KASPERSKY LAB

Kaspersky Anti-Virus® 5.5 pour serveurs de courrier Linux, FreeBSD et OpenBSD

GUIDE DE L'ADMINISTRATEUR

KASPERSKY ANTI-VIRUS® 5.5
POUR SERVEURS DE COURRIER LINUX, FREEBSD ET OPENBSD

Guide de l'administrateur

http://www.kaspersky.com

Date de révision : Mai 2005

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS 5.5 POUR SERVEURS DE COURRIER LINUX, FREEBSD ET OPENBSD

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

Cette application offre les fonctionnalités suivantes :

- *Analyse antivirus* de tous les montages de systèmes de fichiers, ainsi que des messages entrants et sortants faisant partie du trafic SMTP du serveur.
- *Détection des fichiers* infectés, suspects, endommagés et protégés par mot de passe, y compris les fichiers qui ne peuvent être analysés.
- *Désinfection* es objets infectés dans les systèmes de fichiers et les messages de courrier ;
- *Mise en quarantaine* de tous les objets infectés, suspects ou endommagés dans le système de fichiers serveur et dans le trafic de messages. Dans ce dernier cas, les fichiers protégés par mot de passe peuvent également être placés en quarantaine, tout comme les fichiers qui ne peuvent être analysés.
- *Traitement du trafic des messages* conformément à des règles prédéfinies pour des groupes d'expéditeurs ou de destinataires.
- *Assure un filtrage secondaire du trafic de courrier* par nom et type d'objet joint, et utilise des règles de traitement individuel des objets filtrés.
- *Notification à* l'expéditeur, le destinataire et l'administrateur du groupe concernant les messages de courrier contenant des objets infectés, suspects ou similaires.
- *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 virus, en comparant son code avec celui appartenant à des virus individuels, et conservé dans la base antiviurus. Si le fichier est infecté, l'application le nettoie, en utilisant ici aussi les informations conservées dans la base de données.

En raison de l'apparition quotidienne de nouveau virus, il est conseillé de mettre à jour la base antivirus toutes les heures, afin de conserver le produit en parfaites conditions.

- *Configurer Kaspersky Anti-Virus* à l'aide de l'interface Web de l'utilitaire Webmin et du fichier de configuration de l'application.

1.1. Nouveautés de la version 5.5

La version 5.5 de **Kaspersky Anti-Virus pour serveurs de courrier Linux, FreeBSD et OpenBSD** introduit les nouveautés suivantes, par rapport à la version 5.0 :

- Le composant *keepup2date* utilise de nouvelles technologies pour télécharger les mises à jour de base antivirus et de modules d'application, en réduisant au minimum le trafic réseau. Le contrôle d'intégrité des bases de données téléchargées garantit un fonctionnement sécurisé de l'application.
- Une zone de sauvegarde permet de conserver des copies des objets suspects ou infectés, avant leur désinfection ou leur suppression. Ceci permet de récupérer les informations d'origine si une erreur se produit pendant l'analyse antivirus.
- La technologie de base de données iChecker, et le tampon à deux niveaux sur les objets analysés, a été développée pour réduire la surcharge du serveur pendant l'analyse antivirus.
- Il est désormais possible d'utiliser l'application Webmin pour examiner les statistiques d'activité virale pendant une période déterminée, et obtenir des informations sur les types de virus détectés pendant l'analyse.
- Une nouvelle option permet de restreindre le nombre d'objets analysés simultanément en arrière-plan, pour minimiser la charge du serveur.
- Il est maintenant possible de générer une liste des virus détectables.
- La possibilité de sélectionner le protocole actuel (SMTP ou LMTP) pour le fonctionnement du composant *smtpscanner* a été ajoutée.
- Il est maintenant possible de confirmer aux expéditeurs la réception des messages si le protocole SMTP est utilisé.

- La possibilité est donnée d'enregistrer, pour chaque message, les noms des virus détectés et le code d'identification du message, dans le fichier de rapport généré par le composant *smtpscanner*.
- La stratégie de licences de l'application a été modifiée. En particulier, il n'est plus nécessaire de créer ni de gérer une liste d'utilisateurs avec licence ; l'application gère et entretient désormais cette liste automatiquement.
- Il est possible de spécifier la base antivirus activée (jeu standard, étendu ou paranoïa) pour chacun des composants d'application individuels.
- Une nouvelle macro est ajoutée, permettant d'insérer tous les en-têtes du message d'origine, ce qui est utile pour les notifications.
- Les procédures d'installation et de désinstallation de l'application ont été considérablement simplifiées. En particulier, l'application supprime correctement ses propres entrées dans les fichiers de configuration, pendant la procédure de désinstallation.
- Les installations sont désormais plus rapides, en permettant à l'application d'importer la configuration des versions (4.0 ou 5.0) précédentes.
- Le programme d'installation détecte désormais la présence de Kaspersky Anti-Spam, il intègre correctement ce dernier pendant l'installation de l'application, et restaure la configuration précédente lors de la désinstallation.

1.2. Spécifications matérielles et logicielles

Les spécifications minimales du système pour **Kaspersky Anti-Virus** sont :

- Configuration matérielle :
    - Processeur Intel Pentium ou compatible
    - Au moins 32 Mo de RAM
    - Au moins 100 Mo d'espace libre sur disque
- Configuration logicielle :
    - L'un des systèmes d'exploitation suivants :
        - RedHat Linux versions 9.0, Fedora Core 3, Enterprise Linux Advanced Server 3,

- SuSE Linux Enterprise Server 9.0 ou Professional 9.2,
- Mandrake Linux version 10.1
- Debian GNU/Linux version 3.0 mise à jour (r4)
- FreeBSD versions 4.10 ou 5.3
- OpenBSD version 3.6

- L'un des systèmes de messagerie suivants : Sendmail 8.x, Qmail 1.03, Postfix version snapshot_20000529 ou supérieur, Exim 4.0
- L'outil which
- Le logiciel Webmin (www.webmin.com) pour l'administration à distance de Kaspersky Anti-Virus.
- Perl version 5.0 ou supérieur (www.perl.org) pour l'installation de Kaspersky Anti-Virus à l'aide de *install.sh*.

1.3. Contenu de la distribution

Vous pouvez acquérir Kaspersky Anti-Virus chez un détaillant (dans un emballage) ou visiter notre magasin en ligne (www.kaspersky.com, section **E-Store**).

En achetant le paquet au détail vous recevez le kit suivant :

- Une enveloppe cachetée avec un CD d'installation contenant les fichiers de l'application
- Le Guide de l'administrateur ;
- Une clé de licence comprise dans la distribution ou enregistrée sur un disque flexible indépendant ;
- Contrat de licence.

Avant de décacheter l'enveloppe contenant le CD, lisez attentivement le contrat de licence.
L'ouverture de l'enveloppe cachetée contenant le CD ou l'installation de l'application confirme votre acceptation de tous les termes du contrat de licence.

Si vous achetez notre application sur le Web, ou si vous téléchargez celle-ci depuis le site Kaspersky Lab, votre exemplaire contient également ce manuel. Votre clé de licence est présente dans le fichier d'installation, ou vous est envoyée par courrier électronique après paiement.

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

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez retourner le produit non utilisé à votre revendeur Kaspersky Anti-Virus pour un remboursement complet du montant de la souscription, si l'enveloppe contenant le CD est restée fermée.

1.4. Services réservés 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 de cette application logicielle ;
- 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 épidémies virales. Ce service est offert aux utilisateurs ayant souscrit un abonnement à la liste de diffusion de Kaspersky Lab.

Le service support de Kaspersky Lab ne couvre pas le fonctionnement ou l'utilisation de votre système d'exploitation ou d'autres technologies.

1.5. Conventions typographiques

Cet ouvrage utilise plusieurs styles de texte pour mettre en relief les différentes parties significatives de la documentation. Le tableau ci-après illustre les conventions typographiques utilisées dans ce manuel.

Mise en forme	Usage
Gras	Titres de menus, commandes, titres de fenêtres, éléments de boîte de dialogue, etc.
Italiques	Signale un composant du programme.
 Note.	Information complémentaire, remarques.
 Attention !	Informations nécessitant une attention particulière.
 *Pour exécuter une action,* • Étape 1. • …	Description de la succession des étapes que l'utilisateur doit suivre ou des actions possibles.
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du logiciel.
 Solution	Solution du problème exposé.
[argument] – valeur de l'argument.	Paramètres de ligne de commande.
`Texte des messages d'information et de la ligne de commande`	Texte des fichiers de configuration, des messages d'information et de la ligne de commandes.

CHAPITRE 2. SCENARIOS HABITUELS DE DEPLOIEMENT DU PRODUIT

En fonction de l'architecture initiale du serveur de courrier, il existe plusieurs variantes de déploiement de Kaspersky Anti-Virus :

- *Sur le même serveur que le système de messagerie.* Cette variante est utilisée lorsque le serveur héberge un système de messagerie Sendmail, Qmail, Postfix ou Exim (voir section 2.2 à la page 14).
- *Sur un serveur dédié comme filtre secondaire* : Cette méthode est recommandée lorsque le serveur de messagerie principal exploite un système d'exploitation ou de messagerie non pris en charge (voir section 2.4 à la page 17).
- *Sur le même serveur que le système de messagerie en tant que filtre secondaire.* Nous recommandons cette variante dans le cas où un filtre de messagerie, comme Kaspersky Anti-Spam, se trouverait installé sur le serveur de messagerie (voir section 2.3 à la page 16).
- *En tant que filtre pour les boîtes aux lettres externes*. Cette méthode de déploiement est utile lorsque les boîtes aux lettres des utilisateurs de la messagerie se trouvent sur des serveurs externes et qu'il est nécessaire d'assurer la protection antivirus des messages téléchargés (voir section 2.5 à la page 19).

Dans tous les cas précédents, Kaspersky Anti-Virus est capable à la fois de filtrer le trafic des messages et d'analyser touts les points de montage du système de fichiers .

Avant de décrire en détail les scénarios de déploiement précédents, nous allons revoir l'architecture interne de Kaspersky Anti-Virus, afin de bien comprendre son algorithme de fonctionnement.

2.1. Architecture interne de Kaspersky Anti-Virus

Pour bien utiliser Kaspersky Anti-Virus, il est important de comprendre son algorithme de fonctionnement.

Cette section passe en revue l'architecture interne de l'application, spécialement celle qui s'applique à l'analyse du trafic de courrier, dans la mesure où le processus d'analyse des systèmes de fichiers du serveur reste lui-même très simple et n'exige pas d'explications approfondies.

Il faut noter que Kaspersky Anti-Virus est uniquement conçu pour filtrer les messages à la recherche de virus : ce n'est pas un agent de messagerie capable de réceptionner ou d'acheminer le trafic de courrier. Ce travail est assuré par un système de messagerie installé sur le serveur, auquel le logiciel antivirus se trouve intégré après son installation.

Dans les illustrations suivantes sur le fonctionnement interne de l'application une fois celle-ci installée et intégrée au système de messagerie, nous prendrons SendMail comme exemple.

Nous remarquerons que dans le processus d'intégration de l'antivirus dans le système de messagerie Sendmail, un fichier de configuration supplémentaire est créé : *sendmail.cf.listen*.
Lorsqu'il démarre avec ce fichier de configuration, sendmail réceptionne et passe le trafic de courrier à Kaspersky Anti-Virus pour son analyse. S'il démarre avec le fichier de configuration original (*sendmail.cf*),alors il distribue les messages de courrier qu'il reçoit de l'application.

Par conséquent, l'algorithme de fonctionnement est le suivant (voir Figure 1):

1. Sendmail lit le courrier via le protocole SMTP (fichier de configuration *sendmail.cf.listen*). sendmail crée une file d'attente dans laquelle il conserve les messages entrants, avant de les passer via le protocole LMTP au composant *smtpscanner* pour leur analyse.
2. Le composant *smtpscanner* traite le trafic de courrier conformément à sa configuration. L'analyse et le nettoyage des messages de courrier sont réalisés comme ceci :
   a. *smtpscanner* passe le nom de fichier du message au composant *aveserver* à travers le socket local.
   b. *aveserver* analyse et désinfecte l'objet à l'aide des bases antivirus.
   c. *smtpscanner* reçoit de *aveserver* un code retour indiquant l'état du fichier.
   d. En fonction de l'indicateur d'état de l'objet, *smtpscanner* le traite conformément au fichier de configuration.
3. Le trafic du courrier traité, avec les notifications liées aux résultats de l'analyse et de la désinfection, est transféré par protocole SMTP vers le système de messagerie Sendmail (avec *sendmail.cf*), lequel distribue à son tour le courrier aux utilisateurs locaux, ou le réachemine vers d'autres serveurs de courrier.

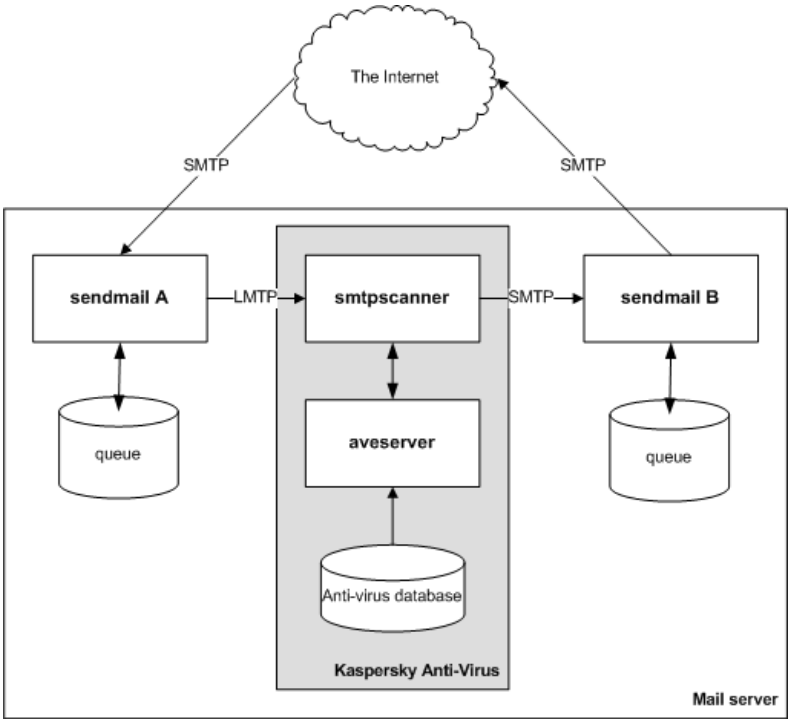

Figure 1. Architecture interne de
Kaspersky Anti-Virus pour serveurs de courrier Unix

2.2. Fonctionnement sur le même serveur que le système de messagerie

Dans ce qui suit, la description du fonctionnement et de la configuration de Kaspersky Anti-Virus est adaptée à la variante dans laquelle l'application se trouve sur le même serveur que le système de messagerie !.

L'installation et le fonctionnement de Kaspersky Anti-Virus sur le même serveur que le système de messagerie n'est possible que s'il existe une prise en charge du système d'exploitation (Linux, FreeBSD ou OpenBSD) et du système de messagerie (Sendmail, Qmail, Postfix ou Exim).

Cette configuration est recommandée si le serveur de messagerie doit faire face à une charge moyenne.

Considérons en détail le fonctionnement de Kaspersky Anti-Virus sur le même serveur pour n'importe lequel des systèmes de messagerie indiqués plus haut (voir Figure 2). La séquence de traitement des messages entrants et sortant est la même, et se décompose dans les étapes suivantes :

1. Le flux des messages de courrier arrive depuis les autres serveurs ou depuis le réseau local, en utilisant le protocole SMTP.
2. Le système de messagerie réceptionne et passe le trafic de courrier à Kaspersky Anti-Virus pour son analyse.
3. L'application traite le trafic de courrier conformément à sa configuration, puis le réexpédie vers le système de messagerie, accompagné d'un jeu de notifications complémentaires.
4. Le système de messagerie achemine le trafic de courrier vers des serveurs externes ou vers des boîtes aux lettres situées sur le réseau local.

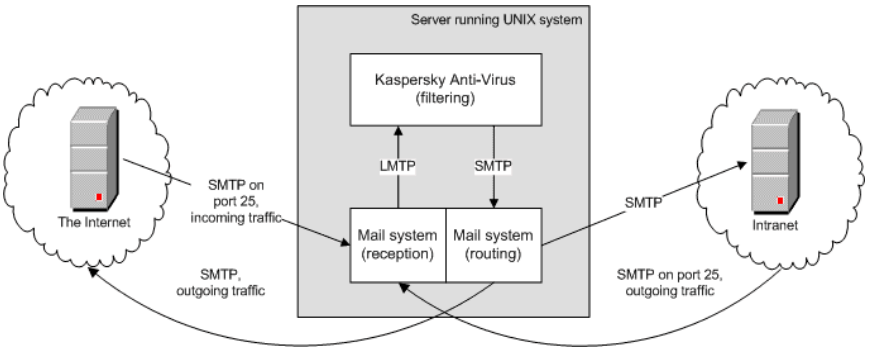

Figure 2. Diagramme de fonctionnement de Kaspersky Anti-Virus sur le même serveur en tant que système de messagerie

D'après le diagramme précédent, au moment ou après l'installation de Kaspersky Anti-Virus, il faut ajuster les paramètres suivants :

- Définissez le port du serveur de messagerie utilisé par Kaspersky Anti-Virus.
- Définissez le port que le système de messagerie utilisera pour la réceptionner le courrier de Kaspersky Anti-Virus après son filtrage.

2.3. Fonctionnement en tant que filtre secondaire

Kaspersky Anti-Virus peut être utilisé comme filtre primaire, ou comme filtre secondaire. Si votre serveur de messagerie est déjà équipé d'un filtre de courrier au moment de l'installation de Kaspersky Anti-Virus, vous devez définir lesquels de ces filtres (Kaspersky Anti-Virus ou l'un de ceux déjà existants) interviendront en tant que filtres primaire ou secondaire, respectivement. ce choix s'appuiera sur les procédés de filtrage utilisés par les deux filtres.

Le filtre primaire (que nous désignerons par MX1) est celui qui filtre le trafic de courrier en fonction de l'adresse IP de l'expéditeur. Ce type de filtre est installé en premier lieu sur le port 25. Il reçoit le courrier entrant, le filtre puis le passe au filtre secondaire pour traitement. Le *filtre secondaire* (désigné par MX2) est installé sur le même poste que le filtre primaire, mais il est affecté à une adresse IP et à un port différents du précédent.

Si votre serveur n'est équipé d'aucun filtre opérant sur l'adresse IP de l'expéditeur, vous pouvez alors installer Kaspersky Anti-Virus comme filtre primaire. Dans le cas où votre filtre IP est installé, installez l'antivirus en tant que filtre secondaire. La raison pour procéder ainsi est que tout le trafic de courrier analysé par Kaspersky Anti-Virus va ressortir par la même adresse IP. Par conséquent, appliquer un filtre par IP après le traitement antivirus n'a aucun intérêt.

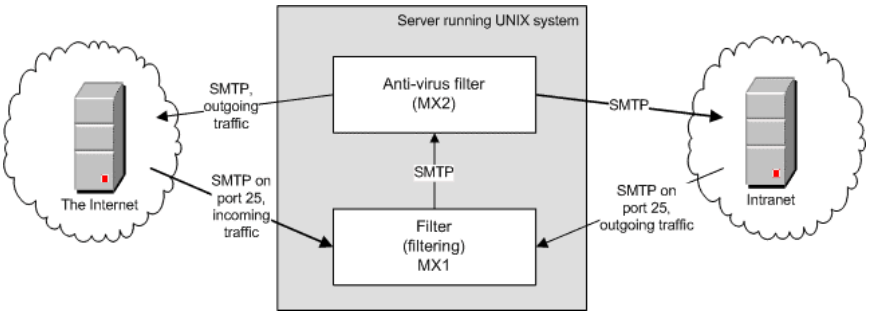

Figure 3. Diagramme de fonctionnement de Kaspersky Anti-Virus
en tant que filtre secondaire sur le même serveur avec système de messagerie

Appliquez la configuration suivante pour les filtres primaires et secondaires :

- Configuration du filtre primaire (MX1) :

  Nom de l'hôte où le filtre est installé : mx1.yourhost.domain

L'adresse IP du filtre : toutes les disponibles adresses

Numéro de port utilisé par le filtre : 25

Nom de l'hôte pour l'envoi de courrier : mx2.yourhost.domain:10026

- Configuration du filtre secondaire (MX2) :

  Nom de l'hôte où le filtre est installé : mx2.yourhost.domain

  L'adresse IP du filtre : 127.0.0.1

  Numéro de port, utilisé par le filtre : 10026

  Nom de l'hôte source du courrier reçu : mx1.yourhost.domain

MX1 et MX2 doivent utiliser des noms d'hôtes différents, car le serveur n'acceptera pas un message pour lequel les noms des hôtes, dans le dialogue helo/ehlo, sont les mêmes. L'état du MX2 doit être approuvé par MX1 et inversement, autrement, la distribution échouera.

2.4. Fonctionnement sur un serveur dédié

Kaspersky Anti-Virus peut filtrer le trafic de courrier et assurer le traitement antivirus même si votre serveur de messagerie est exploité sous un autre système, par exemple sous Windows.

Dans ce scénario, Kaspersky Anti-Virus est installé sur un serveur dédié exploité sous Linux, FreeBSD ou OpenBSD.

Afin de pouvoir recevoir le trafic de courrier et le réexpédier vers le serveur de messagerie Windows, un autre système de messagerie (Sendmail, Qmail, Postfix ou Exim) doit être installé sur le serveur dédié, et intégré avec Kaspersky Anti-Virus (voir section 4.4 à la page 29).

Dans ce scénario, le fonctionnement suit la séquence suivante (voir Figure 4):

1. Le trafic de courrier est reçu par un serveur sous système d'exploitation de type Unix.
2. Le système de messagerie (qmail, par exemple) le réexpédie à Kaspersky Anti-Virus via le protocole LMTP pour son analyse.
3. Le courrier vérifié, avec les notifications créées par l'antivirus, est renvoyé au système de messagerie, qui le réexpédie à son tour au serveur de messagerie principal, afin d'être distribué, ou réacheminé à nouveau.

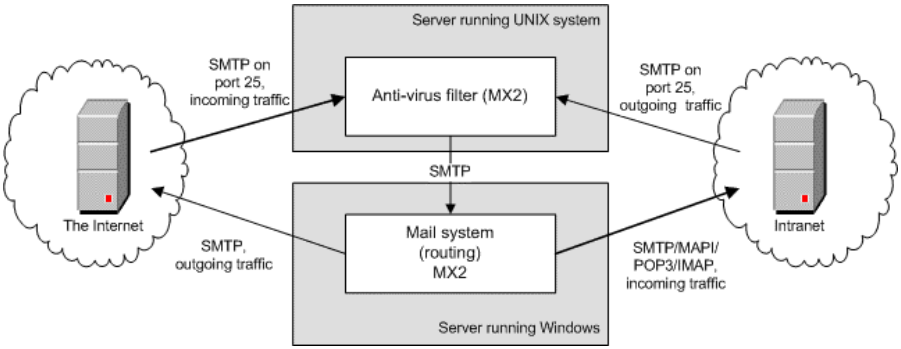

Figure 4. Diagramme de fonctionnement de Kaspersky Anti-Virus sur un serveur dédié

Sur le diagramme précédent, le serveur équipé de Kaspersky Anti-Virus est le serveur primaire, car il reçoit et réexpédie le courrier, tandis que le serveur secondaire est celui avec MS Exchange, qui distribue uniquement le courrier.

Cependant, si avant l'installation de Kaspersky Anti-Virus, votre serveur de messagerie a été utilisé pour filtrer des messages en fonction des adresses IP des expéditeurs, alors il faut définir le serveur équipé de Kaspersky Anti-Virus comme secondaire. En effet, si vous définissez comme primaire le serveur qui héberge Kaspersky Anti-Virus, alors tous les messages électroniques réceptionnés par le serveur secondaire (qui assure le filtrage par IP) proviendront de la même adresse IP, et l'application de filtres sera alors impossible.

Si votre LAN contient des serveurs de courrier, il faut alors faire pointer les enregistrements MX ou les paramètres de réexpédition vers le serveur primaire, et non vers le secondaire.

- Configuration du filtre primaire (MX1) :

  Nom de l'hôte où le filtre est installé : mx1.yourhost.domain

  Nom de l'hôte pour la réexpédition de courrier : mx2.yourhost.domain:25

- Configuration du filtre secondaire (MX2) :

  Nom de l'hôte où le filtre est installé : mx2.yourhost.domain

  Nom de l'hôte source du courrier reçu : mx1.yourhost.domain

2.5. Filtrage du courrier provenant de boîtes aux lettres externes

Actuellement, des boîtes aux lettres externes sur des serveurs comme *www.mail.ru*, *www.aport.ru*, *www.hotmail.com*, etc. sont largement utilisées.

Comment éviter l'infection en cas de téléchargement de messages contaminés depuis ce type de boîtes aux lettres ? En pratique, ce message est distribué par protocole POP3, tandis que Kaspersky Anti-Virus analyse uniquement le trafic de courrier qui utilise le protocole SMTP.

Pour assurer la protection antivirus du courrier externe, la configuration suivante est nécessaire :

1. Bloquer le port 110 (POP3) par défaut et donner aux utilisateurs un accès simple au courrier externe, puis faire opérer la passerelle en tant que serveur proxy pour POP3 à l'aide du paquet **fetchmail**. Ce paquet télécharge les messages de courrier depuis des serveurs externes et les envoie vers le port SMTP local. C'est exactement le but recherché, car une fois arrivés sur le port SMTP, les messages sont alors analysés par Kaspersky Anti-Virus.

   

   Le filtrage du courrier provenant de boîtes aux lettres externes nécessite un serveur SMTP local et un compte utilisateur local sur le poste où le paquet fetchmail est installé.

   La configuration de fetchmail est très simple : chaque utilisateur, dans son répertoire $HOME, possède un fichier *.fetcmailrc*, contenant au moins les lignes suivantes :

   ```
   set postmaster "utilisateur"
   set bouncemail
   set no spambounce
   set properties ""
   poll mail.poste.libre.fr with proto POP3
       utilisateur 'UtilisateurDistant' there with
   password 'pass12345' is 'utilisateur' here
   poll mail2.poste.libre.fr with proto POP3
       utilisateur 'UtilisateurDistant2' there with
   password 'pass123452' is 'utilisateur' here
   ```

   où :

   utilisateur est le nom de l'utilisateur dans le réseau local

mail.poste.libre.fr et *mail2.poste.libre.fr* sont les noms des hôtes sur lesquels les messages doivent être collectés.

UtilisateurDistant et *UtilisateurDistant2* sont des noms de connexion pour les serveurs *mail.poste.libre.fr* et *mail2.poste.libre.fr*, respectivement.

pass12345 et *pass123452* sont les mots de passe des comptes de messagerie *UtilisateurDistant* et *UtilisateurDistant2*.

Avec ces paramètres, le programme fetchmail pourra récupérer les messages de courrier dans les hôtes *mail.poste.libre.fr* et *mail2.poste.libre.fr*, puis les diriger vers le service SMTP local de l'*utilisateur*. Aucun des champs (*De:*, *A:* ni aucun autre) ne sera altéré dans les messages, uniquement un en-tête *received* supplémentaire sera ajouté par fetchmail. L'apparence des messages de courrier reçus par l'utilisateur sera la même que s'ils avaient été reçus normalement.

2. Configurez l'outil cron, dans le crontab, pour démarrer fetchmail toutes les 10 ou 15 minutes, par exemple.

Pour automatiser la mise en place du programme fetchmail pour d'autres utilisateurs de boîtes aux lettres externes, nous avons besoin des informations suivantes :

- Nom de l'hôte externe, où fetchmail récupère les messages de courrier.
- Connexion au compte de l'hôte externe.
- Mot de passe du compte.

En outre, les répertoires de travail de chaque utilisateur doivent contenir un fichier *.fetchmailrc* avec le contenu suivant :

```
set postmaster "utilisateur"
set bouncemail
set no spambounce
set properties ""
```

Le fichier script suivant peut-être utilisé pour ajouter des entrées de boîtes aux lettres :

```
#!/bin/bash
echo "poll $1 with proto POP3 " >>$HOME/.fetchmailrc
echo "utilisateur '$2' with password '$3' is '$4'
here">>$HOME/.fetchmailrc
```

Si vous exécutez ce script avec les paramètres suivants : *pop.mail.ru*, *dan*, *secret*, *admin*, alors les messages pour l'utilisateur *dan@mail.ru* seront réexpédiés à l'adresse *admin@your_hote.votre_domaine*.

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS

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 8. Si une quelconque application n'est pas encore installée, il est conseillé de le faire auparavant, ou un partie de l'application ne sera pas disponible.
- Réalisez des copies de sauvegardes des fichiers de configuration du système de messagerie installé sur votre serveur.
- Configurez votre connexion Internet.
- **Stoppez le serveur de messagerie**, avec lequel vous allez intégrer Kaspersky Anti-Virus.
- Ouvrez une session sur le système en tant que **root**.

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 sur un serveur Linux

Kaspersky Anti-Virus est distribué sous trois différents types de paquets d'installation (rpm, deb ou tar.gz) pour systèmes Linux ; votre choix dépendra du type de distribution de votre système d'exploitation.

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

```
rpm –i <nom_fichier_Paquet_Distribution>
```

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

```
dpkg –i <nom_fichier_Paquet_Distribution>
```

Vous pouvez également utiliser la distribution universelle prévue pour tous les systèmes d'exploitation Linux. Utilisez ce fichier si votre version Linux ne prend pas en charge les formats RPM ou DEB ou si votre administrateur réseau n'utilise pas de gestionnaire de paquets intégré.

Le paquet de distribution universelle de Kaspersky Anti-Virus se présente sous la forme d'un fichier d'archive. Ce fichier d'archive contient l'arborescence de répertoires, les fichiers de la distribution et le script d'installation *install.sh*, qui prend en charge l'installation proprement dite.

Pour installer Kaspersky Anti-Virus à partir du paquet d'installation universel, procédez de la manière suivante :

1. Copiez l'archive du paquet d'installation dans un répertoire du système de fichiers du serveur, et décompressez-le.
2. Lancez le script d'installation : *./install.sh*.

3.2. Installation sur un serveur FreeBSD ou OpenBSD

Le paquet d'installation de Kaspersky Anti-Virus est fournit sous la forme d'un paquet .pkg pour les serveurs exploitant FreeBSD ou OpenBSD.

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

```
pkg_add <NomPaquet>
```

3.3. Procédure d'installation

Si l'installation se termine avec un code d'erreur, assurez-vous que votre système est conforme aux spécifications matérielles et logicielles requises (voir section 1.2 à la p. 8) et que vous vous êtes connecté au système en tant que root.

Pour installer l'application sur un serveur, les étapes sont les suivantes :

1. Copiez les fichiers d'application dans le serveur.
2. Installez une clé de licence.

Si la clé de licence n'est pas installée, le processus de configuration ne démarrera pas et il sera impossible de travailler avec l'application. Si vous

ne disposez pas encore de clé de licence au moment de l'installation (par exemple, si vous avez acheté l'application sur Internet sans avoir encore reçu votre licence par courrier électronique), vous pourrez installer la clé une fois terminée la procédure d'installation, mais avant de pouvoir utiliser effectivement l'application.

3. Configurez le composant *keepup2date*.
4. Installez et mettez à jour les bases antivirus.

Vérifiez que les bases antivirus sont installées avant de commencer à utiliser l'application. Les traitements liés à l'analyse et à la désinfection antivirus dépendent du contenu des bases antivirus ; celles-ci contiennent les descriptions de tous les virus actuellement connus ainsi que les méthodes de désinfection des objets infectés. L'analyse et le traitement de fichiers sont impossibles sans ces bases antivirus !

Notez que la configuration automatique de l'application ne se réalisera pas si les bases antivirus ne sont pas installées.

5. Installez le module Webmin.

La correcte installation du module Webmin, destiné à la gestion décentralisée du logiciel, ne peut se faire que si l'application se trouve placée dans le répertoire par défaut. Après l'installation de Webmin, des instructions détaillées vous guideront afin de configurer le fonctionnement du module avec l'application.

Les sections suivantes décrivent ces étapes de manière plus détaillée.

3.4. Configuration de l'application

Immédiatement après la copie des fichiers d'application dans le serveur, le programme d'installation effectue la configuration du système. Si le gestionnaire de paquets admet les scripts interactifs, la configuration démarre automatiquement : dans le cas contraire, un message vous informe de le démarrer manuellement.

La procédure de configuration se déroule dans les étapes suivantes :

- Recherche d'un serveur de messagerie installé, et comparaison de sa version avec les spécifications logicielles.
- Recherche et modification du fichier de configuration du serveur.

Si des informations supplémentaires sont nécessaires pendant la configuration (par exemple, le chemin d'accès au fichier de configuration du serveur de

messagerie), le programme d'installation affiche des messages en ce sens sur la console du serveur. La saisie de réponses incorrectes mettra fin au processus.

Si toutes les étapes de la configuration sont correctement terminées, l'application est prête pour travailler ; le programme d'installation n'affichera plus aucune notification supplémentaire. Le fichier de configuration inclus dans le paquet d'installation contient tous les paramètres requis pour commencer à fonctionner.

Assurez-vous de redémarrer le serveur de messagerie avant de commencer à utiliser l'application.

CHAPITRE 4. CONFIGURATION POSTERIEURE A L'INSTALLATION

Pendant l'installation de Kaspersky Anti-Virus, le système cible est analysé et certains paramètres de configuration de l'application sont définis automatiquement aux valeurs les plus appropriées en fonction du système (voir section .4.1 à la page 26).

Avant de commencer à utiliser l'application, nous vous conseillons d'installer ou de mettre à jour les bases antivirus (si cela n'a pas été fait pendant l'installation) et d'analyser les systèmes de fichiers du serveur, à la recherche de virus !

Cependant, ceci n'est pas suffisant pour commencer à travailler avec le logiciel. Vous devez faire les actions suivantes :

- Intégrer Kaspersky Anti-Virus avec le système de messagerie installé sur votre serveur.
- Créer une liste d'utilisateurs avec licence dont les courriers entrants et sortants seront analysés à la recherche de virus, et désinfectés.

En outre, nous vous conseillons de mettre en place l'utilisation conjointe de Kaspersky Anti-Virus avec le paquet Webmin.

Ce chapitre décrit la configuration par défaut de Kaspersky Anti-Virus, et s'arrête de manière plus approfondie sur la configuration nécessaire à la bonne exploitation de l'application.

Les exemples ci-dessous utilisent les chemins habituels des distributions pour Linux.

4.1. Configuration par défaut du logiciel

Tous les paramètres de Kaspersky Anti-Virus sont conservés dans le fichier de configuration par défaut */etc/kav/5.5/kav4mailservers.conf*.

Vous pouvez créer vos propres fichiers de configuration, afin de les utiliser pour les tâches courantes, ou en tant que fichiers par défaut.

Cette section explique plus en détail les paramètres du fichier et leurs valeurs par défaut, pour vous aider à déterminer si la configuration de Kaspersky Anti-Virus doit être ajustée (voir Chapitre 6 à la page 60), afin de maximiser son rendement, en fonction des conditions de votre environnement corporatif.

PROTECTION ANTIVIRUS DES SYSTEMES DE FICHIERS DU SERVEUR

Par défaut, la configuration de Kaspersky Anti-Virus est définie de telle sorte que lorsque le composant *kavscanner* est lancé sans paramètres, sur la ligne de commande, il effectue une analyse antivirus récursive des répertoires et fichiers du serveur, en commençant par le répertoire courant.

Si des fichiers infectés, suspects, ou endommagés, sont identifiés, des messages sont affichés sur la console et ajoutés au rapport.

Notez bien que, par défaut, les fichiers infectés détectés par Kaspersky Anti-Virus NE SONT PAS NETTOYÉS !

PROTECTION ANTIVIRUS DU TRAFIC DE COURRIER DU SERVEUR

La protection antivirus du trafic de courrier EST IMPOSSIBLE tant que Kaspersky Anti-Virus n'est pas intégré au système de messagerie. Les explications ci-après décrivent les paramètres qui déterminent le fonctionnement par défaut de l'application, après son intégration au système de messagerie.

La section **[smtpscan.group:default]** du fichier de configuration *kav4mailservers.conf* définit la disponibilité du groupe **default**, qui comprend tous les utilisateurs protégés du serveur de messagerie. Le groupe définit les règles d'analyse et de traitement antivirus du trafic de courrier suivantes :

- Les messages entrants et sortants sont analysés.
- Si des courriers infectés sont détectés, l'application les désinfecte.

  Les messages de courrier désinfectés sont remis aux destinataires et à l'administrateur du groupe (*postmaster@localhost*) accompagnés de notifications indiquant que les messages contenaient des virus et que leur désinfection a réussi. Des messages semblables sont transmis aux auteurs des messages.

Si la désinfection échoue, le message est supprimé et une notification appropriée est envoyée au destinataire, à l'expéditeur et à l'administrateur du groupe.

Toutes les notifications concernant l'analyse, la désinfection, l'élimination, la mise en quarantaine des messages sont envoyées par défaut en provenance de l'adresse *MAILER-DAEMON@localhost*.

- Pendant l'analyse antivirus du courrier, les fichiers suspects, endommagés ou protégés par un mot de passe, ou tout message de courrier dont l'analyse échoue, sont supprimés. Des notifications appropriées sont envoyées au destinataire, à l'expéditeur et à l'administrateur du groupe.
- Toutes les actions de l'application sont enregistrées dans le fichier de rapport.

Notez que le processus *aveserver* doit être en exécution pour que l'analyse antivirus du trafic de courrier soit possible. Si ce processus est désactivé, tout le trafic entrant est automatiquement placé en file d'attente, avant analyse et traitement. Des comptes-rendus sont enregistrés dans le fichier journal de l'application. Voir la section 6.4 à la page 73

4.2. Installation et mise à jour des bases antivirus

Il est conseillé d'installer et de mettre à jour la base antivirus immédiatement après l'installation de l'application.

Pour ce faire, exécutez le composant *keepup2date*. Écrivez ce qui suit sur la ligne de commande :

```
/path/to/keepup2date
```

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

Il est recommandé de mettre à jour la base antivirus TOUTES LES HEURES, en raison de l'apparition quotidienne de nouveau virus et de l'importance de conserver le produit en parfaites conditions. Pour plus d'informations sur la mise à jour de la base de données, reportez-vous aux sections 5.1.3 - 5.1.4 à la page 38 - 39.

4.3. Configuration de l'utilisation conjointe de Webmin

Si vous prévoyez de piloter Kaspersky Anti-Virus à distance, nous vous conseillons de le configurer pour utilisation conjointe avec le paquet Webmin.

Par exemple, Webmin peut être utilisé pour restreindre l'accès au logiciel par un système de mots de passe utilisateur. Pour plus de détails sur le paramétrage de Webmin, reportez-vous à la documentation qui l'accompagne.

Tous les paramètres antivirus modifiés à distance depuis Webmin sont enregistrés dans le fichier de configuration par défaut de l'application.

Si vous souhaitez créer un fichier de configuration alternatif avec l'utilitaire Webmin, procédez comme suit :

- Copiez le contenu du fichier de configuration dans un nouveau fichier et enregistrez-le sous un nom différent. Ensuite, modifiez le nouveau fichier (alternatif) de configuration selon vos besoins.
- Spécifiez le nom du fichier alternatif dans la zone **Full path to KAV config**, sur l'onglet **Config edit**.

4.4. Intégration manuelle avec les systèmes de messagerie

Suivez la procédure ci-après uniquement si vous n'avez PAS UTILISÉ le script setup.sh pendant l'installation de l'application, c'est à dire, si l'application n'est pas configurée automatiquement.

La procédure d'intégration manuelle se fait en trois étapes :

1. Ajustez la configuration du système de messagerie pour fonctionner de manière conjointe avec Kaspersky Anti-Virus.
2. Ajustez la configuration de l'application pour un fonctionnement conjoint avec le système de messagerie.
3. Lancez le système de messagerie avec la nouvelle configuration.

Les utilisateurs dont les comptes sont utilisés pour démarrer et faire fonctionner le système de messagerie doivent posséder des droits en lecture sur les fichiers de configuration des systèmes de messagerie respectifs.

Les sous-sections suivantes décrivent l'intégration manuelle de Kaspersky Anti-Virus avec les systèmes de messagerie pris en charge.

4.4.1. Intégration avec Sendmail

Pour intégrer Kaspersky Anti-Virus avec Sendmail,

1. Copiez le contenu de *sendmail.cf.listen* dans le fichier *sendmail.cf*.
2. Dans le nouveau fichier *sendmail.cf.listen*, créez la règle 98 comme ceci :

   ```
   SParseLocal=98
   R$*[tab_character]$#smtpscanner $@$1 $:$1
   ```

3. Fournissez une description de *smtpscanner* dans le fichier :

   ```
   Msmtpscanner, P=/opt/kav/bin/smtpscanner,
   F=PCXmnz9, S=EnvFromSMTP, R=EnvToSMTP, E=\r\n,
   L=2040,
   T=SMTP,
   A=smtpscanner
   ```

4. Configurez Kaspersky Anti-Virus selon vos besoins (voir section 4.4.5 à la page 33).
5. Ajoutez les deux processus suivants aux scripts de démarrage :

   ```
   /usr/sbin/sendmail -bd -q10m -C
   /etc/mail/sendmail.cf.listen
   ```

   ```
   /usr/sbin/sendmail -q10m -C /etc/mail/sendmail.cf
   ```

   Si vous utilisez Sendmail version 8.12 ou supérieur configuré avec *submit.cf*, ajoutez ces trois processus aux scripts de démarrage :

   ```
   /usr/sbin/sendmail -bd -q10m
   -C /etc/mail/sendmail.cf.listen
   /usr/sbin/sendmail -q10m
   -C /etc/mail/sendmail.cf
   /usr/sbin/sendmail -q10m -C /etc/mail/submit.cf
   ```

4.4.2. Intégration avec Qmail

Quand Kaspersky Anti-Virus est intégré au système de messagerie Qmail, son propre composant *smtpscanner* remplace le logiciel *qmail-queue*. Afin d'envoyer des messages ou de les placer dans la file d'attente, *smtpscanner* invoque le logiciel original *qmail-queue*.

Pour intégrer Kaspersky Anti-Virus avec Qmail,

1. Renommez le fichier *qmail-queue* dans le répertoire **/var/qmail/bin/** à *queue.kav55*.
2. Copiez le fichier *qmail-queue* du répertoire **/opt/kav/5.5/kav4mailservers/bin//** dans le répertoire **/var/qmail/bin**, ou créez un lien symbolique vers ce fichier.
3. Définissez les permissions d'accès suivantes aux fichiers *qmail-queue* et *qmail kav55* :

```
16 -rws--x--x  1 qmailq  qmail    12688 Mar 24
13:56 qmail-que
316 -rwx--x--x  1 qmailq  qmail    315612 Apr 14
11:29 qmail-queue
```

4. Configurez Kaspersky Anti-Virus selon vos besoins (voir section 4.4.5 à la page 33).
5. Redémarrez le système de messagerie.

Si votre système Qmail utilise l'utilitaire *softlimit*, il convient d'incrémenter la quantité de mémoire disponible, ou désactiver les limites de mémoire. Dans le cas contraire, des difficultés peuvent apparaître pendant l'analyse de messages de grande taille.

4.4.3. Intégration avec Postfix

Pour intégrer Kaspersky Anti-Virus avec Postfix,

1. Vérifiez le numéro de version du système de messagerie Postfix. La version doit être postérieure au **snapshot_20000529.** Si la version est plus ancienne, téléchargez la nouvelle sur le site Web de Postfix (www.postfix.org).

2. Ajoutez la ligne suivante au fichier de configuration du système de messagerie Postfix *main.cf* :
```
content_filtre = lmtp:localhost:10025
```

3. Ajoutez les lignes suivantes au fichier de configuration du système de messagerie Postfix *master.cf :*
```
localhost:10025 inet   n      n      n      -
   10     spawn utilisateur=filtre
   argv=/opt/kav/bin/smtpscanner
localhost:10026 inet   n      -      n      -
   10     smtpd -o content_filtre= -o
monNomHote=localhost
```

4. Créez un répertoire **/var/spool/filter**. Créez un **filtre** utilisateur, incluez-le dans le groupe **filtre**, et spécifiez le répertoire **/var/spool/filter** comme répertoire de travail. Assurez-vous de modifier les droits d'accès au répertoire, et tenez compte du fait que *smtpscanner* fonctionnera avec les droits attribués pour au compte du **filtre** utilisateur :
```
mkdir /var/spool/filtre
groupadd filtre
useradd filtre -s /bin/false -d /var/spool/filtre
-g filtre
chown filtre.filtre /var/spool/filtre
```

5. Configurez Kaspersky Anti-Virus selon vos besoins (voir section 4.4.5 à la page 33).

6. Redémarrez le système de messagerie.

4.4.4. Intégration avec Exim

Pour intégrer Kaspersky Anti-Virus avec Exim,

1. Copiez le fichier de configuration, (par exemple *exim.conf)* à *exim.conf.listen*.

2. Introduisez les corrections suivantes dans le fichier *exim.conf:listen :*

   - ajoutez ces lignes sous la section TRANSPORT CONFIGURATION :
```
kav_lmtp_transport :
  driver = lmtp
  command = /opt/kav/bin/smtpscanner
```

- définissez les paramètres de distribution du courrier local sous la section ROUTERS CONFIGURATION :

```
localuser :
 driver=accept
 transport=kav_lmtp_transport
```

définissez les paramètres de distribution à distance du courrier :

```
lookuphost :
 driver=dnslookup
 transport=kav_lmtp_transport
```

3. Configurez Kaspersky Anti-Virus selon vos besoins (voir section 4.4.5 à la page 33).
4. Ajoutez les deux processus suivants aux scripts de démarrage :

```
exim -q10m -bd -C /etc/exim/exim.conf.listen
exim -q10m -C /etc/exim/exim.conf
```

Si vous souhaitez lancer le composant *smtpscanner* à partir d'un autre compte utilisateur, compilez le système de messagerie Exim en modifiant les valeurs des paramètres EXIM_GID et EXIM_UID. Pour plus d'informations, reportez-vous à la documentation fournie avec le système de messagerie Exim.

4.4.5. Intégration de Kaspersky Anti-Virus au système de messagerie

L'autre partie essentielle du travail d'intégration de Kaspersky Anti-Virus avec des systèmes de messagerie, est la configuration du logiciel antivirus lui-même, en modifiant son fichier de configuration.

Pour configurer le fonctionnement de Kaspersky Anti-Virus avec un système de messagerie :

Définissez les paramètres suivants dans le fichier de configuration de Kaspersky Anti-Virus :

- Spécifiez l'adresse expéditrice des notifications :

```
NotifyFromAddress=admin@yourhostname.ru
```

- Configurez l'Id. du système de messagerie sous la section **[smtpscan.general]**. L'Id. du système de messagerie possède la structure suivante : **protocole:hote:port**, où :

protocole est le protocole utilisé pour l'envoi du courrier(**smtp** ou **lmtp**)

hote est le nom de l'hôte ou son adresse IP, d'où les messages seront envoyés, ou le nom du logiciel de courrier.

- Sélectionnez le protocole utilisé (LMTP ou SMTP).

Le chemin complet du logiciel de courrier doit être indiqué entre parenthèses et peut contenir toutes les options de la ligne de commande.

port – numéro du port (port 25 par défaut).

Par exemple, la ligne peut avoir l'apparence suivante : **smtp:localhost.tu:1100** or **lmtp:(local.mail –l)**

- Pour Sendmail :

```
ForwardMailer=smtp:(/usr/sbin/sendmail -bs
-C /etc/mail/sendmail.cf)
```

- Pour Qmail :

```
ForwardMailer=qmail:(/var/qmail/bin/qmail-
que)
```

- Pour Postfix :

```
ForwardMailer=smtp:localhost:10026
```

- Pour Exim :

```
ForwardMailer=smtp:(exim -bs
-C/etc/exim/exim.conf)
```

- Pour le groupe d'utilisateurs, indiquez ce qui suit dans la section **[smtpscan.group:default]**du fichier de configuration :

```
AdminAddress=admin@votreNomHote.fr
AdminNotify=yes
```

- Dans la section **[smtpscan.limits]** définissez le délai de temporisation (en secondes) pour que le processusaveserver exécute une opération.

```
MaxCheckTime=60
```

CHAPITRE 5. UTILISATION DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus vous permet d'organiser la protection antivirus intégrale de votre serveur, à partir d'un fichier du serveur, qui couvre le trafic de courrier entrant et sortant, y compris le courrier récupéré depuis des boîtes aux lettres externes.

L'utilité d'une application se révèle au nombre de tâches qu'un administrateur parvient à résoudre grâce à elle. Les tâches implémentées par Kaspersky Anti-Virus peuvent se diviser en trois catégories :

1. Mise à jour de la base antivirus utilisée pour l'analyse et le nettoyage de tous objets infectés.
2. Protection antivirus du trafic de courrier du serveur.
3. Protection antivirale des systèmes de fichiers du serveur.

Chacun de ces groupes comprend d'autres tâches plus spécifiques, qui font appel à des fonctions particulières de l'application. Ce chapitre examine les plus intéressantes de ces tâches, que l'administrateur peut combiner ou composer lui-même pour couvrir un besoin particulier.

Nous allons décrire comment configurer et exécuter des tâches en local, sur l'invite de commande.

Pour toutes les tâches suivantes, nous supposons que l'administrateur a effectué la configuration postérieure à l'installation (voir Chapitre 4 à la page 26).

Avant d'exécuter des tâches liées à l'analyse du courrier, il est nécessaire de lancer le processus *aveserver*, s'il n'a pas été chargé au démarrage du système d'exploitation.

5.1. Mise à jour des bases antivirus

Le composant *keepup2date* de l'application prend en charge les fonctions indispensables pour conserver en état de fonctionnement les bases antivirus utilisées par Kaspersky Anti-Virus pour l'analyse et la désinfection des fichiers contaminés. Elles peuvent être téléchargées depuis les serveurs de mise à jour de Kaspersky Lab, aux adresses suivantes :

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

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

ftp://downloads1.kaspersky-labs.com/updates/, ainsi que d'autres serveurs.

Vous trouverez une liste d'adresses à partir desquelles il est possible de télécharger les mises à jour dans le fichier *updcfg.xml*, présent dans le paquet de l'application. La liste est mise à jour automatiquement de manière régulière.

La modification manuelle du fichier *updcfg.xml* n'est pas autorisée !

Pendant la procédure de mise à jour, le composant *keepup2date* récupère ce fichier avec la liste de serveurs, y choisit une adresse et tente de télécharger les bases antivirus à partir du serveur correspondant. Si la tentative de mise à jour échoue sur cette adresse, le composant *keepup2date* répète le processus avec l'adresse suivante. Après une mise à jour réussie, l'application redémarre automatiquement par défaut (voir le paramètre **PostUpdateCmd** dans la section **[updater.options]**).

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

Si la structure de votre réseau local est plutôt complexe, nous vous recommandons de télécharger les mises à jour des bases antivirus dans un répertoire du réseau, puis de configurer les autres ordinateurs du réseau pour qu'ils récupèrent les mises à jour à partir de ce répertoire.

Il est fortement conseillé de mettre à jour la base antivirus toutes les heures.

Il est possible de planifier la procédure de mise à jour à l'aide de l'utilitaire **cron** (voir section 5.1.3 à la page 38), ou encore, l'administrateur peut choisir de procéder à partir de la ligne de commande (voir section 5.1.4 à la page 39).

5.1.1. *Composant d'application keepup2date*

Notez que le composant *keepup2date*qui permet de mettre à jour les bases antivirus, remplace le composant *kavupdater* utilisé par les versions précédentes de l'application.

Le composant chargé de la mise à jour des bases antivirus a été remplacé dans la version *5.5* de **Kaspersky Anti-Virus**. Le nouveau composant incorpore plusieurs améliorations et nouveautés par rapport aux fonctions existantes :

- La possibilité de sélectionner le serveur de mise à jour le plus proche géographiquement, d'après la région spécifiée dans le fichier de configuration ;
- La possibilité de télécharger et d'installer des mises à jour incrémentielles, lorsque des mises à jour cumulatives sont disponibles, ce qui est utile pour optimiser le trafic ;
- La possibilité de reprendre le téléchargement de bases antivirus en cas de déconnexion, ou de changement du serveur de mise à jour. Après la reconnexion, le composant ne télécharge que les parties restantes des bases antivirus, plutôt que de recommencer l'opération depuis le début ;
- Les bases antivirus sont rechargées automatiquement après une mise à jour réussie ;
- La possibilité de restaurer la version précédente de la base antivirus ;
- Le nouveau composant ne nécessite pas le programme wget pour fonctionner;
- Les ordinateurs du réseau local peuvent être mis à jour à partir d'un répertoire partagé sur un serveur Samba ou sur un ordinateur sous Microsoft Windows.

5.1.2. Configuration recommandée du composant *keepup2date*

De nombreux paramètres propres au composant *kavupdater* ne sont plus nécessaires, et il est conseillé de les supprimer du fichier de configuration manuellement. Cependant, même si autres options (adresse proxy, par exemple), n'ont aucun sens pour *keepup2date*, il convient de les recopier dans les nouvelles sections du composant.

Les paramètres qui ne sont plus nécessaire et doivent donc être supprimés se trouvent sous la section **[updater.options]** du fichier de configuration de l'application :

- **RandomServerOrder**– Option non disponible en raison de la modification de la procédure de sélection du serveur.
- **ReloadApplication**– Option remplacée par une autre plus générale permettant d'exécuter le script **PostUpdateCmd**.
- **ExtraWgetOptions**– le composant n'utilise plus *wget* comme programme externe.

- **ShowExternalCmdOutput**– Le nouveau composant n'exécute pas de commandes externes.

En outre, le nouveau composant n'utilise plus l'option **UpdateServersFile** dans la section **[path]**, parce que la liste des serveurs est maintenant mise à jour de manière dynamique.

Les bases antivirus peuvent être mises à jour de nombreuses manières. Nous allons les étudier en détail.

Pour configurer le logiciel afin de télécharger les mises à jour depuis l'un des serveurs Kaspersky Lab énumérés dans le composant keepup2date :

Affectez la valeur **Non** au paramètre **UseUpdateServerUrl** dans la section **[updater.options]**.

Pour configurer le logiciel afin de télécharger les mises à jour depuis un serveur choisi par l'utilisateur et terminer l'opération si ce serveur n'est pas disponible :

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

Pour configurer le logiciel afin de télécharger les mises à jour depuis un serveur choisi par l'utilisateur et, si ce dernier n'est pas disponible, d'essayer avec les serveurs énumérés dans le composant keepup2date :

Affectez la valeur **Yes** au paramètre **UseUpdateServerUrl** dans la section **[updater.options]**; tandis que le paramètre **UseUpdateServerUrlOnly** devrait avoir la valeur **Non**. En outre, le paramètre **UpdateServerUrl** doit contenir l'adresse du serveur de mises à jour.

5.1.3. Planification des mises à jour de la base antivirus avec cron

L'utilitaire cron permet de programmer automatiquement la mise à jour régulière de la base antivirus.

Tâche : programmer la mise à jour automatique de la base antivirus toutes les 3 heures. La sélection du serveur de mise à jour doit être aléatoire. Le processus *aveserver* doit être automatiquement redémarré après la mise à jour de la base de données. Seules les erreurs de mise à jour doivent être reportées dans le journal du système. Tenir un journal global de toutes les exécutions de tâches. Ne pas afficher d'informations sur console.

Solution : pour effectuer la tâche, procédez comme ceci :

1. Spécifiez les valeurs appropriées 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 règles du processus cron (**crontab –e**), et ajoutez la ligne suivante :

```
0 * 3/3 * * * /opt/kav/5.5/kav4mailservers
/bin/keepup2date
```

5.1.4. Mise à jour manuelle des bases antivirus

Vous pouvez utiliser à tout moment la ligne de commande pour lancer la mise à jour des bases antivirus.

Tâche : lancer la mise à jour des bases antivirus et rapporter le résultat dans le fichier */tmp/updatesreport.log*.

Solution : écrivez ce qui suit sur la ligne de commande :

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

Si vous devez mettre à jour la base antivirus sur plusieurs ordinateurs, il est peut-être préférable de télécharger et d'enregistrer cette base dans un répertoire partagé sur un serveur, puis de mettre à jour tous les autres ordinateurs à partir de ce répertoire, au lieu de procéder au téléchargement des fichiers séparément.

Tâche : configurer la mise à jour des bases antivirus à partir des fichiers du répertoire de partage réseau **/home/bases.** Si ce répertoire n'est pas disponible, ou s'il est vide, alors utiliser les serveurs de Kaspersky Lab pour la mise à jour. Enregistrer les résultats d'activité dans un fichier de rapport.

Solution : pour accomplir cette tâche :

1. Spécifiez les valeurs appropriées dans le fichier de configuration de l'application :

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

   (ou utilisez le paramètre de ligne de commande `-g /home/bases`)

2. Sur la ligne de commande, tapez :

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

5.1.5. Création d'un répertoire réseau pour les bases antivirus

Pour vous assurer de la distribution correcte des mises à jour des bases antivirus à partir du répertoire réseau vers les ordinateurs locaux, la structure du fichier du répertoire réseau doit être identique à celle des serveurs sources de Kaspersky Lab contenant les mises à jour. Cette section décrit la tâche de création d'un répertoire réseau.

Tâche : création d'un répertoire réseau utilisé comme source des mises à jours par les ordinateurs du réseau.

Solution : pour accomplir cette tâche :

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

   ```
   keepup2date -u rdir
   ```

où `rdir` est le chemin complet au dossier créé.

3. Donnez accès aux ordinateurs du réseau local à ce répertoire.

Tâche : préparer la mise à jour des bases antivirus à travers un serveur proxy.

Solution : pour effectuer la tâche, procédez comme ceci :

1. Affectez la valeur **Yes** au paramètre **UseProxy** dans la section **[updater.options]** du fichier de configuration.
2. Vérifiez que l'entrée **ProxyAddress** dans la section **[updater.options]** du fichier de configuration contient l'adresse du serveur proxy. L'adresse doit être spécifiée dans le format suivant : **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 encore :

1. Affectez la valeur **Yes** au paramètre **UseProxy** dans la section **[updater.options]** du fichier de configuration.
2. Spécifiez la variable d'environnement **http_proxy** dans le format suivant :
http://nom_utilisateur:mot_de_passe@adresse_ip:port. Notez que cette variable ne sera prise en compte que si le paramètre **UseProxy** dans la section **[updater.options]** est absent ou défini à **Yes**.

5.2. Protection antivirus du trafic de courrier du serveur

Le filtrage antivirus du courrier – entrant, sortant ou en transit – est la tâche centrale de Kaspersky Anti-Virus. Ce travail est la responsabilité du composant *smtpscanner*.

Ce composant protège les utilisateurs contre les messages de courrier infectés, il leur distribue des messages nettoyés et désinfectés, accompagnés de comptes-rendus sur chacune de ses vérifications.

Une option de filtrage supplémentaire en fonction du type de fichier joint permet de réduire la charge du serveur pendant le traitement du trafic de courrier.

D'autres fonctions de Kaspersky Anti-Virus sont décrites ci-dessous dans les tâches de protection du trafic.

Tous les paramètres du composant *smtpscanner* sont groupés dans les options **[smtpscan.*]** du fichier de configuration *kav4mailservers.conf*.

Les tâches de protection antivirus du courrier les plus communes sont examinées dans les sections suivantes.

N'oubliez pas que le composant *aveserver* doit être en exécution pour que l'analyse antivirus du trafic de courrier soit activée !

5.2.1. Distribution de messages nettoyés et désinfectés

Cette méthode de configuration de Kaspersky Anti-Virus est utile lorsque vous ne souhaitez pas diviser les utilisateurs en groupes d'expéditeurs et destinataires différents. Ceci est utile, par exemple, quand vous devez remettre uniquement des messages de courrier nettoyés et désinfectés pour tous les comptes du serveur.

Tâche :

- Analyser la totalité du trafic de courrier du serveur à la recherche de virus et nettoyer tous les messages infectés.
- Supprimer les messages infectés qu'il n'est pas possible de nettoyer.
- Remettre les messages désinfectés aux destinataires.
- Informer les expéditeurs, les destinataires et l'administrateur au sujet des messages désinfectés, supprimés, suspects et endommagés, ainsi que des messages qu'il n'est pas possible d'inspecter. Joindre les objets infectés non modifiés aux notifications pour l'administrateur.
- Enregistrer toutes les actions dans le fichier */tmp/report.log*.

Solution : pour accomplir cette tâche :

1. Définissez les paramètres suivants du groupe **[smtpscan.group:default]** :

```
[smtpscan.group:default]
Check=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Les paramètres **Sender***, **Recipient*** et **Admin*** définissent les règles de traitement pour tous les types d'objets, à l'exception de ceux avec le statut **Clean**. Toutes les règles définies pour un objet précis ont la priorité la plus haute. Ainsi, dans cet exemple, tous les types d'objets seront supprimés des courriers des destinataires (**RecipientAction=remove**), sauf si l'objet est **Cured** (**CuredRecipientAction=cured**).

2. Activer le journal des résultats d'activité du composant dans le fichier */tmp/report.log* :

```
[smtpscan.report]
ReportOk=yes
ReportFileName=/tmp/report.log
ReportFilePermission=0660
```

5.2.2. Distribution des messages infectés

Il existe des situations où il est nécessaire de remettre tous les messages à un certain groupe d'utilisateurs, y compris les messages infectés.

Tâche :

- Analyser la totalité du trafic de courrier.
- Nettoyer tous les messages infectés adressés à tous les utilisateurs, sauf à ceux compris dans le groupe **urgent**.
- Nettoyer les messages impossibles à désinfecter, ainsi que ceux suspects et endommagés, au répertoire de Quarantaine pour tous les utilisateurs saufs pour ceux qui font partie du groupe **urgent**.
- Informer les expéditeurs, les destinataires et l'administrateur au sujet des messages bloqués, désinfectés, supprimés, suspects et endommagés, ainsi que des messages qu'il n'est pas possible d'inspecter. Joindre les objets infectés non modifiés aux notifications pour l'administrateur.
- Remettre tous les courriers, y compris ceux qui sont infectés, aux destinataires du groupe **urgent**, avec notification obligatoire en cas de possible infection par un virus.

Pour accomplir cette tâche :

1. Spécifiez les paramètres de configuration suivants pour le groupe **[smtpscan.group:default]** :

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
```

```
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

2. Configurez le groupe **[smtpscan.group:urgent]** de la manière suivante :

```
[smtpscan.group:urgent]
Check=yes
Quarantine=no
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=unchanged
```

5.2.3. Distribution des messages contenant des fichiers d'archives protégés par un mot de passe

Les messages de courrier contiennent souvent en pièce jointe un fichier d'archive protégé par mot de passe. Kaspersky Anti-Virus ne désinfecte pas les fichiers contenus dans les archives. Par conséquent, l'application transfère sans les analyser les archives protégées par un mot de passe. Dans ce cas, un message de l'antivirus est émis, pour indiquer que le fichier d'archive n'a pas été analysé. Cette notification est ensuite envoyée au destinataire et à l'administrateur.

Pour désactiver les notifications concernant les archives non analysées :

- Affectez la valeur **no** au paramètre **ProtectedRecipientAttachReport** dans la section **[smtpscan.group:default]** du fichier de configuration de l'application. Ceci désactivera l'envoi de notifications aux destinataires.

- Affectez la valeur **no** au paramètre **ProtectedAdminNotify** dans la section **[smtpscan.group:default]**. Ceci désactivera l'envoi de notifications à l'administrateur du groupe.

5.2.4. Blocage de la distribution des messages aux destinataires

Normalement, l'administrateur doit bloquer la distribution de certains messages. Une situation de ce type apparaît lorsqu'un message de courrier contenant des informations importantes est suspecté d'infection par un virus. La désinfection pourrait entraîner la perte de ces données. Dans cette situation, le message doit être mis à l'écart et, par exemple, envoyé aux experts de Kaspersky Lab pour son analyse.

Tâche :

- Analyser la totalité du trafic de courrier du serveur à la recherche de virus et nettoyer tous les messages infectés.
- Bloquer la distribution de messages infectés, suspects, endommagés et protégés par mot de passe, y compris ceux qu'il n'est pas possible d'analyser.
- Remettre uniquement des messages sains ou désinfectés aux destinataires.
- Informer les expéditeurs, les destinataires et l'administrateur au sujet des messages désinfectés, supprimés, suspects et endommagés, ainsi que des messages qu'il n'est pas possible d'inspecter. Joindre les objets infectés non modifiés aux notifications pour l'administrateur.

Solution : pour accomplir cette tâche :

Définissez les paramètres suivants dans le fichier de configuration *kav4mailservers.conf* :

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
```

```
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

5.2.5. Filtrage complémentaire en fonction des types de pièces jointes

Très souvent, les messages de courrier possèdent des pièces jointes qui ont de bonnes chances de contenir un virus (des fichiers exe, par exemple). Afin d'éviter l'infection, il est conseillé de filtrer le courrier d'après le nom ou le type de ces objets, et de bloquer les pièces jointes dans un répertoire séparé pour son analyse postérieure.

Par ailleurs, il existe des objets qui ne peuvent pas être infectés. Pour réduire la charge du serveur pendant le traitement antivirus des messages de courrier, nous recommandons de détecter à l'avance ces fichiers d'après leur type ou leur nom et de les mettre à part pendant la vérification du courrier.

Tâche :

- Pour le groupe **utilisateurs** :
  - Analyser les messages électroniques du groupe.
  - Filtrer tous les fichiers .exe joints aux messages de courrier. Placer en quarantaine les fichiers mis à part dans un répertoire spécial.
  - Nettoyer tous les messages infectés. En cas d'échec de désinfection d'un objet, le supprimer du message, mais le remettre sans modification à l'administrateur de groupe.

- Informer l'administrateur du groupe et les destinataires des objets bloqués.
- Informer l'administrateur, les expéditeurs et les destinataires au sujet des objets infectés, endommagés et protégés par mot de passe, ainsi que des messages qu'il n'est pas possible d'analyser.

- Pour tous les autres destinataires :
  - Analyser la totalité du trafic de courrier et nettoyer tous les messages infectés.
  - Mettre en quarantaine les messages infectés qu'il n'est pas possible de nettoyer, les messages et objets suspect et endommagés, ainsi que tout objet qu'il n'est pas possible d'analyser.
  - Remettre les messages désinfectés aux destinataires.
  - Remettre les fichiers protégés par mot de passe aux destinataires, avec notification en cas de possible infection par un virus.
  - Informer les expéditeurs, les destinataires et l'administrateur au sujet des objets infectés ou endommagés, des messages bloqués ainsi que des messages qu'il n'est pas possible d'analyser. Joindre les objets non modifiés, de tous types, aux notifications pour l'administrateur.

Pour effectuer la tâche, procédez comme ceci :

1. Spécifiez les paramètres de configuration suivants pour le groupe **[smtpscan.group:utilisateurs]** :

```
[smtpscan.group:utilisateurs]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
```

```
RecipientAction=remove
FilterName=*.exe$
FilteredQuarantine=yes
FilteredRecipientNotify=yes
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
ProtectedRecipientNotify=yes
ProtectedRecipientAction=unchanged
ProtectedRecipientAttachReport=no
ProtectedSenderNotify=no
ProtectedAdminNotify=no
```

2. Spécifiez les paramètres de configuration suivants pour le groupe **[smtpscan.group:default]** :

```
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
AdminAddress=admin2@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=no
RecipientAction=remove
ProtectedRecipientNotify=yes
ProtectedRecipientAttachReport=yes
ProtectedRecipientAction=unchanged
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Reportez-vous à la section6.1.1 à la page 62 sur la création de groupes d'utilisateurs.

5.3. Protection antivirus des systèmes de fichiers

La protection antivirus des systèmes serveurs de fichiers est assurée par le composant *kavscanner* qui analyse la présence de virus dans les fichiers de l'ordinateur, et traite les fichiers infectés ou suspects en fonction de sa configuration. Le traitement des objets peut se faire à titre d'information (sortie d'informations dans un rapport, sur la console du serveur, ou adressée à l'administrateur), ou en modifiant l'objet (désinfection, déplacement vers la quarantaine ou suppression).

Tous les paramètres du composant *kavscanner* figurent groupés dans les options de la section **[scanner.*]** du fichier de configuration *kav4mailservers.conf*.

Le lancement de l'analyse à la demande du système serveur de fichiers peut se faire depuis la ligne de commande, ou être déclenché par l'utilitaire standard **cron**. Il est possible de préciser l'étendue du système de fichiers à analyser, que ce soit l'ensemble du système de fichiers, ou des répertoires ou des fichiers individuels.

Les sections suivantes décrivent en détail les tâches les plus habituelles associées à la protection du système de fichiers du serveur.

La vérification antivirus de l'ensemble du serveur est consommatrice de ressources. Tenez compte du fait qu'au cours de la vérification, les performances générales du serveur diminuent : il n'est donc pas conseillé de lancer d'autres processus en même temps. Pour éviter ces problèmes, il est conseillé d'analyser des répertoires individuels, à la place.

5.3.1. Analyse à la demande

Kaspersky Anti-Virus permet l'analyse et la désinfection de fichiers dans des répertoires précis.

Tâche : lancer une analyse récursive du répertoire **/tmp**, en désinfectant automatiquement tous les objets infectés. Les objets dont la désinfection échoue devront être supprimés.

Les résultats du travail du composant (date d'exécution, informations détaillées sur tous les fichiers sauf ceux qui ne contiennent pas de virus) doivent être conservés dans un fichier de rapport *kavscanner-<date_courante>-pid.log*, dans le même répertoire.

Solution : pour effectuer cette tâche, indiquez ce qui suit sur l'invite de commande :

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

Si l'analyse révèle la présence d'un objet infecté à l'intérieur d'un fichier d'archive, c'est tout le fichier d'archive qui sera supprimé.

5.3.2. Planification d'une analyse de répertoires quotidienne (cron)

L'utilitaire standard de planification sous Unix, **cron**, permet de programmer l'exécution automatisée de n'importe quelle tâche Kaspersky Anti-Virus, y compris l'analyse régulière d'un répertoire spécifié.

Tâche : programmer une analyse antivirus quotidienne, pour démarrer à 0:00 heures, sur le répertoire **/home**, avec la configuration définie dans le fichier de configuration */etc/kav/kavscanner.conf* .

Solution : pour accomplir cette tâche :

1. Créer le fichier de configuration */etc/kav/kavscanner.cron* avec tous les paramètres d'analyse requis.
2. Modifiez le fichier où sont définies les tâches du processus **cron**: tapez **crontab –e** sur la ligne de commande et ajoutez la ligne suivante :

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

5.3.3. Options avancées : utilisation de fichiers de script

Kaspersky Anti-Virus permet d'appliquer un traitement supplémentaire aux objets soumis à l'analyse antivirus, à l'aide des différentes commandes standard Unix et de scripts. Ces outils permettent à des administrateurs expérimentés d'élargir les fonctions de Kaspersky Anti-Virus en définissant des actions à appliquer sur des objets, en fonction de leurs différents états.

5.3.3.1. Nettoyage d'objets infectés dans les fichiers d'archives

L'analyse de fichiers d'archives implique, pour pouvoir les utiliser, que les logiciels archiveurs soient installés !

Kaspersky Anti-Virus ne désinfecte pas les fichiers compressés infectés ; il se limite à détecter des objets suspects ou infectés dans ces archives. Cette capacité peut cependant être implémentée à l'aide de scripts supplémentaires, par exemple, le script *vox.sh* utilisé pour la désinfection de fichiers d'archives *tar*, *rar*, *tgz* et *zip*, qui accompagne le paquet de distribution de Kaspersky Anti-Virus.

Tâche : analyser tous les fichiers d'archives *tar* et *zip* accessibles sur un serveur et tenter la désinfection de tous les objets infectés qu'ils contiennent, à l'aide du script *vox.sh* script. Utiliser /etc/kav/*kavscanner.conf.in* comme fichier de configuration, dans lequel indiquer le script de désinfection des archives, avant de lancer la procédure d'analyse.

Dresser la liste de tous les objets infectés, avec leur chemin complet, dans le fichier */tmp/infected_archive.lst*. Enregistrer un rapport sur l'activité du composant dans le fichier */tmp/logfile.log*.

Solution : pour effectuer la tâche, procédez comme ceci :

1. Créez un fichier alternatif *kavscanner.conf.in* .
2. Définissez les règles de traitement des objets infectés, en ajoutant la ligne suivante dans la section **[scanner.container]** du fichier :

```
OnInfected=exec
/opt/kav/5.5/kav4mailservers./contrib/vox.sh
%FULLPATH%/%FILENAME%
```

3. Écrivez ce qui suit sur la ligne de commande :

```
# kavscanner -c kavscanner.conf.in -ePASE -qR
-o /tmp/logfile.log -j3
-pi/tmp/infected_archive.lst /
```

5.3.3.2. Courrier de notification à l'administrateur

Kaspersky Anti-Virus permet de configurer les outils standard Unix/Linux pour transmettre des notifications vers l'administrateur, à propos des objets infectés, suspects ou endommagés découverts dans les systèmes de fichiers du serveur.

Tâche : configurer la notification vers l'administrateur des fichiers et archives infectés découverts dans le système serveur de fichiers lors de chaque analyse, conformément aux paramètres définis dans le fichier de configuration de l'application.

Solution : pour effectuer la tâche, procédez comme ceci :

Spécifiez les règles de traitement d'objets simples ou d'objets conteneurs dans le fichier de configuration de l'application :

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% | mail -s kavscanner
admin@localhost.ru
[scanner.container]
OnInfected=exec echo le fichier %FULLPATH%/%FILENAME%
est infecté, la liste de virus se trouve dans le
fichier joint %LIST% | mail -s kavscanner -a %LIST%
admin@localhost.ru
```

5.3.4. Déplacement d'objets vers un répertoire séparé (quarantaine)

Il est possible de configurer Kaspersky Anti-Virus pour que tous les objets infectés, dans le système de fichiers du serveur soient placés dans un répertoire spécial.

Une telle approche est utilisée, au cours de l'analyse d'un répertoire, par exemple, lorsque l'infection d'un fichier contenant des données importantes est détectée. La désinfection pourrait entraîner la perte d'une partie des données,

c'est pourquoi une bonne solution consiste à isoler l'objet dans un répertoire spécial, avant de le transmettre à Kaspersky Lab pour analyse.

Si vous prévoyez de maintenir un répertoire de Quarantaine à l'intérieur du système de fichiers du serveur, nous vous conseillons de l'exclure explicitement des analyses ultérieures, en spécifiant son chemin complet dans le paramètre **ExcludeDir** du fichier de configuration de l'application.

Tâche : analyser tous les objets répertoriés dans le fichier */tmp/download.lst*, déplacer les objets infectés détectés, avec leur chemin complet, vers le répertoire */tmp/infected*. Utiliser l'analyseur de code heuristique. Désactiver l'analyse récursive. Enregistrer des informations sur les objets infectés, suspects ou endommagés dans le fichier de rapport.

Solution : pour effectuer la tâche, procédez comme ceci :

1. Les actions à appliquer sur les objets infectés sont définies par la ligne suivante, ajoutée sous les sections **[scanner.objet]** et **[scanner.container]** du fichier de configuration :

   ```
   OnInfected=movePath /tmp/infected
   ```

2. Désactiver le mode de désinfection (**Cure=no**) s'il était activé.

3. Écrivez ce qui suit sur la ligne de commande :

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

S'il est nécessaire de restreindre l'accès au répertoire */tmp/infected* en lecture et en écriture uniquement, ceci peut être appliqué à l'aide des outils Unix standard (la commande **chmod**), en introduisant les modification suivantes à la structure des tâches :

Utilisez la ligne suivante pour ajouter la règle de traitement des fichiers infectés dans les sections **[scanner.objet]** et **[scanner.container]** du fichier de configuration de l'application :

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

5.3.5. Sauvegarde des objets traités

Si l'action par défaut spécifiée pour des fichiers infectés est la suppression, il existe un risque de perte d'informations importantes. Ce risque existe aussi

pendant l'analyse antivirus des données. Pour éviter ce cas de figure, Kaspersky Anti-Virus offre la possibilité de recopier ces fichiers dans un répertoire de sauvegarde. Le chemin complet de chaque objet est alors enregistré, afin de permettre sa restauration ultérieure, si nécessaire.

Avant de désinfecter ou de supprimer un objet, l'application peut être programmée pour enregistrer automatiquement une copie de cet objet dans un répertoire de sauvegarde, spécifié par le paramètre **BackupPath** dans la section **[scanner.path]**. De nouvelles copies du même objet dans la zone de sauvegarde remplacent donc les anciennes versions.

Notez que le mode de sauvegarde est désactivé par défaut et qu'aucun répertoire n'est défini pour les copies de sauvegarde. Pour activer le mode de sauvegarde, il faut spécifier ce chemin d'accès dans le fichier de configuration.

Après la suppression d'un objet dans le système de fichiers, sa copie de sauvegarde est conservée jusqu'à ce que l'administrateur la supprime à son tour.

5.4. Gestion de la clé de licence

Une clé de licence donne droit à utiliser l'application et contient toutes les informations concernant la licence acquise : type de licence, date de péremption, nombre d'utilisateurs ou volume de trafic autorisé (en fonction du type de licence), informations sur les revendeurs, etc.

Pendant la durée de validité, la licence vous donne droit à :

- support technique 24/24 ;
- mises à jour des bases antivirus toutes les heures ;
- mises à jour de l'application (correctifs) ;
- nouvelles versions de l'application (mises à niveau) ;
- communiqués immédiats sur les nouveaux virus.

Lorsque la licence expire, ces services sont automatiquement interrompus. Kaspersky Anti-Virus continuera d'analyser les systèmes de fichiers du serveur et le trafic de courrier, mais seules les bases antivirus disponibles à la date d'expiration de la licence pourront être utilisée, dès lors que la fonction de mise à jour n'est plus disponible. L'administrateur sera informé de la proximité de la date d'expiration.

Il est donc très important de vérifier régulièrement les informations sur la clé de licence et de la renouveler à temps.

5.4.1. Mécanisme de la licence

Kaspersky Anti-Virus 5.5 emploie une nouvelle technologie de gestion des droits. Au cours de l'installation sur un serveur, l'administrateur doit spécifier une liste de domaines pour lesquels l'application doit analyser le courrier. Des licences peuvent être émises :

- pour un certain volume de trafic analysé,
- pour un certain nombre de comptes d'utilisateurs protégés.

Dans le premier cas, le trafic autorisé inclura la quantité maximum de messages que l'application aura reçu. analysé et qui seront signalés par l'indicateur d'état **Clean** (autrement dit, qui ne contiennent pas de virus).

Dans le second cas, l'application considérera comme utilisateur autorisé tout expéditeur ou destinataire d'un message non infecté, analysé et traité par l'application.

L'application informera l'administrateur 14 jours avant expiration de la licence. La notification sera envoyée une fois par 24 heures et à chaque redémarrage de l'application.

Un mécanisme d'identification identique est utilisé en cas d'expiration de la licence et en cas de dépassement du volume de trafic autorisé.

Toutefois. si le volume de trafic dépasse de 10 % le volume autorisé, l'administrateur recevra la notification correspondante chaque fois que l'application détectera un message avec un autre état que l'indicateur **Clean**.

Le fonctionnement correct du mécanisme de licence nécessite les actions suivantes :

Définissez le paramètre **LicenseDomain** dans la section **[smtpscan.license]**. Ce paramètre détermine les masques de domaines (conformément au standard POSIX d'expressions régulières, ou « regexp ») y compris les utilisateurs avec licence. La valeur du paramètre doit inclure tous les domaines de courrier protégés par Kaspersky Anti-Virus. Les noms de domaines doivent être spécifiés au format regexp POSIX, sur une seule ligne, et séparés par des virgules.

Notez que le caractère "." possède une signification spéciale dans le format regexp POSIX, et doit donc s'écrire précédé du caractère "\".

5.4.2. Affichage des informations de licence

Les informations relatives aux clés de licence installées sont disponibles dans les comptes-rendus générés par les composants *kavscanner, kavmonitor* et *keepup2date*, qui chargent ces informations à chaque exécution.

En outre, Kaspersky Anti-Virus incorpore un composant spécial, le composant *licensemanager*, qui permet d'offrir des informations plus complètes sur les clés, en plus de données analytiques.

Par exemple, si vous avez acheté Kaspersky Anti-Virus avec une licence par VOLUME DE TRAFIC DE COURRIER, le composant *licensemanager* vous permettra de garder la trace du volume de trafic et vous informera de la quantité autorisée (en Mo) de trafic de courrier encore restant.

Vous pouvez également examiner des informations sur le volume de trafic traité pendant la journée (par heures) et savoir quand cette charge atteindra son maximum. Cette information peut être utile si, par exemple, vous rencontrez un problème avec l'application et souhaitez obtenir de l'assistance technique.

Si la licence d'achat de l'application est définie sur la base du NOMBRE D'UTILISATEURS, vous pouvez voir le nombre total d'utilisateurs autorisés par votre licence.

Toutes les informations précédentes peuvent être affichées sur la console du serveur.

Pour afficher les informations relatives à toutes les clés de licence installées,

tapez ce qui suit sur l'invite de commande :

```
licensemanager –s
```

Des informations comme les suivantes, sur les licences installées, sont affichées sur la console du serveur :

```
Kaspersky license manager Version 5.5
Copyright © Kaspersky Lab. 1998-2005.
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix Mail
Servers", expires 04-07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Unix Mail Servers
```

```
(licence per e-mail address)", expires 25-01-2004 in
234 days
```

Pour afficher les informations relatives à une clé de licence spécifique,

Tapez ce qui suit sur l'invite de commande :

```
licensemanager –k 0003D3EA.key
```

Des informations comme les suivantes sont affichées sur la console :

```
Kaspersky license manager Version 5.5
Copyright © Kaspersky Lab. 1998-2005.
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Unix Mail Servers", expires 04-07-2003 in 28 days
```

Pour afficher les informations sur le trafic de courrier autorisé ou sur le nombre d'utilisateurs protégés,

tapez ce qui suit sur l'invite de commande :

```
licensemanager –i
```

Des informations comme les suivantes sont affichées sur la console du serveur :

- Si la licence est définie sur la base du *NOMBRE D'UTILISATEURS* :

```
Kaspersky license manager for Linux. Version
5.5.0/RELEASE #68
Copyright © Kaspersky Lab, 1997-2005.
Portions Copyright © Lan Crypto

License users units : 5
Users units used : 0
Users units left : 5
```

- Si la licence fonctionne sur la base du *VOLUME DE TRAFIC DE COURRIER* :

```
Kaspersky license manager Version 5.5
Copyright © Kaspersky Lab. 1998-2005.
Daily trafic statistic(Bytes) :
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
License trafic units : 10 (MB)
Traffic units used : 0 (MB)
```

```
Traffic units left : 10 (MB)
```

Dans le cas de Kaspersky Anti-Virus avec licence par NOMBRE D'UTILISATEURS, une option supplémentaire est disponible pour vérifier à tout moment si un utilisateur est protégé, c'est à dire si ses messages entrants ou sortants sont soumis à un traitement antivirus.

Cette option est utile, par exemple, lorsque la licence est achetée pour un nombre important d'utilisateurs, et avant d'ajouter un nouvel utilisateur à la liste, pour vérifier si celui-ci est déjà inclus dans la liste de protection.

5.4.3. Renouvellement de la licence

Le renouvellement de votre licence d'utilisation de Kaspersky Anti-Virus vous permet de rétablir toutes les fonctions de l'application, y compris la mise à jour des bases antivirus et les autres services énumérés dans la section 5.3.5 à la page 54.

Pour prolonger la validité de votre licence d'utilisation de Kaspersky Anti-Virus, vous devez :

contacter la société qui vous a vendu l'application et acquérir un renouvellement de licence pour Kaspersky Anti-Virus.

ou encore :

renouveler la licence directement auprès de Kaspersky Lab, par un message envoyé au département commercial (sales@kaspersky.com), ou remplir le formulaire correspondant dans la section **E-Store→ Renew Your License** de notre site (www.kaspersky.com). Après réception du paiement, vous recevrez une clé de licence à l'adresse e-mail indiquée sur votre commande.

La nouvelle clé de licence doit être installée. Pour ce faire, copiez-la dans le répertoire réservé aux clés (spécifié par le paramètre **LicensePath** dans la section **[path]** du fichier de configuration), puis redémarrez l'ordinateur.

Après cela, nous vous conseillons de mettre à jour vos bases antivirus (voir section 5.1 à la page 35).

CHAPITRE 6. PARAMETRES AVANCES

Cette section décrit certains paramètres avancés des fonctions de Kaspersky Anti-Virus. À la différence des paramètres obligatoires du processus d'installation (voir Chapitre 4 à la page 26), sans lesquels le produit ne peut fonctionner, l'utilisation des paramètres avancés est au choix de l'administrateur : extension des fonctions d'application, et ajustements aux besoins spécifiques de votre activité.

6.1. Configuration de la protection antivirus du trafic de courrier

Pour l'analyse antivirus du courrier, les principaux critères dans le choix des règles de traitement de chaque message sont l'adresse de l'expéditeur et l'adresse du destinataire, ainsi que les paramètres du groupe dont ils font partie. Par conséquent, il est de la plus haute importance que leurs adresses figurent dans les groupes appropriés.

Le fait qu'un message appartienne ou pas à un certain groupe dépend de la présence dans le groupe des deux adresses, celles de l'expéditeur et du destinataire. L'application recherche ces deux adresses dans la liste d'adresses du groupe. Si la combinaison de ces deux adresses (expéditeur et destinataire) est détectée à l'intérieur du groupe soumis à analyse, le message est traité conformément aux règles de ce groupe.

Kaspersky Anti-Virus effectue le filtrage antivirus en fonction des paramètres spécifiés dans le fichier de configuration *kav4mailservers.conf*. Vous pouvez modifier ce fichier en local.
La présence d'une ligne avec une adresse de groupe dans un message est vérifiée par un **POSIX regex** (pour plus d'informations sur ce standard. reportez-vous à man 7 regex).

Par défaut, le fichier de configuration inclut le groupe **[smtpscan.group:default]**, qui définit les règles de traitement des messages de courrier. Au départ, le groupe ne contient pas de noms d'expéditeurs ni de destinataires, et les règles décrites s'appliquent à tous les messages. Vous pouvez modifier les paramètres du groupe **default**, ou créer d'autres groupes.

Si d'autres groupes sont ajoutés au fichier de configuration (voir section 6.1.1 à la page 62), alors la séquence des traitements de messages est le suivant :

1. L'application vérifie si les adresses des messages appartiennent aux groupes définis par l'administrateur. Si les adresses du message appartiennent à celle d'un utilisateur du groupe, le message sera traité conformément aux règles définies par les paramètres de ce groupe.

   Si les adresses de l'expéditeur et du destinataire du message appartiennent à plusieurs groupes, le logiciel utilisera les paramètres de la première adresse.

2. Si ces adresses n'appartiennent à aucun groupe d'adresses défini par l'administrateur, les messages seront traités conformément aux règles spécifiées dans le groupe **default**.

Figure 5 illustre la séquence des actions prises par Kaspersky Anti-Virus concernant les messages de courrier reçus.

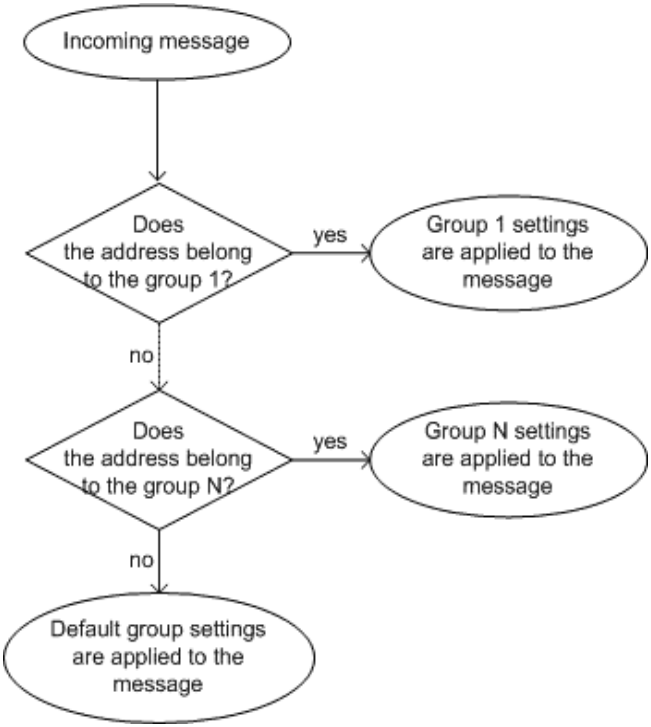

Figure 5. Traitement des messages de courrier

6.1.1. Constitution de groupes d'utilisateurs

Par défaut, le fichier de configuration de Kaspersky Anti-Virus contient le groupe **[smtpscan.group:default]**, qui comprend tous les expéditeurs et destinataires du serveur. Il utilise les règles suivantes de traitement des messages :

- Analyser tous les messages.
- Nettoyer les fichiers infectés qui ont été détectés.
- Ne distribuer que des messages de courrier nettoyés et désinfectés.
- Les messages impossibles à désinfecter, ainsi que ceux suspects, endommagés ou protégés par mot de passe, et ceux qu'il n'est pas possible d'analyser seront remis uniquement à l'administrateur de groupe.
- Informer les expéditeurs, les destinataires et l'administrateur du groupe au sujet des messages infectés, nettoyés, suspects, endommagés et protégés par mot de passe, ainsi que des messages qu'il n'est pas possible d'analyser.

Si vous souhaitez que Kaspersky Anti-Virus traite les messages de courrier adressés à différents expéditeurs et destinataires, en leur appliquant des règles différentes, vous devrez créer des groupes.

Pour créer un nouveau groupe d'utilisateurs :

1. Dans le fichier de configuration, créez une section **[smtpscan.group:<nom_groupe>]**.
2. Inscrivez les adresses, ou les masques d'adresses, des destinataires et des expéditeurs qu'il faut inclure dans le groupe. Pour ce faire, renseignez les paramètres **Senders** et **Recipients**, par une liste de valeurs séparées par des virgules.

La syntaxe **POSIX regex** standard est utilisée pour définir les masques. À partir du second masque, il convient de séparer les masques par des virgules.

Si vous ne définissez pas de valeur dans l'un des paramètres **Recipients** OU **Senders**, celui-ci sera automatiquement interprété comme **.*@.***

Dans la version 5.5 of Kaspersky Anti-Virus, le groupe **kavadministrators** a été saisi dans le fichier de configuration. Au cours de l'installation, le programme d'installation ajoute automatiquement au groupe toutes les adresses des administrateurs énumérées dans le répertoire /var/qmail/alias/postmaster.

Dans certains cas, lorsque l'adresse d'un administrateur est modifiée par la suite (paramètre **AdminAddress** dans la section **[smtpscan.group:default]** ou dans un autre groupe), la nouvelle adresse de l'administrateur et toutes les autres adresses qui l'utilisent sous forme d'alias doivent être ajoutées à la liste des valeurs du paramètre **Recipients** du groupe **[smtpscan.group:kavadministrators]**.

Cette procédure est importante si le système est configuré pour transmettre les messages infectés à l'administrateur,

6.1.2. Mode d'inspection et de désinfection de messages

La modalité de recherche de virus dans le trafic de courrier d'un certain groupe d'expéditeurs/destinataires doit être activée par l'administrateur du serveur, dans les paramètres du groupe.

Pour ce faire, renseignez le paramètre **Check=yes** dans le fichier de configuration *kav4mailservers.conf* du groupe en question.

Quand le mode de vérification est activé, tous les messages de courrier qui se rapportent au groupe, d'après le critère des adresses expéditeur/destinataire, sont analysés par Kaspersky Anti-Virus. Cependant, les messages infectés ne seront pas nettoyés.

Pour *ACTIVER LE MODE DE RÉPARATION* des messages infectés, il est nécessaire de spécifier dans le groupe aux moins un paramètre pour les objets à désinfecter (**Cured**). Par exemple, si parmi les autres paramètres du groupe vous spécifiez :

```
[smtpscan.group:compta]
Check=yes
CuredRecipientNotify=yes
```

Les résultats seront les suivants :

- Tous les messages pour le couple expéditeurs/destinataires présents dans le groupe **compta** seront analysés à la recherche de virus.
- Tous les objets infectés qui sont détectés sont nettoyés.

- Les destinataires recevront les notifications appropriées sur les objets désinfectés.

6.1.3. Actions sur les messages de courrier

Les deux facteurs suivants déterminent les actions à appliquer sur les messages :

- L'état attribué à l'objet après son analyse (voir section 6.2.2 à la page 69).
- L'action définie en fonction de l'indicateur d'état de l'objet dans le fichier de configuration.

L'état de l'objet est donné par le processus *aveserver* immédiatement après son analyse antivirus. L'action à appliquer à l'objet après son analyse est définie par l'administrateur du serveur.

Kaspersky Anti-Virus® permet de définir des actions sur les messages de courrier remis aux destinataires et à l'administrateur de groupe. Dans le cas des expéditeurs, UNIQUEMENT les notifications peuvent être définies.

Vous pouvez définir l'une des actions suivantes sur les objets messages :

Remove– Supprime l'objet dans le message.

Unchanged– Laisse l'objet inchangé. Dans ce cas, l'objet indiqué ne sera pas nettoyé et il sera distribué sous sa forme originale.

Cured– Ne distribuer que des objets désinfectés.

Des actions communes peuvent être définie pour tous les types d'objets, ou séparément, pour chacun des types.

Pour définir des actions communes à tous les types d'objets :

Définissez les valeurs respectives des paramètres **AdminAction** et **RecipientAction**. Ces paramètres définissent des actions applicables à tous les types d'objets. Par exemple :

```
AdminAction=unchanged
RecipientAction=remove
```

Tous les messages du groupe seront remis sans modifications à l'administrateur du groupe, mais ils seront supprimés dans les messages aux destinataires.

Si vous souhaitez définir des actions individuelles selon les types d'objets différents :

Spécifiez les actions souhaitées dans les paramètres **<type_objet>AdminAction** et **<type_objet>RecipientAction**.

Par exemple,

```
AdminAction=unchanged
RecipientAction=remove
CuredRecipientAction=cured
```

Dans ce cas, tous les messages, sans tenir compte du type d'objet, seront remis sans modifications à l'administrateur du groupe, tandis que le destinataire ne recevra que des messages désinfectés. Tous les autres types d'objets seront supprimés des messages.

En plus des actions précédentes, l'application peut **déplacer des objets vers le répertoire de quarantaine**.

Pour déplacer des objets de courrier dans le répertoire de quarantaine :

Définissez les paramètres suivants dans le fichier de configuration du groupe :

```
QuarantinePath=/var/db/Quarantine
Quarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
```

6.1.4. Notifications aux expéditeurs, destinataires et administrateurs

Kaspersky Anti-Virus permet à l'utilisateur de définir des notifications (y compris le mode d'envoi, les paramètres de génération et le texte lui-même) adressées aux expéditeurs, aux destinataires et aux administrateurs de groupe, en fonction d'objets avec n'importe quel indicateur d'état (suspect, infecté, nettoyé, endommagé, etc.) **L'envoi des notifications** est contrôlé par les paramètres de configuration suivants :

- **RecipientNotify**– Envoi de notification au destinataire du message.

- **SenderNotify**– Envoi de notification à l'expéditeur du message.
- **AdminNotify**– Envoi de notification à l'administrateur de groupe.

Ces paramètres définissent le mode d'envoi des notifications selon l'état des objets. Si vous voulez définir des notifications émises pour des objets avec un état donné, activez les modes suivants :

- **<etat_objet>RecipientNotify**
- **<etat_objet>SenderNotify**
- **<etat_objet>AdminNotify**.

Dans ce cas, la notification n'est envoyée que pour les objets avec l'état spécifié.

Par exemple, si vous indiquez le paramètre suivant dans le groupe :

```
InfectedRecipientNotify=yes
CuredRecipientNotify=yes
CorruptedRecipientNotify=yes
SenderNotify=yes
AdminNotify=yes
```

Les notifications seront envoyées à l'administrateur et à l'expéditeur pour des objets de tout type, et au destinataire, uniquement pour des objets infectés, nettoyés, et endommagés.

Afin d'envoyer des notifications, il faut aussi spécifier l'adresse d'expédition (paramètre **NotifyFromAddress** dans la section **[smtpscan.general]**).

Par défaut, Kaspersky Anti-Virus active des notifications pour les objets de n'importe quel état. Toutes ces notifications contiennent un **texte générique** construit sur le modèle */etc/kav/5.0/template_notify_main* présent dans le kit de distribution.

Si vous souhaitez modifier le texte de la notification, vous pouvez soit :

- Modifier le texte du modèle qui accompagne le logiciel.
- Créer un nouveau fichier de modèle et en le chemin complet dans le paramètre **Template** dans la section **[smtpscan.notify]**.

Dans le texte du modèle, vous pouvez utiliser les macros suivantes, qui seront remplacées par leurs valeurs respectives, en fonction de la réponse du processus *aveserver* :

%VERSION% – Version de Kaspersky Anti-Virus .

%SENDER%– Adresse de l'expéditeur du message.

%RECIPIENT%– Liste de tous les destinataires de messages, séparés par un caractère de saut de ligne (LF, line-feed).

%MSGID%– Numéro Id. du message.

%VIRUSNAME%– Texte descriptif du problème. Vous pouvez traduire ce texte dans n'importe quelle langue en précisant les lignes correspondantes à chaque état des objets dans la section **[locale]**.

%SUBJECT%– Insère le contenu du champ Sujet du message de courrier original.

%DATETIME%– Date et heure de traitement du message. La mise en forme de l'heure et de la date est également modifiable.

%HEADERS%– Tous les en-têtes d'origine du message seront ajoutés au texte.

%ACTION% – Description des actions effectuées sur les pièces jointes du message. La macro est utilisée dans tous les modèles, sauf pour les notifications adressées aux expéditeurs des messages. Vous avez le choix entre :

`attachement not modified` – la pièce jointe reste inchangée.

`attachement cured` – la pièce jointe était infectée et la désinfection a réussi.

`attachment removed` – la pièce jointe a été supprimée.

`attachments cured and removed` – les pièces jointes étaient infectées, certaines ont été désinfectées et distribuées au destinataires, d'autres ont été supprimées.

Ces macros sont utilisables pour la création des sujets de messages.

Les **paramètres de génération des notifications** (type MIME, sujet de message, jeu de caractères, etc.) sont regroupés sous la section **[smtpscan.notify]** du fichier de configuration.

6.2. Configuration de la protection antivirus des systèmes de fichiers serveurs

Tous les paramètres de protection des systèmes de fichiers du serveur peuvent être divisés par groupes permettant de définir :

- Zone d'analyse (voir section 6.2.1 à la page 68).
- Analyse de fichiers et mode de désinfection (voir section 6.2.2 à la page 69).

- Opérations sur fichiers (voir section 6.2.3 à la page 70).
- Paramètres des rapports d'activité de l'application (voir section 6.5 à la page 74).

Les sections suivantes décrivent chacun de ces groupes de paramètres l'un après l'autre.

6.2.1. Zone d'analyse

Pour plus de commodité, la zone d'analyse peut être divisée en deux parties :

- *chemin d'analyse* liste des répertoires et fichiers cibles de l'analyse antivirus ;
- *objets d'analyse* types de fichiers qui seront analysés à la recherche de virus (fichiers d'archives, messages de courrier, etc.).

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

L'analyse de tous les systèmes de fichiers du serveur nécessite de s'identifier comme root, ou de spécifier la zone d'analyse **/** en tant que zone d'analyse.

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

- Indiquer la liste des répertoires et fichiers, en précisant leur chemin absolu ou relatif (au répertoire courant), directement sur la ligne de commande, séparés par des espaces, lors du démarrage du composant.
- Définir les chemins d'analyse dans un fichier texte, associés avec des commandes à utiliser, en utilisant la syntaxe **-@ <nom_archive>** sur la ligne de commande. Chaque objet dans ce fichier doit apparaître sur une ligne séparée, avec un chemin d'accès absolu.

  

  Si la ligne de commande contient à la fois un chemin à analyser et un fichier de texte avec une liste d'objets à analyser, l'application analysera uniquement les objets répertoriés dans le fichier. Il ignorera le chemin indiqué sur la ligne de commande.

- Il est possible de restreindre les chemins par défaut (tous commençants à partir du répertoire courant) ou répertoriés sur la ligne de commande, en utilisant les masques d'exclusion de répertoires et de fichiers de la zone d'analyse (paramètres **ExcludeMask** et **ExcludeDirs**, section **[scanner.options]**) du fichier de configuration.
- Désactiver *l'analyse récursive des répertoires* (section **[scanner.options]**, entrée **Recursion** ou paramètre **–r**).

- Créer un fichier de configuration alternatif, pour l'utiliser ensuite avec l'option **–c <nom_fichier>** sur la ligne de commande, au démarrage du composant

Les objets à analyser par défaut sont également définis dans le fichier de configuration *kav4mailservers.conf* (section **[scanner.options]**), et peuvent donc être redéfinis :

- directement dans ce fichier
- par des options sur ligne de commande au démarrage du composant
- lorsqu'un fichier de configuration alternatif est utilisé.

6.2.2. Analyse de fichiers et mode de désinfection

Ces paramètres sont essentiels pour l'analyse, car ils déterminent si l'application devra essayer de désinfecter les fichiers infectés.

Cette option est désactivée par défaut, ce qui signifie que l'application ne fait qu'analyser les objets puis informer de la découverte de virus et d'objets suspects ou endommagés, par des messages présentés sur la console et dans le rapport (voir section 6.5 à la page 74).

D'après le résultat de la procédure d'analyse, chaque objet se voit affecter l'un des états suivants :

- **Clean**– Aucun virus détecté.
- **Infected**– Le fichier est infecté.
- **Warning**– Le code de l'objet ressemble à celui d'un virus connu.
- **Suspicious**– Le fichier est suspecté d'être infecté par un virus inconnu.
- **Corrupted**– Le fichier est endommagé.
- **Protected**– Le fichier est protégé par mot de passe et ne peut pas être analysé.

Quand le mode de désinfection est activé (**section** [scanner.options], paramètre **Cure=yes**), seuls les fichiers avec l'état **Infected** sont soumis au traitement. Après la désinfection, un fichier se voit affecter l'un des états suivants :

- **Cured**– désinfection réussie du fichier.
- **CureFailed**– Échec de désinfection du fichier. Ce type de fichiers est traité conformément aux règles spécifiées pour les fichiers infectés.

6.2.3. Opérations sur des objets suspects ou infectés

Il est possible d'appliquer certaines actions aux fichiers en fonction de leur état (voir section 6.2.2 à la page 69). Par défaut, une notification n'est envoyée que pour des fichiers définitivement infectés. Ces messages de notification sont affichés sur la console et ajoutés au le fichier de rapport.

Cependant, il est possible de définir certaines actions pour des fichiers avec l'état **Infected**, **Suspicious**, **Warning** ou **Corrupted**, et de leur associer des actions comme :

- *transfert vers un certain répertoire*– déplacement des fichiers avec un certain état vers un répertoire *spécifié*, avec possibilité de transfert *normal* ou
- *suppression* du fichier du système de fichiers ;
- *exécution d'une certaine commande*– les fichiers sont traités à l'aide de commandes Unix standard, des fichiers de script, etc.

Dans le cas de fichiers de type **Protected** et **Cured**, l'application affiche uniquement une notification sur console et dans le rapport.

Il convient de noter que Kaspersky Anti-Virus fait la différence entre les objets simples (un fichier) et les objets composés (conteneur de plusieurs objets, un fichier d'archive, par exemple). Les actions correspondantes à ces objets sont également différentes ; elles figurent sous différentes sections dans le fichier de configuration. La section **[scanner.objet]** est consacrée à des objets simples, et la section **[scanner.container]** aux objets composés.

Différentes opérations sont possibles pour des fichiers auto-extractibles : si le conteneur est lui-même infecté, il est traité comme un objet simple ; mais si les objets qu'il contient sont eux-mêmes infectés, le conteneur est alors considéré comme un objet composé. Ces deux opérations séparées sur le fichier sont déterminées par des entrées sous des sections différentes du fichier de configuration

Vous choisissez les actions appliquées sur un fichier de l'une des manières suivantes :

- Définir ces actions dans le fichier de configuration de l'application, si elles sont supposées être des actions prédéfinies (sections **[scanner.object]** et **[scanner.container]**).

- Indiquer les actions dans un fichier de configuration alternatif, et utiliser ce dernier au démarrage du composant.
- Définir ces actions pour la session courante à l'aide de paramètres sur la ligne de commande, lors du lancement du composant *kavscanner.*

La syntaxe est la même pour les objets simples ou les conteneurs.

6.2.4. Copie de sauvegarde

Cette section présente la configuration du mode de sauvegarde, avec l'exemple de la tâche suivante.

Tâche : analyse antivirus de tous les objets à l'intérieur des répertoires et fichiers énumérés dans la liste */tmp/download.lst*, et les désinfecter. Si la désinfection échoue, déplacer les objets infectés avec leur chemin complet dans le répertoire **/tmp/infected**; déplacer les objets suspects sous **/tmp/suspicious**; envoyer des notifications à **/tmp/warning**.

Solution : pour accomplir la tâche, procédez comme ceci :

1. Créez un fichier de configuration alternatif : *scan_sample.conf*
2. Assurez-vous que le mode de désinfection est activé pour les objets infectés (**Cure=yes** dans la section **[scanner.options]**).
3. Définissez les règles de traitement des objets infectés. Pour ce faire, ajoutez l'entrée suivante aux sections **[scanner.objet]** et **[scanner.container]** du fichier de configuration *scan_sample.conf* :

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

4. Tapez ce qui suit sur l'invite de commande :

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

6.3. Optimisation de Kaspersky Anti-Virus

Kaspersky Anti-Virus propose plusieurs méthodes d'optimisation de son fonctionnement. Cette section les présente en détail.

6.3.1. Utilisation de la base de données iChecker

Pour éviter de recommencer sans cesse l'analyse des mêmes fichiers, l'application vérifie vérifiant si le fichier a été modifié entre deux analyses. L'algorithme d'analyse antivirus de l'objet (du fichier) est le suivant :

- Après la première analyse d'un fichier, des informations sur celui-ci (son nom et une somme de contrôle) sont enregistrées dans la base de données iChecker, qui conserve les données des fichiers **nettoyés**, parmi les formats reconnus par le composant *kavscanner*.
- Tous les accès ultérieurs de l'utilisateur sur un fichier provoquent que le nom de ce fichier soit d'abord recherché dans la base de données de iChecker. Le nom de fichier est utilisé comme critère de recherche. Si le fichier se trouve référencé dans la base de données de iChecker, son état actuel est comparé au celui conservé dans la base de données. Le fichier est considéré inchangé et ne sera pas analysé, par conséquent, dans la mesure où son état courant reste absolument identique aux informations conservées.

Si les données du fichier demandé sont introuvables dans la base de données iChecker ou dans le tampon, le fichier est analysé, et les bases de données sont mises à jour en fonction du résultat.

6.3.2. Réduction de la charge de travail du serveur

L'analyse du système serveur de fichiers peut exiger un temps considérable si le volume de données est important, et la charge de travail de l'unité centrale peut alors augmenter de manière significative. COMME LE SERVEUR doit continuer à assurer ses tâches courantes, et il est donc utile de suspendre l'analyse antivirus de l'ordinateur, au delà d'un certain seuil de charge de travail.

La version 5.5 de Kaspersky Anti-Virus possède un mécanisme de ce type. Le paramètre **MaxLoadAvg** a été ajouté dans ce but dans la section **[scanner.options]**. Si le paramètre est spécifié, *kavscanner* vérifie la charge de travail courante de l'unité centrale du serveur (sa **charge moyenne**) avant toute analyse d'un nouveau fichier. Si la valeur dépasse la valeur spécifiée dans le fichier de configuration, l'analyseur interrompt son travail jusqu'à ce que la valeur de **charge moyenne** revienne en dessous du seuil spécifié.

6.4. Configuration du processus *aveserver*

Comme indiqué précédemment, le traitement antivirus du trafic de courrier est assuré par deux composants (*aveserver* et *smtpscanner*) qui réagissent l'un en fonction de l'autre.

Aveserver est lancé au démarrage du système d'exploitation.

Une connexion avec *aveserver* est établie immédiatement après que *smtpscanner* accède au processus.

Le processus *aveserver* est contrôlé par les paramètres de la section **[aveserver.options]** du fichier de configuration *kav4mailservers.conf* :

Detach From Terminal– Le processus est déconnecté du terminal immédiatement après son démarrage. Ce mode devrait rester activé, car le démarrage du système ne reprendra pas avant la déconnexion du processus. Le mode est activé par défaut (sa valeur est **yes**). Le mode ne devrait être désactivé (valeur **no**) que lorsque le processus est contrôlé par un programme tel que **SVC**.

Startup Mode– Fait basculer le processus du mode interactif vers l'arrière-plan, à condition que **DetachFromTerminal=yes**. La valeur **fast** fait basculer le démon en arrière-plan immédiatement après le chargement du fichier de configuration, et retourne le code **0**. La valeur **normal** fait basculer le processus en arrière-plan uniquement après le chargement en mémoire des bases antivirus et des clés de licence.

La sensation de vitesse du lancement en mode **fast** est plus grande, mais il existe une probabilité pour que le démon échoue son chargement en raison d'une erreur fatale quelconque, sans que rien ne soit affiché sur la console.

Local Socket Permission – La valeur octale des permissions utilisées pour créer le socket. Par défaut **Local Socket Permission=0666**.

6.4.1. Rechargement du composant Aveserver

Le processus aveserver est automatiquement rechargé immédiatement après la mise à jour des bases antivirus, si la configuration appropriée figure dans le fichier de configuration.

Le processus est rechargé par la commande **kill –HUP <PID du processus>**. Après exécution, le processus reçoit le signal **SIGHUP**, puis le processus parent recharge le fichier de configuration, les clés de licence et les bases de données ou encore, si le chemin d'accès au fichier est incorrect, il se termine et sort en laissant le message correspondant dans le rapport. Toutes les connexions actives du processus avec les logiciels clients restent activées jusqu'à leur fermeture.

Ce rechargement du processus aveserver est nécessaire, par exemple, après avoir modifié le fichier de configuration, avoir ajouté une nouvelle clé de licence ou avoir mis à jour manuellement les bases antivirus.

6.4.2. Terminaison forcée du fonctionnement du processus *aveserver*

Si vous devez forcer la fin du processus aveserver, utilisez la commande **kill <PID du processus>**. La commande kill sera émise avec le signal **SIGTERM** au processus. Ce signal mettra fin aux opérations d'aveserver et refermera toutes les copies qu'il aura créées.

Nous vous déconseillons fortement d'utiliser la commande **kill –9** pour mettre fin aux opérations du processus aveserver. Cette commande mettra fin au processus, mais laisse ouverts un certain nombre de fichiers temporaires et de travail qu'il faudra supprimer manuellement. Certaines applications (comme Webmin) utilisent ces fichiers pour savoir si le processus se trouve en cours d'exécution.

6.5. Affichage régional de la date et de l'heure

Pendant son exploitation, Kaspersky Anti-Virus produit des rapports pour chaque composant, et génère diverses notifications à l'intention des utilisateurs et des administrateurs, qui sont toujours horodatées au fur et à mesure de leur émission.

Par défaut, Kaspersky Anti-Virus met en forme de l'heure et la date conformément aux formats utilisés par la fonction C strftime :

%H:%M:%S– mise en forme de l'heure.

%d/%m/%y– mise en forme de la date.

L'administrateur peut modifier la mise en forme de l'horodatage dans la section **[locale]** du fichier de configuration *kav4mailservers.conf*. Exemples de mises en forme possibles :

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

%y/%m/%d et **%m/%d/%y** – pour présenter la date (paramètre **DateFormat**) sous la forme année/mois/jour, ou mois/jour/année, respectivement.

6.6. Paramètres de tenue du rapport dans Kaspersky Anti-Virus

Les résultats d'activité de tous les composants de Kaspersky Anti-Virus sont enregistrés dans un fichier de rapport.

Les résultats du traitement antivirus des systèmes de fichiers du serveur sont également affichés sur la console. Par défaut, l'information ajoutée au rapport et celle affichée sur la console est la même. Pour différencier les informations sur console et dans le rapport, certains paramètres supplémentaires sont nécessaires (voir section 6.6.2 à la page 78 pour plus de détails).

Vous pouvez ajuster la quantité d'informations en modifiant le *niveau de détail du rapport*.

Le **niveau de détail** est un nombre qui définit le degré de détail des informations concernant l'activité des composants. Chaque niveau successif (en augmentant la valeur) ajoute ses propres informations à celles des niveaux inférieurs.

<Le tableau suivant répertorie tous les niveaux de détail possibles.

Niveau	Nom du niveau	Usage
	Erreurs fatales	Informations sur les erreurs critiques uniquement, celles qui interrompent le programme, en raison de l'exécution impossible d'une action. Par exemple, l'infection d'un composant de l'application ou l'échec d'une opération vitale, comme l'analyse, le chargement d'une base de données ou d'une clé de licence.
1	Erreurs	Informations sur d'autres erreurs, y compris celles qui n'interrompent pas le composant, comme l'échec de l'analyse d'un fichier.

Niveau	Nom du niveau	Usage
2	Avertissement	Informations d'erreurs pouvant interrompre le fonctionnement du produit (information sur un espace disque insuffisant, par exemple).
3	Info, Notice	Messages importants, par exemple : si le composant est en exécution, le chemin du fichier de configuration, la zone d'analyse, ou des renseignements sur la base antivirus, les clés de licence et les statistiques résultantes.
4	Activité	Comptes-rendus d'analyse des objets, conformément au niveau de détail défini pour le rapport d'analyse (voir section 6.6.1 à la page 77).
10	Debug	Toutes les informations de mise au point, par exemple, le contenu du fichier de configuration.

Des informations sur les erreurs fatales de fonctionnement sont rapportées, sans tenir compte du niveau de détail. Le niveau de détail optimum est **4**, qui est la valeur par défaut.

Le format général de sortie pour tous les niveaux de détail précédents est le suivant :

```
[date heure niveau_détail] CHAINE
```

où :

`[date heure niveau_détail]` est l'horodatage généré par le système (avec la mise en forme définie par l'administrateur) et le niveau de détail du rapport (première lettre du niveau de détail).

La mise en forme de l'heure et de la date peut être modifiée sous la section **[locale]** du fichier de configuration *kav4mailservers.conf*

`STRING`– Une ligne du rapport, qui peut prendre différentes mises en forme selon le type de messag. Les types de messages suivants existent :

- Comptes-rendus d'analyse (voir section 6.6.1 à la page 77).
- Autres messages (démarrage d'un composant, chargement de la base antivirus, codes de retour, etc.).

- Messages affichés sur la console (voir section 6.6.2 à la page 78).

Voici une description détaillée des types et des mises en forme de chaque message.

6.6.1. Format de comptes-rendus d'analyse

Les comptes-rendus d'analyse ne sont générés que pour les composants *kavscanner* et *aveserver*.

La mise en forme des comptes-rendus d'analyse d'un fichier dépend du type d'objet (simple ou conteneur) auquel il correspond.

Pour un objet simple, les messages de l'analyse ressemblent à ceci :

- Format de message étendu (**ShowObjectResultOnly=no**) :

  `"nom_archive" resultat [nom_virus]`

- Format de message court (**ShowObjectResultOnly=yes**) :

  `"nom_archive" resultat`

  où :

  `nom_virus`– nom du virus associé aux événements CURED, INFECTED, CUREFAILED, WARNING et SUSPICIOUS. Le champ reste vide pour les autres événements.

  `resultat` – Indicateur d'état attribué au fichier après analyse et désinfection. Une liste complète des résultats possibles est fournie dans le tableau suivant.

Pour les objets composés (fichiers d'archives) il existe également des formats courts ou étendus de messages :

- Format de message étendu (**ShowContainerResultOnly=no**) :

  ```
  "nom_archive"
  "nom_archive" resultat [nom_virus]
  "nom_archive" resultat [nom_virus]
  ```

- Format de message court (**ShowContainerResultOnly=yes**) :

  `"nom_archive" resultat`

Événement/Résultat	Valeur
Ok	Le fichier n'est pas infecté.
CURED (uniquement si le mode de désinfection est actif)	Le fichier était infecté et le nettoyage a réussi.
INFECTED	Le fichier est infecté par un ou plusieurs virus. Désinfection non demandée.
CUREFAILED (uniquement si le mode de désinfection est actif)	Le fichier est infecté par un ou plusieurs virus. Désinfection demandée, mais l'opération a échoué.
WARNING	Le code du fichier ressemble à celui d'un virus connu.
SUSPICIOUS	Le fichier est suspecté d'infection par un virus inconnu.
ERROR	Vérification impossible du fichier pour cause d'erreur (par exemple, traitement sur un fichier d'archive endommagé)
PROTECTED	Vérification impossible : fichier chiffré.
CORRUPTED	Le fichier est endommagé.

6.6.2. Format des messages de console

Des messages sont affichés sur la console par les composants *kavscanner* et *keepup2date*.

La sortie console du composant *kavscanner* est gouvernée par la présence du paramètre **–q** (quiet) sur la ligne de commande, lors du lancement du composant. Si l'option est utilisée, les informations ne seront pas affichées sur la console. La sortie sur console de messages sur l'activité du composant *keepup2date* est activée dans le fichier de configuration par le paramètre **KeepSilent=no.**

Par défaut, la mise en forme et le contenu des informations affichées à l'écran sont exactement les mêmes que ceux enregistrés dans le fichier de rapport.

Il est possible de configurer le contenu des informations envoyées sur la console par le composant *kavscanner* en ajoutant la section **[display]** dans le fichier de configuration (*kav4mailservers.conf* ou son remplaçant).

Dans cette section, les paramètres déterminent s'il faut afficher des informations sur l'analyse des objets à l'intérieur de l'archive archive (**ShowArchiveContent**, **ShowContainerResultOnly**), sur les objets non infectés (**ShowOK**), et sur les comptes-rendus de l'activité courante du composant (**ShowProgress**).

Le niveau de détail du rapport d'analyse est défini par le paramètre **–x<option>** sur la ligne de commande, à condition que la section **[display]** soit présente.

6.6.3. Statistiques antivirus de l'application

La version 5.5 de Kaspersky Anti-Virus 5.5 dispose d'une fonction permettant de collecter et d'examiner des statistiques d'activité virale pendant une période déterminée. Cette fonction est disponible à travers l'interface Web proposée par Webmin.

Pour mettre en place la récupération automatique des statistiques de l'antivirus,

- Affectez la valeur ci-dessous au paramètre **AVStatistics** dans la section **[smtpscan.report]** du fichier de configuration de l'application :

```
AVStatistics=
/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- Exécutez le script de récupération des statistiques à partir du fichier de rapports à intervalles réguliers, au besoin. Pour ce faire, tapez ce qui suit sur l'invite de commande :

```
perl /usr/libexec/webmin/kavms5.5/parse_avstat.pl \
-sd=/var/db/kav/5.5/kav4mailservers/proc_avstat\
/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- Examinez dans Webmin les informations statistiques mises à jour, uniquement après avoir exécuté le script précédent.

Si Webmin est installé sur un chemin différent de la valeur par défaut, il faut aussi modifier en conséquence le chemin /usr/libexec/webmin/kavms5.5/parse_avstat.pl !

CHAPITRE 7. DESINSTALLATION DE KASPERSKY ANTI-VIRUS

La procédure pour désinstaller Kaspersky Anti-Virus est la suivante :

- Des privilèges de super-utilisateur (**root**). Si vous ne disposez pas de ces privilèges au moment de la désinstallation, ouvrez une session sur le système en tant qu'utilisateur **root** .
- Fichier journal d'installation.
- Le nom et la taille des fichiers faisant partie de l'installation de Kaspersky Anti-Virus doivent coïncider exactement avec les informations contenues dans le journal d'installation.
- Le processus *aveserver* doit être arrêté.
- Le service de messagerie doit être arrêté.

Vous disposez de plusieurs méthodes pour lancer la procédure de désinstallation, en fonction du gestionnaire de paquets. Nous allons étudier en détail les variantes possibles.

Si vous avez installé Kaspersky Anti-Virus à partir de son paquet .rpm, tapez ce qui suit sur l'invite de commande pour lancer la procédure de désinstallation :

```
rpm -e <nom_paquet>
```

Si vous avez installé Kaspersky Anti-Virus à partir de son paquet .deb, tapez ce qui suit sur l'invite de commande pour lancer la procédure de désinstallation :

```
dpkg -r <nom_paquet>
```

Si vous avez installé Kaspersky Anti-Virus à partir de son paquet .pkg, tapez ce qui suit sur l'invite de commande pour lancer la procédure de désinstallation :

```
pkg-delete <nom_paquet>
```

La désinstallation du logiciel est automatique. Aucune notification supplémentaire n'est émise si la suppression du logiciel est réussie.

CHAPITRE 8. VERIFICATION DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

Après avoir installé et configuré Kaspersky Anti-Virus, nous vous conseillons de vérifier l'exactitude des paramètres et le bon fonctionnement du logiciel à l'aide d'une suite de « virus » de test.

Ce virus d'essai a été développé spécialement par l'organisation European Institute for Computer Antivirus Research. eicar 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 l'identifient comme un virus.

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

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

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

Le fichier que vous aurez téléchargé depuis le site de l'organisation **EICAR** ou que vous aurez créé vous-même contient le corps du « virus » d'essai standard. L'application va le détecter, lui attribuer le statut **Infecté** et exécuter l'action définie par l'administrateur pour des objets du même type.

Afin de vérifier le comportement de l'application lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du « virus » d'essai standard en ajoutant un préfixe (reportez-vous au tableau ci-après).

Tableau Modifications du « virus » d'essai

Préfixe	Type d'objet
Pas de préfixe, « virus » d'essai standard.	**Infecté**. L'objet ne peut être réparé.
CORR–	**Endommagé**.
SUSP–	**Suspect** (code d'un virus inconnu).
WARN–	**Avertissement** (modification du code d'un virus connu).
ERRO–	**Erreur pendant l'analyse de l'objet**.
CURE–	**Désinfecté**. L'objet est désinfecté ; le texte du corps du « virus » sera remplacé par CURE.
DELE–	L'objet est effacé automatiquement.

La première colonne reprend les préfixes qu'il faudra ajouter au début de la ligne de code du « virus » d'essai standard (par exemple : CORR–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*). La deuxième colonne contient le type que l'application lui affecte, suite à l'ajout du préfixe. Les actions correspondantes à chacun des types d'objet sont définies dans la configuration de l'application antivirus, et personnalisées par l'administrateur.

CHAPITRE 9. FREQUENTLY ASKED QUESTIONS

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

Question : Est-il possible d'utiliser Kaspersky Anti-Virus en même temps que des produits antivirus d'autres fabricants ?

Pour éviter les conflits, nous vous recommandons de désinstaller tout logiciel antivirus d'autres fabricants avant d'installer Kaspersky Anti-Virus.

Question : Kaspersky Anti-Virus ne recommence pas l'analyse d'un fichier. Pourquoi ?

En effet, Kaspersky Anti-Virus n'analyse pas deux fois de suite les fichiers qui n'ont pas changé depuis l'analyse précédente.

Ceci est possible grâce aux nouvelles technologies iChecker et iStreams. L'application implémente cette technologie à partir de sommes de contrôles de fichiers conservées dans une base de données et dans des flux NTFS alternatifs.

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

La détection des virus est avant tout une tâche mathématique liée à l'analyse de structures, de sommes de contrôle et de conversions de données mathématiques. Pour cette raison, la principale ressource utilisée par tout logiciel antivirus est le processeur et chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse.

D'autres logiciels réduisent la durée de l'analyse en éliminant des bases antivirus les virus les plus complexes à identifier ou les plus rares (dans une zone géographique donnée), ainsi que les fichiers les plus difficiles à analyser (comme les fichiers PDF). Kaspersky Lab estime que le but de tout antivirus est de garantir une véritable protection de l'utilisateur contre les virus.

Il va de soit que Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer la vitesse de l'analyse grâce à l'exclusion de toute une série de différents fichiers. Cependant, tenez compte du fait que le niveau de protection général diminuera.

Kaspersky Anti-Virus reconnaît plus de 700 formats de fichiers archivés ou compressés. Ceci est très important au niveau de la sécurité antivirus car chacun des formats reconnus ci-dessus peut contenir un code malicieux exécutable. Néanmoins, il convient de remarquer que cette nouvelle version de l'application est plus rapide que les précédentes, malgré l'augmentation quotidienne du nombre de virus identifiés par Kaspersky Anti-Virus (plus de 30 nouveaux virus chaque jour) et l'augmentation constante des formats pris en charge. Tout ceci est rendu possible grâce aux nouvelles technologies développées par Kaspersky Lab, comme i-Checker™.

Question : À quoi sert un fichier de clé de licence ? Ma copie du logiciel antivirus peut-elle fonctionner sans ce fichier ?

Non, Kaspersky Anti-Virus ne peut pas fonctionner sans une clé de licence.

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

Question : Qu'arrive-t-il après expiration de la licence ?

Après expiration de la licence, Kaspersky Anti-Virus continuera de fonctionner, mais la mise à jour de la base antivirus sera désactivée. Le logiciel continuera à réparer les objets infectés en utilisant les anciennes bases antivirus.

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

Question : Mon installation de Kaspersky Anti-Virus ne fonctionne pas. Que dois-je faire ?

En premier lieu, vérifiez **si le composant *aveserver* est en exécution**, ou recherchez une solution dans cette documentation, et dans cette section en particulier, ou visitez notre site Web.

En outre, nous vous conseillons de souscrire le contrat de maintenance auprès du distributeur auquel vous avez acheté Kaspersky Anti-Virus, ou d'écrire au service technique de Kaspersky Lab (support@kaspersky.com) ou à l'adresse figurant dans les informations de la clé de licence.

Pour être sûr de recevoir une réponse rapidement, procédez de préférence comme ceci :

1. Indiquez dans le sujet du message la version du système d'exploitation installé sur votre ordinateur, le nom du logiciel de Kaspersky Lab que vous utilisez et le problème. Par exemple : **Linux, Webmin, cannot access settings of the licensed users list**.
2. Utilisez des messages au format de texte simple.
3. Mentionnez au début de votre message la version exacte du système d'exploitation, la distribution de Kaspersky Anti-Virus et le numéro de votre licence.
4. Décrivez clairement et brièvement le problème. N'oubliez pas qu'au moment même où ils lisent vos explications, les membres du service technique ne savent encore rien de votre problème. Ils ne pourront vous aider qu'après l'avoir compris complètement et simulé.
5. Envoyez les données suivantes au service technique dans un fichier compressé :
   - Tous les fichiers de configuration de votre agent de messagerie (MTA)
   - Les fichiers du répertoire */etc/kav/*
   - Fichier de rapports du système de messagerie
   - Le fichier de rapports du composant antivirus, par exemple */var/log/aveserver.log* ;
   - Les informations affichées sur la console par la commande **ps -ax**
   - Le fichier de clé.
6. Pensez à préciser dans votre message si votre système utilise :
   - un contrôleur SCSI ;
   - un processeur très ancien, ou très récent, ou plusieurs processeurs ;
   - moins de 64 Mo, ou plus de 2 Go de mémoire RAM.

7. Spécifiez le trafic journalier aproximatif, et si le serveur connaît des pointes de surcharge.

Question : À quoi servent les mises à jour quotidiennes ?

Il y a encore quelques années, les virus se transmettaient par des disquettes, et il suffisait d'installer un programme antivirus et de mettre à jour de temps en temps les bases antivirus pour assurer une protection adéquate. Cependant, les récentes épidémies de virus se propagent tout autour du monde en quelques heures, et la protection des anciennes bases peut se révéler inutile contre une nouvelle menace. Pour pouvoir résister aux nouveaux virus, il convient de mettre à jour les bases antivirus tous les jours.

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

La mise à jour des modules d'application antivirus est une fonction complémentaire qui permet à la fois de corriger les vulnérabilités découvertes et d'ajouter de nouvelles fonctions.

Question : Quels sont les changements au service de mise à jour dans la version 5.0 ?

L'application Kaspersky Lab 5.0 introduit un nouveau service de mises à jour, développé pour répondre aux demandes de nos utilisateurs. Il permet d'automatiser l'ensemble de la procédure de mise à jour, depuis le préparation des mises à jour dans Kaspersky Lab jusqu'au moment où les fichiers concernés sont mise à jour sur les postes clients.

Les avantages du nouveau service de mise à jour comprend :

- *La capacité de continuer le téléchargement de fichiers après déconnexion.* Lors de la reconnexion, le téléchargement ne continue que sur les fichiers restants.
- *La taille des mises à jour cumulatives est réduite de moitié*. Une mise à jour cumulative contient l'ensemble de la base antivirus ; sa taille dépasse donc considérablement celle des mises à jour normales. Le nouveau service utilise une technologie spéciale, permettant de prendre en compte la présence d'une base antivirus pour la mise à jour cumulative.
- *Téléchargement accéléré depuis Internet*. Kaspersky Anti-Virus retrouve un serveur de mises à jour de Kaspersky Lab situé

dans votre région. Ensuite, les serveurs sont alloués en fonction de leur rendement, de sorte que vous n'êtes pas dirigés vers un serveur surchargé alors qu'un autre serveur inutilisé est disponible.

- *Utilisation de listes noires de clés*. Les utilisateurs non enregistrés ou illégaux sont maintenant empêchés d'utiliser le service de mise à jour. Les utilisateurs enregistrés ne subissent plus de connexions à des serveurs surchargés.
- *Les groupes corporatifs peuvent désormais créer des serveurs de mises à jour en local*. Cette fonction est conçue pour les organisations où un même réseau local permet d'unifier les ordinateurs protégés par des applications Kaspersky Lab. Tout ordinateur de la LAN, transformé en serveur de mises à jour, récupère de son côté les mises à jour sur Internet, puis les partage avec le reste des ordinateurs en réseau.

Un intrus pourrait-il remplacer la base antivirus?

Chaque base antivirus dispose d'une signature unique que Kaspersky Anti-Virus vérifie lors d'une consultation. Si la signature ne correspond pas à celle définie par Kaspersky Lab et si la date de la base de données est postérieure à la date d'expiration de la licence, Kaspersky Anti-Virus n'utilisera pas cette base.

Question : Kaspersky Anti-Virus pour serveurs de courrier Unix fonctionnera-t-il avec ma distribution de Linux ?

La version 5.5 de Kaspersky Anti-Virus pour serveurs de courrier Unix a été testée avec les distributions RedHat, Debian et SuSE, et des paquets Kaspersky Anti-Virus ont été compilés spécialement pour les distributions indiquées.

Consultez les versions pour les S.E. pris en charge dans la section 1.2 à la page 8.

Vous ne rencontrerez vraisemblablement pas de problèmes importants si votre distribution est 100% compatible avec l'une des distributions prises en charge (par exemple, ASPLinux est compatible avec Red Hat Linux).

Les utilisateurs de distributions non comprises dans la liste prise en charge par Kaspersky Lab peuvent rencontrer des problèmes de fonctionnement incorrect de l'application, liés à des particularités spécifiques du système d'exploitation. Par exemple, votre système de

distribution peut utiliser une autre version de bibliothèque, ou les scripts de démarrage son placés dans des emplacements non standards. Dans des cas comme ceux-ci, le service technique de Kaspersky Lab ne pourra pas vous venir en aide.

Question : comment décompresser des archives *.tgz ou .tar.gz ?*

Les fichiers d'archive .tgz ou *.tar.gz* sont décompressés par la commande suivante :

```
tar -zxvf <nom_archive>
```

Reportez-vous aux pages man(1) du logiciel **tar** pour plus de détails.

Question : Tout fonctionnait correctement, jusqu'à ce que j'installe Kaspersky Anti-Virus pour serveurs de courrier Unix et que j'intègre avec lui le système de messagerie Postfix. Après cela, la distribution des messages a été stoppée et l'erreur suivante est reportée dans maillog :

```
Sep 23 15:17:03 server postfix/lmtp[1678] :
8238C38987 : to=<utilisateur@serveur.org
<mailto:utilisateur@serveur.org>>, relay=none,
delay=1, status=bounced (localhost : host not found)
```

Que dois-je faire ?

Ce type de problème peut apparaître dans les cas suivants :

- Votre DNS ne possède pas de domaine, requis par le RFC 2606. Configurez votre DNS suivant les recommandations du RFC. Pour plus de détails, reportez-vous à la page : http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2606.html
- Localhost n'est pas défini dans le fichier /etc/hosts. Normalement, il doit avoir la valeur **localhost=127.0.0.1**. Modifiez le fichier hosts, en spécifiant cette adresse pour localhost.

Question : Est-il possible d'utiliser Network Control Centre for Windows pour l'administration de Kaspersky Anti-Virus?

Il n'est pas possible d'utiliser Network Control Centre pour Windows pour travailler avec Kaspersky Anti-Virus pour serveurs de courrier Unix. Cette version de l'application dispose d'une option de configuration à distance, utilisant un module spécial pour le paquet Webmin.

Question : Comment puis-je enregistrer la sortie sur console dans un fichier ?

Pour enregistrer la sortie sur console de Kaspersky Anti-Virus, vous pouvez modifier en ce sens le fichier de configuration, ou écrire la ligne de commande suivante :

```
$ votre_app > ./fichier_texte 2>&1
```

où :

`votre_app`– Application dont vous voulez enregistrer la sortie standard et les messages d'erreur dans un fichier.

`fichier_texte`– Chemin complet du fichier dans lequel vous allez enregistrer les informations.

`Par exemple :`

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

Dans cet exemple, les messages standard et les messages d'erreur affichés par le composant *keepup2date* sont redirigés dans le fichier *updater.log* du répertoire courant.

ANNEXE A. LOGICIELS MALVEILLANTS SOUS ENVIRONNEMENT UNIX

Les virus sont bien moins fréquents dans les environnements Unix que sous Windows, par exemple, en raison de certaines propriétés de ces plates-formes. Les chevaux de Troie et les vers réseau sont moins rares.

Les logiciels malveillants se disséminent à travers les réseaux en utilisant différents moyens, y compris les « failles » logicielles. Cet annexe examine plus en détail les différents types de logiciels malveillants sous UNIX ainsi que leurs méthodes d'infection du système.

A.1. Virus

Un virus est un logiciel (avec du code ou des instructions exécutables), capable de se recopier soi-même (les copies ne sont pas nécessairement tout à fait identiques à l'original) et de s'infiltrer dans différents objets ou ressources des systèmes informatiques, des réseaux, etc. sans que l'utilisateur en soit informé. De telles copies sont également capables de se multiplier à leur tour.

L'étude des virus en environnement Unix révèle que ceux-ci se rapportent au type de fichier et qu'ils enregistrent leur code dans des fichiers exécutables, ou qu'ils créent des fichiers fantômes.

Les sous-classes suivantes sont organisées en fonction de leur algorithme de fonctionnement :

- *virus résident en mémoire (TSR)*. Virus qui installe une partie résidente après infection de la mémoire RAM du système ; cette portion intercepte ensuite les appels du système à des objets infectables, puis pénètre effectivement ces derniers. Ces virus résidents en mémoire restent actifs, tant que l'ordinateur n'est pas éteint ou redémarré.
- *virus non-résident*. Ce virus n'infecte pas la mémoire de l'ordinateur et reste actif pendant une durée limitée. Certains virus laissent de petits programmes résidents en mémoire, qui ne propagent pas le virus.

En règle générale, les virus sous Unix ne sont pas dangereux – leur influence se limite à réduire l'espace libre, et à provoquer de manière temporaire des effets graphiques, sonores ou autres. Certains sont complètement inoffensifs, car ils n'altèrent en aucune façon le fonctionnement de l'ordinateur, sauf dans la

réduction de la quantité d'espace libre, que provoque leur présence dans le système de fichiers.

Examinons certains exemplaires de virus sous Unix :

ELF_SNOOPY– ce virus infecte les fichiers Unix exécutables.

Algorithme du virus : il recherche tous les fichiers exécutables présents dans un poste de travail, les renomme avec une extension .X23 extension et les déplace dans un nouveau répertoire /E. Le virus recopie ensuite son code à l'intérieur des fichiers d'origine puis définit leurs permissions à **777**. En même temps, un nouvel utilisateur **snoopy**, avec la même permission 777 est créé dans la table principale des mots de passe du poste infecté.

Linux.Bliss est un groupe de virus non-résidents sous Linux qui infecte les exécutables Linux ; ils sont écrits en GNU C et utilisent le format ELF.

Algorithme du virus : après démarrage, le virus parcourt le disque à la recherche de fichiers exécutables dans un poste de travail, et les infecte en se glissant soi-même au début du fichier, et en ajoutant une chaîne d'identification à la fin du fichier. L'activité du virus est limitée par les droits de l'utilisateur qui l'a lancé (seuls les fichiers accessibles sont donc infectés). Si l'utilisateur possède des privilèges système, le virus arrive à se propager à travers tout l'ordinateur.

Linux.Diesel est un virus non-résident sous Linux non dangereux qui infecte les exécutables Linux.

Algorithme du virus : après son lancement, le virus relit son propre code binaire dans le fichier porteur, recherche les fichiers exécutables Linux dans les sous-répertoires du système puis se réplique à l'intérieur des fichiers, en augmentant la taille de leur dernière section de code.

Linux.Siilov est un virus non-résident et non dangereux sous Linux qui infecte les exécutables Linux ; ces virus sont au format ELF.

Algorithme du virus : celui-ci utilise deux procédés d'infection de fichiers : résident et non-résident. Dans le procédé résident, le virus reste dans la mémoire du système et infecte des fichiers en arrière plan. Dans le procédé non-résident, le virus parcourt le disque à la recherche de fichiers exécutables et les infecte.

Linux.Winter est un virus non résident inoffensif sous Linux. Il est de très petite taille – à peine 341 octets.

Algorithme du virus : après lancement, le virus prend le contrôle puis recherche et infecte les fichiers ELF (fichiers Linux exécutables) dans le répertoire courant.

A.2. Cheval de Troie

Un cheval de Troie est un programme qui réalise des actions non autorisées. Une fois lancé, un cheval de Troie s'installe et prend le contrôle du système ; l'utilisateur n'est jamais informé des actions du cheval de Troie dans son système. Cet ordinateur est désormais prêt pour une prise de contrôle à distance.

Le cheval de Troie se répand à travers les réseaux.

Un exemplaire typique de cheval de Troie sous UNIX est **TROJ_IRCKILL**– c'est en fait un ensemble d'outils logiciels utilisés pour déconnecter les utilisateurs de canaux IRC. La collection comprend quatre outils d'attaque : FLOOD, MCB (Multiple Collide BOTs), SUMO BOTs, et FLASH – un procédé par « inondation » utilisé spécialement pour les environnements Linux.

L'attaque FLASH interrompt les connexion modem directes en envoyant une commande **ping** à une certaine adresse IP, en spécifiant des données « incorrectes » à l'intérieur d'une séquence déterminée. Le modem de l'utilisateur interprète alors ces données comme une commande de déconnexion, et l'utilisateur est déconnecté d'Internet. Toutefois, ce type d'attaque ne fonctionne qu'avec certains types de modems seulement.

L'attaque MCB utilise les canaux IRC. Au moment où les serveurs IRC ne sont pas synchronisés les uns avec les autres (« net split »), le cheval de Troie simule une connexion, et crée une copie du pseudo de l'utilisateur (« nickname »). Une fois la synchronisation des serveurs IRC rétablie, le nom de l'utilisateur est invalidé et l'utilisateur se retrouve déconnecté du canal IRC.

L'attaque FLOOD BOTS/SUMO BOTS est également utilisée sur le réseau IRC : elle génère de nombreux pseudonymes d'utilisateur aléatoires. Cette attaque procède en noyant littéralement la bande passante du canal IRC ou de l'ordinateur de l'utilisateur, sous un flot de messages envoyés ou reçus. L'utilisateur est ici aussi déconnecté du canal IRC.

Root kit est un ensemble d'outils logiciels utilisés par les pirates obtenir l'accès avec les privilèges root sur l'ordinateur distant. Il fait appel à des utilitaires Unix standard – ps et ls. La seule méthode efficace pour récupérer les ordinateurs d'une infection par Root kit est d'effacer le contenu du disque dur, de réinstaller le système d'exploitation et de restaurer les données importantes à partir d'une copie de sauvegarde normale.

A.3. Vers réseau

Un ver réseau est un logiciel malveillant qui, au lieu de se propager à travers des objets exécutables, se recopie soi-même sur des ressources réseau. Ce groupe

est ainsi nommé par analogie avec la capacité des vers pour « ramper » à travers les réseaux et autres canaux de données.

Ils pénètrent à l'intérieur de la mémoire des ordinateurs connectés, identifient les adresses d'autres ordinateurs sur le réseau, puis y envoient un exemplaire d'eux-mêmes.

Les vers créent parfois des fichiers de travail sur disque, mais la plupart n'utilisent absolument aucune ressource de l'ordinateur, sauf la mémoire RAM.

Worm.Linux.Ramen a été le premier ver connu ayant infecté des systèmes RedHat Linux. Il infecte des systèmes Linux distants (RedHat Linux) en profitant du problème lié au débordement de tampon. Cette « faille de sécurité » logicielle permet d'envoyer et d'exécuter du code sur un ordinateur distant à l'insu de l'administrateur ou de l'utilisateur.

*Source de l'infection : un fichier d'archive .**tgz*** provenant du réseau.

Algorithme : le ver envoie une courte séquence de son propre code sur des ordinateurs distants en utilisant un débordement de tampon. Après exécution du composant principal (start.sh file), le ver ouvre une connexion et télécharge successivement d'autres composants lui permettant d'identifier l'adresse des systèmes à attaquer ; à travers la faille du débordement de tampon, il envoie à chacun d'eux un chargeur qui, à son tour, reprend le téléchargement et exécute le code principal du ver. La page principale d'un serveur Web est remplacée par un fichier HTML avec le texte suivant : "RameN Crew – Hackers looooooooooooove noodles". Finalement, le ver envoie un message à deux adresses, redémarre le système, puis recommence son exploration du réseau Internet.

En outre, le ver ajoute ses propres instructions au fichier de démarrage du système /etc/rc.d/rc.sysinit. L'exécution du ver se reproduit ainsi avec chaque redémarrage du système infecté.

Worm.Linux.Lion est un ver Internet qui attaque des serveurs Linux. Pour pénétrer dans les ordinateurs, le ver utilise une faille de sécurité du service BIND DNS.

Algorithme : le ver analyse l'Internet à la recherche de systèmes vulnérables à des connexions sous privilèges root. Dès qu'il rencontre un système de ce type, le ver l'infecte, récupère ses informations (adresse IP, utilisateurs et mots de passe) dans le fichier mail.log et envoie celui-ci à l'adresse 1i0nsniffer@china.com.

En outre, le ver tente de se connecter au site Web www.51.net, enregistré en Chine, et y télécharge le fichier *crew.tgz*. Il décompresse alors ce fichier d'archive sur l'ordinateur infecté, puis installe et lance des procédures d'exploration globales des ressources du réseau, à la recherche de nouvelles victimes.

mIRC.Acoragil et **mIRC.Simpsalapim** sont les premiers vers connus pour mIRC. Ces vers sont baptisés ainsi d'après le code-chaîne qui active leur exécution. si le texte transmis sur un canal par n'importe quel utilisateur contient la ligne « *Acoragil* », alors tous les utilisateurs infectés par le ver **mIRC.Acoragil** sont automatiquement déconnectés du canal. De son côté, le ver **mIRC.Simpsalapim** réagit de la même manière à la ligne *Simpsalapim*.

Source de l'infection : les vers utilisent des commandes mIRC à travers le réseau pour envoyer leur code dans le fichier SCRIPT.INI à tout nouvel utilisateur qui se connecte au canal.

Algorithme : une partie du code du ver contient un cheval de Troie. **mIRC.Simpsalapim** peut capturer un canal IRC : si le propriétaire du canal mIRC est infecté, l'intrus intercepte et prend le contrôle du canal en utilisant le code-chaîne *ananas*.

mIRC.Acoragil envoie des fichiers système DOS, Windows ou Unix à travers des codes-chaînes. Certains codes-chaînes sont choisis pour ne pas attirer l'attention de leurs victimes : par exemple, *hi* ou *the*. L'une des variantes de ce ver envoie les fichiers de mots de passe UNIX à un intrus.

Worm.Linux.Adm est un ver Internet qui infecte des serveurs Linux. Le ver envoie et exécute une courte séquence de son propre code sur des ordinateurs distants, il télécharge ensuite le reste du code principal, puis recommence.

Source de l'infection : à travers le réseau ; le ver se réplique et infecte des systèmes Linux distants en profitant d'une faille de sécurité de Linux (lié au débordement de tampon). Cette faille permet d'envoyer et d'exécuter du code sur un ordinateur distant à l'insu de l'administrateur ou de l'utilisateur.

ANNEXE B. KASPERSKY LAB

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

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

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

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les 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 applications 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 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 aux besoins spécifiques de leur activité. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les 3 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 Anti-Virus Personal

Kaspersky Anti-Virus Personal protège les ordinateurs domestiques sous Windows 98/ME/2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (capteurs et ressources à risques -- Riskware). L'application vérifie en permanence toutes les sources possibles de pénétration des virus : courrier électronique, Internet, lecteurs de disquettes et de CD. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Les deux modes d'exploitation du logiciel (utilisables ensemble, ou séparément) sont :

- **Protection en temps réel**– Analyse de tous les fichiers au moment de leur lancement, de leur ouverture ou de leur enregistrement sur l'ordinateur protégé.
- **Analyse à la demande**– Analyse et désinfection de l'ordinateur complètement, ou individuellement par unités de disque, fichiers ou dossiers. Vous pouvez lancer ces analyses manuellement depuis l'interface graphique, ou planifier une analyse périodique.

Kaspersky Anti-Virus Personal n'analyse pas les objets précédemment analysés qui n'ont pas été modifiés depuis. Cette règle s'applique maintenant à la fois à la protection en temps réel et à l'analyse à la demande. Cette fonction améliore **grandement la vitesse et le rendement de l'application**.

Kaspersky Anti-Virus Personal offre une protection efficace contre les virus qui tentent de pénétrer des ordinateurs par la voie du courrier électronique. L'application analyse et désinfecte automatiquement tout le trafic des messages entrant et sortant (POP3 et SMTP) et détecte efficacement les virus dans les bases d'archive de courrier.

Kaspersky Anti-Virus Personal prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirus automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les archives au format **ZIP**, **CAB**, **RAR** ou **ARJ**.

La configuration du programme est facilitée par la possibilité de sélectionner un niveau prédéfini parmi les trois possibles : **Protection maximum**, **Recommandé** et **Vitesse maximum**.

La base antivirus est mise à jour toutes les trois heures. La distribution de la base de données est garantie, même en cas d'interruption ou de commutation de la connexion Internet pendant le téléchargement.

Kaspersky Anti-Virus Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirus intégrale des ordinateurs personnels sous Windows 98/ME/2000/NT/XP, ainsi que des applications MS Office 2000. Kaspersky Anti-Virus Personal Pro est accompagné d'un outil simple d'emploi pour récupérer automatiquement les mises à jour quotidiennes des bases antivirus et des modules de programme. Un analyseur heuristique de seconde génération détecte efficacement même les virus inconnus. L'interface de Kaspersky Anti-Virus Personal inclut de nombreuses améliorations, pour rendre l'utilisation de l'application plus facile que jamais.

Kaspersky Anti-Virus Personal Pro possède les caractéristiques suivantes :

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

Kaspersky Anti-Hacker

Kaspersky Anti-Hacker est un pare-feu personnel conçu pour protéger un ordinateur sous n'importe quelle version du système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les intrusions extérieures provenant du réseau local ou de l'Internet.

Kaspersky Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Ceci améliore la protection de vos données personnelles, et parvient à offrir 100% de sécurité sur les données confidentielles conservées dans votre ordinateur.

L'application utilise la technologie SmartStealth™ pour empêcher la détection de votre ordinateur depuis l'extérieur. Dans ce mode invisible, l'application

fonctionne de manière transparente afin de maintenir votre ordinateur protégé tandis que vous naviguez sur le Web. L'application garantit la transparence et l'accès normal aux données.

- Kaspersky Anti-Hacker bloque également les attaques malicieuses les plus fréquentes en provenance du réseau et surveille les tentatives d'analyse des ports de votre ordinateur.
- La configuration de l'application consiste simplement à choisir parmi cinq niveaux de sécurité. Par défaut, l'application démarre en mode apprentissage, qui permet de configurer automatiquement la sécurité de votre système en fonction de vos réponses à des divers événements. De cette manière, vous pouvez personnaliser le pare-feu en fonction de vos préférences et de vos besoins personnels.

Kaspersky Security pour PDA

Kaspersky Security pour PDA assure une protection antivirus efficace des données d'un PDA sous système d'exploitation Palm ou Windows CE. Il protège également toutes les données provenant d'un PC ou d'une carte d'expansion, de fichiers ROM et de bases de données. Le paquet logiciel contient une combinaison efficace des outils antivirus suivants :

- **analyseur antivirus** pour l'analyse à la demande des données conservées sur le PDA et des cartes d'expansion ;
- **intercepteur antivirus** pour stopper les virus de fichiers copiés à partir d'autres portables ou transférés avec la technologie HotSync™.

Kaspersky Security pour PDA protège votre PDA contre les intrusions non autorisées, en chiffrant à la fois l'accès au dispositif et les données conservées dans les cartes mémoire.

Kaspersky Anti-Virus Business Optimal

Ce paquet offre une solution de sécurité configurable pour des réseaux d'entreprise de taille petite ou moyenne.

Kaspersky Anti-Virus Business Optimal inclut une protection antivirus à échelle complète[1] pour :

- *postes de travail* sous Windows Windows 98/ME/NT/2000/XP pour stations de travail, et Linux ;

[1] Selon le modèle du kit de distribution.

- *Serveurs de fichiers et d'applications* sous Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD et Linux ;
- *Systèmes de messagerie*, concrètement Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelles Internet* : CheckPoint Firewall –1; Microsoft ISA Server.

Le kit de distribution de Kaspersky Anti-Virus Business Optimal inclut Kaspersky Administration Kit, un *outil unique et automatique de déploiement et d'administration*.

Tous ces composants sont interopérables, et vous pouvez choisir n'importe lequel d'entre eux en fonction des systèmes d'exploitation et des applications utilisés.

Kaspersky Corporate Suite

Ce paquet fournit aux réseaux d'entreprise, de n'importe quelle taille et complexité, une protection antivirus complète et évolutive. Les composants du paquet ont été développés pour protéger chaque périmètre du réseau d'entreprise, même dans des configurations matérielles hétérogènes. Kaspersky Corporate Suite est compatible avec la majorité les systèmes d'exploitation et des applications installées dans une entreprise. Tous les composants du paquet sont gérés à partir d'une console utilisant une interface d'utilisateur homogène. Kaspersky Corporate Suite offre un rendement élevé et une protection fiable, et il prend totalement en charge les particularités de votre configuration réseau.

Kaspersky Corporate Suite assure une protection antivirus complète de :

- *Postes de travail* sous Windows 98/ME/NT/2000/XP et Linux ;
- *Serveurs de fichiers et d'applications* sous Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD et Linux ;
- *Clients de messagerie*, y compris Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim et Qmail ;
- *Passerelles Internet* : CheckPoint Firewall –1; Microsoft ISA Server ;
- *Ordinateurs de poche* (PDAs), sous Windows CE et Palm OS.

Le kit de distribution de Kaspersky Corporate Suite inclut Kaspersky Administration Kit, un *outil unique et automatique de déploiement et d'administration*.

Tous ces composants sont parfaitement interopérables, et vous pouvez choisir n'importe lequel d'entre eux en fonction des systèmes d'exploitation et des applications utilisés.

Kaspersky Anti-Spam

Kaspersky Anti-Spam est une suite logicielle avec technologie de pointe, conçue pour permettre aux organisations équipées de réseaux de petite ou moyenne taille, de lutter contre le fléau des messages indésirables (pollupostage, ou Spam). L'application combine les technologies révolutionnaires d'analyse linguistique avec toutes les méthodes modernes de filtrage des messages électroniques (y compris les listes noires et l'analyse formelle des structures). 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 une barrière installée à l'entrée du réseau, qui surveille et empêche le passage de messages indésirables 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 de la base de filtrage, à partir des échantillons fournis par le laboratoire linguistique de Kaspersky Lab.

Kaspersky Anti-Spam Personal

Kaspersky Anti-Spam Personal est conçu pour protéger les utilisateurs de Microsoft Outlook et de Microsoft Outlook Express contre les courriers électroniques indésirables (les « pourriels », ou spam).

Kaspersky Anti-Spam Personal est un outil puissant capable de détecter la présence de contenus indésirables reçus à travers les protocoles POP3 et IMAP4 (Microsoft Outlook seulement).

La méthode de filtrage recouvre l'analyse de tous les attributs du message (adresses de l'expéditeur et destinataire et en-têtes de message), le filtrage des contenus (analyse du contenu du message, y compris le champ Sujet et tous les fichiers joints), et la mise en œuvre d'algorithmes linguistiques et heuristiques exclusifs.

Les hautes performances de l'application sont possibles grâce à des mises à jour quotidiennes de la base de filtrage, à partir des échantillons fournis par le laboratoire linguistique de Kaspersky Lab.

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 tout ce qui concerne notre application par téléphone ou par courrier électronique. Toutes vos recommandations et suggestions sont soigneusement étudiées et prises en compte.

Support technique	Pour une assistance technique, adressez-vous à :http://www.kaspersky.com/supportinter.html
Information générale	WWW : http://www.kaspersky.com http://www.viruslist.com Courriel : sales@kaspersky.com

ANNEXE C. CONTRAT DE LICENCE

Contrat de licence pour utilisateur standard

NOTE A TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE (« LICENCE ») SUIVANT, À PROPOS DE CE LOGICIEL (« LOGICIEL ») FABRIQUÉ PAR KASPERSKY LAB. (« KASPERSKY LAB »).

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

SI VOUS AVEZ ACHETE CE LOGICIEL SOUS FORME PHYSIQUE, EN OUVRANT LE SCELLÉ DU BOÎTIER, VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. SI LE SCELLÉ EST DÉCHIRÉ OU LE BOÎTIER A ÉTÉ OUVERT, VOUS N'AUREZ PAS DROIT AU REMBOURSEMENT DU LOGICIEL. LES LOGICIELS POUR USAGE DOMESTIQUE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) ACHETÉS SOUS FORME DE TÉLÉCHARGEMENT PAR INTERNET PEUT ETRE RETOURNE, ET REMBOURSÉ INTEGRALEMENT DANS LES 14 JOURS APRÈS SON ACHAT, À KASPERSKY LAB, SES REVENDEURS ET DISTRIBUTEURS AGREES. AUTRES PRODUITS NON REMBOURSABLES. LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

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

1. Licence de droits. Sous réserve du paiement du prix d'achat du logiciel et d'acceptation des termes de la présente Licence d'utilisation, Kaspersky Lab vous autorise à utiliser une copie unique et non transférable de la version spécifiée de ce logiciel et de la documentation (la « Documentation ») selon les termes de ce Contrat uniquement pour un usage interne à l'entreprise. Vous

pouvez installer une copie du logiciel sur un seul système, poste de travail, assistant électronique personnel ou autre dispositif numérique pour lequel le Logiciel a été conçu (pour chaque cas, le « Système client »). Si la licence concerne une suite d'applications avec plusieurs produits logiciels, cette licence s'applique à tous les logiciels indiqués, en respectant toute restriction ou limite d'utilisation spécifiée dans la liste de prix ou dans la distribution applicable à chaque produit individuel.

1.1 Utilisation. Ce logiciel ne peut être installé que sur un seul système (un seul ordinateur) par le client, et la licence d'utilisation n'est octroyée qu'à un utilisateur unique.

Le logiciel est « utilisé » sur un système par le client lorsqu'il est lancé dans la mémoire temporaire (RAM) ou installé dans la mémoire permanente (sur un disque dur ou un autre périphérique de stockage) du système du client. La présente licence vous autorise à réaliser une copie unique du logiciel dans son intégralité à des fins de sauvegarde, à condition que les copies contiennent toutes les notices de propriété du Logiciel. Vous devrez garder la trace du nombre et de l'emplacement de toutes les copies du logiciel et de sa documentation, et prendre les précautions nécessaires pour qu'aucune copie ou utilisation illégale ne soit effectuée.

Si vous cédez le système sur lequel le logiciel a été installé, vous devrez le désinstaller au préalable et vérifier qu'il n'en reste aucune copie sur ce système.

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

1.1.4 Il vous est interdit d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, de produire des applications dérivées, non plus qu'à autoriser un tiers à copier le logiciel (sauf autorisation expresse).

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

1.1.6 Vous ne pourrez pas utiliser ce Logiciel avec des outils automatiques, semi-automatiques ou manuels conçus pour créer des signatures de virus, des routines de détection de virus ou tout autre code de détection de code ou de données dangereuses.

1.2 Utilisation en Mode Serveur. Vous pouvez utiliser le Logiciel sur un Système Client ou sur un serveur (« Serveur ») dans un environnement multi-utilisateurs

ou en réseau (« Mode serveur ») uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est nécessaire pour chaque Système Client ou « poste », sans tenir compte du fait que ces systèmes autorisés ou ces postes sont connectés simultanément ou réellement en train d'utiliser le logiciel. L'utilisation de logiciels ou de matériels permettant de réduire le nombre de dispositifs client ou de postes utilisant le Logiciel (par exemple, par "multiplexage" ou "sondage" du logiciel ou du matériel) ne réduit pas le nombre de licences nécessaires : le nombre de licences requises égale le nombre d'entrées séparées gérées en interface par le programme ou matériel multiplexeur ou de sondage. Si le nombre de Systèmes Clients ou postes pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures raisonnables pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. La présente licence vous autorise à télécharger ou à effectuer autant de copies de la documentation que le réseau compte de Clients possédant une licence d'utilisation du logiciel, à condition que la documentation soit complète.

1.3 Licences par volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient.. Vous devez tout mettre en œuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Ce permis vous autorise à tirer ou télécharger une copie de la documentation pour chaque copie additionnelle autorisée par le permis de volume, à condition que chaque une telle copie contienne toutes les notices de propriété industrielle du document.

2. Durée. Ce Contrat de Licence est valable pour une durée d'un an à moins qu'il n'arrive à terme avant ce délai pour l'une des raisons prévues ci-après. Ce Contrat se terminera automatiquement si vous n'en respectez pas les termes, les limites ou les conditions décrites. Dans ce cas, il vous incombe de détruire toute copie du logiciel et de sa documentation que vous auriez réalisée. Vous pouvez mettre un terme à ce contrat à tout moment en détruisant les copies du logiciel et de sa documentation.

3. Support technique.

(i) Kaspersky Lab fournira un support technique (« Support ») comme décrit ci-dessous pour une période d'un an, sous réserve de :

(a) Paiement du service support en vigueur, et :

(b) Compléter correctement le formulaire d'inscription au service de Support Technique fourni avec ce Contrat ou disponible sur le site Web de Kaspersky Lab, ce qui implique la communication du Fichier Clé d'Identification fourni par Kaspersky Lab avec ce Contrat. Il restera à l'entière discrétion de

Kaspersky Lab de juger si vous remplissez les conditions d'accès prévues aux services de support technique.

(ii) Le Support technique se terminera après une durée d'un an à moins qu'il ne soit renouvelé par le paiement des droits requis et par l'envoi d'un nouveau formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription au Support technique, vous acceptez les termes de la Stratégie de Confidentialité de Kaspersky Lab jointe à ce Contrat, et vous consentez explicitement au transfert de données vers d'autres pays que le vôtre en accord avec les termes de la Stratégie de Confidentialité.

(iv) Les « Services de support technique » signifient :

(a) Mises à jour quotidiennes de la base antivirus ;

(b) Versions de mise à jour gratuites

(c) Support technique avancé par courrier électronique et par téléphone, assuré par le revendeur ou le distributeur ;

(d) Mises à jour de détection et d'éradication de virus 24/24.

4. Droits de propriété. Le logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les droits de propriété, brevets, marques déposées et autres droits de propriété intellectuelle applicables. Le fait que vous en possédiez une copie et que vous l'ayez installée ne vous donne aucun droit de propriété intellectuelle sur le logiciel.

5. Confidentialité. Vous acceptez que le Logiciel et la Documentation, y compris la conception et structure des logiciels individuels, ainsi que du Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez pas et ne fournirez en aucun cas ces informations confidentielles sous quelque forme que ce soit à un tiers sans l'autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en œuvre des mesures de sécurité minimale visant à assurer que la confidentialité du Fichier Clé d'Identification est respectée.

6. Limite de garantie

(i) Kaspersky Lab garantit que pour une durée de 90 jours suivant le téléchargement ou l'installation du logiciel ce dernier fonctionnera correctement comme spécifié dans la documentation fournie.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le logiciel et sa documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions ou d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce logiciel reconnaîtra tous les virus connus ou n'affichera pas de message de détection erroné.

(iv) La responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement au paragraphe (i) de la limite de garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous devrez fournir toutes les informations nécessaires au fournisseur pour remédier à tout problème éventuel.

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

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

7. Responsabilité

(i) Rien dans le présent Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (i) de non-satisfaction de l'utilisateur, (ii) de décès ou de dommages physiques résultant d'infractions aux lois en vigueur ou du non-respect des termes du présent Contrat, (iii) de toute infraction aux obligations impliquées par la loi « s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 » ou (iv) de responsabilité qui ne peut être exclue par la loi.

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

(a) Perte de revenus ;

(b) Perte de revenus réels ou potentiels

(c) Perte de moyens de paiement

(d) Perte d'économies prévues

(e) Perte de marché

(f) Perte d'occasions commerciales

(g) Atteinte à l'image

(h) Atteinte à la réputation

(i) Perte, dommage ou altération de données ; ou :

(j) Tout dommage direct ou indirect en dehors de ceux couverts par les limites de garanties prévues dans le présent Contrat de Licence.

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

8. L'interprétation du présent Contrat de Licence sera effectuée en accord avec la législation locale. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Lab était autorisé en tant que requérant à entamer des poursuites auprès de n'importe quelle juridiction compétente.

9. (i) Ce Contrat constitue l'accord complet liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui auraient été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet. En dehors des situations prévues par les paragraphes (ii) – (iii), vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat (« Fausse Représentation ») et Kaspersky Lab ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé.

(ii) Rien dans ce Contrat ne pourra limiter ou exclure la responsabilité de Kaspersky Lab pour toute Fausse Représentation faite en connaissance de cause.

(iii) La responsabilité de Kaspersky Lab pour Fausse Déclaration portant sur une question fondamentale, y compris pour l'obligation du fabricant de respecter ses engagements au titre de ce Contrat, sera sujette à la décharge de responsabilité du paragraphe 7 (iii).