation et sur les objets de démarrage de Microsoft Windows.
- **Protection proactive**: le programme surveille en continu l'activité des applications et des processus exécutés en mémoire vive, pour éviter toute modification dangereuse du système de fichiers ou du Registre, et il restaure le système après toute action malveillante.

La protection contre les fraudes Internet est assurée grâce à sa capacité pour identifier les tentatives d'hameçonnage (phishing), pour éviter les fuites de données confidentielles (à commencer par les mots de passe, les numéros de

comptes bancaires et de carte de crédit) et pour bloquer l'exécution de scripts dangereux sur les pages Internet, dans les fenêtres indépendantes et les bandeaux publicitaires. La fonction de **blocage des numéroteurs** permet d'identifier et d'empêcher l'activité des logiciels qui tentent d'utiliser votre modem pour se connecter à votre insu à des services téléphoniques payants. *Le module de contrôle de privacité* protège la sécurité de vos informations confidentielles contre l'accès ou la transmission non autorisés. *Le contrôle parental* est un composant de Kaspersky Internet Security qui surveille les connexions Internet des utilisateurs.

Kaspersky Internet Security 7. **enregistre les tentatives d'exploration des ports de votre ordinateur**, qui précèdent fréquemment des attaques réseau, et vous défend avec succès contre les attaques de pirates typiques. Le programme fait appel à des **définitions de règles** pour surveiller toutes les transactions réseau et contrôler tous **les paquets de données entrants ou sortants**. **Le mode invisible** (dépendant de la technologie SmartStealth™) **évite la détection de votre ordinateur depuis l'extérieur**. Quand vous activez ce mode, le système bloque toutes les activités réseau, à l'exception des quelques transactions autorisées par les règles personnalisées.

L'application emploie une approche complexe pour filtrer le courrier indésirable dans les messages entrants :

- Vérification sur des listes blanches et noires de destinataires (y compris les adresses de sites d'escroquerie).
- Examen des phrases dans le corps du message.
- Analyse du texte du message par un algorithme d'auto-apprentissage.
- Reconnaissance d'images indésirables.

Kaspersky Anti-virus mobile

Kaspersky ® Anti-virus mobile offre une protection antivirus pour les téléphones portables sous Symbian OS et Microsoft Windows mobile. Le programme offre une vérification antivirus complète, comprenant :

- **Analyses à la demande** de la mémoire interne du périphérique mobile, des cartes mémoire, d'un dossier individuel ou d'un fichier spécifique ; si un fichier infecté est détecté, il est déplacé vers la quarantaine ou supprimé.
- **Analyse en temps réel -–** tous les fichiers entrants et sortants sont analysés automatiquement, ainsi que les fichiers auxquels on tente d'accéder.
- **Protection contre les messages de texte indésirables**.

Kaspersky Anti-Virus for File Servers

Ce paquet logiciel offre une protection fiable des systèmes de fichiers sur des serveurs sous Microsoft Windows, Novell NetWare, Linux et Samba, contre tous les types de logiciels malveillants. La suite comprend les applications Kaspersky Lab suivantes :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Fonctions et caractéristiques :

- *Protection en temps réel des systèmes de fichiers du serveur*: tous les fichiers serveur sont analysés lors de leur accès ou de leur enregistrement sur le serveur ;
- *Prévention contre les offensives virales* ;
- *Analyses à la demande* du système de fichiers complet ou de dossiers ou fichiers individuels ;
- *Utilisation de technologies d'optimisation* lors de l'analyse d'objets dans le système de fichiers du serveur ;
- *Restauration du système après une attaque virale* ;
- *Évolutivité du paquet logiciel* en tenant compte des ressources système disponibles ;
- *Surveillance de la répartition de charge du serveur* ;
- *Création d'une liste de processus de confiance* dont l'activité serveur n'est pas contrôlée par le paquet logiciel ;
- *Administration distante* du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- *Enregistrement de copies de sauvegarde des objets infectés ou supprimés* en prévision d'une possible restauration ;
- *Mise en quarantaine d'objets suspects* ;
- *Envoi à l'administrateur de notifications sur des événements* pendant l'activité du logiciel ;
- *Enregistrement de rapports détaillés* ;

- *Mise à jour automatique* des bases du programme.

Kaspersky Open Space Security

Kaspersky Open Space Security est un paquet logiciel qui offre une nouvelle approche de la sécurité aux réseaux d'entreprise de toutes tailles, avec des systèmes de gestion centralisés et la prise en charge de poste distants et d'utilisateurs mobiles.

La suite contient quatre applications :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Les particularités de chaque programme figurent ci-après.

Kaspersky WorkSpace Security est un programme de protection centralisé des postes de travail situés à l'intérieur et à l'extérieur de réseaux d'entreprise contre toutes les menaces contemporaines de l'Internet (virus, logiciels espions, piratages et courrier indésirable).

Fonctions et caractéristiques :

- *Protection complète contre les virus, les logiciels espions, les tentatives de piratage et le courrier indésirable* ;
- *Défense proactive* contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- *Pare-feu personnel* doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- *Restauration des modifications malveillantes dans le système* ;
- *Protection contre les tentatives de fraude et le publipostage indésirable* ;
- *Répartition dynamique des ressources* pendant les analyses complètes du système ;
- *Administration distante* du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- *Compatibilité Cisco® NAC* (Network Admission Control) ;
- *Analyse des messages et du trafic Internet* en temps réel ;
- *Interdiction des fenêtres indépendantes et des bandeaux publicitaires* pendant la navigation sur Internet ;

- *Fonctionnement sécurisé sur tous types de réseaux*, y compris les réseaux WiFi ;
- *Outils de création de disque de secours* permettant de restaurer le système après une offensive virale ;
- *Système complet de rapports* sur l'état de la protection ;
- *Mises à jour automatique des bases* ;
- *Prise en charge complète des systèmes d'exploitation de 64 bits* ;
- *Optimisation des performances du programme sur les portables* (technologie Intel® Centrino® Duo) ;
- *Fonctions de réparation à distance* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources d'information de votre société contre les menaces contemporaines de l'Internet. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichier contre tous les types de virus, de chevaux de Troie et de vers, il protège contre les offensives virales et il sécurise vos données, tout en offrant aux utilisateurs un accès instantané aux ressources d'information du réseau.

Fonctions et caractéristiques :

- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- *Compatibilité Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Technologie iSwift pour éviter l'analyse répétée des fichiers réseau* ;
- *Répartition de charge entre les processeurs du serveur* ;
- *Mise en quarantaine d'objets suspects* depuis les postes de travail ;
- *Restauration des modifications malveillantes dans le système* ;
- *Évolutivité du paquet logiciel en tenant compte* des ressources système disponibles ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- *Analyse des messages et du trafic Internet* en temps réel ;

- *Pare-feu personnel* doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- *Protection des utilisateurs de* réseaux WiFi ;
- *Autodéfense contre les logiciels malveillants* ;
- *Mise en quarantaine* d'objets suspects ;
- *Mises à jour automatique des bases de données*.

Kaspersky Enterprise Space Security

Ce logiciel dispose de composants de protection pour les postes de travail et les serveurs liés, contre toutes les menaces contemporaines de l'Internet. Il supprime les virus des messages et préserve vos données tout en fournissant un accès sécurisé aux ressources réseau des utilisateurs.

Fonctions et caractéristiques :

- *Protection des postes de travail et des serveurs de fichiers contre les virus, les chevaux de Troie et les vers* ;
- *Protection des serveurs de messagerie Sendmail, Qmail, Postfix et Exim* ;
- *Analyse de tous les messages sur Microsoft Exchange Server*, y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et des autres objets sur serveurs Lotus Domino* ;
- *Protection contre les tentatives de fraude et le publipostage indésirable* ;
- *Prévention contre les publipostages et les épidémies virales* ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- Compatibilité Cisco® NAC (Network Admission Control) ;
- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- *Fonctionnement sécurisé sur les* réseaux WiFi networks ;

- *Analyse du trafic Internet* en temps réel ;
- *Restauration des modifications malveillantes dans le système* ;
- *Répartition dynamique des ressources* pendant les analyses complètes du système ;
- Mise en quarantaine d'objets suspects ;
- *Système complet de rapports* sur l'état de la protection ;
- *Mises à jour automatique des bases de données*.

Kaspersky Total Space Security

Cette solution surveille tous les flux de données en entrée et sortie (messages, Internet et toutes les interactions réseau). Cette solution contient des composants de protection des postes de travail fixes ou de périphériques mobiles, qui protège les données tout en offrant aux utilisateurs un accès sécurisé aux ressources d'information de la société et à Internet, et des communications par messagerie sécurisées.

Fonctions et caractéristiques :

- *Protection intégrale contre les virus, les logiciels espions, les tentatives de piratage et le courrier indésirable* à tous les niveaux du réseau d'entreprise, depuis les postes de travail jusqu'aux passerelles Internet ;
- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- *Protection de serveurs de messagerie et de serveurs liés* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui circule sur le réseau local en temps réel ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- *Interdiction de connexion depuis des postes de travail infectés* ;
- *Prévention contre les offensives virales* ;
- *Génération centralisée de rapports sur la protection* ;
- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- *Compatibilité Cisco® NAC* (Network Admission Control) ;
- *Prise en charge de serveurs proxy en boîtier* ;

- *Filtrage du trafic Internet* moyennant une liste de serveurs, de types d'objets et de groupes d'utilisateurs de confiance ;
- *La technologie iSwift évite l'analyse répétée de fichiers à l'intérieur* du réseau ;
- Répartition dynamique des ressources pendant les analyses complètes du système ;
- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- *Fonctionnement sécurisé sur tous types de réseaux*, y compris les réseaux WiFi ;
- *Protection contre les tentatives de fraude et le publipostage indésirable* ;
- *Fonctions de réparation à distance* (Intel® Active Management, Intel® vPro™) ;
- *Restauration des modifications malveillantes dans le système* ;
- *Autodéfense contre les logiciels malveillants* ;
- *Prise en charge complète des systèmes d'exploitation de 64 bits* ;
- *Mises à jour automatique des bases de données*.

Kaspersky Security for Mail Servers

Ce logiciel permet de protéger des serveurs de messagerie et des serveurs liés contre les logiciels malveillants et le courrier indésirable. Le logiciel contient une application pour la protection de tous les serveurs de messagerie standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim) et permet également de configurer une passerelle de messagerie dédiée. La solution comprend :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Les caractéristiques comprennent :

- *Protection fiable contre les logiciels malveillants ou potentiellement dangereux* ;
- *Filtrage des pollupostages indésirables* ;

- *Analyse des pièces jointes dans les messages entrants et sortants* ;
- *Analyse antivirus de tous les messages sur* Microsoft Exchange Server y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et des autres objets sur serveurs Lotus Notes/Domino* ;
- *Filtrage* des messages par type de pièce de jointe ;
- *Mise en quarantaine des* objets suspects ;
- *Système convivial d'administration du* logiciel ;
- *Prévention contre les offensives virales* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Génération de rapports* sur le fonctionnement du programme ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- *Mises à jour automatique des bases de données*.

Kaspersky Security for Internet Gateways

Ce logiciel offre un accès Internet sécurisé à tous les employés d'une entreprise, en supprimant automatiquement les logiciels malveillants ou à risque dans les données HTTP/FTP entrantes. La solution comprend :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Les caractéristiques comprennent :

- *Protection fiable contre les logiciels malveillants ou potentiellement dangereux* ;
- *Analyse du trafic Internet* (HTTP/FTP) en temps réel ;
- *Filtrage du trafic Internet* moyennant une liste de serveurs, de types d'objets et de groupes d'utilisateurs de confiance ;
- *Mise en quarantaine des* objets suspects ;
- *Système convivial d'administration* ;
- *Génération de rapports sur le fonctionnement du programme* ;

- *Prise en charge de serveurs proxy en boîtier* ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- *Mises à jour automatique des bases de données*.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle de pointe, conçue pour permettre aux organisations équipées de réseaux de petite ou moyenne taille, de lutter contre le fléau des messages indésirables (“spam”, pourriel). Le produit combine des technologies révolutionnaires d'analyse linguistique avec toutes les méthodes modernes de filtrage des messages électroniques, y compris les listes noires de DNS et la reconnaissance de structures formelles. Sa combinaison unique de services permet aux utilisateurs d'identifier et d'éliminer près de 95% du trafic indésirable.

Kaspersky® Anti-Spam se comporte comme un barrage contre le courrier indésirable, installé à l'entrée du réseau, qui analyse les flux de courrier entrant à la recherche de spam. Le logiciel prend en charge tous les systèmes de messagerie, et 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 pour le filtrage, à partir des échantillons fournis par les spécialistes du laboratoire linguistique de notre Société. Les bases de données sont mises à jour toutes les 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-virus® for MIMESweeper for SMTP assure une analyse antivirus à haute vitesse du trafic SMTP sur des serveurs exploités sous les versions Clearswift MIMESweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

L'application se présente comme un complément logiciel (plug-in) et réalise l'analyse antivirus et le traitement préventif de tous les messages entrants et sortants en temps réel.

B.2. Comment nous contacter

Si vous avez des questions, des commentaires ou des suggestions, adressez-vous à nos revendeurs ou directement à Kaspersky Lab. Nous serons heureux de vous renseigner sur notre produit par téléphone ou par courrier électronique. Toutes vos recommandations et suggestions sont soigneusement étudiées et prises en compte.

Support technique	Pour le service d'assistance technique, visitez : http://www.kaspersky.com/supportinter.html Helpdesk : www.kaspersky.com/helpdesk.html
Informations générales	WWW : http://www.kaspersky.com http://www.viruslist.com E-mail : info@kaspersky.com

ANNEXE C. LOGICIELS D'AUTRES FABRICANTS

Cette section contient la liste et les conditions d'utilisation de logiciels d'autres fabricants, qui ont été utilisés dans le développement de Kaspersky Anti-Virus 5.6 for Linux Mail Server. Cette section reproduit les textes des licences en anglais.

C.1. *Pcre* library

The following terms regulate Pcre library use:

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.2. *Expat* library

The following terms regulate Expat library use:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

C.3. *AgentX++v1.4.16* library

The following terms regulate AgentX++v1.4.16 library use:

AGENTX++ LICENSE AGREEMENT

==========

THIS LICENSE AGREEMENT (this "Agreement") is made effective as of the date the product is installed by and between (i) Frank Fock, the author of AgentX++ ("LICENSOR") and the party executing this Agreement as Licensee ("LICENSEE").

1. DEFINITIONS.

1.1. The term "Software Product" means Frank Fock's AgentX++ computer software (including Source Code, derived Object Code, and derived Executable Code as defined in Section 1.3, 1.4, and 1.5) and documentation thereof, as specified in Exhibit A, that is provided by LICENSOR to LICENSEE hereunder, including bug fixes and updates thereto provided by LICENSOR to LICENSEE in connection with this Agreement. The term "derived" in the above context refers to the process of creating machine executable code from the original Source Code only. It does not refer to amendment or alteration of the original Source Code by LICENSOR or any third party.

1.2. The term "Intellectual Property Rights" means patent rights, copyright rights, trade secret rights, and any other intellectual property rights.

1.3. The term "Executable Code" is a fully compiled and linked program that contains any code derived from the Software Product. It can no longer be altered or combined with any other code. Executable code is ready to be executed by a computer and is essentially a complete software image for use in a specific product.

1.4. The term "Object Code" is any compiled version of the Software Product that can be linked and therefore combined with other code to create Executable Code. Examples of Object Code are libraries and software development kits, in particular SNMP agent development kits.

1.5. The term "Source Code" is the human readable form of the Software Product, as specified in Exhibit A.

1.6. Documentation means the documentation regarding the Licensed Software provided by LICENSOR to LICENSEE hereunder.

1.7. The term "Site" is a specific address belonging to a single business unit operating at that address.

2. GRANT OF LICENSE.

2.1. Source Code Site License. Subject to the terms and conditions of this Agreement, and upon payment by LICENSEE to LICENSOR of the one-time license fee set forth in Addendum A, LICENSOR grants LICENSEE a perpetual (subject to termination rights in Section 6), non-exclusive, non-transferable license to reproduce, use, modify, or have modified by a third party contractor (modifications in accordance to Section 2.6) subject to a confidentiality agreement no less restrictive than this Agreement, the Source Code for internal use only, for the sole purpose of developing AgentX-enabled SNMP agents at

the Site (hereafter "Licensed Site") specified by LICENSEE during license purchase. Additionally, Customer's contractors and employees reporting directly and only to a manager at the Licensed Site, such as telecommuters, may use the Software Product at remote locations. Off-site employees re-porting in any way to a manager at their location are not covered under this Site License.

2.2. Except as specified in 2.1, neither the Software Product Source Code nor Object Code derived from the Software Product may be redistributed or resold. Executable Code programs derived from the Software Product may be redistributed and resold without limitation and without royalty, provided that LICENSEE added significant functionality to those derived Excecutable Code programs. Functionality in this context refers to the program's behavior, not appearance.

2.3. No Sublicense Right. LICENSEE has no right to transfer, or sublicense the Licensed Software to any third party, except as specified in 2.2 and except if the third party takes over the business of LICENSEE.

2.4. Other Restrictions in License Grants. LICENSEE may not: (i) copy the Licensed Software, except as necessary to use the Licensed Software in accordance with the license granted under Section 2.1 and 2.2, and except for a reasonable number of backup copies.

2.5. No Trademark License. LICENSEE has no right or license to use any trademark of LICENSOR during or after the term of this Agreement.

2.6. Proprietary Notices. The Licensed Software is copyrighted. All proprietary notices incorporated in, marked on, or affixed to the Licensed Software by LICENSOR shall be duplicated by LICENSEE on all copies, in whole or in part, in any form of the Licensed Software and not be altered, removed, or obliterated on such copies.

2.7. Reservation. LICENSOR reserve all rights and licenses to the Licensed Software not expressly granted to LICENSEE under this Agreement.

2.8 Delivery. Upon execution of this Agreement, and payment of the amounts due and owing under this Agreement, LICENSOR will provide LICENSEE with one (1) copy of the Software Product by downloading from LICENSOR's Web site.

3. PRODUCT WARRANTY.

3.1. LICENSOR warrants to LICENSEE that, at the date of delivery of the Software Product to LICENSEE and for a period ending 90 days following the date of

delivery of the Software Product to LICENSEE the Software Product shall perform substantially in accordance with the published specifications and Documentation. If notified in writing by LICENSEE, LICENSOR may, at its option, correct significant program errors in the Software Product within a reasonable

time period. THE FOREGOING PRODUCT WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHETHER IMPOSED BY CONTRACT, STATUTE, COURSE OF DEALING, CUSTOM OR USAGE OR OTHERWISE.

3.2. In no event shall LICENSOR be liable to LICENSEE, in excess of the price paid to LICENSOR by LICENSEE for the Software Product hereunder, for any breach of warranty or any claim, loss or damage arising from or relating to the installation, use or performance of the Software Product (including, without limitation, any indirect, special, incidental or consequential damages).

3.3. LICENSOR reserves the right at any time to make changes to the Software Product.

3.4. IN NO EVENT SHALL LICENSOR BE LIABLE (WHETHER IN TORT, NEGLIGENCE, CONTRACT, WARRANTY, PRODUCT LIABILITY OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS OF PROFITS OR SAVINGS ARISING OUT OF ITS PERFORMANCE OR NONPERFORMANCE OF TERMS OF THIS AGREEMENT OR THE USE, INABILITY TO USE OR RESULTS OF USE OF THE SOFTWARE PRODUCT EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 In no event will LICENSOR be liable for any third-party products used with, or installed in, the Software Product. LICENSOR does not warrant the compatibility of the Software Product with any third-party products, whether hardware or software.

3.6 The above sections do not apply for liability for damages caused by gross negligence or wilful default.

3.7 General Provision. This warranty shall not apply in any case of amendment or alterations of the Software Product made by LICENSEE.

4. INTELLECTUAL AND PROPERTY INDEMNIFICATION.

4.1. LICENSOR agrees to indemnify and hold LICENSEE harmless from any final award of costs and damages against LICENSEE for any action based on infringement of any German intellectual property rights as a result of the use of the Licensed Software: (i) under the terms and conditions specified herein; (ii) under normal use; and (iii) not in combination with other items; provided that LICENSOR is promptly notified in writing of any such suit or claim against LICENSEE and further provided that LICENSEE permits LICENSOR to defend, compromise or settle the same and gives LICENSOR all available information, reasonable assistance and authority to enable LICENSOR to do so. LICENSOR'S LIABILITY TO LICENSEE PURSUANT TO THIS ARTICLE IS LIMITED TO THE TOTAL FEES PAID BY LICENSEE TO LICENSOR IN THE

CALENDAR YEAR IN WHICH ANY FINAL AWARD OF COSTS AND DAMAGES IS DUE AND OWING.

5. TRADE SECRETS AND PROPRIETARY INFORMATION.

5.1. LICENSEE acknowledges that LICENSOR is the owner of the Software Product, that the Software Product is confidential in nature and not in the public domain, that LICENSOR claims all intellectual and industrial property rights granted by law therein and that, except as set forth herein, LICENSOR does not hereby grant any rights or ownership of the Software Product to LICENSEE or any third party. Except as set forth herein, LICENSEE agrees not to copy or otherwise reproduce the Software Product, in whole or in part, without LICENSOR's prior written consent. LICENSEE further agrees to take all reasonable steps to ensure that no unauthorized persons shall have access to the Software Product and that all authorized persons having access to the Software Product shall refrain from any such disclosure, duplication or reproduction except to the extent reasonably required in the performance of LICENSEE'S rights under this Agreement.

5.2. LICENSEE agrees to accord the Software Product and the Documentation and all other confidential information relating to this Agreement the same degree and methods of protection as LICENSEE undertakes with respect to its confidential information, trade secrets and other proprietary data.

5.3. LICENSEE agrees not to challenge, directly or indirectly, the right, title and interest of LICENSOR in and to the Software Product, nor the validity or enforceability of LICENSOR's rights under applicable law. LICENSEE agrees not to directly or indirectly, register, apply for registration or attempt to acquire any legal protection for the Software Product or any proprietary rights therein or to take any other action which may adversely affect LICENSOR's right, title or interest in or to the Software Product in any jurisdiction.

5.4. LICENSEE acknowledges that, in the event of a material breach by LICENSEE of its obligations under this Article 5, LICENSOR may immediately terminate this Agreement, without liability to LICENSEE and may bring an appropriate legal action to enjoin any such breach hereof, and shall be entitled to recover from LICENSEE reasonable legal fees and costs in addition to other appropriate relief.

5.5. LICENSEE agrees to notify LICENSOR immediately and in writing of all circumstances surrounding the unauthorized possession or use of the Software Product and Documentation by any person or entity. LICENSEE agrees to cooperate fully with LICENSOR in any litigation relating to or arising from such unauthorized possession or use.

6. TERMINATION.

6.1. LICENSOR may terminate this Agreement at any time after the occurrence of any of the following events if LICENSOR provides 30 days notice of its

intention to terminate as a result of the occurrence and LICENSEE fails to cure such occurrence within such 30 days:

(a) LICENSEE is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors of LICENSEE;

(b) LICENSEE assigns or transfers this Agreement or any of its rights to obligations hereunder, without LICENSOR's prior written consent; or (c) LICENSEE violates any material provision of this Agreement, including without limitation, the payment obligations set forth in Addendum A.

6.2. LICENSEE may terminate this Agreement at any time after the occurrence of any of the following events if LICENSEE provides 30 days notice of its intention to terminate as a result of the occurrence and LICENSOR fails to cure such occurrence within such 30 days:

(a) LICENSOR is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors or LICENSOR; or

(b) LICENSOR violates any material provision of this Agreement.

6.3. Upon the termination of this Agreement for any reason, LICENSEE will discontinue all use of the Software Product and, within ten (10) days after termination, will destroy or delete all copies of the Software Product then in its possession, including but not limited to, any back-up or archival copies of the Software Product and Documentation. At LICENSOR's request, LICENSEE will verify in writing to LICENSOR that such actions have been taken.

6.4. No termination of this Agreement for any reason whatsoever shall in any way affect the continuing obligations of the parties under Articles 5 hereof.

7. APPLICABLE LAW

This LICENSE shall be deemed to have been made in, and shall be construed pursuant to, the laws of Germany, without reference to conflicts of laws principles. All controversies and disputes arising out of or relating to this Agreement shall be submitted to the exclusive jurisdiction of Esslingen am Neckar, Germany, as long as LICENSEE is deemed to be a merchant (as defined by Handelsgesetzbuch, §1-7). The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

8. GENERAL PROVISIONS.

8.1. This Agreement does not create any relationship of association, partnership, joint venture or agency between the parties.

8.2. This Agreement (including the Exhibit and Addendum attached to the Agreement) sets forth the entire agreement and understandings between the parties hereto with respect to the subject matter hereof. This Agreement merges all previous discussions and negotiations between the parties and supersedes and replaces any and every other agreement, which may have existed between LICENSOR and LICENSEE with respect to the contents hereof.

8.3. Except to the extent and in the manner specified in this Agreement, any modification or amendment of any provision of this Agreement must be in writing and bear the signature of the duly authorized representative of each party.

8.4. The failure of either party to exercise any right granted herein, or to require the performance by the other party hereto of any provision if this Agreement, or the waiver by either party of any breach of this Agreement, shall not prevent a subsequent exercise or enforcement of such provisions or be deemed a waiver of any subsequent breach of the same or any other provision of this Agreement.

8.5. Except in the case of merger, acquisition or the sale of substantial assets or equity of Licensee or assignment to any direct or indirect subsidiary or affiliate of LICENSEE, LICENSEE shall not sell, assign or transfer any of its rights, duties or obligations hereunder without the prior written consent of LICENSOR. LICENSOR reserves the right to assign or transfer this Agreement or any of its rights, duties and obligations hereunder, to any direct or indirect subsidiary or affiliate of LICENSOR.

8.6. All notices required by this Agreement must be sent by certified mail in order to be deemed effective when sent to the following:

FOR LICENSOR:

Frank Fock

Schlossstrasse 8

73765 Neuhausen, Germany

EXHIBIT A

Licensed Software

AgentX++

a. Source Code - (ANSI C++ for Linux, Solaris, Win32) Includes AgentX++ and Agent++Win32 Source Code.

b. Executable Code - AgentX++Win32 Master Agent (Win XP/2000/NT4)

ADDENDUM A

For evaluation purposes and non commercial use only, a free license is granted, provided that the LINCENSEE accepts this license agreement.

In order to obtain a license to use AgentX++ in a commercial environment,

LICENSEE has to purchase a commercial license from LICENSOR. The actual pricing list and other related information can be found at http://www.agentpp.com

C.4. *Agent++v3.5.28a* library

The following terms regulate Agent++v3.5.28a library use:

AGENT++ API Version 3.x

Copyright (C) 2001 Frank Fock, Jochen Katz

LICENSE AGREEMENT

WHEREAS, Frank Fock and Jochen Katz are the owners of valuable intellectual property rights relating to the AGENT++ API and wish to license AGENT++ subject to the terms and conditions set forth below; and WHEREAS, you ("Licensee") acknowledge that Frank Fock and Jochen Katz have the right to grant licenses to the intellectual property rights relating to AGENT++, and that you desire to obtain a license to use AGENT++ subject to the terms and conditions set forth below; Frank Fock and Jochen Katz grants Licensee a non-exclusive, non-transferable, royalty-free license to use AGENT++ and related materials without charge provided the Licensee adheres to all of the terms and conditions of this Agreement.

By downloading, using, or copying AGENT++ or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of Germany, and to all of the terms and conditions of this Agreement, and agrees to take all necessary steps to ensure that the terms and conditions of this Agreement are not violated by any person or entity under the Licensee's control or in the Licensee's service.

Licensee shall maintain the copyright and trademark notices on the materials within or otherwise related to AGENT++, and not alter, erase, deface or overprint any such notice.

Except as specifically provided in this Agreement, Licensee is expressly prohibited from copying, merging, selling, leasing, assigning, or transferring in any manner, AGENT++ or any portion thereof.

Licensee may copy materials within or otherwise related to AGENT++ that bear the authorr's copyright only as required for backup purposes or for use solely by the Licensee.

Licensee may not distribute in any form of electronic or printed communication the materials within or otherwise related to AGENT++ that bear the authorr's copyright, including but not limited to the source code, documentation, help files,

examples, and benchmarks, without prior written consent from the authors. Send any requests for limited distribution rights to sales@agentpp.com.

Licensee hereby grants a royalty-free license to any and all derivatives based upon this software code base, that may be used as a SNMP agent development environment or a SNMP agent development tool.

Licensee may modify the sources of AGENT++ for the Licensee's own purposes. Thus, Licensee may not distribute modified sources of AGENT++ without prior written consent from the authors.

The Licensee may distribute binaries derived from or contained within AGENT++ provided that:

1) The Binaries are not integrated, bundled, combined, or otherwise associated with a SNMP agent development environment or SNMP agent development tool; and.

2) The Binaries are not a documented part of any distribution material.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.5. *Boost v 1.0* library

The following terms regulate Boost v 1.0 library use:

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT

SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE

FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER

DEALINGS IN THE SOFTWARE.

C.6. *Milter* library

The following terms regulate Milter library use:

The following license terms and conditions apply, unless a different license is obtained from Sendmail, Inc., 6425 Christie Ave, Fourth Floor, Emeryville, CA 94608, USA, or by electronic mail at license@sendmail.com.

License Terms:

Use, Modification and Redistribution (including distribution of any modified or derived work) in source and binary forms is permitted only if each of the following conditions is met:

1. Redistributions qualify as "freeware" or "Open Source Software" under one of the following terms:

a) Redistributions are made at no charge beyond the reasonable cost of materials and delivery.

b) Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means the complete compilable and linkable source code of sendmail including all modifications.

2. Redistributions of source code must retain the copyright notices as they appear in each source code file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 1998-2004 Sendmail, Inc. All rights reserved."

4. Neither the name of Sendmail, Inc. nor the University of California nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. The name "sendmail" is a trademark of Sendmail, Inc.

5. All redistributions must comply with the conditions imposed by the University of California on certain embedded code, whose copyright notice and conditions for redistribution are as follows:

a) Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

b) Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

i. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Ii. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

iii. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

6. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY SENDMAIL, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR

IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C.7. *Libkavexim.so* library

The libkavexim.so library is distributed in accordance with GPLv2, and its use is regulated by the following terms:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification"). Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of

any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published
by the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.