

KASPERSKY LAB

---

Kaspersky<sup>®</sup> Anti-Spam 3.0

KASPERSKY® ANTI-SPAM 3.0

---

# Manuel de l'administrateur

©Kaspersky Lab Ltd  
<http://www.kaspersky.com>

Date d'édition : Novembre 2006

# Sommaire

CHAPITRE 1. KASPERSKY® ANTI-SPAM 3.0.....	6
1.1. Nouveautés de la version 3.0 .....	7
1.2. Licence.....	9
1.3. Configuration requise .....	9
1.4. Contenu du pack logiciel.....	10
1.4.1. Contrat de licence.....	11
1.4.2. Carte d'enregistrement.....	11
1.5. Services réservés aux utilisateurs enregistrés.....	11
1.6. Notations conventionnelles .....	12
CHAPITRE 2. ARCHITECTURE DE KASPERSKY ANTI-SPAM ET PRINCIPES DE FILTRAGE DU POURRIEL .....	14
2.1. Composition du logiciel .....	14
2.2. Technologies d'identification .....	18
2.2.1. Analyse des signes formels.....	18
2.2.2. Filtrage du contenu.....	18
2.2.3. Vérification à l'aide de services extérieurs.....	20
2.2.4. Technologie UDS (Urgent Detection System).....	20
2.3. Résultats de l'identification et actions exécutées sur les messages .....	21
2.4. Bases de filtrage du contenu.....	23
2.5. Stratégies de filtrage.....	23
2.6. Centre d'administration.....	24
2.7. Surveillance .....	24
CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-SPAM.....	26
3.1. Préparatifs en vue de l'installation.....	26
3.2. Installation de la distribution de Kaspersky Anti-Spam .....	27
3.3. Configuration de l'accès au Centre d'administration .....	28
3.4. Installation de la clé de licence.....	29
3.5. Intégration de Kaspersky Anti-Spam au serveur de messagerie.....	30
3.6. Configuration de la mise à jour des bases de filtrage du contenu et de l'utilisation du service UDS .....	32
CHAPITRE 4. ADMINISTRATION DU SERVEUR DE FILTRAGE DU COURRIER INDESIRABLE.....	34
4.1. Lancement et administration des composants de Kaspersky Anti-Spam.....	34
4.2. Centre d'administration de Kaspersky Anti-Spam.....	35
4.3. Administration de la stratégie de filtrage.....	36
4.3.1. Stratégie de filtrage globale.....	37
4.3.1.1. Section <i>General</i> .....	39
4.3.1.2. Section <i>DNS &amp; SPF Checks</i> .....	41
4.3.1.3. Section <i>Headers Checks</i> .....	42
4.3.1.4. Section <i>Eastern Encodings</i> .....	44

4.3.1.5. Section <i>Obscene Content</i> .....	45
4.3.2. Administration des listes "blanche" et "noire" .....	45
4.3.3. Administration des listes des services DNSBL utilisés .....	47
4.3.4. Administration de la liste des domaines protégés .....	49
4.3.5. Administration des groupes .....	50
4.3.6. Administration de la stratégie de filtrage de groupe .....	53
4.3.7. Actions à exécuter sur les messages .....	54
4.4. Mise à jour des bases de filtrage du contenu .....	57
4.4.1. Configuration de la mise à jour .....	58
4.4.2. Lancement de la mise à jour .....	60
4.5. Configuration du serveur de filtrage du courrier indésirable .....	61
4.5.1. Paramètres généraux du serveur de filtrage .....	62
4.5.2. Paramètres de fonctionnement du processus maître de filtrage .....	64
4.5.3. Paramètres des processus de filtrage .....	65
4.5.4. Paramètres d'identification du courrier indésirable .....	66
4.5.5. Paramètres des modules clients .....	68
4.5.6. Notifications de non-réception d'un message .....	69
4.6. Configuration du Centre d'administration .....	71
4.7. Gestion des clés de licence .....	72
4.7.1. Consultation des informations relatives aux licences .....	73
4.7.2. Installation d'une nouvelle clé de licence .....	74
4.7.3. Suppression de la clé de licence .....	75
4.8. Surveillance du fonctionnement du serveur de filtrage .....	75
4.8.1. Messages généraux sur l'état du logiciel .....	75
4.8.1.1. Informations détaillées sur le moteur du serveur de filtrage .....	77
4.8.1.2. Informations détaillées sur le module de mise à jour .....	78
4.8.1.3. Informations détaillées sur le module de licence .....	80
4.8.2. Messages et rapports du système de surveillance .....	81
4.9. Statistiques de Kaspersky Anti-Spam .....	82
CHAPITRE 5. SUPPRESSION DE KASPERSKY ANTI-SPAM .....	84
CHAPITRE 6. QUESTIONS FREQUEMMENT POSEES .....	86
ANNEXE A. INFORMATIONS COMPLEMENTAIRES SUR KASPERSKY ANTI- SPAM .....	90
A.1. Répartition des fichiers du logiciel dans les divers répertoires .....	90
A.2. Modules clients des serveurs de messagerie .....	91
A.2.1. Interaction des modules clients avec le serveur de filtration .....	92
A.2.2. Paramètres généraux des modules clients .....	92
A.2.3. <i>kas-milter</i> : module client pour le serveur de messagerie Sendmail .....	94
A.2.4. <i>kas-pipe</i> : module client pour les serveurs de messagerie Postfix et Exim .....	96
A.2.5. <i>kas-exim</i> : module client pour le serveur de messagerie Exim .....	103
A.2.6. <i>kas-qmail</i> : module client pour le serveur de messagerie Qmail .....	105
A.2.7. <i>kas-cgpro</i> : module client pour le serveur de messagerie Communigate Pro .....	107
A.3. Fichiers de configuration de Kaspersky Anti-Spam .....	109
A.3.1. Fichier de configuration principal <i>filter.conf</i> .....	109

---

A.3.2. Fichier de configuration <i>kas.httppd.conf</i> .....	115
A.4. Utilitaires de Kaspersky Anti-Spam .....	116
A.4.1. <i>kas-htpasswd</i> .....	116
A.4.2. <i>kas-show-license</i> .....	116
A.4.3. <i>install-key</i> .....	117
A.4.4. <i>remove-key</i> .....	118
A.4.5. <i>kas-restart</i> .....	119
A.4.6. <i>mkprofiles</i> .....	120
A.4.7. <i>sfmonitoring</i> .....	121
A.4.8. <i>sfupdates</i> .....	122
A.5. Champs d'en-tête spéciaux du module de filtrage.....	123
A.6. Paramètres du service <i>cron</i> .....	126
ANNEXE B. ENVOI D'EXEMPLES DE POURRIELS AUX EXPERTS DE KASPERSKY LAB.....	130
ANNEXE C. KASPERSKY LAB LTD.....	132
C.1. Autres produits antivirus .....	133
C.2. Comment nous contacter .....	142

# CHAPITRE 1. KASPERSKY®

## ANTI-SPAM 3.0

**Kaspersky® Anti-Spam 3.0** (par la suite, *Kaspersky Anti-Spam* ou le logiciel) est une suite logicielle chargée de filtrer le courrier électronique afin que la boîte aux lettres de l'utilisateur du système de messagerie ne soit pas inondée par le pourriel, cet ensemble de messages non sollicités.

Sur la base de règles définies par l'administrateur, Kaspersky Anti-Spam peut traiter les messages de différentes manières : délivrer le message tel quel au destinataire, le bloquer, créer un message sur l'impossibilité de recevoir ce message, ajouter ou modifier les champs de l'en-tête ou d'autres actions.

La présence d'indices caractéristiques des messages non sollicités est recherchée dans chaque message.

**Tout d'abord**, l'analyse porte sur divers paramètres du message : adresses de l'expéditeur et du destinataire (enveloppe), taille du message et les différents champs de l'en-tête (y compris les champs *From* et *To*). De plus, Kaspersky Anti-Spam en profite pour réaliser les vérifications suivantes :

Recherche de l'adresse de l'expéditeur du message (courrier électronique et/ou adresse IP) dans les listes "noire" et "blanche" ;

Recherche de l'adresse IP de l'expéditeur dans les listes noires DNS (DNSBL) ;



**DNSBL (liste noire DNS)** est une base de données d'adresses IP de serveurs de messagerie connus pour les envois non contrôlés. Ces serveurs acceptent le courrier de n'importe où et le transmettent à n'importe qui. Grâce à l'utilisation des listes DNSBL, il est possible d'interdire automatiquement la réception de courrier en provenance de ces serveurs. La politique de composition de ces listes varie en fonction des services qui les proposent. Il est conseillé d'étudier attentivement la politique du service avant d'utiliser la liste qu'il propose pour filtrer le courrier.

- Recherche d'enregistrements DNS sur le serveur d'origine (reverse DNS lookup) ;
- Recherche de l'adresse IP de l'expéditeur dans la liste des adresses autorisées pour le domaine grâce à la technologie SPF (Sender Policy Framework) ;
- Vérification des adresses et des liens repris dans le message à l'aide du service SURBL (Spam URI Realtime Blocklist).

**Ensuite**, le logiciel exploite le filtrage selon le contenu. Autrement dit, le contenu du message (y compris le champ *Subject* de l'en-tête) et les fichiers joints<sup>1</sup> sont analysés. Cette opération repose sur des algorithmes linguistiques bâtis autour de la comparaison d'échantillons et sur la recherche d'expressions types (mots ou groupes de mots).

Kaspersky Anti-Spam analyse également les images et les compare aux signatures de messages non sollicités connus. Les résultats de cette comparaison sont pris en compte lorsqu'il s'agit de décider si un message est indésirable ou non.

Les messages présentant des signes caractéristiques des messages non sollicités sont soumis aux actions définies par la stratégie de filtrage (cf. point 2.3, p. 21).

C'est l'administrateur qui configure la stratégie de filtrage à l'aide du Centre d'administration (cf. point 2.6, p. 24).

## 1.1. Nouveautés de la version 3.0

Kaspersky Anti-Spam 3.0 intègre toutes les fonctions éprouvées des versions antérieures et propose quelques améliorations :

### 1. Nouvelle version du moteur de filtrage SpamTest.

Le nouveau moteur de filtrage intégré à Kaspersky Anti-Spam 3.0 possède les caractéristiques suivantes :

- Performances et stabilité accrues ;
- Très peu gourmand en mémoire vive ;
- Trafic Internet (actualisation des bases de filtrage du contenu) réduit.

### 2. Perfectionnement des méthodes de filtrage.

La presque totalité des méthodes d'identification du courrier indésirable utilisées dans les versions antérieures ont été perfectionnées :

- Améliorations des algorithmes d'interprétation des objets HTML dans les messages (renforce l'efficacité de la lutte contre les différentes astuces employées par les spammeurs afin de déjouer les filtres) ;

---

<sup>1</sup> L'analyse porte sur les fichiers au format Plain text, HTML, Microsoft Word et RTF (pour de plus amples renseignements, consultez le point 2.2.2 à la page 18).

- Elargissement et amélioration du système d'analyse des en-têtes des messages électroniques ;
- Perfectionnement de l'analyse des pièces jointes graphiques (GSG) ;
- Ajout des technologies SPF (Sender Policy Framework) et SURBL (Spam URL Realtime Blocklists).
- Intégration du service Urgent Detection System (UDS) développé par Kaspersky Lab afin d'obtenir des données en temps réel sur certains types de pourriels.

### 3. Interface utilisateur refondue.

Kaspersky Anti-Spam 3.0 utilise le Centre d'administration qui permet de :

- Configurer le logiciel : règles de filtrage, actions à exécuter sur les messages, paramètres de performance, etc. ;
- Administrer les licences d'utilisation : installation des clés de licence, consultation des données relatives à la licence actuelle ;
- Surveiller le fonctionnement du logiciel et consulter les statistiques.

### 4. Facilité de la configuration des stratégies de filtrage.

A partir de la version 3.0, la configuration des stratégies de filtrage s'opère via l'interface intuitive du Centre d'administration, ce qui donne les avantages suivants :

- **Facilité de l'administration : l'interface** dépouillée propose une sélection minimale d'outils indispensables à l'administration du système et offre de grandes possibilités d'adaptation du système à des conditions d'exploitation particulières ;
- **Configurations différentes en fonction des groupes d'utilisateurs** : il est possible pour chaque groupe distinct d'activer ou de désactiver certaines méthodes de vérification et de définir les actions à exécuter sur les messages.

### 5. Améliorations des outils d'intégration et des infrastructures du logiciel :

- Les modules d'interaction avec les serveurs de messagerie tels que Sendmail et Communigate Pro ont été refondus et améliorés ;
- Mise au point d'un nouveau système de livraison des actualisations des bases de filtrage du contenu ;

- Tous les paramètres sont regroupés au sein d'un fichier de configuration unique, ce qui contribue à la simplicité de la configuration et de l'administration du système.

## 1.2. Licence

La politique de licence applicable à Kaspersky Anti-Spam 3.0 impose des restrictions d'utilisation en fonction des critères suivants :

- Volume du trafic de messagerie ;
- Nombre d'adresses de courrier électronique protégées.

Les limitations indiquées sont applicables uniquement aux messages adressés aux utilisateurs des domaines protégés. La liste des domaines protégés dont le trafic de messagerie est filtré par le logiciel est composée à l'aide du Centre d'administration (cf. point 4.3.4, p. 49). Le courrier adressé aux utilisateurs de domaines qui ne figurent pas dans la liste n'est pas filtré.



Composez la liste des domaines à protéger avant de commencer à utiliser Kaspersky Anti-Spam.

## 1.3. Configuration requise

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

- Processeur Intel Pentium III, 500 Mhz.
- Au moins 512 Mo de RAM disponible.
- Un des systèmes d'exploitation suivants :
  - RedHat Linux 9.0.
  - Fedora Core 3.
  - RedHat Enterprise Linux Advanced Server 3.
  - SuSe Linux Enterprise Server 9.0.
  - SuSe Linux Professional 9.2.
  - Mandrakelinux version 10.1.
  - Debian GNU/Linux 3.1.
  - FreeBSD 4.10.

- FreeBSD 5.4 .
- Un des serveurs de messagerie suivant :
  - Sendmail 8.13.5 avec prise en charge de Milter API.
  - Postfix 2.2.2.
  - Qmail 1.03.
  - Exim 4.50.
  - CommuniGate Pro 4.3.7.
- Les utilitaires *bzip2* et *which*.
- Interprète Perl.

## 1.4. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Spam chez un distributeur ou détaillant, ou en visitant un de nos magasins en ligne (par exemple, [www.kaspersky.com/fr](http://www.kaspersky.com/fr), rubrique **Boutique en ligne**).

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



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

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

## 1.4.1. Contrat de licence

Le contrat de licence est l'accord légal conclu entre vous et Kaspersky Lab qui précise les conditions d'utilisation du logiciel que vous venez d'acquérir.

*Lisez attentivement le contrat de licence !*

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

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

## 1.4.2. Carte d'enregistrement

Veillez remplir le talon détachable de la carte d'enregistrement en indiquant de manière exhaustive vos coordonnées : nom de famille, prénom, numéro de téléphone, adresse électronique (le cas échéant) et envoyez-le au distributeur chez qui vous avez acheté ce logiciel.

Veillez signaler toute modification de vos coordonnées (adresse postale/électronique et numéro de téléphone) à l'organisation à laquelle vous avez envoyé le talon détachable de la carte d'enregistrement.

La carte d'enregistrement est le document attestant votre statut d'utilisateur enregistré auprès de notre société. Ceci vous donne accès à notre service d'assistance technique pendant la durée de validité de la licence. De plus, les utilisateurs enregistrés qui s'abonnent au bulletin d'informations de Kaspersky Lab Ltd. sont régulièrement informés du lancement de nouveaux logiciels.

## 1.5. Services réservés aux utilisateurs enregistrés

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

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

- Nouvelles versions de ce logiciel, fournies gratuitement ;

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



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

## 1.6. Notations conventionnelles

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

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

<b>Mise en forme</b>	<b>Fonction sémantique</b>
 Solution	Solution du problème exposé
[argument] – valeur de l'argument.	Argument de la ligne de commande.
Texte des messages d'information et de la ligne de commandes	Texte des fichiers de configuration, des messages d'information et de la ligne de commandes.

# CHAPITRE 2. ARCHITECTURE DE KASPERSKY ANTI-SPAM ET PRINCIPES DE FILTRAGE DU POURRIEL

Ce chapitre décrit les principaux composants du logiciel ainsi que les principes de filtrage. Il présente également l'outil principal utilisé pour l'administration de Kaspersky Anti-Spam, à savoir le Centre d'administration.

## 2.1. Composition du logiciel

Kaspersky Anti-Spam 3.0 est un système d'identification et de filtrage du pourriel intégré au serveur de messagerie. Kaspersky Anti-Spam 3.0 n'est pas un serveur de messagerie à part entière capable de recevoir le courrier, de le relayer ou d'acheminer les messages électroniques dans les boîtes aux lettres des utilisateurs finaux. L'architecture interne de Kaspersky Anti-Spam est présentée dans l'illustration 1.

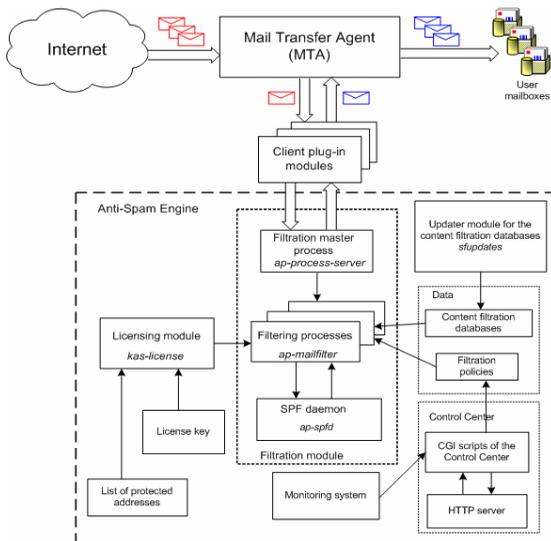


Illustration 1. Architecture de Kaspersky Anti-Spam

Kaspersky Anti-Spam contient les composants suivants :

- **Modules clients** : responsables de l'intégration du logiciel au serveur de messagerie.
- **Serveur de filtrage** : composant chargé de l'analyse, du classement et du traitement des messages. Le serveur de filtrage renferme des modules auxiliaires qui lui permettent de réaliser son travail et qui assurent l'intégration aux serveurs de messagerie :
  - Module de filtrage : module chargé du filtrage du courrier indésirable.
  - Module de licence : module chargé de l'administration des licences et de la liste des domaines protégés.
  - Bases de filtrage du contenu : données exploitées par le serveur de filtrage lors du classement des messages ; les mises à jour des bases de filtrage du contenu sont publiées toutes les 20 minutes sur les serveurs de Kaspersky Lab.
  - Module d'actualisation des bases de filtrage du contenu : système chargé du téléchargement automatique des bases de filtrage du contenu depuis les serveurs de mise à jour et de leur installation en vue de l'utilisation par le serveur de filtrage du pourriel.
  - Centre d'administration : interface Web qui permet à l'administrateur système de configurer le logiciel et d'analyser son état et ses capacités.
  - Système de surveillance : système chargé du contrôle de l'état de Kaspersky Anti-Spam et de ses composants et qui signale à l'administrateur les divers incidents qui surviennent lors de l'utilisation du logiciel.

**Les modules clients** interviennent au niveau de l'intégration de Kaspersky Anti-Spam à divers serveurs de messagerie. Chaque module client tient compte des particularités du serveur de messagerie et du mode d'intégration sélectionné.

Kaspersky Anti-Spam est livré avec des modules clients pour les serveurs de messagerie Sendmail, Postfix, Exim, Qmail et Communigate Pro.

En règle générale, le module client est installé en guise de filtre et il reçoit du serveur les messages à filtrer et renvoie les messages modifiés.

C'est le serveur de messagerie qui lance les modules clients. Sendmail constitue la seule exception en la matière. Le serveur de messagerie peut lancer plusieurs modules clients afin de pouvoir traiter plusieurs messages en parallèle. Consultez le point A.2 à la page 91 pour obtenir de plus amples informations sur les modules clients et les modes d'intégration aux serveurs de messagerie.

Quelles que soient les particularités d'un module client ou d'un autre, son interaction avec le serveur de filtrage s'opère via le socket de réseau ou le socket local à l'aide du protocole interne d'échange de données.

**Le serveur de filtrage** répond aux requêtes des clients, reçoit les messages à vérifier et renvoie les résultats.

Dans le cadre de la procédure d'installation standard, le serveur de messagerie avec le module client intégré et le serveur de filtrage sont installés sur la même machine.

Il est possible toutefois d'installer le serveur de filtrage de Kaspersky Anti-Spam sur un serveur distinct : dans ce cas, les modules clients tournant sur un autre ordinateur (serveur) échangeront les données avec le serveur de filtrage via le réseau local en utilisant le protocole TCP.

Lorsqu'il tourne sur un ordinateur dédié, le serveur de filtrage peut surveiller simultanément plusieurs serveurs de messagerie à condition que la puissance de l'ordinateur utilisé soit suffisante pour traiter l'ensemble du trafic de messagerie.

**Le serveur de filtrage** contient :

- Le module de filtrage chargé de la vérification du courrier.
- Le module de licence, chargé de vérifier l'existence d'une clé de licence active et le respect des restrictions imposées par la licence acquise.
- Le démon de traitement des requêtes SPF.
- Le script de chargement et de compilation automatique de l'actualisation des bases de filtrage du contenu.
- Le Centre d'administration.
- Les programmes et les scripts auxiliaires.

Le processus maître de filtrage (*ap-process-server*) est le composant principal du module de filtrage. Il remplit les fonctions suivantes :

- Suivi des requêtes de connexion au processus de filtrage émanant des modules clients ;
- Lancement de nouveaux processus de filtrage lorsque tous les processus existants sont occupés ;
- Contrôle de l'état des processus exécutés ;
- Arrêt des processus fils suite à la réception du signal correspondant (par exemple, SIGHUP).

Lorsque le trafic de messagerie est volumineux, le nombre de processus de filtrage exécutés peut atteindre plusieurs dizaines. Lorsque la charge sur le

serveur de messagerie diminue, les processus de filtrage libérés s'arrêtent. Les nombres maximum et minimum de processus de filtrage exécutés sont définis dans les paramètres du serveur de filtrage (cf. point A.3.1, p. 109).

Le processus de filtrage (ap-mailfilter) charge les stratégies de filtrage utilisées ainsi que les bases de filtrage de contenu lorsqu'il est lancé. Une fois que la connexion avec le module client a été établie, le processus de filtrage reçoit de celui-ci les en-têtes et le corps des messages, les analyse et renvoie au module les résultats de ces analyses.

Si l'expéditeur du message doit être vérifié conformément à la stratégie SPF, le processus de filtrage transmet la requête au démon SPF (ap-sfpd) qui se chargera de sonder le serveur DNS avant de renvoyer les résultats de l'analyse au processus de filtrage.

L'analyse des messages et l'application des règles définies dans les stratégies de filtrage sont possibles uniquement lorsqu'il existe une clé de licence en cours de validité.

Toutes les vérifications liées à la licence incombent au module de licence (*kas-license*) sur requête du processus de filtrage.

Lorsqu'il a terminé de traiter un message, le processus de filtrage ne s'arrête pas pour autant : il attend la requête suivante. Le processus de filtrage s'arrête uniquement lorsqu'il a traité le nombre maximum de messages pour un processus (en général, 300) ou lorsqu'il reste trop longtemps en attente.

**L'exécution du script de chargement automatique des mises à jour** (*sfupdates*) est programmée (à l'aide du service **cron**). Il permet de télécharger la dernière version des bases de filtrage de contenu depuis les serveurs de mise à jour, de récolter les versions de la base et de l'installer en vue d'une utilisation par le serveur de filtrage.

**Le Centre d'administration** est une interface Web qui permet à l'administrateur du système de configurer le logiciel et les stratégies de filtrage du pourriel.

**Le système de surveillance contrôle** l'état des composants de Kaspersky Anti-Spam et prévient l'administrateur du système chaque fois qu'un incident survient dans le fonctionnement du serveur de filtrage et des autres composants du logiciel.

Kaspersky Anti-Spam 3.0 traite le flux de messagerie selon l'algorithme suivant :

1. Le module client du logiciel s'intègre au serveur de messagerie installé.
2. Le serveur de messagerie transmet les messages au module client en vue d'une analyse par le serveur de filtrage.
3. Le serveur de filtrage recherche la présence d'indices de pourriel dans les messages et en fonction du résultat obtenu, il modifie les messages conformément aux règles définies.

4. Les messages traités sont renvoyés au serveur de messagerie par le module client en vue d'être envoyés aux destinataires.

## 2.2. Technologies d'identification

Kaspersky Anti-Spam est un puissant outil de détection des pourriels dans le flux de messagerie électronique. Cette rubrique est consacrée au survol des technologies d'identification du pourriel mise en oeuvre dans le logiciel.

### 2.2.1. Analyse des signes formels

Cette méthode exploite un ensemble de règles qui reposent sur la vérification de la présence de champs d'en-tête déterminés dans un message et sur la comparaison de ceux-ci à une sélection de champs d'en-tête propres aux messages non sollicités. En plus de l'analyse des en-têtes lors de la découverte de messages non sollicités, le système tient compte de la structure du message, de sa taille, de la présence de pièces jointes et d'autres indices similaires.

La méthode permet également d'analyser les données transmises par l'expéditeur lors d'une séance SMTP. L'analyse porte plus particulièrement sur les informations suivantes :

- Adresse IP du serveur d'où arrive le message et présence de celle-ci dans les listes "noire" ou "blanche" d'expéditeurs ;
- Adresse IP des serveurs intermédiaires de transmission tirée du champ Received de l'en-tête ;
- Adresses électroniques de l'expéditeur et des destinataires transmises dans les commandes de la séance SMTP ;
- Présence des adresses de l'expéditeur et des destinataires dans les listes "noire" ou "blanche" d'adresses ;
- Correspondance entre les adresses transmises dans la séance SMTP et le groupe d'adresses indiquées dans les en-têtes des messages ainsi que toute une série d'autres vérifications.

### 2.2.2. Filtrage du contenu

Kaspersky Anti-Virus 3.0 réalise un filtrage au niveau du contenu lors de l'analyse des messages électroniques. Qui plus est, les technologies intelligentes permettent d'analyser non seulement le contenu du message (y compris le champ *Subject* de l'en-tête), mais également les pièces jointes au format suivant :

- Texte : plain text (ASCII, non multioctet) ;
- HTML (2.0, 3.0, 3.2, 4.0, XHTML 1.0) ;
- Microsoft Word (version 6.0, 95/97/2000/XP) ;
- RTF.



Le filtrage du courrier indésirable vise à réduire le nombre de messages sollicités qui arrivent dans les boîtes aux lettres des utilisateurs. Il est impossible de garantir une exclusion à 100 pour cent du courrier indésirable car des critères de filtrage trop stricts entraîneraient le rejet de messages normaux.

Trois groupes de méthodes sont utilisés pour identifier le courrier indésirable :

- **Comparaison du message à des exemples sémantiques** de diverses catégories (sur la base de la recherche de mots clés dans le corps du texte (mots et expressions) et leur analyse de probabilité ultérieure). Cette méthode lance une recherche heuristique de phrases et de tournures typiques dans le texte.
- **Comparaison du message analysé à un ensemble d'exemples** au niveau des signatures. Cette méthode permet d'identifier les modifications de messages non sollicités.
- **Analyse des pièces jointes graphiques.**

Toutes les données utilisées par Kaspersky Anti-Spam pour le filtrage au niveau du contenu (*répertoire* (liste hiérarchisée des catégories), exemples de message, termes caractéristiques) sont sauvegardées dans les bases de filtrage du contenu



L'équipe de spécialistes de l'identification du courrier indésirable de Kaspersky Lab travaille en permanence à l'enrichissement des bases de filtrage de contenu. Il est dès lors conseillé d'actualiser ces bases régulièrement (cf. point 4.4, p. 57).

Kaspersky Lab accepte également les échantillons de pourriels qui n'ont pas été identifiés par Kaspersky Anti-Spam ainsi que les messages considérés par erreur comme courrier indésirable. Ces échantillons nous aideront à améliorer nos bases de filtrage du contenu et à réagir plus efficacement face aux nouveaux types de courrier indésirable. Pour obtenir de plus amples informations, consultez le point 0 à la page 130.

### 2.2.3. Vérification à l'aide de services extérieurs

En plus de l'analyse du texte et des en-têtes de message, Kaspersky Anti-Virus permet de réaliser les vérifications suivantes à l'aide de services de réseau externes :

- Recherche de l'adresse IP de l'expéditeur dans le DNS (reverse DNS lookup) ;
- Recherche de l'adresse IP de l'expéditeur dans un ou plusieurs services DNSBL (DNS-based black hole list) ;
- Correspondance entre l'adresse de l'expéditeur et la stratégie SPF (Sender Policy Framework) du domaine auquel appartient le serveur de messagerie qui a envoyé le message ;
- Vérification des liens du message dans la base des adresses de pourriel grâce au service SURBL (Spam URL Realtime Blocklists, [www.surbl.org](http://www.surbl.org)).
- Identification des messages électroniques grâce à la technologie UDS (Urgent Detection System).

Toutes ces vérifications, à l'exception des vérifications UDS, reposent sur l'utilisation du protocole DNS et ne requièrent aucune configuration complémentaire du réseau.

### 2.2.4. Technologie UDS (Urgent Detection System)

La technologie **UDS** (Urgent Detection System) est une technologie originale développée et soutenue par Kaspersky Lab pour l'identification des messages non sollicités. Cette technologie repose sur les principes suivants :

1. Les indices contribuant à l'identification du courrier sont isolés dans le message à analyser. Ces indices peuvent regrouper des informations des en-têtes, des extraits de texte et d'autres renseignements sur le message traité.
2. Sur la base des indices obtenus, le serveur de filtrage compose une requête UDS compacte et l'envoie à un des serveurs UDS de Kaspersky Lab.



Dans la mesure où aucune donnée permettant d'établir l'identité des destinataires ou le contenu du message traité n'est envoyée au serveur, cette méthode ne présente aucun risque en matière de confidentialité des données.

3. Une fois que la requête est arrivée au serveur UDS, elle est analysée à l'aide de la base des pourriels connus. Si la requête correspond à un pourriel connu, le serveur de filtrage reçoit une notification indiquant que le message en question est plus que probablement un courrier indésirable. Ce renseignement est pris en compte lors de l'attribution d'un état au message.



La technologie UDS permet d'isoler les messages non sollicités connus sans devoir attendre l'actualisation des bases de filtrage du contenu.

Les échanges entre le serveur de filtrage et les serveurs UDS de Kaspersky Lab s'opèrent via le protocole UDP sur le port 7060. Afin de pouvoir utiliser la technologie UDS, le serveur de filtrage doit pouvoir établir des connexions sortantes sur ce port.

Les informations relatives aux serveurs UDS accessibles sont reprises dans les bases de filtrage du contenu. La sélection du serveur UDS qui analysera les messages est réalisée automatiquement sur la base de l'analyse du temps de réponse des serveurs UDS disponibles.

## 2.3. Résultats de l'identification et actions exécutées sur les messages

Après l'analyse, chaque message reçoit un des états suivants :

- **Spam** : le message a été classé comme courrier indésirable avec un coefficient de certitude élevé.
- **Probable Spam** : le message contient certains signes caractéristiques des messages non sollicités mais il ne peut pas être classé définitivement comme un message non sollicité.
- **Formal** : le message est un courrier formel, par exemple la notification d'un serveur de messagerie sur la délivrance ou non d'un message ou sur la présence d'un virus dans le courrier. Cette catégorie reprend les messages diffusés automatiquement par les programmes de messagerie. Ils ne sont jamais considérés comme du courrier indésirable.

- **Trusted** : message reçu d'une source de confiance (par exemple, un serveur de messagerie interne). La liste des sources de confiance (liste "blanche" d'expéditeurs) est rédigée par l'administrateur. Le statut **Trusted** est également octroyé aux messages destinés aux utilisateurs pour lesquels la stratégie de recherche de pourriels dans le courrier est désactivée.
- **Blacklisted** : le message provient d'une adresse figurant sur la liste "noire" des expéditeurs. C'est l'administrateur qui compose la liste "noire" des expéditeurs.
- **Not detected** : le message n'est pas considéré comme un courrier indésirable.

Chaque message ne peut recevoir qu'un seul des statuts repris ci-dessus. Le statut attribué au message est repris dans le champ spécial **X-Spamtest-Status-Extended** de l'en-tête. Pour obtenir de plus amples informations sur les champs ajoutés aux en-têtes des messages après le filtrage, consultez le point A.5 à la page 123.

Après l'identification, le message électronique sera soumis à une des actions suivantes :

- Acceptation du message ;
- Transfert du message ou de sa copie vers une autre adresse ;
- Ajout d'un commentaire dans le sujet du message ;
- Ajout d'un champs spécial dans l'en-tête du message ;
- Suppression du message ;
- Rejet du message.

L'administrateur décide de l'action qui sera exécutée sur le message correspondant à un état particulier.



Dans le cadre de la configuration du logiciel, la priorité de l'administrateur doit être la conservation de tous les messages utiles car la perte d'un seul message important peut avoir des conséquences bien pire pour le destinataire que la réception de dizaines de messages non sollicités. Afin d'éviter la perte d'informations importantes, il est conseillé de ne pas appliquer un traitement radical aux messages considérés comme du courrier indésirable ou du courrier indésirable potentiel suite à l'analyse du contenu. Par exemple, le simple texte **[!! SPAM]** dans l'objet du message peut suffire.

## 2.4. Bases de filtrage du contenu

L'identification des pourriels s'opère sur la base des informations contenues dans les bases de filtrage du contenu régulièrement mises à jour. Les bases de filtrage du contenu contiennent les ensembles de règles, de termes et de signatures de messages utilisés lors du filtrage.

Les bases de filtrage du contenu sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab à l'aide du module de mise à jour. Afin de réduire le volume des informations téléchargées, chaque fois que le système de mise à jour contacte le serveur, il télécharge uniquement les fichiers qui ont été actualisés.

Dans la mesure où de nouveaux types de courriers indésirables apparaissent chaque jour, il est conseillé de maintenir les bases de filtrage du contenu à jour afin de garantir le bon fonctionnement du logiciel. La fréquence d'actualisation recommandée est toutes les vingt minutes.



**N'oubliez pas d'actualiser les bases de filtrage du contenu directement après avoir installé le logiciel sur votre ordinateur !**

## 2.5. Stratégies de filtrage

Les stratégies de filtrage sont appliquées par Kaspersky Anti-Spam afin de définir la méthode d'identification du courrier indésirable, les actions à exécuter sur les messages et les listes "noire" et "blanche" d'expéditeurs.

Le logiciel exploite une stratégie de filtrage à deux niveaux : une stratégie de filtrage globale et des stratégies de filtrage de groupe. La stratégie de filtrage globale contient les paramètres communs à tous les groupes : méthodes utilisées pour l'identification des messages et les listes "noire" et "blanche" des expéditeurs. Les stratégies de groupe définissent, en plus des paramètres cités, les actions qui seront exécutées sur les messages en fonction de leur état.

Avant de configurer les stratégies de groupe, l'administrateur doit créer les groupes sous la forme de liste d'adresses de destinataires.

L'application des stratégies suit la règle suivante : la stratégie de filtrage globale détermine les valeurs par défaut des paramètres pour tous les groupes tandis que la configuration des stratégies de groupe peut conserver ces valeurs ou les modifier. Ainsi, les groupes d'utilisateurs qui requièrent un filtrage plus strict du courrier peuvent avoir des méthodes d'identification renforcées et des actions plus dures.

La sélection des paramètres d'identification est étroitement liée aux propriétés des bases de filtrage du contenu et elle peut être étendue en fonction de

l'émergence de nouveaux types de pourriels et de nouvelles règles d'identification. Les nouveaux paramètres seront ajoutés à l'interface du Centre d'administration de Kaspersky Anti-Spam au fil des mises à jour.

## 2.6. Centre d'administration

Le centre d'administration (*Control center*) est une application Internet qui permet à l'administrateur de commander et de configurer Kaspersky Anti-Spam.

Le Centre d'administration remplit les fonctions suivantes :

- Surveillance de l'état du logiciel et de ses divers composants ;
- Installation des clés de licence et administration de la liste des domaines protégés ;
- Affichage et exportation des statistiques relatives aux messages traités ;
- Administration des stratégies globale et de groupe de filtrage du courrier indésirable ;
- Configuration du serveur de filtrage et des autres composants du logiciel.

## 2.7. Surveillance

Le module de surveillance permet à Kaspersky Anti-Spam de contrôler l'état du serveur de filtrage du courrier indésirable.

Les informations relatives à l'état du système sont reprises dans la section **Monitoring** du Centre d'administration.

The screenshot shows the 'Monitoring' section of the Kaspersky Anti-Spam Administration Console. The interface has a dark green header with the Kaspersky logo and 'Anti-Spam' text. Below the header, there are tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' tab is active, showing a 'System Information' table with the following data:

System Information		12:06
Host Name:	mail.test.local	
System:	FreeBSD 5.4-RELEASE-p7 i386	
Load Average:	0.13	

Below the system information, there is a 'Kaspersky Anti-Spam' section with the following data:

Product:	Kaspersky Anti-Spam Enterprise Edition
Version:	3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45
Anti-Spam Engine:	Errors...
Updates:	OK
License:	Errors...

At the bottom of the console, there is a copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 2. Section **Monitoring** du Centre d'administration

Cette section contient les paramètres qui définissent la surveillance du système et les messages du module qui vous permettent d'analyser l'état actuel des composants de Kaspersky Anti-Spam.

Le processus de surveillance produit également des notifications et des rapports. Le script de surveillance est exécuté régulièrement et dès qu'un problème est identifié, l'administrateur reçoit un message avec les données relatives à l'incident. Les messages sont envoyés dès que le problème a été décelé. L'administrateur est ainsi toujours au courant des situations qui nécessitent son intervention.

Si le problème n'est pas réglé, le système de surveillance enverra chaque jour un rapport reprenant tous les problèmes identifiés et non résolus.

Le Centre d'administration permet de définir l'adresse électronique à laquelle le système de surveillance enverra les messages.

# CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-SPAM

Ce chapitre est consacré à l'installation du logiciel, à l'intégration des modules clients au serveur de messagerie et à la configuration de l'accès au Centre d'administration, le principal outil d'administration de l'application.

## 3.1. Préparatifs en vue de l'installation

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

- Assurez-vous que la configuration matérielle et logicielle du système répond aux exigences minimales pour l'installation de Kaspersky Anti-Spam (cf. point 1.3, p. 9).
- Assurez-vous que vous détenez une clé de licence pour Kaspersky Anti-Spam 3.0 ;
- Assurez-vous que les programmes *bzip2*, *perl* et *which* sont installés ;
- Assurez-vous que votre serveur de messagerie fonctionne correctement ;
- Conservez une copie de sauvegarde des fichiers de configuration du serveur de messagerie ;
- Ouvrez une session avec les privilèges de l'utilisateur **root**.



Il est conseillé de procéder à l'installation du logiciel au cours d'une période où le serveur de messagerie n'est pas fort sollicité.

Kaspersky Anti-Spam s'installe en cinq étapes :

1. Installation de la distribution de Kaspersky Anti-Spam.
2. Installation de la clé de licence.
3. Intégration des modules clients au serveur de messagerie.
4. Configuration du serveur HTTP pour l'accès au Centre d'administration.
5. Configuration de la mise à jour des bases de filtrage du contenu et de l'utilisation du service UDS.

Les points suivants offrent une description détaillée de chacune de ces étapes.

## 3.2. Installation de la distribution de Kaspersky Anti-Spam

La distribution de Kaspersky Anti-Spam 3.0 existe en plusieurs variantes :

- Un paquetage rpm pour la majorité des versions du système d'exploitation Linux (RedHat, SuSe, Mandrake, Fedora, etc.) ;
- Un paquetage deb pour la distribution Debian ;
- Un paquetage tgz pour le système d'exploitation FreeBSD 4.10 ;
- Un paquetage tbz pour le système d'exploitation FreeBSD 5.4 ;

Le choix du paquet d'installation dépend du système d'exploitation installé.

Pour lancer l'installation de Kaspersky Anti-Spam au départ du paquetage rpm, saisissez dans la ligne de commande :

```
# rpm -i kas-3-<version de la distribution>.i386.rpm
```

Pour lancer l'installation de Kaspersky Anti-Spam au départ du paquetage deb, saisissez dans la ligne de commande :

```
# dpkg -i kas-3-<version de la distribution>.i386.deb
```

Pour lancer l'installation de Kaspersky Anti-Spam au départ du paquetage tgz, saisissez dans la ligne de commande :

```
# pkg_add kas-3-<version de la distribution>.tgz
```

Pour lancer l'installation de Kaspersky Anti-Spam au départ du paquetage tbz, saisissez dans la ligne de commande :

```
# pkg_add kas-3-<version de la distribution>.tbz
```

- Les actions suivantes sont exécutées au cours de l'installation :
- Création de l'utilisateur et du groupe **mailflt3** sous les privilèges duquel Kaspersky Anti-Spam sera exécuté ;
- Installation de l'ensemble des programmes faisant partie de Kaspersky Anti-Spam dans le répertoire `/usr/local/ap-mailfilter3` ;
- Création et installation du script responsable du lancement automatique du processus maître de filtrage (`ap-process-server`), du démon SPF

(*ap-spf*), du module de licence (*kas-license*) et du serveur HTTP (*kas-thttpd*) au démarrage du système d'exploitation ;

- Lancement des programmes et services indispensables ;
- Création de la tâche cron de l'utilisateur **mailflt3** pour le lancement automatique du script de chargement des mises à jour des bases de filtrage du contenu et du script de surveillance du fonctionnement du serveur de filtrage.

Une fois que le serveur de filtrage est installé, installez la clé de licence et procédez à l'intégration de Kaspersky Anti-Spam au serveur de messagerie.

### 3.3. Configuration de l'accès au Centre d'administration

Le service *kas-thttpd*, chargé d'ouvrir l'accès local au centre d'administration, est lancé à la fin de l'installation. Les paramètres par défaut suivants sont utilisés pour le centre d'administration :

- Adresse : <http://127.0.0.1:3080/>
- Nom d'utilisateur : **admin**
- Mot de passe : **admin**



Il faudra absolument modifier le nom d'utilisateur et le mot de passe pour l'accès au Centre d'administration après l'installation de Kaspersky Anti-Spam. L'utilisation des valeurs standard constitue un risque pour la sécurité de votre système.

Il est également conseillé de modifier le port de connexion au Centre d'administration.

Le nom d'utilisateur et le mot de passe sont conservés dans le fichier *.htpasswd* qui se trouve dans le répertoire */usr/local/ap-mailfilter3/control/www/* des scripts cgi du Centre d'administration.

La création d'un nouvel utilisateur ou la modification d'un mot de passe existant s'opère grâce à l'utilitaire *kas-htpasswd* qui fait partie de Kaspersky Anti-Spam. Lors du lancement de cet utilitaire, il faut absolument indiquer le chemin d'accès au fichier renfermant les mots de passe et ainsi que le nom du nouvel utilisateur ou de l'utilisateur existant dont le mot de passe doit être modifié :

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd  
/usr/local/ap-mailfilter3/control/www/.htpasswd <nom  
d'utilisateur>
```

Une fois que vous aurez saisi cette commande, vous serez invité à saisir le mot de passe pour cet utilisateur.

Pour créer un nouveau fichier contenant le mot de passe de l'utilisateur indiqué, utilisez l'argument `-c` :

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd -c
/usr/local/ap-mailfilter3/control/www/.htpasswd <nom
d'utilisateur>
```

Le nouveau mot de passe entre en vigueur dès la modification du fichier `.htpasswd`.



Le mot de passe d'accès au Centre d'administration est crypté dans le fichier `.htpasswd`.

L'interface et le numéro du port de connexion au Centre d'administration sont définis dans le fichier de configuration `/usr/local/ap-mailfilter3/etc/kas-thttpd.conf` à l'aide des paramètres **host** et **port** respectivement. Par exemple, les valeurs :

```
host=0.0.0.0
port=3080
```

indiquent que le Centre d'administration attend une connexion sur le port 3080 sur toutes les interfaces du serveur. Par défaut, l'accès au Centre d'administration est uniquement possible au départ du serveur sur lequel Kaspersky Anti-Spam est installé (la valeur **127.0.0.1** est attribuée au paramètre **host**).

En cas de modification du numéro de port, rechargez la configuration du Centre d'administration. Pour les distributions Linux, exécutez la commande :

```
# /etc/init.d/kas3-control-center restart
```

Pour les distributions FreeBSD, exécutez la commande :

```
/usr/local/etc/rc.d/kas3-control-center.sh restart
```

## 3.4. Installation de la clé de licence

La clé de licence conformément à la licence acquise est livrée avec la distribution de Kaspersky Anti-Spam.



Si pour une raison quelconque vous ne disposez pas de la clé de licence, contactez le service d'assistance technique de Kaspersky Lab (rubrique **Support et Services/Centre de support** sur le site Web de la société).



Pour installer une nouvelle clé de licence à l'aide du Centre d'administration, procédez comme suit :

1. Ouvrez votre navigateur Internet et saisissez **http://localhost:3080/** dans la barre d'adresses pour vous connecter au Centre d'administration. Le nom d'utilisateur est **admin** et le mot de passe est **admin**.
2. Ouvrez la page d'administration des clés de licence License → License Keys.
3. Saisissez, dans le champ de la partie inférieure de la page de la rubrique **Install a New License Key**, le chemin d'accès au fichier de clé de licence ou cliquez sur **Choose** afin de sélectionner le fichier requis.
4. Cliquez sur **Apply**.



Pour installer une nouvelle clé de licence localement à l'aide de la ligne de commande, saisissez la commande suivante :

```
# /usr/local/ap-mailfilter3/bin/install-key <key>
```

où **key** représente le chemin d'accès au fichier contenant la clé de licence.

Kaspersky Anti-Spam ne pourra pas filtrer le courrier si la clé de licence n'est pas installée ou si elle est invalide. Cela n'a aucune influence sur le fonctionnement du serveur de messagerie. Le trafic de messagerie n'est tout simplement pas analysé.

N'oubliez pas que le filtrage du courrier concerne uniquement les utilisateurs des domaines protégés.



N'oubliez pas de composer la liste des domaines protégés avant d'utiliser Kaspersky Anti-Spam. Pour obtenir de plus amples informations, consultez le point 4.3.4 à la page 49.

## 3.5. Intégration de Kaspersky Anti-Spam au serveur de messagerie

L'intégration de Kaspersky Anti-Spam au serveur de messagerie consiste à installer le module client et à introduire les modifications requises dans les fichiers de configuration.

Ces actions peuvent être réalisées automatiquement à l'aide d'un script universel de configuration ou à l'aide d'un script de configuration d'un serveur de messagerie particulier si l'intégration à l'aide d'un script universel est impossible (par exemple, en cas d'utilisation d'une configuration hors normes du serveur de messagerie).

Pour obtenir de plus amples informations sur les modes d'intégration des modules clients pour chacun des serveurs de messagerie pris en charge et sur les modifications à introduire dans les fichiers de configuration, consulter l'Annexe A.2 à la page 91.



*Afin d'intégrer Kaspersky Anti-Spam au serveur de messagerie sur votre serveur, lancez le script de configuration universel :*

```
# /usr/local/ap-mailfilter3/bin/MTA-config.pl
```

Ce script détermine le type de serveur de messagerie utilisé et introduit les changements requis dans son fichier de configuration.

Il se peut toutefois que le script *MTA-config.pl* ne parvienne pas à trouver les fichiers de configuration du serveur si l'installation ou la configuration de ce dernier n'est pas standard. Dans ce cas, il faudra utiliser le script de configuration d'un serveur de messagerie particulier :

- Pour intégrer Kaspersky Anti-Spam au serveur de messagerie Sendmail, exécutez la commande suivante au nom de l'utilisateur **root** :

```
# /usr/local/ap-mailfilter3/bin/config-sendmail.pl  
<path>
```

où **path** représente le chemin d'accès au fichier de configuration de Sendmail.

- Pour intégrer Kaspersky Anti-Spam au serveur de messagerie Postfix, exécutez la commande suivante au nom de l'utilisateur **root** :

```
# /usr/local/ap-mailfilter3/bin/config-postfix.pl  
<path>
```

où **path** représente le chemin d'accès au fichier de configuration *master.cf* de Postfix.

- Pour intégrer Kaspersky Anti-Spam au serveur de messagerie Exim, exécutez la commande suivante au nom de l'utilisateur **root** :

```
# /usr/local/ap-mailfilter3/bin/config-exim.pl <path>
```

où **path** représente le chemin d'accès au fichier de configuration d' Exim.



Pour la distribution Debian, il existe plusieurs particularités pour l'intégration de Kaspersky Anti-Spam au serveur de messagerie Exim. Pour une intégration réussie, utilisez le script `/usr/local/ap-mailfilter3/bin/config-exim-debian.pl`. Pour obtenir de plus amples informations, consultez le point A.2.4.2 à la page 101.

- Pour intégrer Kaspersky Anti-Spam au serveur de messagerie Qmail, exécutez la commande suivante au nom de l'utilisateur **root** :

```
# /usr/local/ap-mailfilter3/bin/config-qmail.pl <path>
```

où **path** représente le chemin d'accès au répertoire Qmail.



L'intégration correcte au serveur de messagerie Qmail à l'aide du script `config-qmail.pl` est possible uniquement lorsque Qmail utilise le compte **qmailq** et le groupe **qmail** (utilisé par défaut).

L'intégration de Kaspersky Anti-Spam au serveur de messagerie Exim à l'aide du module client `kas-exim` et l'intégration au serveur de messagerie Communicate Pro sont exécutées manuellement par l'administrateur.

Les propriétés de chacun des modules clients et les modes d'intégration sont décrites en détail au point A.2 à la page 91.

Le Chapitre 5 (p. 84) explique en détail comment annuler l'intégration et revenir aux paramètres initiaux des serveurs de messagerie.

## 3.6. Configuration de la mise à jour des bases de filtrage du contenu et de l'utilisation du service UDS

La mise à jour des bases de filtrage du contenu et l'utilisation des services UDS est désactivée par défaut après l'installation de Kaspersky Anti-Spam. Afin d'autoriser l'actualisation des bases et l'utilisation de la technologie UDS, exécutez le script `enable-updates.sh` :

```
# /usr/local/ap-mailfilter3/bin/enable-updates.sh
Restarting as mailflt3
Enabling UDS...
uds-rtts finished successfully
```

Enabling automatic updates...

Install crontab for user mailflt3 - ok

=====

You can adjust automatic updates settings via control center.

=====

Automatic updates and UDS are now enabled.

Il est possible également d'utiliser l'interface du Centre d'administration pour activer la mise à jour des bases de filtrage du contenu (cf. point 4.4, p. 57) et autoriser le recours au service UDS (cf. point 4.44.5.4, p. 66).

# CHAPITRE 4. ADMINISTRATION DU SERVEUR DE FILTRAGE DU COURRIER INDESIRABLE

Grâce à Kaspersky Anti-Spam, vous pouvez organiser la protection du flux de messagerie contre les messages non sollicités. Le système de protection repose sur l'exécution de tâches, qui concentrent les principales fonctions du logiciel. Les tâches exécutées via Kaspersky Anti-Spam peuvent être scindées en trois groupes principaux:

- Protection du trafic de messagerie contre les pourriels.
- Actualisation des bases de filtrage de contenu utilisées pour identifier les pourriels.
- Surveillance du fonctionnement du serveur de filtrage.

Chaque groupe contient des tâches plus détaillées. Ce chapitre est consacré aux tâches les plus caractéristiques que l'administrateur peut combiner et compliquer en fonction des besoins d'une entreprise en particulier.

Cette documentation contient une description des paramètres et du lancement des tâches localement via la ligne de commande. Il aborde également l'administration du logiciel à l'aide du Centre d'administration.

## 4.1. Lancement et administration des composants de Kaspersky Anti-Spam

Le lancement des composants du serveur de filtrage auquel sont associés le processus maître de filtrage (*ap-process-server*), le module de licence (*kas-license*) et le démon SPF (*ap-process-server*) lors du démarrage du système d'exploitation est le résultat de l'exécution d'un script particulier dont le nom et l'emplacement varient selon qu'il s'agit du système d'exploitation Linux ou FreeBSD. Pour le système d'exploitation Linux, il s'agit du script *kas3* situé dans

le répertoire */etc/init.d* et pour FreeBSD, il s'agit de *kas3.sh*, situé dans le répertoire */usr/local/etc/rc.d*.

L'administrateur peut utiliser ces scripts et les paramètres de la ligne de commande décrits ci-après pour lancer, arrêter ou redémarrer les principaux composants du serveur de filtrage :

**start** : lancement des principaux composants du serveur de filtrage ;

**stop** : arrêt des principaux composants du serveur de filtrage ;

**restart** : redémarrage des principaux composants du serveur de filtrage ; cette action entraîne le même résultat que la combinaison **stop** et **start**.

Le lancement du service *kas-thttpd*, qui donne accès au Centre d'administration, est provoqué par le script *kas3-control-center* (sous Linux) ou *kas3-control-center.sh* (sous FreeBSD).

Afin de lancer, d'arrêter ou de redémarrer le service *kas-thttpd*, utilisez le script avec les paramètres de la ligne de commande décrit ci-dessus pour le script *kas3*.

## 4.2. Centre d'administration de Kaspersky Anti-Spam

Le Centre d'administration est le principal outil d'administration de Kaspersky Anti-Spam. Il se présente sous la forme d'une application Internet permettant d'opérer la configuration à distance des paramètres du serveur de filtrage. Ce point propose une description détaillée de tous les éléments de l'interface de l'application.

Dans la partie supérieure de la fenêtre principale de l'application se trouve une série d'onglets qui permettent d'accéder aux fonctions suivantes du Centre d'administration :

- **Monitoring** : cet onglet contient les informations relatives à l'état des composants du serveur de filtrage ; ces informations permettent de mettre en évidence les erreurs qui surviennent.
- **Statistics** : cet onglet présente les statistiques qui permettent d'analyser le nombre de messages traités par le système.
- **Policies** : cet onglet permet de configurer les stratégies de filtrage du courrier indésirable.

The screenshot displays the Kaspersky Anti-Spam administration interface. At the top left is the Kaspersky logo. The main header shows 'Monitoring - General Status' with a clock icon and the time '12:06'. Below the header is a navigation menu with tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' tab is active, showing a sidebar with links for 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is divided into two sections: 'System Information' and 'Kaspersky Anti-Spam'. The 'System Information' section lists: Host Name: mail.test.local, System: FreeBSD 5.4-RELEASE-p7 i386, and Load Average: 0.13. The 'Kaspersky Anti-Spam' section lists: Product: Kaspersky Anti-Spam Enterprise Edition, Version: 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45, Anti-Spam Engine: Errors..., Updates: OK, and License: Errors... At the bottom of the interface, a copyright notice reads: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 3. Centre d'administration de Kaspersky Anti-Spam

- **Setting** : cet onglet contient les paramètres du serveur de filtrage du courrier indésirable, du Centre d'administration et du système de mise à jour des bases de filtrage du contenu.
- **License** : cet onglet est destiné à l'administration des licences de Kaspersky Anti-Spam et à l'enregistrement des utilisateurs autorisés à administrer le logiciel.

La partie droite de la fenêtre principale contient un menu où figurent le titre des différentes pages de l'onglet sélectionné. La composition de ce menu change en fonction de l'onglet.

En plus de ces modes de navigation, la partie supérieure de la fenêtre principale propose également, sous la forme de liens, le chemin d'accès à la page ouverte dans la hiérarchie des sections du Centre d'administration.

Vous trouverez ci-après une description des principales tâches liées à l'administration du serveur de filtrage et de ses composants.

## 4.3. Administration de la stratégie de filtrage

Le rôle premier de Kaspersky Anti-Spam est d'identifier et de filtrer les messages non sollicités. Le système d'administration permet de réaliser une configuration poussée du processus d'identification et du traitement des messages.

L'onglet **Policies** du Centre d'administration reprend les paramètres des stratégies de filtrage des messages.

Le menu de l'onglet **Policies** contient les éléments suivants :

- **Common** : configuration de la stratégie de filtrage globale. Le sous-menu est composé de :
  - **Default Rules** : administration des règles d'identification du courrier indésirable.
  - **Black List** : administration de la liste "noire" des expéditeurs dont les messages seront bloqués.
  - **White List** : administration de la liste "blanche" des expéditeurs dont les messages ne seront pas soumis à la recherche de courrier indésirable.
  - **DNS Black Lists** : administration de la liste des services DNSBL utilisés.
- **Groups** : configuration des groupes d'utilisateurs, des stratégies d'identification appliquées à certains groupes et des actions à exécuter sur les messages :
  - **Group list** : administration des groupes d'utilisateurs : création ou suppression de groupes et modification des propriétés du groupe.

La configuration des paramètres des stratégies de groupe s'opère dans l'éditeur de stratégie de groupe. L'éditeur est ouvert au départ de la fenêtre Group list.

Le lien Rebuild All Policies du menu **Build** est utilisé pour la compilation forcée des stratégies de filtrage (calcul et application des paramètres de configuration). La compilation forcée s'impose, par exemple, lors de l'actualisation des paramètres de stratégies de filtrage après une erreur de calcul par le logiciel.

### 4.3.1. Stratégie de filtrage globale

Les paramètres de la stratégie de filtrage commune à tous les groupes figurent dans la rubrique **Default Rules** (cf. ill. 4). Pour accéder à cette rubrique, cliquez sur Default Rules dans le menu **Common** de l'onglet **Policies**.

The screenshot shows the 'Default Rules' configuration page in the Kaspersky Anti-Spam software. The interface includes a top navigation bar with 'Policies → Common → Default Rules', a secondary navigation bar with 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License', and a left sidebar with 'Common', 'Groups', and 'Build' sections. The main content area lists five rule categories, each with a description and a 'Rules' count. A copyright notice for 2002-2006 Kaspersky Lab is at the bottom.

Category	Description	Rules
1. <b>General</b>	General settings: may affect rules in other sections	5
2. <b>DNS &amp; SPF Checks</b>	All checks in this section will be skipped if the corresponding settings on the 'General' page are 'Disabled'	3
3. <b>Headers Checks</b>		6
4. <b>Eastern Encodings</b>		4
5. <b>Obscene Content</b>	Use of "[_Obscene-]" mark	1

Illustration 4. Paramètres de la stratégie globale de filtrage

Les paramètres des règles d'identification du courrier indésirable sont regroupés selon la proximité fonctionnelle. La page principale présente la liste des rubriques.



Les paramètres et les rubriques fonctionnelles sont définies par les bases de filtrage de contenu. La sélection de rubriques et de paramètres peut être modifiée après l'actualisation des bases.

En plus du nom des rubriques, la liste propose également les informations suivantes :

- Une description succincte de la rubrique ;
- Le total de règles de la rubrique ;
- Le nombre de règles modifiées par rapport à la première installation des bases de filtrage du contenu.

Le bouton ( ) permettant d'ouvrir l'éditeur de règle est situé à droite de la description de chaque rubrique. Lorsque des règles d'une rubrique ont été modifiées, le bouton correspondant à cette rubrique devient orange. En cliquant sur le bouton, vous ouvrez la page de l'éditeur de stratégie de filtrage. Vous pouvez également ouvrir l'éditeur en cliquant sur le nom de la rubrique fonctionnelle. Pour annuler les modifications introduites dans une rubrique, cliquez sur .

### 4.3.1.1. Section **General**

Pour accéder à la page de configuration **General**, cliquez sur le nom de la rubrique dans la liste des règles de stratégie globale de filtrage (cf. ill. 5).

The screenshot displays the configuration page for 'Default Rules: General' in the Kaspersky Anti-Spam interface. The page is organized into a sidebar with 'Common' and 'Default Rules' sections. The main content area shows several settings, each with a dropdown menu currently set to 'Enabled'. Below the settings are 'Apply', 'Reset', and 'Default' buttons. A footer bar at the bottom contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 5. Section de règles **General** de la stratégie globale de filtrage

La section **General** permet de configurer les paramètres suivants :

- **Detection** : active ou non la recherche de messages non sollicités dans le courrier. Lorsque l'identification est désactivée, tous les messages reçoivent le statut **Trusted** (pour de plus amples informations sur les statuts, consultez le point 2.3 à la page 21).



Il est déconseillé de désactiver l'identification au niveau de la stratégie globale. Cette possibilité peut s'avérer utile lors de l'essai du logiciel ou lorsqu'il faut filtrer le courrier uniquement pour certains groupes d'utilisateurs.

- **Detection Level** : détermine le niveau de flexibilité dans l'identification du courrier indésirable. Pour décider si un message particulier appartient à la catégorie des pourriels, le module de filtrage tient compte de divers facteurs dans le message. Ce paramètre définit la manière dont le filtre va évaluer chacun de ces indices au moment d'attribuer un statut au message. La politique de filtrage se décline en quatre niveaux :

**Minimum, Standard, High et Maximum.** Plus l'identification est stricte, plus le nombre d'indices débouchant sur l'identification d'un message comme pourriel est réduit. Au niveau le moins strict, un même groupe d'indices entraînera l'attribution d'un état suspect au message (statut Probable Spam), voire la non-identification du message en tant que pourriel.



Il est conseillé d'utiliser le niveau **Standard**.

Le niveau de filtrage plus strict peut être utilisé lorsque Kaspersky Anti-Spam ne découvre aucun pourriel ou lorsqu'il considère les messages comme suspects (statut **Probable Spam**). Cette configuration augmente toutefois le risque de faux positifs où des messages normaux peuvent être considérés comme des pourriels.

Un niveau moins strict réduit le risque de faux positifs mais augmente la probabilité de voir les pourriels contourner le filtre.



Le résultat du filtrage est non seulement influencé par le degré de flexibilité mais également par les méthodes utilisées pour l'identification du courrier indésirable. Lorsque des faux positifs surviennent, il faut également vérifier la méthode utilisée pour identifier le courrier indésirable.

- **Assignment of the 'Probable Spam' status** – :activation/désactivation de l'attribution du statut **Probable Spam**. Si le paramètre a la valeur **Disable**, alors Kaspersky Anti-Spam n'attribuera pas le statut **Probable Spam** aux messages électroniques.
- **DNS & SPF Checks** : recherche des informations relatives à l'expéditeur dans le DNS et à l'aide de service reposant sur le DNS : DNSBL, SPF et etc.



Les vérifications selon le DNS et les services reposant sur le DNS peuvent ralentir considérablement le traitement des messages. Désactivez cette méthode si vous remarquez qu'elle entraîne une diminution sensible des performances du filtre.

Le paramètre définit l'utilisation par le serveur de filtrage des services DNS. L'activation et la désactivation de services déterminés s'opère sur la page **DNS & SPF Checks** (cf. point 4.3.1.2, p. 41).

Pour obtenir de plus amples informations sur la configuration de l'application des services DNSBL, consultez le point 4.3.3 à la page 47.

**SURBL Check** : utilisation du service SURBL.

**Use of White and Black Lists** : utilisation des listes "blanche" et "noire" d'adresses IP et d'adresses électroniques. Pour obtenir de plus amples

informations sur les listes "blanche" et "noire", consultez le point 4.3.2 à la page 45.

Le bouton Apply permet d'enregistrer les paramètres. Une fois que vous avez cliqué sur ce bouton, les paramètres sont enregistrés, la stratégie de filtrage est compilée et le module de filtrage est relancé. Autrement dit, les modifications introduites entre immédiatement en vigueur.

Le bouton Reset rétablit les paramètres à leur valeur initiale (c.-à-d. que les modifications non enregistrées sont annulées).

Le bouton Default remet les paramètres aux valeurs par défaut pour les bases de filtrage du contenu. Pour rétablir les valeurs par défaut, vous pouvez également cliquer sur le bouton  situé en regard du nom de la rubrique dans la liste des règles de la stratégie globale de filtrage.

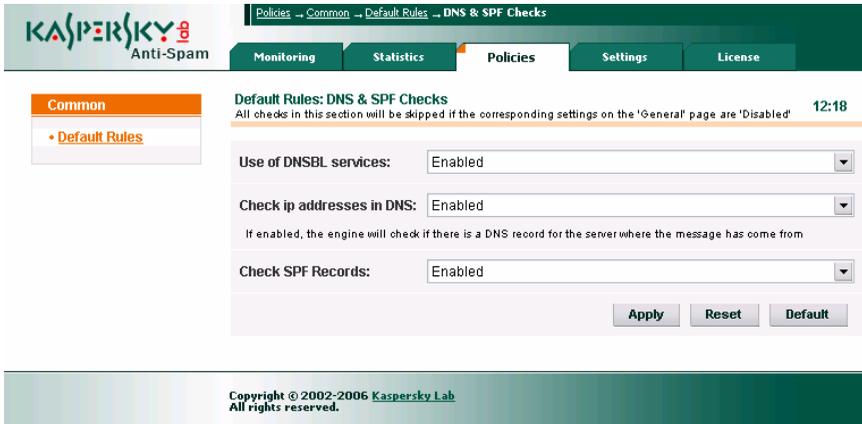
Pour revenir à la liste des règles de la stratégie globale de filtrage, cliquez sur Apply (les modifications seront enregistrées) ou utilisez le lien [Default rules](#) du menu **Common** (les modifications ne seront pas enregistrées).

### 4.3.1.2. Section **DNS & SPF Checks**

La section **DNS & SPF Checks** (cf. ill. 6) regroupe les paramètres qui définissent les services externes utilisés pour identifier le courrier indésirable.

Les paramètres de cette section permettent d'activer ou de désactiver l'utilisation des méthodes suivantes :

- **Use of DNSBL services** : recherche de l'adresse IP de l'expéditeur dans un ensemble de services DNSBL. La liste des services consultés pour l'analyse est composée sur la page [Policies](#) → [Common](#) → [DNS Black Lists](#). Pour obtenir de plus amples informations, consultez le point 4.3.3 à la page 47.
- **Check ip addresses in DNS** : recherche de l'adresse IP de l'expéditeur dans le DNS (reverse DNS lookup).
- **Check SPF Records** : analyse de l'adresse IP de l'expéditeur à l'aide de la technologie SPF.



**Default Rules: DNS & SPF Checks** 12:18

All checks in this section will be skipped if the corresponding settings on the 'General' page are 'Disabled'

Use of DNSBL services:

Check ip addresses in DNS:

If enabled, the engine will check if there is a DNS record for the server where the message has come from

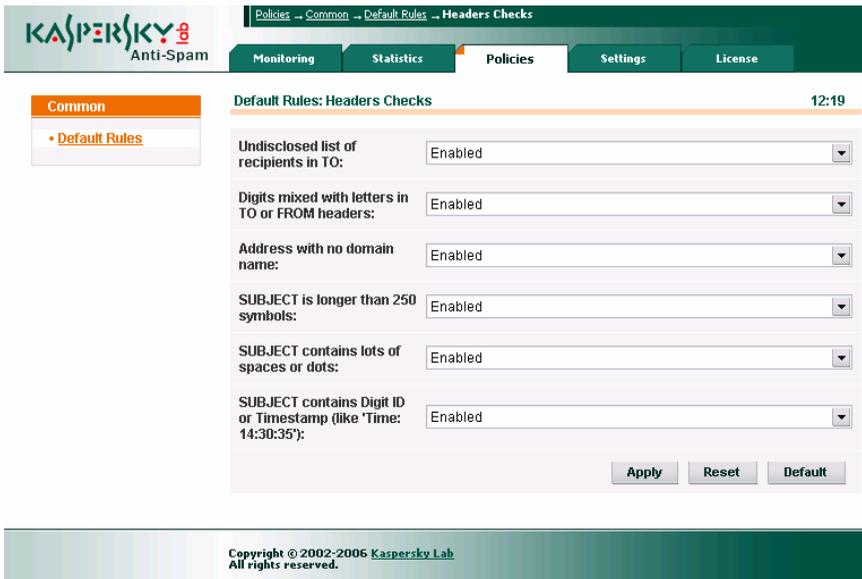
Check SPF Records:

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 6. Section **DNS & SPF Checks**.

### 4.3.1.3. Section **Headers Checks**

La section **Headers Checks**(cf. ill. 7) permet de configurer les règles d'analyse du contenu des en-têtes des messages électroniques.



**Default Rules: Headers Checks** 12:19

Undisclosed list of recipients in TO:

Digits mixed with letters in TO or FROM headers:

Address with no domain name:

SUBJECT is longer than 250 symbols:

SUBJECT contains lots of spaces or dots:

SUBJECT contains Digit ID or Timestamp (like 'Time: 14:30:35'):

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 7. Section des règles **Headers Checks** de la stratégie globale de filtrage

Cette section contient une liste partielle des règles utilisées par Kaspersky Anti-Spam lors de l'analyse des en-têtes des messages électroniques. Il s'agit des règles dont l'application pourrait filtrer des messages normaux contenant des indices connus de pourriel. Parmi ces indices, citons :

- **Undisclosed list of recipients in TO** – présence d'une liste dissimulée de destinataires dans le champ A.
- **Digits mixed with letters in TO or FROM headers** (présence de chiffres dans l'adresse de l'expéditeur ou du destinataire). Les programmes utilisés pour diffuser le courrier indésirable utilisent souvent en guise d'adresse de l'expéditeur ou du destinataire dans le message des adresses générées automatiquement et contenant des groupes de chiffres. Si les utilisateurs du serveur de messagerie n'utilisent pas d'adresses contenant des chiffres, il est recommandé d'activer cette règle.
- **Address with no domain name** (absence de nom de domaine dans l'adresse). Lors de la diffusion de messages non sollicités, les adresses ne sont pas toujours complètes (absence du domaine de messagerie) alors que les clients de messagerie utilisent en général l'adresse électronique complète avec le domaine, par exemple utilisateur@domaine.com. Il est conseillé de désactiver cette règle pour les destinataires qui acceptent l'envoi de messages électroniques avec des adresses incomplètes.
- **SUBJECT is longer than 250 symbols** (longueur de l'objet du message). Les programmes utilisés pour diffuser les pourriels tentent souvent de déjouer les filtres en plaçant dans le champ de l'objet (Objet) de longues chaînes aléatoires (plus de 250 caractères) de caractères ou de mots. Désactivez cette règle si le service de messagerie que vous utilisez accepte l'envoi de tels messages.
- **SUBJECT contains lots of white space or dots** (l'objet du message contient beaucoup d'espaces ou de points). Toujours dans le même but de déjouer les filtres, les programmes de diffusion de pourriels ajoutent souvent aux en-têtes des messages de longs groupes d'espaces ou de points. Désactivez cette règle si le service de messagerie que vous utilisez accepte l'envoi de tels messages.
- **SUBJECT contains DIGIT ID or Timestamp (like 'Time: 14:30:35')** (le texte de l'objet du message contient un identifiant numérique ou l'heure). L'insertion d'un identifiant numérique ou de l'heure dans l'objet du message est une autre technique exploitée par les programmes de diffusion du courrier indésirable afin de déjouer les filtres.

Dans la liste déroulante située à droite de chacune des règles, sélectionnez **Enabled** pour activer la règle ou **Disabled** pour la désactiver.



La décision finale pour l'attribution d'un statut particulier repose sur l'analyse de nombreux indices. Autrement dit, l'activation ou la désactivation d'une règle en particulier ou d'un groupe de règles ne signifie pas que les messages traités seront toujours considérés comme du courrier indésirable ou qu'ils seront ignorés par le serveur de filtrage. La configuration des règles permet de réduire le risque d'erreur d'identification des messages.

Les règles citées peuvent être activées et désactivées non seulement pour tous les utilisateurs dans la stratégie globale de filtrage mais également pour des groupes particuliers d'utilisateurs à l'aide des stratégies de groupe.

#### 4.3.1.4. Section *Eastern Encodings*

La section **Eastern Encodings** (cf. ill. 8) permet d'indiquer les langues et les encodages des messages adressés aux utilisateurs de votre système de messagerie sans que ces messages soient considérés comme des pourriels.

The screenshot shows the Kaspersky Anti-Spam interface. At the top, there is a navigation bar with the following tabs: Monitoring, Statistics, Policies (selected), Settings, and License. Below the navigation bar, the 'Common' section is expanded, showing 'Default Rules'. Under 'Default Rules', the 'Eastern Encodings' section is visible, displaying a list of languages and their encodings with dropdown menus. The current selection for all languages is 'is allowed'. The languages listed are: Chinese (gb2312), Korean (iso-ir-149), Thai (windows, dos-874), and Japanese (iso-2022-jp). At the bottom of the list, there are three buttons: Apply, Reset, and Default. The time 12:20 is displayed in the top right corner of the interface.

Illustration 8. Section des règles **Eastern Encodings** de la stratégie globale de filtrage

Cette version du logiciel contrôle les langues asiatiques suivantes lors du filtrage du courrier indésirable : le chinois, le coréen, le thaï et le japonais.

Si les utilisateurs du système de messagerie entretiennent une correspondance dans une de ces langues, sélectionnez la valeur **is allowed** dans la liste déroulante correspondant à cette langue. Si ces langues ne sont pas utilisées par les utilisateurs du système de messagerie, sélectionnez la valeur **is treated as suspicious**.

### 4.3.1.5. Section *Obscene Content*

La section **Obscene Content** (cf. ill. 9) permet de décider de marquer ou non les messages au contenu obscène. Kaspersky Anti-Spam peut reconnaître les termes obscènes en russe et en anglais.



Illustration 9. Section **Obscene Content** de la stratégie globale de filtrage.

Si la valeur **mark in Subject** est attribuée au paramètre **Message with obscene words and phrases**, alors l'élément **[--Obscene--]** sera ajouté à l'objet de tous les messages contenant des termes obscènes.

## 4.3.2. Administration des listes "blanche" et "noire"

La liste "blanche" des expéditeurs (**White List**) sert à indiquer clairement les adresses des expéditeurs dont les messages ne doivent pas être soumis à la recherche d'indices propres au courrier indésirable. Par exemple, vous pouvez inclure dans cette liste l'adresse IP des serveurs de messagerie utilisés pour le transfert du courrier à l'intérieur de l'entreprise ou les adresses des listes de diffusion internes. Les messages en provenance d'expéditeurs de la liste "blanche" recevront toujours le statut Trusted.

La liste "noire" (**Black List**) des utilisateurs remplit la fonction opposée. L'administrateur du serveur de filtrage peut ajouter à cette liste les adresses des diffuseurs de courrier indésirable. Les messages en provenance d'expéditeurs repris dans la liste "noire" recevront l'état Blacklisted.

L'administration de ces deux types de liste est identique. A titre d'exemple, nous proposons la configuration de la liste "blanche" (cf. ill. 10).

Pour accéder au formulaire de modification de la liste "blanche", sélectionnez le menu **Policies** → **Common** → **White List** (pour la liste "noire", il s'agira de **Policies** → **Common** → **Black List**).

La liste des adresses de confiance est scindée entre une liste des adresses de courrier électronique et une liste des adresses IP. Le champ situé dans la partie centrale de la page permet de saisir les adresses. Vous pouvez basculer entre les types d'adresses de la liste "blanche" à l'aide des liens e-mails | ip addresses.

Le bouton **Apply** permet d'enregistrer les informations saisies. Pour annuler les modifications qui n'ont pas été enregistrées, cliquez sur le bouton **Reset**.



Enregistrez les modifications avant de cliquer sur les liens **e-mails** | ip addresses. Toutes les modifications seront perdues si vous changez de type d'adresses sans avoir enregistré les modifications.

Illustration 10. Page de configuration de la liste "blanche"

Les adresses de courrier électronique doivent être saisies selon le format suivant :

- *utilisateur@domaine* : indique une adresse en particulier ;
- *@domaine* : représente toutes les adresses de courrier électronique du domaine **domaine**.

Des caractères spéciaux peuvent être saisis dans les adresses de courrier électronique :

- \* (ASTERISQUE) : CHAINE DE CARACTERES DE N'IMPORTE QUELLE LONGUEUR ;
- ? (POINT D'INTERROGATION) : UN CARACTERE ALEATOIRE.

Par exemple, la valeur utilisateur\*@monentreprise.com représente toutes les adresses commençant par utilisateur dans le domaine monentreprise.com.

La saisie des adresses IP s'effectue selon la notation CIDR qui accepte les variantes suivantes :

- *aaa.bbb.ccc.ddd* : une adresse IP en particulier, par exemple 192.168.0.17 ;
- *aaa.bbb.ccc.ddd/mm* : adresse du sous-réseau avec un numéro et un masque défini, par exemple 192.168.0.0/16.

Les adresses dans la liste peuvent être séparées par un espace, par un retour à la ligne ou une virgule ou un point virgule.

### 4.3.3. Administration des listes des services DNSBL utilisés

Pour passer à l'administration des services DNSBL, cliquez sur le lien [DNS Black Lists](#) dans le menu **Common** de la section **Policies** (cf. ill. 11).

La configuration de la liste des services DNSBL utilisés est en rapport avec la stratégie globale de filtrage. Par la suite, il est possible de définir pour chaque groupe d'utilisateurs si les résultats de l'analyse à l'aide des services DNSBL seront utilisés pour ce groupe ou non. La liste des services utilisés est commune à l'ensemble des groupes d'utilisateurs.

La partie centrale de la page contient la liste des services utilisés. Chaque service DNSBL est accompagné de l'adresse utilisée pour envoyer les requêtes au service et de son classement.

Le classement d'un service définit la confiance que l'administrateur du serveur de filtrage accorde au service en question. Lors de la recherche de l'adresse IP de l'expéditeur dans DNSBL, Kaspersky Anti-Spam envoie la requête à tous les services repris dans cette liste. Une fois que les résultats ont été obtenus, les classements des services ayant identifié l'adresse IP comme une adresse à l'origine d'envois non sollicités sont additionnés.

**DNS Black Lists** 13:39  
List of DNS-based Black List services

	Hostname	Rate	
1	<a href="#">combined-hib.dnswllists.completewhois.com</a>	70	✗
2	<a href="#">bl.spamcop.net</a>	30	✗
3	<a href="#">list.dsbl.org</a>	50	✗
4	<a href="#">dnswl.njabl.org</a>	50	✗
5	<a href="#">relays.ordb.org</a>	70	✗
6	<a href="#">xbl-sbl.spamhaus.org</a>	50	✗
+			

Apply Reset

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 11. Administration des listes de services DNSBL

Si la somme des classements DNSBL dépasse 100, le système en déduit que l'expéditeur se trouve dans la liste "noire" et le message reçoit le statut **blacklisted**, quels que soient les résultats des analyses selon les autres méthodes. Lorsque le niveau d'analyse est moins strict, il peut arriver que la somme des classements des services contenant l'adresse de l'expéditeur dans leur liste "noire" est inférieure à 100. Dans ce cas, l'information relative à la présence de l'expéditeur dans la liste noire est uniquement un indice complémentaire et le message sera traité comme un pourriel uniquement si d'autres indices de courrier indésirable sont identifiés par les autres méthodes d'analyse.

Les opérations suivantes peuvent être réalisées à l'aide de la liste des services DNSBL :

- Ajout d'un nouveau service.
- Modification du classement d'un service.
- Suppression d'un service.

Voici une présentation détaillée de chacune de ces opérations :

- Pour **ajouter un nouveau service à la liste**, il faut :
  1. Indiquer l'adresse du service sur la dernière ligne de la liste signalée par l'icône + ;
  2. Indiquer le classement du service ;

3. Enregistrer le résultat en cliquant sur le bouton Apply.
- Pour **modifier le classement d'un service DNSBL existant**, il faut :
    1. Indiquer la nouvelle valeur du classement dans la colonne **Rate** du service existant ;
    2. Enregistrer le résultat en cliquant sur le bouton Apply.
  - Pour **supprimer un service de la liste**, il faut :

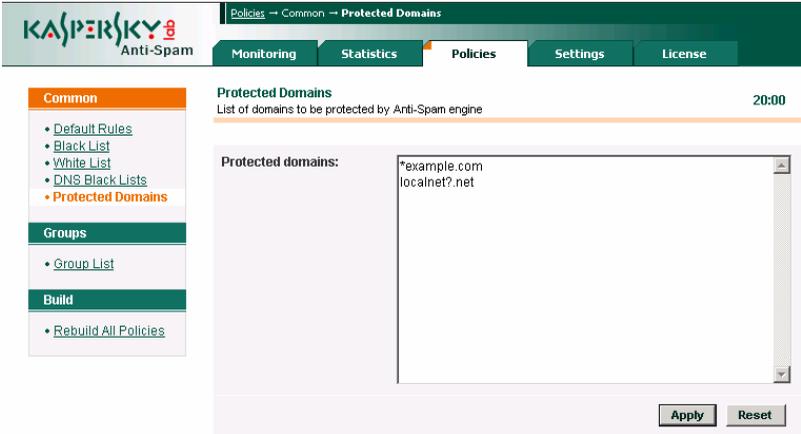
Cliquer sur le bouton  situé à droite de l'adresse du service.



Il faut être prudent lors de la sélection des listes DNSBL utilisées. La politique de composition de ces listes varie en fonction des services qui les proposent. Il est conseillé d'étudier attentivement la politique du service avant d'utiliser la liste qu'il propose pour filtrer le courrier.

## 4.3.4. Administration de la liste des domaines protégés

La liste des domaines protégés contient le nom des domaines pour lequel le flux de courrier entrant est soumis à la recherche de messages non sollicités. L'administration de la liste s'opère au départ de la page située à l'adresse Politiques → Common → Protected Domains (cf. ill. 12).



The screenshot displays the Kaspersky Anti-Spam web interface. The breadcrumb navigation at the top reads "Policies → Common → Protected Domains". The main navigation tabs include "Monitoring", "Statistics", "Policies", "Settings", and "License". The left sidebar has three sections: "Common" (with links for Default Rules, Black List, White List, DNS Black Lists, and Protected Domains), "Groups" (with Group List), and "Build" (with Rebuild All Policies). The main content area is titled "Protected Domains" and shows a list of domains to be protected by the Anti-Spam engine, with a timestamp of 20:00. The list contains two entries: "\*example.com" and "localnet?.net". Below the list are "Apply" and "Reset" buttons. At the bottom of the page, the copyright notice reads "Copyright © 2002-2006 Kaspersky Lab. All rights reserved."

Illustration 12. Liste des domaines protégés

Les domaines à protéger peuvent être saisis en utilisant entre autres des caractères spéciaux : \* pour n'importe quel nombre de caractères et ? pour n'importe quel caractère. Ainsi, pour ajouter le domaine **exemple.com** et tout ses sous-domaines, il suffit d'ajouter ceci :

```
*exemple.com
```

Si vous souhaitez que le logiciel filtre tout le courrier entrant, ne remplissez pas la liste ou ajoutez-y la valeur suivante :

```
*
```

Une fois que les modifications souhaitées ont été introduites, cliquez sur **Apply** afin de confirmer ces modifications ou sur **Reset** pour les annuler.



S'agissant des domaines repris dans la liste des domaines protégés, le système vérifie si les restrictions de la licence sont bien respectées (par exemple, contrôle du volume du trafic si la licence est définie par rapport à ce paramètre).

Il est également possible de modifier la liste des domaines localement via la ligne de commande. La liste originale des domaines est conservée dans le fichier texte *protected\_domains* situé dans le répertoire */usr/local/ap-mailfilter3/conf*.

Une fois que les modifications ont été introduites, exécutez la commande suivante sous le nom d'utilisateur **root** :

```
# /usr/local/ap-mailfilter3/bin/kas-restart -f
```



Kaspersky Anti-Spam ajoutera le champ suivant à l'en-tête de tous les messages envoyés aux utilisateurs des domaines qui ne figurent pas sur la liste des domaines protégés :

X-SpamTest-Info: Not protected

Pour obtenir de plus amples informations sur les champs particuliers d'en-tête, consultez le point A.5 à la page 123.

## 4.3.5. Administration des groupes

L'administrateur du serveur de filtrage peut définir diverses configuration d'identification du courrier indésirable pour divers utilisateurs. C'est à cela que serve les stratégies de filtrage de groupe du courrier indésirable.

Avant de configurer les règles de la stratégie de groupe, il convient de constituer la liste des adresses de courrier électronique soumises à la stratégie de groupe.

En plus des groupes créés par l'administrateur, le logiciel utilise également le groupe **All** créé par défaut lors de l'installation. Ce groupe définit les règles de traitement des messages qui ne tombent pas sous le coup d'autres groupes. Le

groupe **All** est un groupe système qui, à la différence des autres groupes, ne peut pas être supprimé.

Le menu **Groups** situé dans la partie gauche de la fenêtre de la section **Policies** donne accès à la configuration des groupes.

Le lien Group List ouvre la page contenant la liste de tous les groupes existant (cf. ill. 13).

The screenshot shows the 'Policies → Group List' page in the Kaspersky Anti-Spam interface. The left sidebar contains navigation menus for 'Common', 'Groups', and 'Build'. The 'Groups' menu is active, showing 'Group List' as the selected option. The main content area displays a table of recipient groups:

Group List		13:44
List of recipient groups		
1.	<b>Accounting</b> Accounting department employees	[Edit] [Delete]
2.	<b>Managers</b> Company managers	[Edit] [Delete]
3.	<b>Sales</b> Sales department employees	[Edit] [Delete]
4.	<b>All</b> All recipients not included in any other group	[Edit]

At the bottom of the main content area, a green checkmark icon and the message 'Settings have been saved and applied successfully' are displayed.

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 13. Liste des groupes utilisés par Kaspersky Anti-Spam.

Les opérations suivantes peuvent être réalisées sur les groupes :

- Modification des propriétés du groupe.
- Création d'un nouveau groupe.
- Suppression d'un groupe existant.
- Modification de l'ordre de consultation des groupes.

Voici une présentation détaillée de chacune de ces tâches :



*Pour ouvrir l'éditeur des propriétés du groupe :*

Cliquez sur le bouton  situé à droite du nom du groupe dont vous souhaitez modifier les propriétés.

L'éditeur des propriétés du groupe permet de configurer :

- Les paramètres généraux du groupe tels que le nom, les commentaires et la liste des adresses électroniques qui seront soumises aux règles définies par le groupe ;
- Les règles d'identification du courrier indésirable ;
- Les actions exécutées sur les messages ;
- Les listes "noire" et "blanche" d'expéditeurs.



Le nom et la liste des adresses de courrier électronique du groupe **All** ne peuvent pas être modifiés vu que ce groupe définit les règles de traitement de tous les messages dont les expéditeurs et les destinataires ne figurent dans aucun des groupes créés par l'administrateur.



*Pour créer un nouveau groupe, procédez comme suit :*

1. Cliquez sur le bouton  situé sous la liste de groupes.
2. Dans la fenêtre qui s'ouvre (cf. ill. 14), indiquez le nom du groupe, ajouter un commentaire (le cas échéant) et constituez la liste des adresses électroniques.

Le champ **Group Id** contient l'identifiant du groupe attribué au moment de la création. Ce paramètre ne peut être modifié.

Le texte saisi dans le champ **Comments** figurera dans la liste des groupe sous le nom du groupe créé.

La saisie des adresses respecte le format utilisé pour la saisie des adresses dans les listes "noire" et "blanche" des expéditeurs (cf. point 4.3.2, p. 45).



*Pour supprimer un groupe existant :*

Cliquez sur le bouton  situé à droite du nom du groupe.



*Pour modifier l'ordre d'affichage des groupes :*

Cliquez sur le bouton  situé à gauche du nom du groupe. Le groupe sélectionné sera déplacé vers le haut de la liste.

Lors du traitement des messages, le module de filtrage consulte les groupes dans l'ordre de la liste des groupes (du début de la liste jusque la fin). Le message est traité conformément aux règles du premier groupe rencontré dont

la liste contient l'adresse du destinataire du message. Si le destinataire du message ne figure dans aucun de ces groupes, alors le message est traité conformément aux règles du groupe **All**.

The screenshot displays the Kaspersky Anti-Spam administration console. At the top, the navigation bar includes 'Policies -> Group Policy -> General'. Below this, there are tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The main content area is titled 'General Settings - Group: Sales' with a timestamp of 12:41. It contains several form fields: 'Group Name' (Sales), 'Group Id' (1), and 'Description' (Sales employees). A section for 'E-mail addresses of group members' lists several email addresses: alice@sales.local, bob@sales.local, jack@sales.local, john@sales.local, mike@sales.local, ann@sales.local, and bob@sales.local. At the bottom right of the form are 'Apply' and 'Reset' buttons. A sidebar on the left shows a tree view with 'Groups' and 'Group Policy' sections, with 'General' selected under 'Group Policy'. A footer bar at the bottom contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 14. Page de création d'un nouveau groupe

### 4.3.6. Administration de la stratégie de filtrage de groupe

Il est possible de définir des configurations d'identification et des listes "noire" et "blanche" d'expéditeurs propres à chaque groupe, y compris au groupe **All**. L'administrateur peut de la sorte définir différentes règles d'identification du courrier indésirable pour divers groupes d'utilisateurs.

Par défaut, la configuration des règles d'identification suivies par chaque groupe est identique à la configuration de la stratégie globale. Ces valeurs peuvent toutefois être redéfinies.

Pour configurer les règles d'identification adoptées par une stratégie de filtrage de groupe, cliquez sur le lien [Rules](#) du menu **Group Policy** dans l'éditeur des propriétés du groupe. La structure des règles est identique à celle de la stratégie globale de filtrage (cf. point 4.3.1, p. 37).

La seule différence pour les paramètres de la stratégie de groupe est que la liste des paramètres contient la valeur by default qui signifie que le paramètre adoptera la valeur définie dans la stratégie globale de filtrage.

L'illustration 15 présente la fenêtre **Rules** de la stratégie de filtrage de groupe.

Comme vous le voyez, le groupe adopte tous les paramètres de la stratégie globale (valeur by default), à l'exception du paramètre DNS & SPF Checks. L'utilisation de cette méthode est désactivée.

Les listes "noire" et "blanche" des expéditeurs son définies à l'aide des liens [White List](#) et [Black List](#) du menu **Group Policy**. La configuration des listes pour les groupes est identique aux configurations des listes pour la stratégie globale de filtrage (cf. point 4.3.1, p. 37).

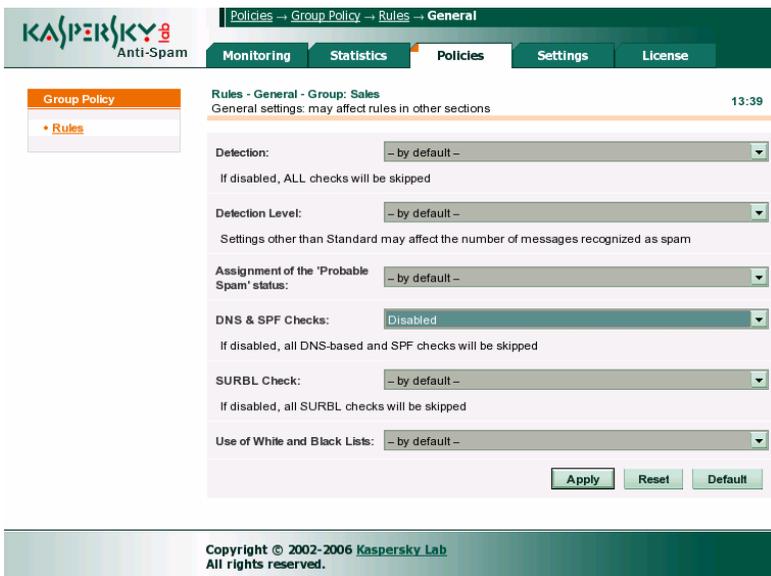


Illustration 15. Page **Rules** de la stratégie de groupe de filtrage

## 4.3.7. Actions à exécuter sur les messages

La stratégie de groupe contient également les actions de transfert et de modification des messages identifiés par le module de filtrage. Pour configurer

les actions, cliquez sur le lien Actions dans le menu Group Policy de l'éditeur des propriétés du groupe.

L'action exécutée sur un message est définie par le statut attribué à ce message suite au traitement par le module de filtrage. La page Actions (cf. ill. 16) contient le formulaire qui permet de définir l'action pour chacun des états possibles.

La liste déroulante située sous le titre avec la description de l'état du message permet de définir les actions.

L'administrateur a le choix entre les valeurs suivantes :

- **Accept this message** : le serveur de messagerie accepte le message et le remet au destinataire.
- **Send a copy of this message to other recipient(s)** : le serveur de messagerie accepte le message, le remet au destinataire et envoie une copie à l'adresse indiquée dans le champ **Send message to**.
- **Redirect this message to other recipient(s)** : le serveur de messagerie accepte le message et le transmet à l'adresse reprise dans le champ **Send message to**. Le destinataire d'origine ne reçoit pas le message. Cette option peut être utilisée pour transférer les messages dans une boîte aux lettres destinée à la conservation des archives de courrier indésirable.
- **Reject this message** : le serveur de messagerie rejette le message et envoie une notification à l'expéditeur pour le prévenir de l'impossibilité de délivrer le message. Si le message est rejeté pour tous les destinataires, le serveur de messagerie envoie un message directement dans le processus de la session SMTM (reject message). Si la délivrance est autorisée pour un destinataire au moins, l'expéditeur reçoit une notification sur l'impossibilité de délivrer le message à certains destinataires (bounce message). La rédaction du texte de la notification s'opère dans la section **Settings** → **Reject Messages** (pour de plus amples informations, consultez le point 4.5.4 à la page 66 ).
- **Delete this message** : le serveur de messagerie reçoit le message et le supprime sans l'avoir transmis au destinataire. Dans ce cas, l'expéditeur du message ne reçoit aucune notification relative à l'impossibilité de délivrer le message.

The screenshot displays the Kaspersky Anti-Spam 3.0 interface. At the top, there is a navigation bar with 'Policies' selected, leading to 'Group Policy' and then 'Actions'. Below this, there are tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. On the left, a sidebar shows 'Groups' with a 'Group List' link and 'Group Policy' with a list of options: 'General', 'Actions' (highlighted), 'Rules', 'Black List', and 'White List'. The main content area is titled 'Actions - Group: Sales' with a timestamp of 12:45. It contains several sections for configuring actions based on message recognition:

- If a message is recognized as 'Spam':**
  - Action: Accept this message
  - Prepend to the Subject: [! SPAM]
  - Set X-SpamTest-Header: [Empty field]
- If a message is recognized as 'Probable Spam':**
  - Messages suspected of being spam
  - Action: Accept this message
  - Prepend to the Subject: [?? Probable Spam]
  - Set X-SpamTest-Header: [Empty field]
- If a message is recognized as 'Blacklisted':**
  - Messages from senders or relays included in common or group black lists
  - Action: Accept this message
  - Prepend to the Subject: [! BLACKLISTED]
  - Set X-SpamTest-Header: [Empty field]
- If a message is recognized as 'Formal':**
  - Automatic replies or notifications
  - Action: Accept this message
  - Prepend to the Subject: [-- Formal Message--]
  - Set X-SpamTest-Header: [Empty field]
- If a message is recognized as 'Trusted':**
  - Messages from trusted senders or relays (included in common or group white lists)
  - Prepend to the Subject: [Empty field]
  - Set X-SpamTest-Header: [Empty field]
- If a message is recognized as 'Not Detected':**
  - Other messages
  - Prepend to the Subject: [Empty field]
  - Set X-SpamTest-Header: [Empty field]

At the bottom right, there are 'Apply' and 'Reset' buttons.

Illustration 16. Page **Actions** de la stratégie de groupe de filtrage

Les messages correspondant au statut Not detected (message non considéré comme un pourriel) ou Trusted (message en provenance d'une source de confiance ou destinée à un membre d'un groupe pour lequel la recherche de courrier indésirable a été désactivée) sont toujours transmis au destinataire indiqué.



Bien que le logiciel fasse l'objet d'un développement continu afin d'améliorer la qualité de l'identification du courrier indésirable et de réduire le nombre de faux positifs, il n'est pas exclu que des messages normaux soient considérés comme des pourriels. Pour cette raison, il est conseillé d'être prudent lors de l'utilisation d'actions qui entraînent la suppression des messages.

En plus des actions relatives au transfert des messages, l'administrateur peut définir des actions de modification du message, ce qui peut être utile pour visualiser les résultats de l'identification et exploiter les règles définies au niveau du client de messagerie de l'utilisateur.

Kaspersky Anti-Spam permet d'introduire les modifications suivantes dans les messages :

- Ajout d'un commentaire dans le champ de l'objet du message (au début du texte). Le texte à ajouter est saisi dans le champ Prepend to Subject.
- L'ajout au message du champ spécial *X-Spamtest-Header*, dont le contenu est défini par l'administrateur, à l'en-tête. Cet en-tête peut servir ultérieurement au traitement automatique des messages par le client de messagerie de l'utilisateur. Le texte de l'en-tête est défini dans le champ **Set X-Spamtest-Header**. Pour obtenir de plus amples informations sur les champs d'en-tête ajoutés aux messages après le filtrage, consultez le point A.5 à la page 123.

## 4.4. Mise à jour des bases de filtrage du contenu

La mise à jour des bases de filtrage du contenu utilisées pour l'analyse du contenu des messages est prise en charge par le module spécial de mise à jour :*sfupdates*.

La mise à jour des bases de filtrage du contenu peuvent être téléchargées depuis Internet (serveur de mises à jour de Kaspersky Lab) ou depuis un répertoire de réseau.

La mise à jour est lancée manuellement à l'aide d'un script de mise à jour exécuté depuis la ligne de commande ou automatiquement selon l'horaire défini à l'aide du service cron.

## 4.4.1. Configuration de la mise à jour

La configuration de la mise à jour s'opère sur la page Settings → Maintenance → Updater du Centre d'administration (cf. ill. 17).

The screenshot shows the 'Updater Settings' page in the Kaspersky Anti-Spam administration interface. The page is titled 'Updater Settings' and contains the following sections:

- Updater Settings:**
  - Run updater automatically: every 20 minutes
  - Updater log level: activity
  - Network timeout (in seconds): 20
  - Use passive FTP mode:
- Updates Server:**
  - Region: Russia
  - Updates server URL: (empty)
  - Use updates server URL:  Use updates server URL only:
- Proxy Server:**
  - Proxy address: http://proxy.local:8080
  - User: proxyuser
  - Password: (masked with asterisks)
  - Use proxy:

At the bottom right, there are 'Apply' and 'Reset' buttons. The footer of the page reads: Copyright © 2002-2006 Kaspersky Lab. All rights reserved.

Illustration 17. Configuration du module de mise à jour de Kaspersky Anti-Spam

La section **Updater Settings** contient les paramètres généraux de la mise jour :

- **Run updater automatically** : intervalle entre les chargements des bases de LBfiltrage du contenu depuis les serveurs de mise à jour. Cet intervalle peut être compris entre 20 minutes et 3 heures.



Dans la mesure du possible, il est conseillé d'utiliser l'intervalle le plus court. Une mise à jour plus rapide des bases de filtrage du contenu améliore la vitesse de réaction du serveur de filtrage face aux nouveaux types de courrier indésirable. L'intervalle de mises à jour recommandé est de 20 minutes.

La valeur du paramètre détermine l'intervalle de lancement de la tâche cron de mise à jour du logiciel. Le cas échéant, la configuration de la tâche cron peut être réalisée manuellement. Pour obtenir de plus amples informations sur la configuration manuelle, consultez le point 4.4.2 à la page 60.

- **Updater log level** : ce paramètre définit le niveau de détail des informations consignées dans le journal lors de la mise à jour. Vous avez le choix entre les niveaux suivants :
  - **fatal** : seules les notifications relatives aux erreurs critiques sont enregistrées ;
  - **error** : les notifications relatives à toutes les erreurs (critiques ou non) sont enregistrées.
  - **warning** : les avertissements et les notifications relatives aux erreurs sont enregistrés ;
  - **info** : les notifications à caractère informatif (informations sur le lancement du module de mise à jour, sur les résultats de la mise à jour, etc.), en plus des avertissements et des notifications relatives aux erreurs, sont enregistrées ;
  - **activity** : toutes les informations correspondantes au niveau **info** sont enregistrées, ainsi que les informations relatives au processus d'actualisation (connexion au serveur de mise à jour, copie des fichiers depuis le serveur, etc) ;
  - **debug** : toutes les informations relatives au niveau **activity** ainsi que les données de débogage sont enregistrées.
- **Network timeout** : délai de connexion (en secondes) pour les opérations de réseau lors de la mise à jour des bases de filtrage du contenu. La valeur recommandée est égale à **30**.
- **Use passive FTP mode** : paramètre qui indique qu'il convient d'utiliser la connexion en mode passif (recommandé) lors de la connexion au serveur de mise à jour via le protocole FTP.

La section **Updates Server** contient les paramètres du serveur faisant office de source des mises à jour.

- **Region** : définit la région où se trouve l'utilisateur. Le logiciel choisit le serveur de mise à jour le plus adéquat (géographiquement parlant) sur la base de ce paramètre.

- **Updates server URL** : adresse du serveur utilisé pour les mises à jour. Ce paramètre est utilisé conjointement aux paramètres : Use updates server URL et Use updates server URL only. Par défaut, la liste des serveurs utilisés pour la mise à jour des bases de filtrage du contenu est définie dans le fichier updcfg.xml repris dans la distribution du logiciel. Lors de la mise à jour, Kaspersky Anti-Spam choisit automatiquement un serveur dans cette liste. Grâce au paramètre **Use updates server URL**, vous pouvez indiquer qu'il est préférable de télécharger les mises à jour depuis l'adresse définie par le paramètre Updates server URL. Si vous utilisez l'option Use updates server URL only, alors Kaspersky Anti-Spam utilisera uniquement le serveur indiqué pour la mise à jour des bases de filtrage du contenu et ne tentera pas d'utiliser d'autres adresses.

En guise de source de la mise à jour, ce paramètre peut être :

- Serveur HTTP. *Format* : http://<adresse du serveur>
- Serveur FTP. *Format* : ftp://<adresse du serveur>
- Répertoire local. *Format* /<chemin d'accès au répertoire>/

*L'utilisation d'un répertoire local en guise de source de la mise à jour permet d'organiser l'actualisation de plusieurs serveurs dans un grand réseau au départ d'une source unique.*

La section **Proxy Server** contient les paramètres d'accès au serveur proxy :

- **Proxy address** : adresse du serveur proxy utilisé pour accéder à Internet. Le paramètre prend la forme : http://url:port où url et port représentent l'adresse et le port de connexion au serveur proxy. Si l'adresse n'est pas indiquée, sa valeur sera celle de la variable http\_proxy.
- **User** : nom d'utilisateur pour accéder au serveur proxy.
- **Password** : mot de passe pour accéder au serveur proxy.
- **Use proxy** : ce paramètre indique que la connexion au serveur de mise à jour doit se faire impérativement via le serveur proxy HTTP.

## 4.4.2. Lancement de la mise à jour

La mise à jour des bases de filtrage du contenu peut être lancée de deux manières :

- Automatiquement selon un horaire ;
- Manuellement via la ligne de commande.

Il est conseillé de programmer la mise à jour car cela permet de maintenir l'actualité des bases de filtrage du contenu pour un filtrage plus efficace du courrier indésirable.



Pour lancer la mise à jour manuellement, saisissez dans la ligne de commande :

```
# /usr/local/ap-mailfilter3/bin/sfupdates [argument]
```

où [argument] représente le paramètre de lancement du script de mise à jour. La liste complète des paramètres du script *sfupdates* est reprise au point A.4.8 à la page 122.

Lorsque le script est exécuté sans argument via la ligne de commande, les nouvelles mises à jour seront copiées depuis le serveur, leur intégrité sera vérifiée, elles seront installées et le module de filtrage sera relancé afin de pouvoir utiliser les nouvelles bases.

Lors de l'installation de Kaspersky Anti-Spam, la configuration automatique du service *cron* s'opère par défaut afin de lancer le script de mise à jour toutes les vingt minutes pour l'utilisateur **mailflt3**. Si pour une raison quelconque il convient de configurer manuellement le lancement du script de mise à jour, procédez comme suit :

1. Ouvrez l'éditeur du fichier de tâche du processus **cron** pour l'utilisateur **mailflt3** à l'aide de la commande

```
# crontab -u mailflt3 -e
```

2. Ajoutez au fichier de tâche la ligne suivante par exemple :

```
*/20 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -  
q
```



Avant de configurer le lancement automatique de la mise à jour, assurez-vous que l'utilisateur **mailflt3** jouit des privilèges d'écriture dans les répertoires : */usr/local/ap-mailfilter3/cfdata* et */usr/local/ap-mailfilter3/conf*.

## 4.5. Configuration du serveur de filtrage du courrier indésirable

Les pages de la section **Settings** contiennent les paramètres des composants du serveur de filtrage du courrier indésirable. Pour naviguer entre les pages, il suffit de cliquer sur les liens du menu **Anti-Spam Engine** :

- Common : paramètres généraux du serveur de filtrage.

- Process Server : paramètre du processus maître de filtrage *ap-process-server*.
- Filtration Process : paramètres de fonctionnement des processus de filtrage *ap-mailfilter*.
- Check Options : paramètres d'identification du courrier indésirable.
- MTA Clients : paramètres des modules clients.
- Reject Messages : textes des messages envoyés à l'expéditeur lorsque le message électronique n'est pas délivré.

Les paramètres des composants du serveur de filtrage peuvent également être définis manuellement en modifiant le fichier de configuration *filter.conf*. Pour obtenir de plus amples informations sur le fichier de configuration *filter.conf*, consultez le point A.3.1 à la page 109.

## 4.5.1. Paramètres généraux du serveur de filtrage

Les paramètres généraux du serveur de filtrage sont regroupés sur la page **Settings** → Anti-Spam Engine → **Common** (cf. ill. 18). Il s'agit de :

- **Syslog facility** : catégorie du journal système sous laquelle les messages des composants de Kaspersky Anti-Spam seront enregistrés. Par défaut, les enregistrements sont réalisés dans la catégorie **mail** mais, le cas échéant, l'administrateur du serveur de filtrage peut choisir une autre catégorie parmi celles-ci : **mail**, **user**, **local0** – **local7**.



Une fois que le paramètre **Syslog facility** a été modifié, configurez le démon **syslog** pour enregistrer les messages de la catégorie désignée. Cette configuration s'effectue manuellement en modifiant le contenu du fichier */etc/syslog.conf*. Pour obtenir de plus amples informations à ce sujet, consultez les [manual pages pour syslogd et syslog.conf](#).

Le système de surveillance utilise le journal système pour afficher les messages relatifs au fonctionnement du serveur de filtrage et de ses composants. Pour définir le répertoire où seront conservés les fichiers nécessaires, il faut utiliser les valeurs des paramètres du fichier de configuration */etc/syslog.conf*.

- **Verbose level** : degré de détail des informations consignées dans le protocole de fonctionnement des modules de Kaspersky Anti-Spam. Ce paramètre peut prendre les valeurs suivantes : **minimum**, **low**, **normal**,

**high, debug** et **more debug**. Lors de la définition d'un paramètre, il ne faut pas oublier que les paramètres contenus dans le fichier de configuration `/etc/syslog.conf` peuvent imposer des limites complémentaires sur le niveau de détails des informations en fonction de la catégorie (syslog facility). Ainsi, le niveau **mail.info** défini par défaut sous FreeBSD pour la catégorie **mail** réduit le niveau de détail même si le paramètre `Verbose level` possède la valeur `more debug`.



Le recours au niveau **more debug** impose une charge supplémentaire sur le serveur et peut entraîner une réduction des performances. Utilisez ce niveau uniquement lorsque vous devez résoudre un problème de fonctionnement de l'application.

The screenshot shows the Kaspersky Anti-Spam web interface. The main content area is titled 'Common Settings' and displays two configuration items: 'Syslog facility' set to 'mail' and 'Log level' set to 'normal'. There are 'Apply' and 'Reset' buttons at the bottom right of the settings area. The left sidebar shows a navigation menu with 'Anti-Spam Engine' and 'Maintenance' sections. The footer contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 18. Paramètres généraux du serveur de filtrage

Une fois que vous aurez modifié les paramètres généraux du serveur de filtrage, cliquez sur le bouton **Apply** et redémarrez le serveur de filtrage à l'aide de la commande :

```
# /etc/init.d/kas3 restart
```

pour les distributions de Linux :

```
# /usr/local/etc/rc.d/kas3.sh restart
```

pour le système d'exploitation FreeBSD.

## 4.5.2. Paramètres de fonctionnement du processus maître de filtrage

La page [Settings](#) → [Anti-Spam Engine](#) → [Process Server](#) contient les paramètres du processus maître de filtrage suivants (cf. ill. 19) :

- **Max. number of filtration processes** : nombre maximum de processus de filtrage lancés simultanément. La valeur par défaut est égale à **10**.
- **Number of filtration processes at server start-up** : nombre de processus de filtrage lancés au démarrage du serveur de filtrage. La valeur par défaut de ce paramètre est égale à **0**, ce qui signifie que les processus du module de filtrage seront lancés uniquement lorsque des messages arrivent.
- **Number of spare filtration processes** : nombre maximum de processus de filtrage lancés et en attente d'une requête d'analyse. Si le nombre de processus dépasse la limite définie, le système procède à l'arrêt forcé des processus inutilisés. La valeur par défaut est égale à **0**.

The screenshot displays the 'Process Server Settings' page in the Kaspersky Anti-Spam interface. The page title is 'Process Server Settings' with a timestamp of 12:48. The settings include:

- Max. number of filtration processes:** 10
- Number of filtration processes at server start-up:** 0
- Number of spare filtration processes:** 0

There are 'Apply' and 'Reset' buttons at the bottom right. The left sidebar shows navigation options like 'Common', 'Process Server', 'Filtration Process', 'Check Options', 'MTA Clients', 'Reject Messages', 'Updater', and 'Control Center'.

Illustration 19. Paramètres de fonctionnement du processus maître de filtrage

Une fois que vous aurez modifié les paramètres du processus maître de filtrage, cliquez sur le bouton **Apply** et redémarrez le serveur de filtrage à l'aide de la commande :

```
# /etc/init.d/kas3 restart
```

pour les distributions de Linux ;

```
# /usr/local/etc/rc.d/kas3.sh restart
```

pour le système d'exploitation FreeBSD.

### 4.5.3. Paramètres des processus de filtrage

La page Settings → Anti-Spam Engine → Filtration Process (cf. ill. 20) contient les paramètres des processus de filtrage *ap-mailfilter* :

- **Max. number of mail messages to be processed** : nombre maximum de messages traité par un processus de filtrage. Une fois que le processus a traité le nombre défini de messages, il s'arrête et un nouvel exemplaire du processus de filtrage est lancé. La valeur de ce paramètre peut être modifiée en fonction de la charge du serveur de filtrage. La valeur recommandée est égale à **300**.
- **Max. number of mail messages randomization** : valeur utilisée par Kaspersky Anti-Spam pour définir le nombre maximum de messages pouvant être traités par un processus de filtrage déterminé. Pour chacun des processus de filtrage, ce nombre est choisi au hasard dans une plage dont la limite inférieure est définie par la valeur **Max. number of mail messages to be processed** et la limite supérieure, par la somme des nombres **Max. number of mail messages to be processed** et **Max. number of mail messages randomization**. Autrement dit, si la valeur de ces paramètres est respectivement de **300** et **30**, chaque processus de filtrage traitera entre 300 et 330 messages. Le paramètre permet d'éviter l'arrêt et la reprise simultanée d'un grand nombre de nouveaux processus de filtrage lorsque le serveur est fortement sollicité.
- **Max. idle time (in seconds)** : période maximale (en secondes) durant laquelle le processus de filtrage peut être en attente. Si le processus de filtrage ne reçoit aucun message au cours de cette période, il s'arrête. La valeur par défaut est égale à **300**.
- **Exit delay (in seconds)** : durée maximale (en secondes) du décalage de l'arrêt du processus lorsque celui-ci reçoit la commande d'arrêt. La valeur de ce paramètre est égale à **0** par défaut, ce qui signifie que lorsqu'ils reçoivent la commande adéquate, tous les processus de filtrage s'arrêtent directement après le traitement du message actuel.

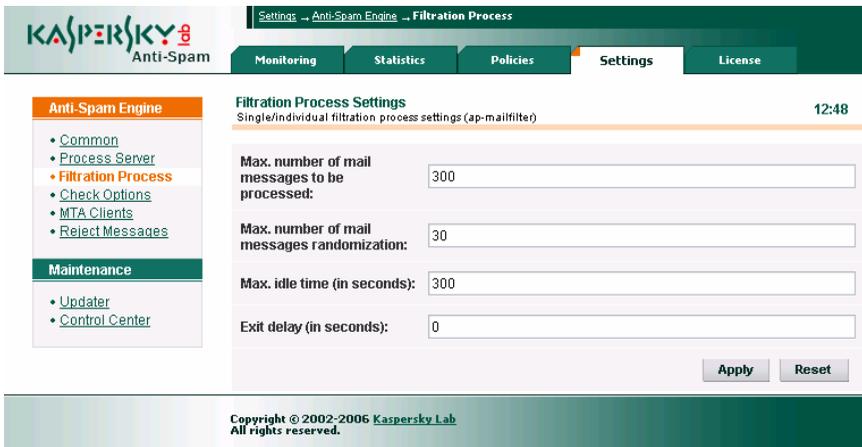


Illustration 20. Paramètres des processus de filtrage

## 4.5.4. Paramètres d'identification du courrier indésirable

La page Settings → Anti-Spam Engine → Check Options (cf. ill. 21) contient les paramètres des processus de filtrage *ap-mailfilter* :

- **Number of 'Received' headers to be parsed while retrieving ip address (for use in DNSBL checks)** : ce paramètre indique la nécessité de vérifier les serveurs intermédiaires à l'aide du service DNSBL. Normalement, l'adresse IP du serveur d'où provient le message reçu par le serveur de filtrage est utilisée lors de la vérification de l'adresse IP de l'expéditeur du message. Toutefois, lorsque le message électronique transite par plusieurs serveurs intermédiaires, l'adresse IP d'origine de l'expéditeur est cachée. Afin de pouvoir vérifier l'adresse IP non seulement du dernier serveur de la chaîne mais également de tous les serveurs intermédiaires, indiquez à l'aide de ce paramètre, le nombre de serveurs à vérifier. L'analyse repose sur le champ Received de l'en-tête. La valeur **0** signifie que le champ Received de l'en-tête ne sera pas vérifié.



Une valeur plus élevée de ce paramètre indique au serveur de filtrage qu'il doit analyser un plus grande nombre de serveurs intermédiaires. Cela permet d'augmenter les chances d'identification de messages non sollicités en provenance de serveurs de diffusions de pourriels via plusieurs serveurs intermédiaires. Le revers de la médaille est que la charge du serveur de filtrage augmente considérablement et qu'il peut y avoir des faux positifs.

- **Overall timeout of all DNS requests (in seconds)** : délai d'attente (en secondes) de la réponse du serveur DNS lors des vérifications sur la base du DNS. La valeur par défaut est égale à **10**.
- **Check MS Word and RTF files** : ce paramètre active/désactive l'analyse du texte des pièces jointes au format Word (doc) et RTF.

The screenshot shows the 'Check Options' settings page in the Kaspersky Anti-Spam interface. The page is titled 'Settings → Anti-Spam Engine → Check Options' and has a timestamp of 13:41. The left sidebar contains a navigation menu with categories like 'Anti-Spam Engine' (with sub-items: Common, Process Server, Filtration Process, Check Options, MTA Clients, Rejected Messages) and 'Maintenance' (with sub-items: Updater, Control Center). The main content area is titled 'Check Options' and 'Settings of different check options'. It contains several settings:

- 'Number of 'Received' headers to be parsed while retrieving ip address (for use in DNSBL checks):' set to 12.
- 'Overall timeout of all DNS requests (in seconds):' set to 10.
- 'Check MS Word and RTF files:': an unchecked checkbox.
- 'UDS enabled:': a checked checkbox.
- 'Timeout for receiving response from UDS server (in seconds):' set to 10.

At the bottom right of the settings area are 'Apply' and 'Reset' buttons. A footer at the bottom of the page reads 'Copyright © 2002-2006 Kaspersky Lab All rights reserved.'

Illustration 21. Paramètres d'identification du courrier indésirable

- **UDS enabled** : ce paramètre active/désactive le mode de vérification des messages à l'aide du service UDS. Ce service permet de bloquer efficacement les messages non sollicités sans devoir attendre le chargement de la mise à jour des bases de filtrage du contenu. Il est conseillé de désactiver le service UDS uniquement si ce dernier a un impact négatif sur les performances du serveur de filtrage ou s'il est impossible d'assurer l'interaction du serveur de filtrage avec les serveurs UDS de Kaspersky Lab.

Pour obtenir de plus amples informations sur le service UDS, consultez le point 2.2.4 à la page 20.

- **Timeout for receiving response from UDS server (in seconds)** : délai d'attente pour l'établissement de la connexion entre le serveur de filtrage et le serveur UDS. Si le serveur de filtrage ne reçoit aucune réponse du serveur UDS au cours de l'intervalle défini, il tente de se connecter à un autre serveur UDS de Kaspersky Lab.

## 4.5.5. Paramètres des modules clients

La page Settings → Anti-Spam Engine → MTA Clients (cf. ill. 22) contient les paramètres des modules clients chargés de l'interaction entre le serveur de messagerie et le serveur de filtrage :

- **Filtering size limit (KB)** : taille maximale des messages (en Ko) traités par le serveur de filtrage. Si la taille du message dépasse la valeur définie, le serveur de filtrage ne le traitera pas. La valeur par défaut est égale à **500**.
- **On filtering error** : réaction du module client en cas d'erreur lors de l'interaction avec le serveur de filtrage. Le paramètre peut prendre les valeurs suivantes :
  - **accept message** : lorsqu'une erreur se produit, le message est envoyé au destinataire sans intervention du serveur de filtrage ;
  - **reject message** : lorsque le traitement du message se solde par une erreur, le message n'est pas délivré ;
  - **generate temporary error** : le message n'est pas délivré et l'expéditeur reçoit une notification relative à l'erreur temporaire du serveur de messagerie. Dans ce cas, le serveur de messagerie de l'expéditeur procédera à une nouvelle tentative d'envoi du message après un certain temps.
- **Default domain** : nom du domaine de messagerie dans l'adresse où le domaine de messagerie n'est pas indiqué. Par exemple, lorsque le domaine par défaut est le domaine monentreprise.com, alors l'adresse unutilisateur sera interprétée comme unutilisateur@monentreprise.com.
- **Connection timeout (in seconds)** : délai (en secondes) pour l'établissement d'une connexion entre le module client et le serveur de filtrage. La valeur par défaut est égale à **40**.
- **Data exchange timeout (in seconds)** : délai (en secondes) pour l'exécution des opérations de réseau de lecture et d'écriture lors de

l'échange de données entre le serveur de filtrage et le module client. La valeur par défaut est égale à **30**.



Lorsque des erreurs systématiques surviennent dans le fonctionnement du serveur de filtrage, il faut s'adresser au service d'assistance technique de Kaspersky Lab. Les coordonnées du service d'assistance technique sont reprises au point C.2. page 142.

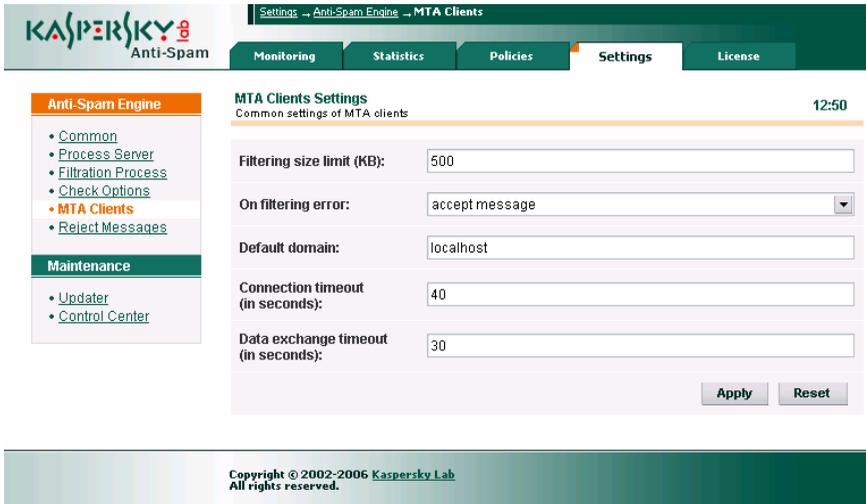


Illustration 22. Paramètres des modules clients

## 4.5.6. Notifications de non-réception d'un message

Lorsque l'action **Reject this message** a été sélectionnée pour les messages correspondant à un certain statut, le serveur de filtrage ne délivrera pas les messages aux destinataires originaux. L'expéditeur, quant à lui, recevra un message sur l'impossibilité de délivrer le courrier.

Le serveur de filtrage exploite deux types de message. Le type de message utilisé dépend de la configuration du logiciel et des résultats de l'identification.

Le premier type de message est **Reject message**. Ce message est envoyé à l'expéditeur directement lors de la session SMTP avec un code d'erreur pour signaler que le message n'a pas été délivré. L'exemple de session SMTP fourni ci-après contient le texte d'un message **Reject message** :

```
Serveur: 220 mail.mycompamy.com ESMTTP
Client: HELO spamhost.whatever.com
Serveur: 250 mail.mycompamy.com
Client: MAIL FROM: <spamer@whatever.com>
Serveur: 250 Ok
Client: RCPT TO: <someuser@mycompany.com>
Serveur: 250 Ok
Client: DATA
Serveur: 354 End data with <CR><LF>.<CR><LF>
Client: >>>
Client: >>> Texte du message...
Client: >>>
Client: .
Serveur: 550 The message is rejected by spam filtering
engine.
Client: QUIT
Serveur: 221 Bye...
```

Le serveur de filtrage utilise les messages Reject message uniquement lorsque le message ne peut être délivré à tous les destinataires suite aux résultats de la vérification.

Si le message est envoyé à plusieurs destinataires et qu'au moins un d'entre eux ne peut recevoir le message en raison de la configuration des stratégies de filtrage, le serveur signale lors de la session SMTP que le message a été délivré. L'expéditeur reçoit ensuite un message Bounce message reprenant les informations relatives aux destinataires qui n'ont pas reçu le message en question.

La modification du texte de ces messages s'opère sur la page du Centre d'administration **Settings** → **Anti-Spam Engine** → **Reject Messages** (cf. ill. 23).

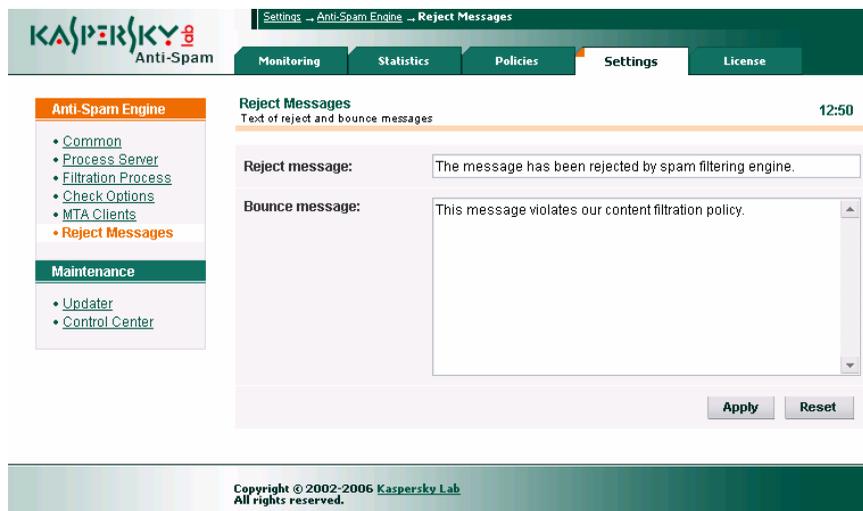


Illustration 23. Page de modification du message relatif à l'échec de la délivrance du courrier

## 4.6. Configuration du Centre d'administration

La page **Settings** → **Maintenance** → **Control Center** (cf. ill. 24) contient les paramètres qui vous permettront de :

- Indiquer l'adresse pour l'envoi des messages du système de surveillance et des messages relatifs aux erreurs d'exécution des scripts à l'aide du service cron (paramètre **Send alerts to**) ;
- Activer/désactiver la surveillance du fonctionnement du serveur HTTP kas-thttpd (paramètre **Monitoring of kas-thttpd daemon**) ;
- Activer/désactiver la surveillance du fonctionnement du module client kas-milter utilisé pour l'interaction avec le serveur de messagerie Sendmail (paramètre **Monitoring of kas-milter daemon**).

Les messages composés lors de la surveillance du fonctionnement des modules kas-thttpd et kas-milter sont repris sur la page **Monitoring** → **Anti-Spam Engine** (cf. point 4.8.1.1, p. 77).

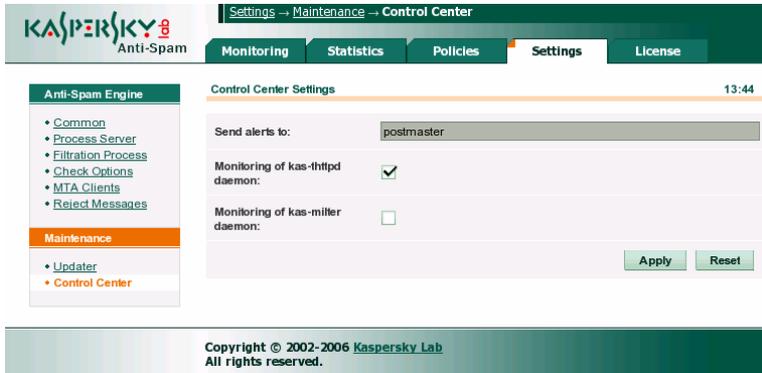


Illustration 24. Configuration du Centre d'administration

## 4.7. Gestion des clés de licence

L'utilisation de Kaspersky Anti-Spam est liée à l'existence d'une *clé de licence*. Elle fait partie du pack logiciel et vous donne le droit d'utiliser Kaspersky Anti-Spam dès l'acquisition et l'installation de la clé.



**Kaspersky Anti-Spam NE FONCTIONNERA PAS sans la clé de licence ! Aucun message ne sera filtré.**

La clé de licence contient toutes les informations requises liées à la licence que vous avez achetée telles que : le type de licence, sa date d'expiration, les informations relatives aux distributeurs, etc.

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

- Assistance technique 24h/24 ;
- Actualisation toutes les 20 minutes des bases de filtrage du contenu ;

Lorsque la durée de validité de la licence est écoulée, l'application continue à fonctionner mais il ne sera plus possible d'actualiser les bases de filtrage du contenu. Vous pourrez continuer à filtrer le courrier à l'aides des bases d'actualité au moment où la clé est parvenue à échéance. Par conséquent, Kaspersky Anti-Spam ne pourra plus lutter efficacement contre les pourriels.

Il est dès lors vivement conseillé de renouveler à temps la licence d'utilisation de Kaspersky Anti-Spam. Il est possible également d'installer une clé de réserve qui sera utilisée par l'application dès que la clé actuelle sera parvenue à échéance.

Toutes les opérations liées à l'administration des clés de licence installées peuvent être réalisées à l'aide du Centre d'administration.

## 4.7.1. Consultation des informations relatives aux licences

Pour consulter les informations relatives aux licences et pour administrer ces dernières, rendez-vous à la page License → License Keys (cf. ill. 25) du Centre d'administration.

La partie supérieure de la page contient la section **Active** Licence Information qui propose les données suivantes :

- Nom du logiciel installé ;
- Type de licence actuelle ;
- Durée de validité de la licence ;

The screenshot shows the 'License → License Keys' page in the Kaspersky Anti-Spam administration console. The page has a green header with the Kaspersky logo and navigation tabs for Monitoring, Statistics, Policies, Settings, and License. The 'License' tab is active. On the left, there is a sidebar with 'License' and 'License Keys' options. The main content area is titled 'Active License Information' and shows the following details:

- Product:** Kaspersky Anti-Spam
- License:** Users 10
- Valid till:** Jul 24 2006 (expires in 90 days)

Below this, there is a table for 'License Key Files':

File	Serial	Type	Volume	Valid till
000FF1AE.key	02B1-0004A0-000FF1AE	Users (Beta)	10	Jul 24 2006

At the bottom, there is a section for 'Install a New License Key' with a text input field for the license key file, a 'Choose' button, and an 'Apply' button.

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 25. Informations relatives à la licence de Kaspersky Anti-Spam

Grâce aux informations présentées dans les deux dernières lignes, l'administrateur peut surveiller les conditions de la licence acquise (durée de validité, restrictions définies).

En fonction de l'état, l'icône dans la partie gauche de la ligne peut ressembler à ceci :

- ✔ Les conditions de la licence sont respectées.
- ! Le logiciel est proche des limites imposées par la licence ou la licence arrivera à échéance au cours des deux prochaines semaines.
- ✖ La licence n'est plus valide ou les limites imposées par la licence ont été dépassées (par exemple, volume de messages traités).

Dans les deux derniers cas, la ligne contient également un message explicatif.

Vous trouverez au-dessous du bloc d'informations la liste des clés de licence de Kaspersky Anti-Spam installées ainsi que de brefs renseignements sur chacune d'entre elles.

## 4.7.2. Installation d'une nouvelle clé de licence

Afin de pouvoir installer une nouvelle clé de licence, l'administrateur doit soit utiliser le Centre d'administration, soit procéder à une installation locale via la ligne de commande.



*Pour installer une nouvelle clé de licence à l'aide du Centre d'administration, procédez comme suit :*

- Ouvrez la page d'administration des clés de licence License → License Keys.
- Saisissez, dans le champ de la partie inférieure de la page dans la rubrique **Install a New License Key**, le chemin d'accès au fichier de clé de licence ou cliquez sur le bouton de navigation dans le système de fichiers situé à droite du champ de saisie.
- Cliquez sur **Apply**.



*Pour installer une nouvelle clé de licence localement via la ligne de commande, saisissez la commande :*

```
# /usr/local/ap-mailfilter3/bin/install-key <key>
```

où **key** représente le chemin d'accès au fichier contenant la clé de licence.

Si vous souhaitez activer une nouvelle clé de licence avant la date d'expiration de la licence en cours, vous pouvez attribuer à la nouvelle clé le statut de

réserve. La clé de réserve commence à fonctionner dès la fin de la période de validité de la clé actuelle. La durée de validité de la clé de réserve est calculée à partir de son activation. Une seule clé de réserve peut être installée.

### 4.7.3. Suppression de la clé de licence

Pour supprimer une clé de licence active ou de réserve, saisissez dans la ligne de commande :

```
# /usr/local/ap-mailfilter3/bin/remove-key -a
```

Pour supprimer une clé de licence de réserve, saisissez dans la ligne de commande :

```
# /usr/local/ap-mailfilter3/bin/remove-key -r
```



Les clés de licence ne peuvent être supprimées via l'interface du Centre d'administration.

## 4.8. Surveillance du fonctionnement du serveur de filtrage

Kaspersky Anti-Spam propose un système de surveillance de l'état des différents composants afin de pouvoir contrôler efficacement le fonctionnement du logiciel et informer l'administrateur en cas d'incidents dans le système à l'aide de l'interface du Centre d'administration.

### 4.8.1. Messages généraux sur l'état du logiciel

La page située à l'adresse **Monitoring** → **General Status** fournit à l'administrateur du système des informations succinctes sur Kaspersky Anti-Spam et sur l'état de ses principaux composants (cf. ill. 26).

En plus des informations relatives à l'état de chacun de ces composants, cette page propose également des renseignements sur les événements survenus en rapport avec le composant.

The screenshot shows the 'Monitoring - General Status' window of Kaspersky Anti-Spam. It features a navigation bar with 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' section is active, displaying a sidebar with links to 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is divided into two sections: 'System Information' and 'Kaspersky Anti-Spam'. The 'System Information' section shows 'Host Name: mail.test.local', 'System: FreeBSD 5.4-RELEASE-p7 i386', and 'Load Average: 0.13'. The 'Kaspersky Anti-Spam' section shows 'Product: Kaspersky Anti-Spam Enterprise Edition', 'Version: 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45', 'Anti-Spam Engine: Errors...', 'Updates: OK', and 'License: Errors...'. Each item has an icon indicating its status: a blue 'i' for information, a green checkmark for OK, and a red 'x' for error.

Monitoring - General Status

Monitoring | Statistics | Policies | Settings | License

**Monitoring**

- [General Status](#)
- [Anti-Spam Engine](#)
- [Updates](#)
- [License](#)

**System Information** 12:06

- Host Name:** mail.test.local
- System:** FreeBSD 5.4-RELEASE-p7 i386
- Load Average:** 0.13

**Kaspersky Anti-Spam**

- Product:** Kaspersky Anti-Spam Enterprise Edition
- Version:** 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45
- Anti-Spam Engine:** [Errors...](#)
- Updates:** OK
- License:** [Errors...](#)

Copyright © 2002-2006 Kaspersky Lab  
All rights reserved.

Illustration 26. Notifications générales sur l'état des composants de Kaspersky Anti-Spam

Les icônes placées à côté du nom des paramètres constituent un moyen supplémentaire de transmettre des informations. L'icône témoigne de l'état du fonctionnement du composant contrôlé :

- Erreur : échec du composant ou dépassement de la valeur définie pour le paramètre contrôlé.
- Avertissement : problème de fonctionnement du composant qui ne présente pas un caractère critique pour le logiciel dans son ensemble ou la valeur du paramètre contrôlé est proche des limites définies.
- Etat normal : le composant fonctionne normalement et la valeur du paramètre contrôlé est admissible.

La section **System information** contient les renseignements suivants sur le serveur où Kaspersky Anti-Spam est installé :

- **Host Name** : nom du serveur.
- **System** : nom, version et type d'architecture utilisée par le système d'exploitation.
- **Load Average** : paramètre numérique qui indique la charge du serveur. Pour obtenir de plus amples informations à ce sujet, consultez les manuels pages pour les utilitaires *top* et *uptime*.

La section **Kaspersky Anti-Spam** contient la synthèse des informations relatives au logiciel et à l'état de ses composants clés. La section contient les champs suivants :

- **Product** : nom complet du logiciel installé.
- **Version** : renseignements relatifs à la version et au numéro de construction du module de filtrage utilisé.
- **Anti-Spam Engine** : état du fonctionnement du serveur de filtrage.
- **Updates** : état des bases de filtrage du contenu et du système de mise à jour.
- **License** : état du module de licence.

### 4.8.1.1. Informations détaillées sur le moteur du serveur de filtrage

En cliquant sur le lien [Anti-Spam Engine](#) du menu **Monitoring**, vous ouvrez la page contenant les détails de l'état des composants du serveur de filtrage (cf. ill. 27).

The screenshot displays the Kaspersky Anti-Spam Monitoring interface. The main title is "Monitoring - Anti-Spam Engine". The navigation menu includes "Monitoring", "Statistics", "Policies", "Settings", and "License". The "Monitoring" section is active, showing a summary of the Anti-Spam Engine status. The status is "OK" with a timestamp of 14:03. The version is 3.0.0 [0232] KAS30/Release, built at May 17 2006, 17:57:59. The components listed are: ap-process-server (OK, pid=70527), ap-mailfilter (OK, processes: 0), ap-spfid (OK, processes: 17), kas-httpd (OK, pid=71493), and Monitoring & Statistics (OK). Below this, there is a section for "Last Anti-Spam Engine Events" with a view filter set to "Notifications, Warnings and Errors". Two events are shown: "05:22 13:50:48 kas-restart: kas-milter is restarted" and "05:22 12:50:42 kas-restart: No ap-mailfilter processes running". The footer contains the copyright information: "Copyright © 2002-2006 Kaspersky Lab All rights reserved."

Illustration 27. Page de surveillance de l'état du moteur du serveur de filtrage

La section **Anti-Spam Engine** contient les champs suivants :

- **Version** : version et numéro de construction du module de filtrage utilisé.

- **ap-process-server** : état du processus maître de filtrage. Si le processus fonctionne normalement, cette ligne contient également les informations relatives à l'identifiant de processus (**pid**).
- **ap-mailfilter** : état des processus de filtrage. Lors du fonctionnement normal, cette ligne contient également les renseignements relatifs au nombre de processus exécutés à cet instant.
- **ap-spf** : état du démon SPF. Si le démon fonctionne normalement, ce champ affiche le nombre de processus exécutés.
- **kas-thttpd** : état du serveur HTTP utilisé par le Centre d'administration.
- **Monitoring & Statistics** : renseignements sur le fonctionnement des scripts liés à la surveillance et au traitement des statistiques. De plus, le système vérifie l'existence d'une tâche cron pour le lancement de ces scripts pour l'utilisateur **mailfit3**. Pour obtenir de plus amples informations, consultez le point A.6 à la page 126.

La section **Last Anti-Spam Engine Events** contient le protocole des messages des composants du serveur de filtrage consignés dans le journal système (syslog). Les messages sont classés par date d'apparition et sont accompagnés d'une icône précisant le niveau de gravité du message. La liste déroulante **View** permet à l'administrateur de définir la catégorie de messages qui seront repris dans le protocole. La liste déroulante contient les valeurs suivantes :

- **All messages** : affiche tous les messages possibles ;
- **Notices, Warnings and Errors** : affiche tous les messages, sauf les messages à caractère informatif ;
- **Warnings and Errors** : affiche uniquement les messages relatifs aux erreurs critiques et aux avertissements ;
- **Errors only** : affiche uniquement les messages relatifs aux erreurs critiques.

#### 4.8.1.2. Informations détaillées sur le module de mise à jour

Afin d'ouvrir la page contenant les informations relatives au module de mise à jour et à l'état des bases de filtrage du contenu, cliquez sur le lien [Updates](#) du menu Monitoring (cf. ill. 28).

La section **Anti-Spam Updates**, dans la partie supérieure de la page, contient les champs suivants :

- **Automatic Updates** : ce champ indique si la mise à jour automatique des bases de filtrage du contenu est activée ou non. Pour obtenir de plus

amples informations sur le script de mise à jour des bases de filtrage du contenu, consultez le point 4.4.1 à la page 58 et le point A.6 à la page 126.

- **Anti-Spam Database Id** : informations relatives aux bases de filtrage du contenu installées : date et heure de publication des bases et de la dernière mise à jour.
- **Last Update** : date et heure de la dernière mise à jour des bases de filtrage du contenu. Le système de surveillance prévient l'administrateur lorsque les bases de filtrage du contenu n'ont plus été actualisée depuis un certain temps.

The screenshot displays the Kaspersky Anti-Spam Monitoring interface. At the top, there is a navigation bar with tabs for Monitoring, Statistics, Policies, Settings, and License. The main content area is titled 'Monitoring: Updates' and shows the following information:

- Automatic Updates:** Enabled
- Anti-Spam Database Id:** Daily update 17.02.2006 (day060217) + Recent 21.02.06 12:44:00 (MSK)
- Last Update:** 2006-02-21 13:13

Below this, the 'Last Updater Events' section is shown with a 'View' dropdown menu set to 'Notifications, Warnings and Errors'. The event log contains three entries:

- 02-21 13:33:02 sfupdates: Data are up to date (upd time = 21.02.06 12:44:00 (MSK))
- 02-21 13:13:11 sfupdates: New data installed (upd time = 21.02.06 12:44:00 (MSK))
- 02-21 11:09:05 sfupdates: New data installed (upd time = 21.02.06 10:44:00 (MSK))

At the bottom of the page, the copyright notice reads: Copyright © 2002-2006 Kaspersky Lab. All rights reserved.

Illustration 28. Page de surveillance du module de mise à jour

La section **Last Updater Events** contient le protocole des messages du système de mise à jour du logiciel consignés dans le journal système (syslog). Les messages sont classés par date d'apparition et sont accompagnés d'une icône précisant le niveau de gravité du message. La liste déroulante **View** permet à l'administrateur de définir la catégorie de messages qui seront repris dans le protocole. Les valeurs de la liste déroulante et leur significations sont identiques à celles des valeurs présentées dans la description de la page de surveillance du serveur de filtrage (cf. point 4.8.1.1, p. 77).

### 4.8.1.3. Informations détaillées sur le module de licence

La page située à l'adresse Monitoring → License offre à l'administrateur des informations sur la licence utilisée et contient le protocole des messages du module de licence (cf. ill. 29).

La section **Monitoring** → **License**, dans la partie supérieure de la page, contient les champs suivants :

- **Product** : nom du logiciel installé.
- **License** : type de licence utilisée et informations sur les restrictions imposées.

The screenshot displays the 'Monitoring License' page in the Kaspersky Anti-Spam interface. The page title is 'Monitoring → License'. The main content area is divided into two sections. The first section, 'Monitoring: License', shows the following details:

Product:	Kaspersky Anti-Spam
License:	Users 10
Valid till:	Jul 24 2006 (expires in 90 days)
License Daemon:	OK, pid=15994

The second section, 'Last License Daemon Events', has a 'View' dropdown set to 'Notifications, Warnings and Errors'. It contains a list of four events:

- 04-24 19:17:17 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/000FF1AE.key has been installed successfully
- 04-24 19:16:53 remove-key: License key was successfully removed
- 04-24 19:13:47 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/black-0010617B.key has been installed successfully
- 04-24 19:13:30 remove-key: License key was successfully removed

At the bottom of the page, the copyright notice reads: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

Illustration 29. Page de surveillance du fonctionnement du module de licence

- **Valid till** : date d'expiration de la licence. Le système de surveillance commencera à avertir l'administrateur de l'expiration prochaine de la licence un mois avant la fin de la validité ;
- **License Daemon** : état du service de licence. Lorsque ce service fonctionne normalement, ce champ contient également l'identifiant du processus (**pid**).

La section **Last Updater Daemon Events** contient le protocole des messages du module de licence du logiciel consignés dans le journal système (syslog). Les

messages sont classés par date d'apparition et sont accompagnés d'une icône précisant le niveau de gravité du message. La liste déroulante **View** permet à l'administrateur de définir la catégorie de messages qui seront repris dans le protocole. Les valeurs de la liste déroulante et leur significations sont identiques à celles des valeurs présentées dans la description de la page de surveillance du serveur de filtrage (cf. point 4.8.1.1, p. 77).

## 4.8.2. Messages et rapports du système de surveillance

En plus des outils de surveillance proposé par le Centre d'administration, Kaspersky Anti-Spam offre également le script *sfmonitoring* qui assure le contrôle permanent de l'état du serveur de filtrage. Ce script est lancé automatiquement à l'aide du service *cron*. Une fois que le script *sfmonitoring* a été lancé, l'état du serveur de filtrage est vérifié et en cas de problèmes, une notification est envoyée à l'administrateur.

Le script de surveillance peut envoyer deux types de message à l'administrateur :

- **messages relatifs aux erreurs à nouveau relevées** : message sur la découverte d'un problème dans le fonctionnement du serveur de filtrage qui propose une description de la situation. Ce message relatif à l'erreur est envoyé une fois. Si le problème n'est pas résolu, le message sera également inclus dans le rapport sur les problèmes connus envoyé chaque jour.
- **rapports journaliers sur les problèmes connus** : liste de toutes les erreurs et des avertissements connus au moment de l'envoi du rapport. Ce rapport contient aussi bien les nouvelles erreurs que les erreurs décelées antérieurement et qui n'ont pas été corrigées au moment de la création du rapport. Ce rapport est envoyé une fois par jour à minuit (en fonction du réglage de l'heure du serveur). Pour procéder à l'envoi forcé du rapport, exécutez la commande suivante au nom de l'utilisateur **root**.

```
# su -m mailflt3 -c '/usr/local/ap-mailfilter3/control/bin/sfmonitoring -m'
```

Pour afficher le rapport sur la console du serveur :

```
# su -m mailflt3 -c '/usr/local/ap-mailfilter3/control/bin/sfmonitoring -p'
```



Si Kaspersky Anti-Spam est installé sur un serveur tournant sous la distribution RedHat, le lancement de l'utilitaire sfmonitoring s'opère à l'aide de la commande suivante :

```
su - -m mailft3 -c '/usr/local/ap-mailfilter3/control/bin/sfmonitoring -<paramètres>'
```

Les messages du système de surveillance sont envoyés à l'adresse indiquée sur la page **Settings** → **Maintenance** → **Control center** (cf. point 4.6, p. 71).

## 4.9. Statistiques de Kaspersky Anti-Spam

Le Centre d'administration possède un module chargé de recueillir les données statistiques sur les messages traités et de les afficher via les outils de l'interface du Centre d'administration. Il est ainsi possible d'analyser les résultats du fonctionnement du logiciel.

Les données statistiques sont recueillies et traitées par des scripts spéciaux exécutés à l'aide du service *cron* (pour obtenir de plus amples informations sur ces scripts, consultez le point A.6 à la page 126). Les résultats du traitement sont présentés sous la forme de diagrammes dans les pages de la section **Statistics** (cf. ill. 30).

Chacune des pages de la section **Statistics** contient les données statistiques pour une période définie. Les liens vers ces pages sont repris dans le menu **Period** dans la partie gauche de la fenêtre de la section **Statistics**:

- Last Day : statistiques relatives aux messages traités au cours des dernières 24 heures ;
- Last Week : statistiques relatives aux messages traités au cours des 7 derniers jours ;
- Last Month : statistiques relatives aux messages traités au cours des 30 derniers jours ;
- Last Year : statistiques relatives aux messages traités au cours des 365 derniers jours ;

La partie supérieure de la page présente un tableau qui contient une synthèse des informations sur le nombre de messages traités et leur taille.

Sous ce tableau, vous trouverez une représentation graphique de la distribution du volume de messages de divers types identifiés en fonction du temps (conformément à la période sélectionnée) ainsi qu'un diagramme circulaire

représentant la part (en pour cent) de chaque type de message dans le volume globale.

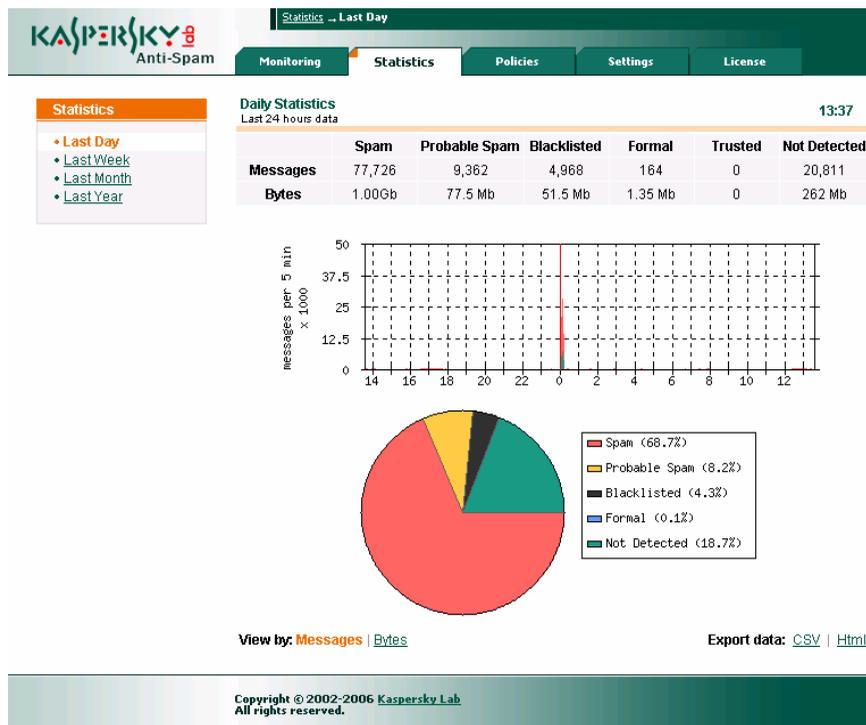


Illustration 30. Représentation des données statistiques



Dans le diagramme circulaire, les messages auxquels le même état a été attribué suite à l'analyse sont représentés par une même couleur. Pour contribuer à la lisibilité du diagramme, les segments dont la taille est minime par rapport aux autres sont regroupés au sein du segment **Other**.

Les liens Messages et Bytes du coin inférieur gauche permettent de choisir l'unité de mesure pour l'affichage des statistiques relatives au volume de messages traités, à savoir le nombre de messages ou le nombre d'octets.

Les liens Export data CSV | Html du coin inférieur droit permettent d'exporter les données statistiques au format CSV (Comma Separated Values) ou dans un tableau HTML.

# CHAPITRE 5. SUPPRESSION DE KASPERSKY ANTI-SPAM

La suppression de Kaspersky Anti-Spam requiert les privilèges de l'utilisateur **root**. Si vous ne disposez pas de ces privilèges au moment de la désinstallation, vous devrez absolument vous connecter en tant que **root**.



La procédure de suppression arrête automatiquement tous les services de Kaspersky Anti-Spam !

Au cours de la désinstallation de Kaspersky Anti-Spam, les services sont arrêtés et les fichiers et répertoires créés lors de l'installation sont supprimés. Toutefois, les répertoires et les fichiers créés ou modifiés par l'administrateur (fichiers de configuration, bases de filtrage du contenu, fichier de clé de licence) sont conservés. Les paramètres de fonctionnement du serveur de messagerie sont également restaurés à leur valeur antérieure à l'installation de Kaspersky Anti-Spam.



Si le fichier de configuration du serveur de messagerie a été modifié après l'installation de Kaspersky Anti-Spam, la restauration automatique des paramètres n'aura pas lieu et l'administrateur devra supprimer manuellement les modifications introduites par le logiciel lors de l'installation.

Le compte **mailft3** et son groupe correspondant **mailft3** sont conservés pour des raisons de sécurité. L'administrateur pourra supprimer ces comptes manuellement.

La procédure de suppression de l'application peut être lancée selon diverses méthodes en fonction du gestionnaire de paquetage utilisé :

- Si Kaspersky Anti-Spam a été installé au départ d'un paquetage rpm, lancez la désinstallation en saisissant la commande suivante :  

```
# rpm -e kas-3-<version de la distribution>
```
- Si Kaspersky Anti-Spam a été installé au départ d'un paquetage deb, lancez la désinstallation en saisissant la commande suivante :  

```
# dpkg -P kas-3
```
- Si Kaspersky Anti-Spam a été installé au départ d'un paquetage tgz ou tbz, lancez la désinstallation en saisissant la commande suivante :  

```
# pkg_delete kas-3-<version de la distribution>
```



Dans la mesure où l'intégration au serveur de messagerie CommuniGate Pro est réalisée manuellement, il est conseillé de supprimer les paramètres relatifs à Kaspersky Anti-Spam dans la configuration de CommuniGate Pro avant de supprimer le logiciel (cf. point A.2.7, p. 107).

Si vous souhaitez revenir à la configuration du serveur de messagerie en vigueur avant l'installation de Kaspersky Anti-Spam sans le supprimer, utilisez le script *MTA-unconfig.pl* situé dans le répertoire */usr/local/ap-mailfilter3/bin*. Ce script rétablira les valeurs d'origine des paramètres du serveur de messagerie en vigueur avant l'installation de Kaspersky Anti-Spam.

Ce script ne pourra cependant pas être utilisé si :

- Le fichier de configuration du serveur de messagerie a été modifié après l'installation de Kaspersky Anti-Spam ;
- Si le serveur de messagerie Exim est utilisé avec kas-exim en guise de module client ;
- Le serveur de messagerie CommuniGate Pro est utilisé.

Dans ce cas, l'administrateur devra supprimer manuellement les modifications introduites dans le fichier de configuration du serveur de messagerie. Les modifications introduites dans le fichier de configuration des serveurs de messagerie lors de l'intégration de Kaspersky Anti-Spam sont décrites en détail au point A.2 à la page 91.

# CHAPITRE 6. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus souvent posées par les utilisateurs sur l'installation, la configuration et l'utilisation de l'application.



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

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

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



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

Lorsque la licence est parvenue à échéance, Kaspersky Anti-Spam continue à fonctionner mais il n'est plus possible de procéder à la mise à jour des bases de filtrage du contenu. L'application continuera à filtrer le courrier mais sera incapable de reconnaître les nouveaux types de courrier indésirable.

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



*à quoi servent les mises à jour fréquentes ?*

Le courrier indésirable constitue un sérieux problème pour tous les utilisateurs du réseau et s'agissant des entreprises, il représente une véritable menace commerciale. Selon les dernières estimations, le volume de courrier indésirable en circulation dans le réseau Internet russe représente de 75 à 80% du volume total de messages. De plus, de nouveaux types d'envoi ne cessent de voir le jour. Afin de pouvoir réagir efficacement aux nouvelles formes de courrier indésirable et de bloquer leur diffusion, il est indispensable d'actualiser fréquemment les bases de filtrage du contenu utilisée pour l'identification des messages non sollicités. Les

versions actualisées des bases de filtrage du contenu sont publiées toutes les 20 minutes sur les serveurs de mise à jour de Kaspersky Lab.



**Question** : *l'application ne fonctionne pas. Que puis-je faire ?*

Si vous rencontrez des difficultés lors de l'utilisation de l'application, assurez-vous que la solution n'est pas fournie dans cette documentation et plus précisément dans ce chapitre ou dans la rubrique **Services / Banque de solutions** du site de Kaspersky Lab ([www.kaspersky.com/fr](http://www.kaspersky.com/fr)).

Si vous ne trouvez pas la solution à votre problème dans ce document ou dans la banque de solutions, contactez le service d'assistance technique de Kaspersky Lab.

Si le problème est urgent, composez le numéro de téléphone repris dans la section **Coordonnées** de la présente documentation. L'assistance téléphonique est offerte en russe, en anglais, en français et en allemand, 24h/24. N'oubliez pas que pour bénéficier de ce service, vous devez être un utilisateur enregistré. L'opérateur du service d'assistance technique vous demandera votre numéro d'enregistrement (si vous avez acheté le logiciel en boîte) ou les informations relatives à la commande (en cas d'achat en ligne).

Vous pouvez également envoyer un message au service d'assistance technique via le formulaire proposé dans la rubrique **Services / Centre de support / Résoudre un problème** du site de Kaspersky Lab.

Soyez précis lors de la saisie des informations : indiquez les détails du logiciel de Kaspersky Lab utilisé, les données d'enregistrement et tentez de décrire le plus exactement possible le problème rencontré. Dans les champs obligatoires, saisissez :

- Le type de requête. Sélectionnez le sujet de votre requête.
- Le nom du logiciel de Kaspersky Lab que vous utilisez (par exemple : **Kaspersky Anti-Spam 3.0**).
- Le texte du message. Décrivez le problème qui survient lors de l'utilisation du logiciel de Kaspersky Lab.
- Les données d'enregistrement. Indiquez le type d'enregistrement : **clé de licence** si vous avez acheté le logiciel en boîte ou **commande en ligne** si vous avez acheté le logiciel en ligne. En fonction du type d'enregistrement sélectionné,

saisissez dans le champ en dessous le numéro de série de la licence ou le numéro de référence de votre commande en ligne.

Le numéro de série de Kaspersky Anti-Spam figure sur la page **License** du Centre d'administration (cf. point 4.7.1, p. 73).

- L'adresse électronique à laquelle les experts du service d'assistance technique pourront vous contacter.

A la page suivante du formulaire, saisissez vos coordonnées ainsi que le code de protection contre les envois automatiques puis cliquez sur le bouton **Envoyer**. Les experts du service d'assistance technique tenteront de résoudre votre problème le plus rapidement possible.



***Question** : comment puis-je vérifier si Kaspersky Anti-Spam identifie bel et bien les messages non sollicités ?*

Vous pouvez vérifier le filtrage à l'aide du modèle spécial **GTUBE** (Generic Test for Unsolicited Bulk Email). La vérification de l'identification des messages non sollicités à l'aide de GTUBE est identique à la vérification du fonctionnement des logiciels antivirus à l'aide du virus d'essai EICAR.

Créez un message électronique contenant la ligne suivante (sans espace ni retour à la ligne) :

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-  
TEST-EMAIL*C.34X
```

et envoyez-le à l'adresse protégée par Kaspersky Anti-Spam. Suite à l'identification, le message recevra le statut **SPAM** et l'action définie par la stratégie pour le groupe du destinataire sera appliquée au message.



***Question** : lorsque la charge du serveur est élevée, Kaspersky Anti-Spam ne filtre pas le courrier indésirable. Les messages traités contiennent le champ suivant dans l'en-tête :*

*X-SpamTest-Info: Not processed*

La cause la plus probable de ce problème est que lors du traitement intense d'un volume important de messages électroniques, les processus de filtrage de l'application ne parviennent pas à se connecter au module de licence (*kas-license*) au cours de la période définie afin de vérifier si la requête est conforme aux prescriptions de la licence.

Pour régler ce problème, il est conseillé d'augmenter les délais de connexion et d'échange de données avec le module *kas-license* définis par les paramètres **FilterLicenseConnectTimeout** et **FilterLicenseDataTimeout**. Si le problème persiste malgré tout,

contactez le service d'assistance technique de Kaspersky Lab (cf. ci-dessus).



**Question :** *Kaspersky Anti-Spam ne filtre pas le courrier indésirable. Les messages traités contiennent le champ suivant dans l'en-tête :*

*X-SpamTest-Info: No License*

Ce problème est lié à l'expiration de la licence ou à l'absence d'une clé de licence. Assurez-vous que la clé de licence est installée et qu'elle est toujours valide. Pour obtenir de plus amples informations sur l'administration des clés de licence, consultez le point 4.7 à la page 72.



**Question :** *Kaspersky Anti-Spam ne vérifie pas les adresses IP de la norme IPv6 obtenues du champ Received de l'en-tête.*

Kaspersky Anti-Spam 3.0 ne prend pas en charge l'analyse des adresses IP de la norme IPv6.



**Question :** *il est impossible de réaliser l'intégration au serveur de messagerie Exim à l'aide du script MTA-config.pl. Le message suivant apparaît sur la console du serveur :*

```
Your Exim configuration file
/usr/local/etc/exim/configure already contains
kas-exim local_scan configuration parameters.
If your Exim hasn't been integrated with kas-
exim, remove all local_scan parameters and try
again.
```

Ce message indique que l'intégration au serveur de messagerie Exim a déjà été réalisée manuellement à l'aide du module client kas-exim. Le script *MTA-config.pl* tente d'installer le module client kas-pipe. Supprimer les paramètres d'interaction avec le module kas-exim (pour de plus amples informations sur l'utilisation de kas-exim, consultez le point A.2.5 à la page 103) dans la configuration d'Exim et procédez à une nouvelle tentative d'intégration.

# ANNEXE A.

## INFORMATIONS COMPLEMENTAIRES SUR KASPERSKY ANTI-SPAM

### A.1. Répartition des fichiers du logiciel dans les divers répertoires

Lors de l'installation de Kaspersky Anti-Spam, les fichiers de la distribution sont répartis de la manière suivante :

*/usr/local/ap-mailfilter3/* : répertoire principal où est installé le logiciel. Il comprend :

*bin/* : le répertoire contenant les fichiers exécutables et les scripts du logiciel ;

*cfdata/* : le répertoire contenant les bases de filtrage du contenu et les mises à jour des modules de Kaspersky Anti-Spam.

*conf/* : le répertoire contenant les fichiers de configuration. Ce répertoire contient les sous-répertoires :

*def/* : le répertoire contenant les fichiers indispensables à la compilation des stratégies de filtrage des messages, y compris les fichiers source des bases de filtrage du contenu et les fichiers renfermant les informations relatives aux stratégies de filtrage ;

*data/* : le répertoire contenant les fichiers binaires de configuration ;

*src/* : le répertoire contenant la représentation intermédiaire des fichiers de règles de filtrage utilisée lors de la compilation des règles.

*tmp/* : le répertoire contenant les fichiers temporaires utilisés lors de la manipulation des données de configuration.

*control/* : le répertoire contenant les fichiers du Centre d'administration. Il renferme les sous-répertoires :

*bin/*: le répertoire contenant les fichiers exécutables et les scripts du Centre d'administration ;

*lib/*: le répertoire contenant les fichiers des bibliothèques utilisées par le Centre d'administration ;

*stat/*: les fichiers de données du système de traitement des protocoles de travail et les statistiques ;

*tmp/*: le répertoire contenant les fichiers temporaires du Centre d'administration ;

*www/*: les scripts cgi et les images utilisées dans l'interface Web du Centre d'administration.

*etc/*: le répertoire contenant les fichiers de configuration de Kaspersky Anti-Spam ;

*lib/*: les bibliothèques utilisées par le logiciel lors de son fonctionnement.

*log/*: le répertoire contenant les fichiers du protocole de fonctionnement du serveur de filtrage utilisés pour la composition des statistiques ;

*run/*: le répertoire de travail du logiciel. Ce répertoire abrite également les fichiers pid des processus lancés du serveur de filtrage.

*src/*: le répertoire contenant les textes sources du module *kas-exim*.

## A.2. Modules clients des serveurs de messagerie

Kaspersky Anti-Spam contient les modules clients suivants qui interviennent lors de l'intégration du logiciel à divers serveurs de messagerie :

- *kas-milter* : module client pour le serveur de messagerie Sendmail ;
- *kas-pipe* : module client universel ; il est utilisé par défaut pour les serveurs de messagerie Postfix et Exim ;
- *kas-exim* : module client pour le serveur de messagerie Exim (alternative) ;
- *kas-qmail* : module client pour le serveur de messagerie Qmail ;
- *kas-cgpro* : module client pour le serveur de messagerie Communicate Pro ;

L'intégration du logiciel au serveur de messagerie a lieu lors de l'installation de Kaspersky Anti-Spam à l'aide de scripts de configuration spéciaux.

Cette annexe contient des informations plus détaillées sur les modes de fonctionnement des modules clients, sur leur fichiers de configuration et sur les particularités des configurations des serveurs de messagerie.

## A.2.1. Interaction des modules clients avec le serveur de filtration

L'interaction du module client avec le serveur de filtrage s'opère selon l'algorithme suivant :

1. Le module client reçoit le message du serveur de messagerie et envoie une requête de connexion au serveur de filtrage.
2. Le processus maître de filtrage choisit un processus de filtrage déjà lancé ou en crée un nouveau et établit la connexion entre le module client et le processus de filtrage en question.
3. Une fois la connexion établie, le module client envoie le message à vérifier et le processus de filtrage lui renvoie les résultats du traitement du message.
4. En fonction du résultat obtenu, le module client modifie, le cas échéant, le message et le renvoie au serveur de messagerie.

L'interaction entre le module client, le processus maître de filtrage et le processus de filtrage s'opère via le protocole interne sur un socket local ou de réseau.

Le socket de réseau permet de placer le serveur de filtrage et le serveur de messagerie avec le module client intégré sur différents serveurs. Si le trafic de messagerie traité le permet, le serveur de filtrage dédié peut desservir plusieurs serveurs de messagerie. Cette configuration requiert la configuration manuelle des paramètres d'interaction des composants de Kaspersky Anti-Spam et du serveur de messagerie.

## A.2.2. Paramètres généraux des modules clients

Dans Kaspersky Anti-Spam 3.0, les paramètres des modules clients sont repris dans le fichier de configuration général du serveur de filtrage *filter.conf* placé dans le répertoire */usr/local/ap-mailfilter3/etc/*.

Les paramètres suivants sont communs à l'ensemble des modules clients :

- **ClientConnectTo** : adresse du socket d'interaction avec le serveur de filtrage. Le format **tcp:<host>:<port>** où **<host>** représente l'adresse IP du serveur et **<port>**, le port de connexion est réservé au socket de réseau, tandis que le format

**unix:<chemin\_d'accès\_au\_fichier>** où **<chemin\_d'accès\_au\_fichier>** représente le chemin d'accès au fichier du socket est réservé au socket local.

- **ClientConnectTimeout** : délai d'attente maximum (en secondes) lors de l'établissement de la connexion avec le serveur de filtrage.
- **ClientDataTimeout** : délai d'attente maximum (en secondes) lors de l'échange de données avec le serveur de filtrage.
- **ClientOnError** : mode de traitement des erreurs (impossible d'établir la connexion avec le serveur de filtrage, délai d'attente dépassé lors de l'échange de données, etc.). Valeurs possibles :
  - **reject** : refus des messages, renvoi du code 5xx dans le processus de la session SMTP ;
  - **tempfail** : refus temporaire des messages, renvoi du code 4xx dans le processus de la session SMTP (utilisé par défaut) ;
  - **accept** : acceptation du message.



En cas d'utilisation d'un serveur de messagerie Sendmail, l'action **accept** signifie l'acceptation des messages sans traitement ultérieur par les autres filtres Milter utilisés par le serveur de messagerie après Kaspersky Anti-Spam.

- **ClientDefault domain** : nom du domaine de messagerie dans l'adresse où le domaine de messagerie n'est pas indiqué. Exemple : lorsque le domaine par défaut est le domaine monentreprise.com, alors l'adresse utilisateur sera interprétée comme utilisateur@monentreprise.com. Si ce paramètre n'est pas défini, la suggestion du nom de domaine ne se produit pas (ce paramètre n'est pas défini par défaut).
- **ClientFilteringSizeLimit** : taille maximale (en Ko) des messages qui peuvent être transmis au serveur de filtrage. Les messages dont la taille est supérieure ne sont pas traités par le serveur de filtrage. La valeur par défaut est égale à **500**.
- **ClientMessageStoreMem** : taille minimale (en Ko) des messages pour la sauvegarde des données intermédiaires sur le disque. Ce mode permet de contrôler le volume de mémoire vive utilisé. Si le paramètre est égal à **0** (valeur par défaut), alors toutes les données seront toujours sauvegardées dans la mémoire vive.
- **ClientTempDir** : chemin d'accès au répertoire de sauvegarde des fichiers temporaires.

## A.2.3. *kas-milter* : module client pour le serveur de messagerie Sendmail

Kaspersky Anti-Spam assure son intégration au serveur de messagerie à l'aide du module client *kas-milter*. L'interaction entre le module client et le serveur de messagerie s'opère via la bibliothèque *libmilter*.

L'interaction entre les modules en cas d'utilisation de Kaspersky Anti-Spam avec Sendmail est illustré dans le schéma 31.

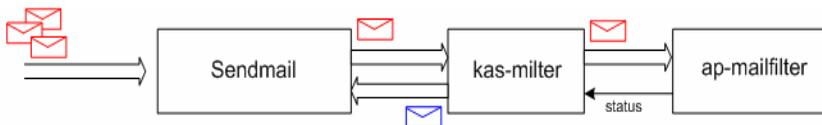


Illustration 31. Interaction entre Kaspersky Anti-Spam et le serveur de messagerie Sendmail

La configuration des paramètres d'interaction du module client et du serveur de messagerie peut être réalisée à l'aide de scripts spéciaux (cf. point 3.5, p. 30) ou manuellement.

La configuration manuelle des paramètres de fonctionnement du module client nécessite la modification du fichier de configuration *filter.conf* situé dans le répertoire */usr/local/ap-mailfilter3/etc/*. Voici un extrait de ce fichier contenant les paramètres du module client :

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
SendMailAddress unix:/var/run/kas-milter.socket
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
  
```

En plus des paramètres décrits ci-dessus au point A.2.2 de l'annexe, le module *kas-milter* possède dans le fichier *filter.conf* un paramètre complémentaire, à savoir **SendMailAddress** qui définit le socket d'interaction avec Sendmail.

Pour configurer l'interaction entre Sendmail et *kas-milter*, ajoutez les lignes suivantes au fichier de configuration *sendmail.cf* :

```

Xkasfilter,S=local:/var/run/kas-milter.socket,
T=C:10s,S:20s,R:30s
O InputMailFilters=kasfilter
  
```

La documentation de Sendmail contient une description détaillée des paramètres des filtres dans *sendmail.cf*.



En règle générale au moment du démarrage du système d'exploitation, Sendmail est lancé avant Kaspersky Anti-Spam. Par conséquent, Sendmail ne parvient pas à trouver le socket d'interaction et l'entrée suivante apparaît dans le journal système :

**WARNING: Xkas: local socket name <fichier\_du\_socket> missing**

Cet avertissement n'indique aucun problème dans la mesure où le fichier manquant sera créé par le module client kas-milter après le lancement de Kaspersky Anti-Virus.

Particularités de l'utilisation du module client kas-milter avec le serveur de messagerie Sendmail :

- kas-milter ne crée pas de copies des messages lors du traitement. Si le message est envoyé à plusieurs destinataires issus de différents groupes dont les règles de traitement varient, alors les actions définies pour chacun des groupes seront exécutées. Exemple :

un message est envoyé à `alice@monentreprise.com` et `pierre@monentreprise.com`. Ces adresses appartiennent respectivement aux groupes **sales** et **managers**. Suite au filtrage, le message reçoit l'état **Spam** pour le groupe **sales** et **Not detected** pour le groupe **managers**. Conformément aux règles du groupe **sales**, les messages dont l'état est **Spam** sont modifiés par l'ajout du texte **[!! SPAM]** dans l'objet du message tandis que conformément aux règles du groupe **managers**, les messages dont l'état est **Not Detected** sont soumis à l'action **Accept this message**. Dans ce cas précis, un message avec le texte **[!! SPAM]** est délivré aux deux destinataires. Ce message contiendra les champs suivants dans l'en-tête :

**X-Spamtest-Status-Extended: SPAM**

**X-Spamtest-Status-Extended: Not detected**

**X-Spamtest-Group-ID: 00000002**

**X-Spamtest-Group-ID: 00000001**

Cela signifie que le message a été traité selon les règles des groupes 1 et 2 (identifiant des groupes **sales** et **managers**) et qu'il s'est vu attribué les statuts **SPAM** et **Not Detected**. Pour obtenir de plus amples informations sur les champs d'en-tête cités, consultez le point A.5 à la page 123.

- Si le message est envoyé à plusieurs destinataires et que la délivrance du message est interdite pour certains d'entre eux (actions **reject message**) et autorisée pour d'autres (action **accept message**), alors

l'expéditeur ne recevra pas de notification sur l'impossibilité de délivrer le message à certains destinataires (bounce message) ;

- étant donné qu'il est impossible pour Sendmail de limiter le nombre de connexions simultanées sur le port 25, le nombre de processus de filtrage *ap-mailfilter* lancés dépend directement du nombre de connexions entrantes, ce qui peut entraîner une surcharge du serveur.

## **A.2.4. kas-pipe : module client pour les serveurs de messagerie Postfix et Exim**

Le module *kas-pipe* est un module client universel de Kaspersky Anti-Spam et il peut servir à l'intégration avec n'importe lequel des serveurs de messagerie compatibles.

Dans l'installation standard, *kas-pipe* sert à l'intégration à Postfix et Exim.

Le module *kas-pipe* reçoit le courrier et le renvoie au serveur de messagerie, via le protocole SMTP ou LMTP, après le filtrage.

Le lancement du module *kas-pipe* est réalisé par une application externe (par exemple, le serveur de messagerie). Le transfert ultérieur du courrier est réalisé via le socket de réseau ou local. Il est possible également de lancer l'application de réception à l'aide des commandes *fork* et *exec*.

L'interaction entre les modules en cas d'utilisation de Kaspersky Anti-Spam avec *kas-pipe* est illustrée dans le schéma 32.

Ce mode de fonctionnement peut être mis en oeuvre avec n'importe quel serveur de messagerie compatible soit avec le lancement d'une deuxième copie avec d'autres paramètres, soit avec la délivrance via le protocole LMTP, soit avec la délivrance de tout le courrier via le protocole SMTP au serveur de messagerie défini.

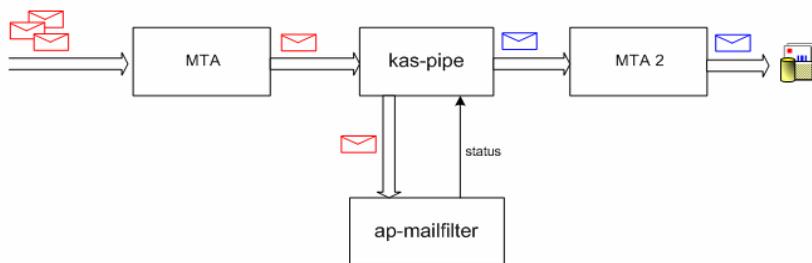


Illustration 32. Utilisation du module kas-pipe

La configuration des paramètres d'interaction du module client et du serveur de messagerie peut être réalisée à l'aide de scripts spéciaux (cf. point 3.5, p. 30) ou manuellement.

La configuration manuelle des paramètres de fonctionnement du module client nécessite la modification du fichier de configuration *filter.conf* situé dans le répertoire */usr/local/ap-mailfilter3/etc/*. Voici un extrait de ce fichier contenant les paramètres du module client :

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
PipeInProtocol lmtpl
PipeOutProtocol lmtpl
PipeOutgoingAddr exec:/usr/sbin/sendmail -bs
PipeMultipleMessagesAllowed yes
ClientDefaultDomain localhost
ClientOnError accept
ClientFilteringSizeLimit 500

```

En plus des paramètres définis ci-dessus au point A.2.2 de l'annexe, le fichier de configuration *filter.conf* pour le module kas-pipe contient également les paramètres suivant :

- **PipeInProtocol** : protocole utilisé pour la réception des messages. Valeurs possibles : **smtp** ou **lmtpl**.
- **PipeOutProtocol** : protocole utilisé pour le transfert des messages traités. Valeurs possibles : **smtp** ou **lmtpl**.
- **PipeHELOGreeting** : nom du domaine utilisé par le module *kas-pipe* dans la session SMTP pour les salutations. La valeur par défaut est égale à **kas30pipe.+ <nom de domaine du serveur>**.

- **PipeOutgoingAddr** : adresse du socket utilisé pour le transfert des messages traités. Le format **tcp:<host>:<port>** où **<host>** représente l'adresse IP du serveur et **<port>**, le port de connexion est réservé au socket de réseau, tandis que le format **unix:<chemin\_d'accès\_au\_fichier>** où **<chemin\_d'accès\_au\_fichier>** représente le chemin d'accès au fichier du socket est réservé au socket local et le format **exec:/<chemin d'accès au fichier exécutable du programme> -<paramètres>** indique le programme qui sera lancé pour le transfert des messages.
- **PipeOutConnectTimeout=5...600** : délai d'attente de la connexion au socket ou au programme utilisé pour le transfert des messages traités (le paramètre **PipeOutgoingAddress** défini).
- **PipeOutDataTimeout=5...600** : délai d'attente pour le transfert des données via le socket ou le programme déterminé par le paramètre **PipeOutgoingAddr**.
- **PipeMultipleMessagesAllowed** : mode de création d'une copie des messages lorsque les résultats du filtrage sont différents en fonction des utilisateurs. Valeurs possibles : **yes** ou **no**.
- **PipeUseXForward** : prise en charge de la commande XForward qui permet d'obtenir l'adresse IP du serveur d'où provient le message (uniquement en cas d'utilisation de Postfix). Valeurs possibles : **yes** ou **no**.
- **Pipe8BitHack** : utilisation de l'extension 8BITMIME. Valeurs possibles : **yes** ou **no**. Choisissez la valeur **yes** si votre serveur de messagerie est compatible avec l'extension 8BITMIME.
- **PipeBufferedIO** : utilisation de la mise en tampon lors du traitement des messages électroniques. La mise en tampon permet d'accélérer le traitement des messages en utilisant un volume de mémoire vive complémentaire. Valeurs possibles : **yes** ou **no**.

#### Particularités de l'utilisation du module client kas-pipe :

- Vu que kas-pipe transmet les messages via le protocole SMTP ou LMTP, il n'est pas possible (pour tous les serveurs de messagerie à l'exception de Postfix) de définir l'adresse IP du serveur d'où provient ce message. Toutes les vérifications DNS peuvent être réalisées uniquement sur la base des adresses IP reprises dans le champ Received des en-têtes. Si vous utilisez Postfix, attribuez la valeur **yes** au paramètre **PipeUseXForward** afin que kas-pipe puisse recevoir l'adresse IP du serveur d'où provient le message électronique.
- Vu que kas-pipe s'intègre au serveur de messagerie après la file de messages entrants, le module client ne peut exécuter l'action **reject** au

cours du processus de la session SMTP. Si l'action **reject this message** a été définie pour les messages, alors l'expéditeur recevra une notification sur l'impossibilité de délivrer le message au destinataire (bounce message) ;

### A.2.4.1. Configuration de Postfix pour fonctionner avec *kas-pipe*

Cette rubrique contient un exemple de configuration de *kas-pipe* et du serveur de messagerie Postfix en vue du mode de fonctionnement suivant :

- *kas-pipe* fonctionne comme filtre du contenu (*content\_filter*) ;
- *kas-pipe* reçoit le courrier via le socket de réseau *localhost:9026* et en utilisant le service *kas3scan* défini manuellement dans la configuration de Postfix.
- *kas-pipe* renvoie le courrier traité par Kaspersky Anti-Spam via le protocole SMTP sur le socket *localhost:9025*.



Le service *kas3scan* établit une restriction sur le nombre de connexion simultanées et utilise l'option *smtp\_send\_xforward\_command* pour transmettre au module *kas-pipe* l'adresse IP du serveur d'où provient le message électronique.



Pour mettre en oeuvre le mode de fonctionnement décrit, procédez comme suit :

1. Dans le fichier de configuration *filter.conf*, attribuez les valeurs suivantes aux paramètres :

```
ClientConnectTo tcp:127.0.0.1:2277
PipeMultipleMessagesAllowed Yes
PipeInProtocol smtp
PipeOutProtocol smtp
PipeOutgoingAddr tcp:127.0.0.1:9025
PipeUseXForward yes
```

2. Introduisez les modifications suivantes dans le fichier de configuration de Postfix (*master.cf*) :

```
smtp inet n - n - - smtpd
### KASPERSKY ANTI-SPAM BEGIN ###
-o content_filter=kas3scan:127.0.0.1:9026
```

```

### KASPERSKY ANTI-SPAM END ###

pickup fifo n - n 60 1 pickup
### KASPERSKY ANTI-SPAM BEGIN ###
-o content_filter=kas3scan:127.0.0.1:9026
### KASPERSKY ANTI-SPAM END ###

### KASPERSKY ANTI-SPAM BEGIN ###
127.0.0.1:9026 inet n n n - 20 spawn
user=mailflt3 argv=/usr/local/ap-mailfilter3/bin/
kas-pipe
127.0.0.1:9025 inet n - n - 25 smtpd
-o smtpd_authorized_xforward_hosts=127.0.0.0/8
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,
reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=no
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000

kas3scan unix - - n - 10 smtp
-o smtp_send_xforward_command=yes
### KASPERSKY ANTI-SPAM END ###

```



Pour Posfix version 2.1 et suivante, il est possible de configurer kas-pipe en tant que filtre proxy (*smtpd\_proxy\_filter*). Cela permet d'utiliser l'action **reject** dans le processus de la session SMTP, ce qui accélère le traitement des messages. Cette configuration est recommandée uniquement pour les serveurs de messagerie dont la configuration est faible. Pour configurer kas-pipe en tant que filtre proxy, remplacez les deux premières lignes de l'exemple ci-dessus par les lignes suivantes :

```

smtp inet n - n - - smtpd
-o smtpd_proxy_filter=127.0.0.1:9026

```

## A.2.4.2. Configuration d'Exim pour fonctionner avec *kas-pipe*

L'intégration de *kas-pipe* au serveur de messagerie Exim s'opère en ajoutant un nouveau routeur dans la configuration d'Exim au début de la liste des routeurs ainsi que son transport correspondant utilisé pour lancer *kas-pipe*. Ce routeur est conditionnel. Il ne fonctionne pas avec le courrier envoyé localement à l'aide du protocole ESMTP.

La vérification des messages électroniques avec le module client *kas-pipe* et Exim s'opère selon le schéma suivant :

1. Exim reçoit le courrier entrant sur le port 25 et le place dans la file d'attente.
2. Exim choisit un message dans la file et consulte la liste des routeurs afin d'identifier celui qui est convient au message sélectionné. Etant donné que le routeur indiqué pour *kas-pipe* est situé en première position dans la liste, tous les messages sont envoyés par le transport correspondant au module client *kas-pipe*.
3. Une fois que le message a été vérifié, *kas-pipe* le renvoie grâce à la commande `exim -bs`. Le message électronique retrouve une place dans la file d'attente Exim, mais cette fois, le routeur pour le module *kas-pipe* n'intervient pas car le courrier est envoyé localement.
4. Exim délivre le message au destinataire.



*Pour mettre en oeuvre le mode de fonctionnement décrit, procédez comme suit :*

- Dans le fichier de configuration *filter.conf*, attribuez les valeurs suivantes aux paramètres :

```
PipeInProtocol lmtpl
PipeOutProtocol smtp
PipeOutgoingAddr exec:/usr/local/sbin/exim -bs
```

- Introduisez les modifications suivantes dans le fichier de configuration d'Exim :

- Ajoutez les lignes suivantes dans la section **ROUTERS**:

```
begin routers
# ROUTER ADDED BY KAS 3.0 INSTALLER
```

```

kas30router:
    driver = accept
    local_parts = passwd; $local_part : lsearch
    condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
    transport = kas30transport

```

- Ajoutez les lignes suivantes dans la section **TRANSPORTS**:

```

begin transports
# TRANSPORT ADDED BY KAS 3.0 INSTALLER
kas30transport:
driver = lmtpl
batch_max = 100
command = /usr/local/ap-mailfilter3/bin/kas-pipe
return_path_add = false

```

S'agissant de la distribution Debian, l'intégration du logiciel à Exim possède plusieurs particularités liées au fait que la configuration du serveur de messagerie est réalisée par le script spécial *update-exim4.conf* du modèle */etc/exim4/exim4.conf.template* ou de plusieurs modèles situés dans le répertoire */etc/exim4/conf.d/*. L'utilisation d'un ou de plusieurs modèles est définie par le paramètre **use\_split\_files** du fichier de configuration d'Exim *exim4-update.conf.conf*. La configuration obtenue est conservée dans le fichier */var/lib/exim4/config.autogenerated*.

L'intégration de Kaspersky Anti-Spam au serveur de messagerie Exim pour la distribution Debian peut être réalisée automatiquement à l'aide d'un script spécial (cf. point 3.5, p. 30) ou manuellement.



*Pour configurer le fonctionnement d'Exim avec le module kas-pipe, procédez comme suit :*

- Si la configuration d'Exim s'opère sur la base du modèle *exim4.conf.template*, ajoutez les lignes indiquées ci-dessus aux sections **ROUTERS** et **TRANSPORTS**.
- Si la configuration s'opère sur la base d'un des modèles du répertoire */etc/exim4/conf.d/*, alors
  1. créez dans le répertoire */etc/exim4/conf.d/router/* le fichier *099\_exim4-config\_kas30router* et ajoutez-y les lignes suivantes :

```

kas30router:
    driver = accept

```

```

local_parts = passwd;$local_part : lsearch
condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
transport = kas30transport

```

2. créez dans le répertoire `/etc/exim4/conf.d/transport/` le fichier `30_exim4-config_kas30transport` et ajoutez-y les lignes suivantes :

```

kas30transport:
driver = lmtp
batch_max = 100
command = /usr/local/ap-mailfilter3/bin/kas-pipe
return_path_add = false

```

Après avoir introduit les modifications, exécutez le script `update-exim4.conf` afin que le système utilise les nouveaux paramètres.

## A.2.5. kas-exim : module client pour le serveur de messagerie Exim

Le module `kas-exim` est responsable de l'intégration de Kaspersky Anti-Spam au serveur de messagerie Exim version 4.xx avec utilisation de `localscan API`.

L'utilisation de `kas-exim` est une solution alternative. En cas d'installation standard, l'intégration à Exim est réalisée via le module client `kas-pipe`. A la différence du module `kas-pipe`, `kas-exim` ne requiert pas le lancement d'une deuxième copie du serveur de messagerie pour le transfert des messages.

L'application de `localscan API` requiert une recompilation d'Exim, ce qui explique pourquoi le module `kas-exim` est fourni sous la forme du code source en langage C et qu'il est installé manuellement.



*Pour compiler le serveur de messagerie Exim avec connexion du module `kas-exim`, procédez comme suit :*

- Déplacez le fichier `kas_exim.c` du répertoire `/usr/local/ap-mailfilter3/src/` vers le répertoire `Local` de l'arborescence des fichiers source d'Exim.
- Introduisez les modifications suivantes dans le fichier `Makefile` du répertoire `Local` :

```

CFLAGS= -I/usr/local/ap-mailfilter3/include
EXTRALIBS_EXIM=-L/usr/local/ap-mailfilter3/lib
-lspamtest

```

```
LOCAL_SCAN_SOURCE=Local/kas_exim.c
LOCAL_SCAN_HAS_OPTIONS=yes
```

- Compilez Exim.



Tous les paramètres de fonctionnement du module kas-exim sont définis dans le fichier de configuration d'Exim et non pas dans *filter.conf*.

Voici un extrait du fichier de configuration d'Exim avec les paramètres du module kas-exim :

```
begin local_scan
kas_connect_to = tcp:127.0.0.1:2277
kas_connect_timeout = 40
kas_data_timeout = 30
kas_default_domain = localhost
kas_filtering_size_limit = 500
kas_on_error=accept
kas_log_level=3
```

Cet extrait contient les paramètres suivants :

- **kas\_connect\_to** : adresse du socket d'interaction avec le serveur de filtrage. Le format **tcp:<host>:<port>** où **<host>** représente l'adresse IP du serveur et **<port>**, le port de connexion est réservé au socket de réseau, tandis que le format **unix:<chemin\_d'accès\_au\_fichier>** où **<chemin\_d'accès\_au\_fichier>** représente le chemin d'accès au fichier du socket est réservé au socket local.
- **kas\_connect\_timeout** : délai d'attente maximum (en secondes) lors de l'établissement de la connexion avec le serveur de filtrage.
- **kas\_data\_timeout** : délai d'attente maximum (en secondes) lors de l'échange de données avec le serveur de filtrage.
- **kas\_default\_domain** : nom du domaine de messagerie dans l'adresse où le domaine de messagerie n'est pas indiqué.
- **kas\_filtering\_size\_limit** : taille maximale (en Ko) des messages qui peuvent être transmis au serveur de filtrage. Les messages dont la taille est supérieure ne sont pas traités par le serveur de filtrage.
- **kas\_on\_error** : mode de traitement des erreurs (impossible d'établir la connexion avec le processus de filtrage, délai d'attente dépassé lors de l'échange de données, etc.). Valeurs possibles :

- **reject** : refus des messages, renvoi du code 5xx dans le processus de la session SMTP ;
- **tempfail** : refus temporaire des messages, renvoi du code 4xx dans le processus de la session SMTP (utilisé par défaut) ;
- **accept** : réception du message ;
- **kas\_log\_level** : niveau de détail des entrées dans le fichier journal. L'enregistrement est réalisé en mode de débogage d'Exim.

Particularités de l'utilisation du module client kas-exim avec le serveur de messagerie Exim :

- kas-exim, à l'instar de kas-milter, ne crée pas de copie des messages lors du traitement. Si le message est envoyé à plusieurs destinataires issus de différents groupes dont les règles de traitement varient, alors les actions définies pour chacun des groupes seront exécutées.
- Si le message est envoyé à plusieurs destinataires et que la délivrance du message est interdite pour certains d'entre eux (actions **reject message**) et autorisée pour d'autres (action **accept message**), alors l'expéditeur ne recevra pas de notification sur l'impossibilité de délivrer le message à certains destinataires (bounce message).

## A.2.6. kas-qmail : module client pour le serveur de messagerie Qmail

Le module kas-qmail est chargé de l'intégration de Kaspersky Anti-Spam au serveur de messagerie Qmail. L'utilisation de ce module entraîne le traitement du courrier selon l'algorithme suivant :

1. Le module *qmail-queue* du serveur de messagerie Qmail remplace le module client kas-qmail chargé du transfert du courrier entrant au serveur de filtrage en vue du traitement.
2. Le courrier traité est renvoyé par le module kas-qmail et est transféré au module *qmail-queue*.

L'interaction entre les modules en cas d'utilisation de Kaspersky Anti-Spam avec *kas-qmail* est illustrée dans le schéma 33.

La configuration des paramètres d'interaction du module client et du serveur de messagerie peut être réalisée à l'aide de scripts spéciaux (cf. point 3.5, p. 30) ou manuellement.

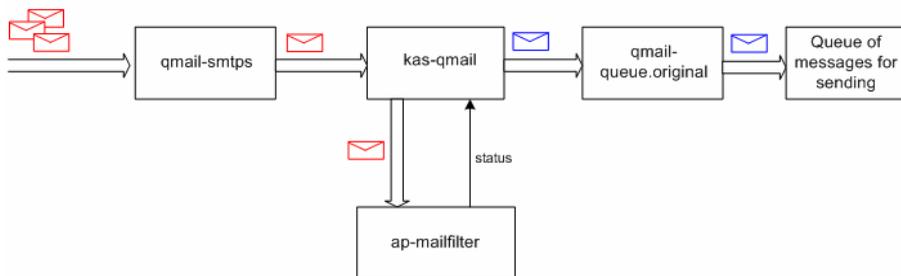


Illustration 33. Interaction entre Kaspersky Anti-Spam et le serveur de messagerie Qmail

La configuration manuelle des paramètres de fonctionnement du module client nécessite la modification du fichier de configuration *filter.conf* situé dans le répertoire */usr/local/ap-mailfilter3/etc/*.

Voici un extrait du fichier de configuration *filter.conf*, avec les paramètres du module *kas-qmail* :

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
QMailOriginalQueue /var/qmail/bin/qmail-queue.kas
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
  
```

En plus des paramètres décrit au point A.2.2 de l'annexe, ce fichier contient également le paramètre **QMailOriginalQueue** qui détermine le chemin d'accès complet au module original *qmail-queue*.



*Pour configurer le fonctionnement de Qmail avec le module client *kas-qmail*, procédez comme suit :*

1. Renommez le fichier du module original *qmail-queue* à l'aide de la commande suivante :

```
# mv /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.kas
```

2. Installez le module *kas-qmail* avec *qmail-queue* en exécutant les commandes suivantes :

```
# cp /usr/local/ap-mailfilter3/bin/kas-qmail
/var/qmail/bin/qmail-queue
# chown qmailq /var/qmail/bin/qmail-queue
```

```
# chgrp qmail /var/qmail/bin/qmail-queue
# chmod 04755 /var/qmail/bin/qmail-queue
```

## A.2.7. kas-cgpro : module client pour le serveur de messagerie **Communigate Pro**

Le module `kas-cgpro` est chargé de l'intégration de Kaspersky Anti-Spam au serveur de messagerie `Communigate Pro`. Le traitement du courrier est réalisé selon cet algorithme :

1. `Communigate Pro` transmet tout le courrier reçu au module client `kas-cgpro`.
2. *Le module `kas-cgpro` traite les messages, les modifie (ajoute un titre particulier à chaque message) et les range dans le répertoire `Submitted`. `Communigate Pro` renvoie `DISCARD`.*
3. Le pilote `PIPE` transmet à nouveau les messages du répertoire `Submitted` au serveur de messagerie `Communigate Pro` qui transmet à son tour à nouveau le message au module `kas-cgpro`.
4. Etant donné que le module `kas-cgpro` *ne traite pas à nouveau les messages qui ont été filtrés (titre spécial ajouté au message)*, `Communigate Pro` renvoie le statut `OK` et le message est délivré au destinataire.

L'intégration à `Communigate Pro` peut être réalisée uniquement manuellement. Les paramètres d'interaction du module client sont définis en modifiant le fichier de configuration `filter.conf` et ceux de `Communigate Pro`, via l'interface Internet du serveur de messagerie.

Voici un extrait du fichier `filter.conf` contenant les paramètres du module client :

```
ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
CGProSubmittedFolder Submitted
CGProMaxThreadCount 50
CGProLoopHeader X-Proceed_240578_by_spamtest
CGProAllTransports No
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

En plus des paramètres décrits au point A.2.2 de l'annexe, les paramètres complémentaires suivants interviennent également dans la configuration de kas-cgpro :

- **CGProSubmittedFolder** : nom du répertoire où sont placés les messages traités.
- **CGProMaxThreadCount** : nombre maximum de messages traités simultanément.
- **CGProLoopHeader** : en-tête ajouté aux messages traités.
- **CGProAllTransports** : autorisation/interdiction du traitement du courrier qui arrive avec tous les transports. Valeurs possibles : **yes**, tout le courrier est traité ; **no**, seul le courrier du transport SMTP est traité (valeur par défaut).



*Pour configurer le fonctionnement de Communicate Pro avec le module client kas-cgpro, exécutez les opérations suivantes au départ de l'interface Internet du serveur de messagerie :*

1. **Dans le menu Settings→General→Helpers, ajoutez un nouveau content-filter doté des paramètres suivants :**

```
Use Filter: kas-cgpro
Log: Problems
Path: /usr/local/ap-mailfilter3/bin/kas-cgpro
Time-Out: 5 minutes
Auto-Restart: 15 seconds
```

2. **Dans le menu Settings→Rules,(Settings→Queue→Rules pour les versions Communicate Pro suivant la version 5.0), créez une nouvelle règle pour la recherche de spam dans tous les messages dont la taille ne dépasse pas 500 Ko :**

```
Data: Message Size
Operation: less than
Parameter: 500000
Action: external filter
Parameters: kas-cgpro
```

Particularités de l'utilisation du module client kas-cgpro avec Communicate Pro :

- Le module client kas-cgpro n'est pas capable dans le processus de la session SMTP de refuser la réception des messages pour lesquels la règle **reject this message** a été définie. Au lieu de cela, Communicate Pro envoie à l'expéditeur une notification sur l'impossibilité de délivrer le message (bounce message).

- Le contenu du message bounce message est défini au niveau du serveur de messagerie et non pas par le paramètre **Bounce message** défini à l'aide de l'interface du Centre d'administration (cf. point 4.5.4, p. 66).
- L'envoi des messages du système de surveillance et des messages relatifs aux erreurs survenues lors de l'exécution des scripts est réalisé par le serveur de filtrage au nom de l'utilisateur **mailfit3**. Etant donné que Communicate Pro n'ajoute pas à sa propre base les comptes des utilisateurs système, créez manuellement dans la base des utilisateurs de Communicate Pro le compte pour **mailfit3**.
- Lors de l'utilisation de l'option **Drop Root** dans Communicate Pro, le serveur de messagerie passe à l'utilisation des privilèges de l'utilisateur **nobody**. Cette permutation n'a pas lieu pour le module kas-cgpro, ce qui entraîne la perte de l'interaction entre le serveur de messagerie et le module client. Pour rétablir l'interaction, procédez comme suit :
  1. Dans le menu de Communicate Pro **Settings**→**General**→**Helpers**, désactivez l'utilisation du filtre kas-cgpro en désélectionnant la case **Use Filter**. Pour actualiser la configuration, cliquez sur **Update**.
  2. Ajoutez à nouveau le filtre kas-cgpro. Les paramètres du filtre sont indiqués ci-dessus dans la description des paramètres de Communicate Pro pour le fonctionnement avec le module client kas-cgpro.

## A.3. Fichiers de configuration de Kaspersky Anti-Spam

Cette rubrique offre une description des fichiers de configuration de Kaspersky Anti-Spam avec les paramètres des principaux composants du serveur de filtrage.

### A.3.1. Fichier de configuration principal *filter.conf*

Le fichier de configuration `/usr/local/ap-mailfilter3/etc/filter.conf` contient les paramètres de fonctionnement de tous les composants de Kaspersky Anti-Spam, à l'exception du module de chargement des mises à jour

## Paramètres généraux :

**RootPath** : chemin d'accès au répertoire d'installation de Kaspersky Anti-Spam. La valeur par défaut est égale à **/usr/local/ap-mailfilter3**.

**LogFacility=mail|user|local0|local1|local2|local3|local4|local5|local6|local7** : catégorie sous laquelle les messages sont enregistrés dans le journal système (syslog facility). La valeur par défaut est égale à **mail**.

**LogLevel=0|1|2|3|4|5** : niveau de détail des entrées dans le journal système (syslog). La valeur par défaut est égale à **2**.

**User** : utilisateur avec les privilèges duquel les processus du serveur de filtrage sont lancés. La valeur peut être le nom symbolique de l'utilisateur ou son *uid*.

**Group** : groupe avec les privilèges duquel les processus du serveur de filtrage sont lancés. La valeur peut être le nom symbolique du groupe ou son *gid*.

## Paramètres du serveur de filtrage

**ServerListen** : socket d'interaction du serveur de filtrage avec le module intégré au serveur de messagerie. Le format **tcp:<host>:<port>** où **<host>** représente l'adresse IP (ou le nom) du serveur de messagerie et **<port>**, le port de connexion est réservé au socket de réseau, tandis que le format **unix:<chemin\_d'accès\_au\_fichier>** où **<chemin\_d'accès\_au\_fichier>** représente le chemin d'accès au fichier du socket est réservé au socket local. Pour configurer le serveur de filtrage pour une connexion avec n'importe quelle interface, attribuez la valeur **0.0.0.0** au paramètre **<host>**.



Le socket local, créé pour l'interaction du serveur de messagerie et du serveur de filtrage, permet à des fins de compatibilité de créer une opération d'enregistrement dans le socket pour n'importe quel utilisateur authentifié dans le système.

**FilterPath** : chemin d'accès au fichier exécutable du processus de filtrage *ap-mailfilter*.

**ServerMaxFilters=1...200** : nombre maximum de processus de filtrage *ap-mailfilter* fonctionnant simultanément. La valeur par défaut est égale à **10**.

**ServerStartFilters** : nombre de processus de filtrage *ap-mailfilter* lancés au démarrage du module de filtrage. La valeur par défaut est égale à **0**. La

valeur du paramètre **ServerStartFilters** ne peut pas dépasser la valeur du paramètre **ServerMaxFilters**.

**ServerSpareFilters** : nombre minimum de processus de filtrage lancés en état d'attente (qui ne traitent pas les messages). Si le nombre de processus dépasse la limite définie, le système procède à l'arrêt forcé des processus inutilisés. La valeur par défaut est égale à **0**. La valeur du paramètre **ServerSpareFilters** ne peut pas dépasser la valeur du paramètre **ServerMaxFilters**.

## Paramètres des processus de filtrage

**FilterMaxMessages=10...1000** : nombre maximum de messages qui peuvent être traités par le processus de filtrage. Une fois que le nombre de messages indiqué a été traité, le processus de filtrage s'arrête. La valeur par défaut est égale à **300**.



Le nombre maximum de messages qui peuvent être traités par un processus de filtrage défini est un nombre aléatoire choisi par le logiciel dans une plage définie par **[FilterMaxMessages; FilterMaxMessages + (FilterRandMessages-1)]**. Ce paramètre permet d'éviter l'arrêt et la reprise simultanée d'un grand nombre de nouveaux processus de filtrage lorsque le serveur est fortement sollicité.

**FilterRandMessages=0...50** : valeur utilisée lors de la définition du nombre maximum de messages pouvant être traités par un processus de filtrage particulier.

**FilterMaxIdle=30...3600** : durée maximum (en secondes) de la période au cours de laquelle le processus de filtrage peut être en état d'attente. Si le processus de filtrage ne reçoit aucun message au cours de cette période, il s'arrête. La valeur par défaut est égale à **300**.

**FilterDelayedExit=0...30** : durée maximale (en secondes) du décalage de l'arrêt du processus lorsque celui-ci reçoit la commande d'arrêt. Si la valeur de ce paramètre n'est pas égale à 0, alors le processus de filtrage s'arrête après la réception du signal à la fin de la période qui est une durée aléatoire choisie dans la plage **[0; (FilterDelayedExit-1)]**. La valeur par défaut est égale à **0**.

**FilterDataTimeout=10...100** : délai d'attente (en secondes) pour la réception par le processus de filtrage des données en provenance du module client. Si le processus de filtrage ne reçoit aucune donnée au cours de cette période, le traitement des messages est suspendu. La valeur par défaut est égale à **30**.

**FilterLicenseConnectTimeout=1..10** : délai d'attente (en secondes) pour la connexion du processus de filtrage au module de licence (*kas-license*) pour vérifier si la requête respecte les conditions imposées par la licence. La valeur par défaut est égale à **2**.

**FilterLicenseDataTimeout=1..10** : délai d'attente (en secondes) pour les opérations d'écriture/de lecture pour le socket d'interaction du processus de filtrage avec le module de licence. La valeur par défaut est égale à **1**.

**FilterSPFDataTimeout=1..10** : délai d'attente (en secondes) pour les opérations d'écriture/de lecture pour le socket d'interaction du processus de filtrage avec le démon SPF. La valeur par défaut est égale à **1**.

**FilterDNSTimeout=1...60** : délai d'attente (en secondes) pour l'exécution de toutes les vérifications possibles à l'aide du DNS. La valeur par défaut est égale à **10**.

**FilterLicenseConnectTo** : chemin d'accès au fichier du socket d'interaction avec le module de licence. La valeur par défaut est égale à **/usr/local/ap-mailfilter3/run/kas-license.socket**.

**FilterSPFConnectTo** : chemin d'accès au fichier du socket d'interaction avec le démon SPF. La valeur par défaut est égale à **/usr/local/ap-mailfilter3/run/ap-spf.socket**.

**FilterReceivedHeadersLimit=0...100** : nombre de champs d'en-tête Received analysés selon les listes d'adresses IP et à l'aide des services DNSBL. La valeur par défaut est égale à **2**.

**FilterParseMSOffice=yes|no** : paramètre définissant la vérification ou nom du texte des pièces jointes au format Word Document (doc) et RTF. La valeur par défaut est égale à **no**.

**FilterStatLogFile** : chemin d'accès au fichier utilisé par l'application pour conserver les statistiques relatives aux messages traités.

**FilterUserLogFile** : chemin d'accès au fichier contenant les données statistiques lors de la saisie des statistiques selon les paramètres de l'utilisateur.

**FilterUDSCfgFile** : chemin d'accès au fichier contenant la configuration du service UDS.

**FilterUDSEnabled=yes|no** : paramètre d'activation/de désactivation de la vérification du courrier à l'aide du service UDS.

**FilterUDSTimeout=1...60** : délai d'attente pour l'établissement de la connexion entre le serveur de filtrage et le serveur UDS. Si le serveur de filtrage ne reçoit aucune réponse du

serveur UDS au cours de l'intervalle défini, il tente de se connecter à un autre serveur UDS de Kaspersky Lab.

### Paramètres du module de licence

**LicenseListen** : chemin d'accès au socket utilisé par le module de licence pour l'interaction avec les processus de filtrage. La valeur par défaut est égale à **/usr/local/ap-mailfilter3/run/kas-license.socket**.

**LicenseKeysPath** : chemin d'accès au répertoire contenant les clés de licence. La valeur par défaut est égale à **/usr/local/ap-mailfilter3/conf/lk-license/**.

**LicenseMaxConnections=10...300** : nombre maximum autorisé de connexions simultanées au module de licence. La valeur par défaut est égale à **200**.

**LicenseIdleTimeout=1...100** : durée maximum (en secondes) de la période au cours de laquelle le module de licence maintient la connexion avec le processus de filtrage sans transmettre aucune donnée. Une fois cette période écoulée, la connexion est coupée si le processus de filtrage n'a reçu aucune requête. La valeur par défaut est égale à **30**.

**LicenseDataTimeout=1..100** : délai d'attente (en secondes) pour les opérations d'écriture/de lecture pour le socket d'interaction avec les processus de filtrage. La valeur par défaut est égale à **1**.

### Paramètres du démon SPF

**SPFDListen** : chemin d'accès au socket utilisé par le démon SPF pour l'interaction avec les processus de filtrage. La valeur par défaut est égale à **/usr/local/ap-mailfilter3/run/ap-spf.socket**.

**SPFDPoolSize=1...50** : nombre de processus fils du démon SPF lancés simultanément. La valeur par défaut est égale à **5**.

**SPFDMaxRequestsPerChild=50...10000** : nombre maximum de requêtes traitées par le processus fil du démon SPF. Après que le processus fils a traité le nombre défini de requêtes, il s'arrête et le démon SPF lance un nouveau processus. La valeur par défaut est égale à **1000**.

**SPFDMaxQueueSize=10...1000** : nombre maximum de requêtes qui peuvent être placées simultanément dans la file d'attente de traitement. La valeur par défaut est égale à **200**.

**SPFDCleanupInterval=30...3600** : intervalle (en secondes) de purge du cache du démon SPF. La valeur par défaut est égale à **600**.

## Paramètres généraux des modules clients

**ClientConnectTo** : adresse du socket d'interaction du module client avec le module de filtrage. Le format **tcp:<host>:<port>** où **<host>** représente l'adresse IP du serveur et **<port>**, le port de connexion est réservé au socket de réseau, tandis que le format **unix:<chemin\_d'accès\_au\_fichier>** où **<chemin\_d'accès\_au\_fichier>** représente le chemin d'accès au fichier du socket est réservé au socket local.

**ClientConnectTimeout=10...100** : délai d'attente (en secondes) pour l'établissement de la connexion entre le module client et le processus de filtrage. La valeur par défaut est égale à **40**.

**ClientDataTimeout=10...100** : délai d'attente (en secondes) pour l'échange de données entre le module client et le module de filtrage.

**ClientOnError** : mode de traitement des erreurs (impossible d'établir la connexion avec le module de filtrage, délai d'attente dépassé lors de l'échange de données, etc.). Valeurs possibles :

- **reject** : refus des messages, renvoi du code 5xx dans le processus de la session SMTP ;
- **tempfail** : refus temporaire des messages, renvoi du code 4xx dans le processus de la session SMTP (utilisé par défaut) ;
- **accept** : acceptation du message.

**ClientDefault domain** : nom du domaine de messagerie dans l'adresse où le domaine de messagerie n'est pas indiqué. Exemple : lorsque le domaine par défaut est le domaine monentreprise.com, alors l'adresse unutilisateur sera interprétée comme unutilisateur@monentreprise.com. Si ce paramètre n'est pas défini, la suggestion du nom de domaine n'a pas lieu. Ce paramètre n'est pas défini par défaut.

**ClientFilteringSizeLimit=0...10000** : taille maximale (en Ko) des messages qui peuvent être transmis au module de filtrage. Les messages dont la taille est supérieure ne sont pas filtrés. La valeur par défaut est égale à **500**.

**ClientMessageStoreMem** : taille minimale (en Ko) des messages pour la sauvegarde des données intermédiaires sur le disque. Ce mode permet de contrôler le volume de mémoire vive utilisé. Si le paramètre est égal à **0** (valeur par défaut), alors toutes les données seront toujours sauvegardées dans la mémoire vive.

**ClientTempDir** : répertoire de conservation des fichiers temporaires.

## Configuration du Centre d'administration

**ControlCenterSendAlertsTo** : adresse pour l'envoi des messages du système de surveillance et des messages relatifs aux erreurs d'exécution des scripts à l'aide du service cron ;

**ControlCenterLang=en** : langue de l'interface du Centre d'administration.

**MonitoringHttpd=yes|no** : paramètre définissant la surveillance ou non du serveur HTTP *kas-thttpd*.

**MonitoringKasMilter=yes|no** : paramètre définissant la surveillance ou nom du module client *kas-milter* utilisé pour l'interaction avec le serveur de messagerie Sendmail.



La description des paramètres caractéristiques de chacun des modules clients est proposée au point A.2 à la page 91.

## A.3.2. Fichier de configuration

### ***kas.thttpd.conf***

Le fichier de configuration *kas-thttpd.conf*, placé dans le répertoire */usr/local/ap-mailfilter3/etc/*, renferme les paramètres du serveur HTTP pour l'interface Internet du Centre d'administration, le principal outil de configuration de Kaspersky Anti-Spam.

Ce fichier contient les paramètres suivants :

**user** : nom de l'utilisateur sous les privilèges duquel les scripts du Centre d'administration sont exécutés. Il est déconseillé de modifier la valeur **mailft3** proposée car cela pourrait entraîner des erreurs de fonctionnement du système.

**host** : adresse IP de l'interface où le serveur Web attend les requêtes de connexion au Centre d'administration. La valeur **0.0.0.0** indique que le serveur attendra les requêtes sur toutes les interfaces réseau du serveur.

**port** : numéro du port de connexion au Centre d'administration.

**pidfile** : nom du fichier pid du serveur HTTP. La valeur par défaut est : */usr/local/ap-mailfilter3/run/kas-thttpd.pid*

**logfile** : nom du fichier journal du serveur HTTP. La valeur par défaut est : */usr/local/ap-mailfilter3/log/kas-thttpd.log*

**dir** : chemin d'accès au répertoire contenant les scripts cgi du Centre d'administration. La valeur par défaut est égale à `/usr/local/ap-mailfilter3/control/www`.

**cgipat** : modèle de noms de scripts cgi. La valeur doit être égale à `**cgi`.

## A.4. Utilitaires de Kaspersky Anti-Spam

Voici une description des principaux utilitaires de Kaspersky Anti-Spam, de leurs fonctions et des arguments de la ligne de commande utilisés pour chacun des composants. Le lancement d'un utilitaire requiert les privilèges de l'utilisateur `root`.

### A.4.1. kas-htpasswd

L'utilitaire `kas-htpasswd` intervient dans l'administration des fichiers de mots de passe d'accès au Centre d'administration.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd [-c]
<fichier_de_mots_de_passe> <nom_d'utilisateur> [-h]
```

Arguments de la ligne de commande :

- **fichier\_de\_mots\_de\_passe** : chemin d'accès au fichier contenant les mots de passe d'accès. Le fichier `.htpasswd` est utilisé par défaut. L'utilitaire peut soit ajouter un nouvel utilisateur au fichier des mots de passe ou modifier le mot de passe d'un utilisateur existant ;
- **nom\_d'utilisateur** : nom de l'utilisateur pour lequel le mot de passe est défini ;
- **-c** : crée un nouveau fichier de mots de passe ; si cet argument n'est pas utilisé, alors le paramètre **fichier\_de\_mots\_de\_passe** doit faire référence à un fichier existant ;
- **-h** : affiche l'aide relative à l'utilitaire sur la console.

### A.4.2. kas-show-license

L'utilitaire `kas-show-license` permet de consulter depuis la ligne de commande les informations relatives aux fichiers de licence installés.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/kas-show-license
[-k <fichier_de_clé>] [-c <fichier_de_configuration>]
```

Arguments de la ligne de commande :

- k **<fichier\_de\_clé>** : affiche les informations relatives à la clé de licence **fichier\_de\_clé**;
- c **<fichier\_de\_configuration>** : redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf*.



Si l'utilitaire est lancé sans indication de paramètres via la ligne de commande, la console du serveur affichera les données relatives à toutes les clés de licence installées.

### A.4.3. *install-key*

L'utilitaire *install-key* intervient dans l'installation des clés de licence de Kaspersky Anti-Spam.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/install-key -i [-q] [-d]
[-v] [-l] [-V <niveau_de_détail>]
[-L <niveau_de_détail>] [-c
<fichier_de_configuration>]
[-k <script_kas-conf>] [-h]
```

Arguments de la ligne de commande :

- i : n'affiche pas les informations relatives à la licence sur la console après l'installation de la clé ;
- q : affiche sur la console uniquement les messages relatifs aux erreurs ;
- d : affiche sur la console un rapport détaillé sur la procédure d'installation de la clé de licence ;
- v : utilise un niveau de détail plus élevé pour l'affichage des messages sur la console que celui défini par défaut ;
- V **<niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages affichés sur la console. Les valeurs admises sont : **1...10**;
- l : utilise un niveau de détail plus élevé pour les messages enregistrés dans le fichier journal que celui défini par défaut ;
- L **<niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages enregistrés dans le fichier journal. Les valeurs admises sont : **1...10**;

- c **<fichier\_de\_configuration>** : redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf* ;
- k **<script\_kas-conf>** : redéfinit le chemin d'accès au script *kas-conf* chargé de la lecture de la configuration de Kaspersky Anti-Spam ; si *kas-conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **script\_kas-conf** le chemin d'accès complet au fichier *kas-conf* ;
- h : affiche l'aide relative à l'utilitaire sur la console.

### A.4.4. *remove-key*

L'utilitaire *remove-key* intervient dans la suppression des clés de licence de Kaspersky Anti-Spam.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/remove-key [-a|-r] [-q]
[-d] [-v] [-l] [-V <niveau_de_détail>]
[-L <niveau_de_détail>] [-c
<fichier_de_configuration>]
[-k <script_kas-conf>] [-h]
```

Arguments de la ligne de commande :

- a : supprime toutes les clés de licence installées ;
- r : supprime la clé de licence de réserve ;
- q : affiche sur la console uniquement les messages relatifs aux erreurs ;
- d : affiche sur la console un rapport détaillé sur la procédure de suppression de la clé de licence ;
- v : utilise un niveau de détail plus élevé pour l'affichage des messages sur la console que celui défini par défaut ;
- V **<niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages affichés sur la console. Les valeurs admises sont : **1...10** ;
- l : utilise un niveau de détail plus élevé pour les messages enregistrés dans le fichier journal que celui défini par défaut ;
- L **<niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages enregistrés dans le fichier journal. Les valeurs admises sont : **1...10** ;
- c **<fichier\_de\_configuration>** : redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au

paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf* ;

**-k <script\_kas-conf>** : redéfinit le chemin d'accès au script *kas-conf* chargé de la lecture de la configuration de Kaspersky Anti-Spam ; si *kas-conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **script\_kas-conf** le chemin d'accès complet au fichier *kas-conf* ;

**-h** : affiche l'aide relative à l'utilitaire sur la console.

## A.4.5. kas-restart

L'utilitaire *kas-restart* intervient dans le redémarrage de Kaspersky Anti-Spam et de ses divers composants.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/kas-restart [-f] [-p]
[-s] [-m] [-w] [-W] [-q] [-d] [-v] [-l]
[-V <niveau_de_détail>] [-L <niveau_de_détail>]
[-c <fichier_de_configuration>] [-k <script_kas-conf>]
[-h]
```

Arguments de la ligne de commande :

- **-f** : redémarre les processus de filtrage *ap-mailfilter*. Les processus traitent les messages et s'arrêtent conformément aux paramètres de décalage temporisé et du nombre de message (pour de plus amples informations, consultez le point 4.5.3 à la page 65) ;
- **-p** : redémarrage du processus maître de filtrage *ap-process-server*. Il entraîne également le redémarrage des processus de filtrage *ap-mailfilter*. Lorsque cet argument est utilisé, les processus de filtrage redémarrent directement après le traitement du message en cours. Cet argument est utile en cas de modification des paramètres liés au mode de lancement des processus de filtrage ;
- **-s** : relance le module de licence *kas-license* ;
- **-m** : relance le module *kas-milter* ;
- **-w** : relance le serveur *kas-thttpd* ;
- **-W** : assure la rotation des fichiers journaux du serveur Internet *kas-thttpd* (création d'un nouveau fichier journal pour l'écriture).
- **-q** : utilisation du mode "silencieux" ; seuls les messages relatifs aux erreurs et les avertissements sont affichés sur la console ;
- **-d** : affiche sur la console un rapport détaillé sur le fonctionnement de l'utilitaire ;

- **-v** : utilise un niveau de détail plus élevé pour l'affichage des messages sur la console que celui défini par défaut ;
- **-V <niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages affichés sur la console. Les valeurs admises sont : **1...10**;
- **-l** : utilise un niveau de détail plus élevé pour les messages enregistrés dans le fichier journal que celui défini par défaut ;
- **-L <niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages enregistrés dans le fichier journal. Les valeurs admises sont : **1...10**;
- redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf*.
- **-k <script\_kas-conf>** : redéfinit le chemin d'accès au script *kas-conf* chargé de la lecture de la configuration de Kaspersky Anti-Spam ; si *kas-conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **script\_kas-conf** le chemin d'accès complet au fichier *kas-conf*,
- **-h** : affiche l'aide relative à l'utilitaire sur la console.



Le lancement d'un utilitaire sans argument dans la ligne de commande revient à le lancer avec l'argument **-f**.

## A.4.6. mkprofiles

L'utilitaire *mkprofiles* intervient dans la collecte et la compilation des stratégies de filtrage de Kaspersky Anti-Spam.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/mkprofiles
[-c <fichier_de_configuration>] [-l
<fichier_de_rapport>] [-q] [-v] [-h]
```

où

- **-c <fichier\_de\_configuration>** : redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf* ;
- **-l <fichier\_de\_rapport>** : conserve les résultats du fonctionnement de l'utilitaire dans le rapport défini par le paramètre **fichier\_de\_rapport**;

- **-q** : utilisation du mode "silencieux" ; seuls les messages relatifs aux erreurs et les avertissements sont affichés sur la console ;
- **-v** : affiche sur la console tous les messages liés au processus de compilation ;
- **-h** : affiche l'aide relative à l'utilitaire sur la console.

Lorsque l'utilitaire est lancé sans argument, la console affiche les messages d'erreur et les avertissements ainsi que les messages relatifs à la réussite d'une opération.

## A.4.7. sfmonitoring

L'utilitaire sfmonitoring est chargé de la vérification de l'état actuel des composants de Kaspersky Anti-Spam et d'afficher les messages de circonstance sur la console en cas de problèmes.

Ligne pour le lancement :

```
su -m mailflt3 -c '/usr/local/ap-  
mailfilter3/control/bin/  
sfmonitoring [-p] [-m] [-q] [-h]'
```

Si Kaspersky Anti-Spam est installé sur un serveur tournant sous la distribution RedHat, le lancement de l'utilitaire sfmonitoring s'opère à l'aide de la commande suivante :

```
su - -m mailflt3 -c '/usr/local/ap-  
mailfilter3/control/bin/  
sfmonitoring [-p] [-m] [-q] [-h]'
```

Arguments de la ligne de commande :

- **-p** : vérifie l'état du système et publie sur la console les messages sur tous les incidents survenus dans le fonctionnement de Kaspersky Anti-Spam ;
- **-m** : vérifie l'état du système et envoie par courrier électronique un rapport journalier sur les incidents survenus ;
- **-q** : utilisation du mode "silencieux" ; seuls les messages relatifs aux erreurs et les avertissements sont affichés sur la console ;
- **-h** : affiche l'aide relative à l'utilitaire sur la console.

Lorsque l'utilitaire est lancé sans argument, il vérifie l'état actuel du système et en cas de problème, il envoie un message d'avertissement.

## A.4.8. sfupdates

L'utilitaire sfupdates intervient dans le téléchargement des mises à jour des bases de filtrage du contenu et leur installation en vue de l'utilisation par le serveur de filtrage.

Ligne pour le lancement :

```
# /usr/local/ap-mailfilter3/bin/sfupdates
[-c <fichier_de_configuration>] [-f] [-k <script_kas-
conf>] [-s] [-q] [-v] [-d] [-V <niveau_de_détail>] [-
l]
[-L <niveau_de_détail>] [-h]
```

Arguments de la ligne de commande :

- **-c <fichier\_de\_configuration>** : redéfinit le chemin d'accès au fichier de configuration *filter.conf*. Si le fichier *filter.conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **fichier\_de\_configuration** le chemin d'accès complet au fichier *filter.conf* ;
- **-f** : exécute le lancement forcé de la collecte de configuration. Si l'argument n'est pas utilisé, alors la compilation de la configuration aura lieu uniquement après la réception des mises à jour des bases de filtrage du contenu ;
- **-k <script\_kas-conf>** : redéfinit le chemin d'accès au script *kas-conf* chargé de la lecture de la configuration de Kaspersky Anti-Spam ; si *kas-conf* se trouve dans un répertoire différent du répertoire utilisé par défaut, attribuez au paramètre **script\_kas-conf** le chemin d'accès complet au fichier *kas-conf* ;
- **-s** : passe l'étape du chargement des mises à jour ;
- **-q** : affiche sur la console uniquement les messages relatifs aux erreurs ; Ce mode est recommandé pour le lancement à l'aide du service *cron* ;
- **-v** : utilise un niveau de détail plus élevé pour l'affichage des messages sur la console que celui défini par défaut ;
- **-d** : utilise le niveau de détail le plus élevé pour les messages affichés sur la console ;
- **-V <niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages affichés sur la console. Les valeurs admises sont : **1...10** ;
- **-l** : utilise un niveau de détail plus élevé pour les messages enregistrés dans le fichier journal que celui défini par défaut ;

- **-L <niveau\_de\_détail>** : utilise le niveau de détail indiqué pour les messages enregistrés dans le fichier journal ;
- **-h** : affiche l'aide relative à l'utilitaire sur la console.

Si aucun de ces arguments n'est utilisé, alors la console affichera les messages relatifs aux erreurs et les avertissements ainsi que les messages relatifs aux opérations réussies.

## A.5. Champs d'en-tête spéciaux du module de filtrage

Lors du traitement des messages électroniques, Kaspersky Anti-Spam ajoute les champs d'en-tête suivants aux messages :

- **X-Spamtest-Version** : champ contenant les informations relatives à la version de la distribution de Kaspersky Anti-Spam.
- **X-Spamtest-Status** et **X-Spamtest-Status-Extended** : champ contenant l'état des messages attribué après le filtrage. Le champ d'en-tête X-Spamtest-Status était utilisé dans les versions antérieures du logiciel. Ce champ d'en-tête contient l'ensemble des états correspondant à Kaspersky Anti-Spam 2.0 et il est utilisé par souci de compatibilité. Les différentes valeurs de ce champ d'en-tête sont reprises dans le tableau ci-dessous.

Champ d'en-tête	Signification	Description
X-Spamtest-Status	<b>Trusted</b>	L'expéditeur du message figure dans la liste blanche des expéditeurs et la recherche du courrier indésirable est désactivée dans la stratégie de groupe du destinataire.
	<b>SPAM</b>	Le message est un courrier indésirable.
	<b>Probable Spam</b>	Le message est peut-être un courrier indésirable.

Champ d'en-tête	Signification	Description
	<b>Not detected</b>	Le message n'est pas considéré comme un courrier indésirable confirmé ou potentiel.
<b>X-Spamtest-Status-Extended</b>	<b>trusted</b>	L'expéditeur du message figure dans la liste blanche des expéditeurs et la recherche du courrier indésirable est désactivée dans la stratégie de groupe du destinataire.
	<b>blacklisted</b>	L'expéditeur du message figure dans la liste noire des expéditeurs.
	<b>Spam</b>	Le message est un courrier indésirable.
	<b>probable_spam</b>	Le message est peut-être un courrier indésirable.
	<b>formal</b>	Le message est une réponse automatique d'un serveur de messagerie.
	<b>not_detected</b>	Le message n'est pas considéré comme un courrier indésirable confirmé ou potentiel.

- **X-Spamtest-Header** : champ d'en-tête contenant le texte défini par l'administrateur à l'aide des paramètres du Centre d'administration (cf. point 4.3.7, p. 54) ;
- **X-Spamtest-Obscene** : champ d'en-tête ajouté aux messages contenant des expressions obscènes.
- **X-SpamTest-Formal** : champ d'en-tête ajouté au message électronique dont l'état est **Formal**.

- **X-Spamtest-Rate** : champ d'en-tête contenant le classement attribué au message lors du filtrage. Kaspersky Anti-Spam utilise cette valeur lorsqu'il doit attribuer un état au message ;
- **X-Spamtest-Group-ID** : champ d'en-tête contenant l'identifiant du groupe dont les règles ont été utilisées pour le traitement du message.
- **X-SpamTest-Categories** : champ d'en-tête contenant le nom de la catégorie attribuée au message après le filtrage.
- **X-SpamTest-Info** : champ d'en-tête contenant des données purement informatives.
- **X-Spamtest-Envelope-From** : en-tête contenant l'adresse de l'expéditeur reprise dans l'enveloppe SMTP. Elle sert pour suivre les interventions des listes noire et blanche locales.
- **X-SpamTest-Method** : champ d'en-tête contenant le nom des méthodes dont les résultats ont été utilisés pour définir l'état du message. Les valeurs possibles sont reprises dans le tableau ci-après.

Signification	Méthode
<b>white ip list</b>	Vérification par rapport à la liste blanche des adresses IP d'expéditeurs.
<b>white email list</b>	Vérification par rapport à la liste blanche des adresses électroniques d'expéditeurs.
<b>black ip list</b>	Vérification par rapport à la liste "noire" des adresses IP d'expéditeurs.
<b>black email list</b>	Vérification par rapport à la liste "noire" des adresses électroniques d'expéditeurs.
<b>GSG</b>	Analyse des signatures graphiques.
<b>headers</b> et <b>headers plus</b>	Analyse des en-têtes.
<b>DNSBL</b>	Vérification à l'aide des services DNSBL.

Signification	Méthode
<b>UDS</b>	Vérification à l'aide du service UDS.
<b>UDS BL</b>	Analyse à l'aide du service UDS. Il s'agit d'une analyse associant les règles heuristiques et les listes noires.
<b>SURBL</b>	Vérification à l'aide du service SURBL.
<b>Content</b>	Analyse du contenu du message électronique.
<b>probable</b>	Méthode du courrier indésirable probable.
<b>detection disabled</b>	La recherche de messages non sollicités dans le courrier a été désactivée dans la stratégie de groupe pour le destinataire.
<b>Multiple</b>	Les résultats de plusieurs méthodes ont été utilisés pour attribuer l'état.
<b>None</b>	Aucune des méthodes ne permet de classer le message. De tels messages reçoivent l'état <b>Not detected</b> .

## A.6. Paramètres du service *cron*

Pour garantir le bon fonctionnement de Kaspersky Anti-Spam, il faut pouvoir lancer toute une série de scripts à l'aide du service cron pour l'utilisateur **mailflt3**.

La commande suivante permet de modifier les paramètres des scripts à exécuter :

```
# crontab -u mailflt3 -e
```

Dans la liste des tâches à lancer, introduisez les scripts suivants :

- **Script de mise à jour des bases de filtrage du contenu.**

Commande d'exécution : `/usr/local/ap-mailfilter3/bin/sfupdates -q`

Intervalle d'exécution recommandé : toutes les vingt minutes.



Définissez l'heure de lancement du script de mise à jour avec une certaine souplesse vis-à-vis de l'heure de lancement pour éviter la surcharge des serveurs de mise à jour. Par exemple `7,27,47 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -q`

- **Script de surveillance.**

Commande d'exécution :

```
/usr/local/ap-mailfilter3/control/bin/sfmonitoring -q
```

Intervalle d'exécution recommandé : toutes les cinq minutes.

- **Script de traitement des protocoles de fonctionnement et de mise à jour des statistiques.**

Le script recueille les données statistiques sur les messages traités dans les protocoles de fonctionnement de Kaspersky Anti-Spam. Il traite également les protocoles de fonctionnement du serveur de filtrage afin d'afficher les messages via l'interface du Centre d'administration.

Commande d'exécution :

```
/usr/local/ap-mailfilter3/control/bin/dologs.sh -q
```

Intervalle d'exécution recommandé : toutes les minutes.

- **Script de rafraîchissement des diagrammes statistiques.**

Le script élabore les diagrammes statistiques sur la base des résultats des messages traités dans la section **Statistics** du Centre d'administration.

Commande d'exécution :

```
/usr/local/ap-mailfilter3/control/bin/dograph.sh -q
```

Intervalle d'exécution recommandé : toutes les cinq minutes.

- **Script de rotation des fichiers des protocoles de fonctionnement.**

Pour éviter le débordement des disques et la réduction des performances, il est conseillé de procéder régulièrement à une rotation des fichiers des protocoles de fonctionnement du serveur de filtrage. Ce script réalise la rotation des protocoles internes utilisés par le Centre d'administration et le système de statistiques.

Commande d'exécution :

```
/usr/local/ap-mailfilter3/control/bin/logrotate.sh -q
```

Horaire recommandé : deux fois par jour. Lorsque la charge sur le système augmente, la rotation peut être plus fréquente.

- **Script de calcul du temps d'accès aux serveurs UDS.**

Le script `uds-rtts.sh` est utilisé par l'application afin de définir le temps d'accès aux serveurs UDS de Kaspersky Lab. Les valeurs obtenues permettent de sélectionner le serveur optimal pour la réception d'une requête UDS.

Commande d'exécution :

```
/usr/local/ap-mailfilter3/bin/uds-rtts.sh -q
```

Intervalle d'exécution recommandé : Toutes les 10 à 15 minutes.

En plus de la configuration des scripts cités, il est conseillé également d'exécuter les actions suivantes :

- Ajout du chemin d'accès au répertoire d'exécution des scripts cités dans la variable `HOME`. Chemin recommandé : `/usr/local/ap-mailfilter3/run`.
- Ajout de la liste des chemins d'accès aux utilitaires système principaux, y compris l'utilitaire `sendmail` dans la variable `PATH`. La valeur par défaut est égale à `/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin`
- Définition de l'adresse pour l'envoi des messages relatifs à l'exécution des scripts à l'aide de la variable `MAILTO`. La valeur par défaut est égale à `postmaster`.

Voici un exemple du fichier `crontab` à titre d'illustration des paramètres décrits :

```
MAILTO=admin@mycompany.com
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr
/local/sbin
HOME=/usr/local/ap-mailfilter3/run
7,27,47 * * * * /usr/local/ap-
mailfilter3/bin/sfupdates -q
*/5 * * * * /usr/local/ap-
mailfilter3/control/bin/sfmonitoring -q
* * * * * /usr/local/ap-
mailfilter3/control/bin/dologs.sh -q
*/5 * * * * /usr/local/ap-
mailfilter3/control/bin/dograph.sh -q
0 */12 * * * /usr/local/ap-
mailfilter3/control/bin/logrotate.sh -q
```

---

<sup>2</sup> Le script de surveillance est utilisé.

---

```
4-59/11 * * * * /usr/local/ap-mailfilter3/bin/uds-  
rtts.sh -q
```

# ANNEXE B. ENVOI D'EXEMPLES DE POURRIELS AUX EXPERTS DE KASPERSKY LAB

Kaspersky Lab remercie tous les utilisateurs qui envoient de nouveaux exemples de courriers indésirables à son équipe d'experts. Ces exemples nous permettent de réagir efficacement face aux nouveaux modes de diffusion et d'intervenir au stade initial.

Vous pouvez également nous envoyer des exemples de messages qui ont été considérés par erreur comme des pourriels. Les experts de notre laboratoire linguistique les étudieront minutieusement afin d'améliorer la qualité de l'identification et de réduire le nombre de faux positifs.

L'envoi de pourriels conformément aux instructions fournies ci-après permettra d'automatiser au maximum le processus de traitement des messages et d'accélérer les réactions de Kaspersky Anti-Spam face aux nouvelles astuces utilisées par les diffuseurs de courrier indésirable.

Adresse où envoyer les exemples de pourriels :	<a href="mailto:spam@kaspersky.com">spam@kaspersky.com</a>
Adresse où envoyer les messages considérés par erreur comme du pourriel :	<a href="mailto:notspam@kaspersky.com">notspam@kaspersky.com</a>



Les exemples de pourriels doivent être envoyés en tant que pièce jointe.

Différents clients de messagerie proposent divers moyens permettant de conserver au maximum les en-têtes des messages lors du transfert. Nous présentons la marche à suivre pour les utilisateurs des clients de messagerie les plus répandus.

1. Pour envoyer des exemples de pourriels avec Microsoft Office Outlook, procédez comme suit :
  - Si vous souhaitez envoyer un message, créez un nouveau message à l'aide du bouton **Nouveau** ou de la commande

**Nouveau message** et ajoutez le pourriel au moyen d'un glisser-déposer avec la souris.

- Si vous souhaitez envoyer plusieurs messages, sélectionnez-les puis cliquez sur **Transférer**. Le client de messagerie enverra automatiquement les messages sélectionnés en tant que pièces jointes à un nouveau message.
2. Pour envoyer des exemples de pourriels avec The Bat!, procédez comme suit :
- Si vous souhaitez envoyer manuellement le message, sélectionnez le ou les messages que vous souhaitez envoyer puis utiliser la commande **Transférer (méthode alternative)** ou **Alternative Forward**. Cette commande est accessible dans la barre d'outils du menu **Specials**.
  - si vous souhaitez configurer l'envoi automatique des pourriels, créez une règle de tri de la manière suivante :
    - Désélectionnez la case **Ne pas envoyer les fichiers joints** ;
    - Cochez la case **Utiliser la norme MIME**.
3. Pour transférer des pourriels à l'aide de Microsoft Outlook Express,, sélectionnez le ou les messages souhaités puis exécutez la commande **Message → Forward as Attachmen (Message → Transférer en tant que pièce jointe)**.

# ANNEXE C. KASPERSKY LAB LTD

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

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

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

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

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

Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

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

## C.1. Autres produits antivirus

### Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

### **Kaspersky Anti-Virus® Personal Pro**

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

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

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

### **Kaspersky® Anti-Hacker**

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

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte

n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

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

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

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

### **Kaspersky® Personal Security Suite**

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

Kaspersky® Personal Security Suite possède les fonctions suivantes :

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

### **Kaspersky Lab News Agent**

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

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;

- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

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

### **Kaspersky OnLine Scanner**

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

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

### **Kaspersky® OnLine Scanner Pro**

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

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

### **Kaspersky Anti-Virus 6.0**

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

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

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

### **Kaspersky® Internet Security 6.0**

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

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les

plus utilisés (Microsoft Office Outlook, Microsoft Outlook Express et The Bat!)

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

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

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

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

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

### **Kaspersky® Security for PDA**

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos

téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

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

### **Kaspersky Anti-Virus Mobile**

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

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

### **Kaspersky Anti-Virus® Business Optimal**

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

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale<sup>3</sup> intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Windows 2003 Server,

---

<sup>3</sup> En fonction du type de livraison

Novell Netware, FreeBSD et Linux et les entrepôts de fichiers sous Samba ;

- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail et gmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition.

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

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

### **Kaspersky® Corporate Suite**

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

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

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

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

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

## **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

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

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

## **Kaspersky SMTP Gateway**

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

## **Kaspersky Security® for Microsoft Exchange 2003**

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

## **Kaspersky® Mail Gateway**

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie. L'application contient un ensemble d'outils de filtrage du courrier selon les noms et les types MIME des pièces jointes ainsi que divers moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques.

### **Kaspersky® Anti-Virus for Proxy Server**

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

## **C.2. Comment nous contacter**

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

Assistance technique	Pour l'assistance technique, adressez-vous à <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a>
Informations générales	Sites Internet : <a href="http://www.kaspersky.com/">http://www.kaspersky.com/</a> <a href="http://www.viruslist.com/">http://www.viruslist.com/</a> Mèl. : <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>