KASPERSKY LAB

Kaspersky Anti-Virus® 5.0 for Windows File Servers

MANUEL DE L'ADMINISTRATEUR

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS FILE SERVERS

Manuel de l'administrateur

http://www.kaspersky.com/fr

Date d'édition: mai 2006

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS® FOR WINDOWS FILE SERVERS

Kaspersky Anti-Virus® for Windows File Servers (par la suite, Kaspersky Anti-virus) a été conçu pour assurer la protection des serveurs de fichiers contre les virus et les programmes malveillants.

Le logiciel offre les fonctions suivantes :

- *Protection en temps réel du système de fichiers contre les codes malicieux en mode surveillance :* interception et analyse des requêtes adressées au système de fichiers , réparation, suppression des objets infectés et isolement des objets suspects en vue d'une analyse ultérieure.
- *Recherche et neutralisation du code malicieux à la demande de l'administrateur :* recherche et analyse des objets suspects et infectés dans les zones d'analyse définies ; réparation, suppression ou isolement des objets en vue d'une analyse ultérieure.
- *Protection en temps réel contre les scripts VBScript et JavaScript dangereux*. L'analyse a lieu avant l'exécution du script par le module de traitement des scripts du système d'exploitation ; blocage de l'exécution des scripts dangereux.
- *Analyse des riskwares :* analyse des programmes exécutés sur l'ordinateur ou téléchargés depuis Internet, ou se trouvant sur le disque dur ou des disques amovibles. Lors de la découverte d'un riskware, l'application (en fonction des paramètres définis) autorise ou non son exécution ou le supprime.
- *Placement des objets suspects en quarantaine* : les objets suspects sont conservés dans le répertoire de quarantaine ; envoi d'objets définis à Kaspersky Lab en vue d'une analyse approfondie ; restauration des objets à la demande de l'administrateur.
- *Création d'une copie de l'objet infecté dans le répertoire de quarantaine avant la* réparation *et la suppression* afin de pouvoir éventuellement le restaurer à la demande au cas où il contiendrait des données importantes ou d'étudier l'infection.
- *Mise à jour des bases antivirus et des modules* faisant partie de Kaspersky Anti-Virus depuis les serveurs de mise à jour de Kaspersky Lab ; création d'une copie de sauvegarde de tous les fichiers actualisés

au cas où la dernière mise à jour devrait être annulée ; placement des mises à jours dans un répertoire de distribution accessible aux autres ordinateurs du réseau afin de réduire l'intensité du trafic Internet.

N'oubliez pas que de nouveaux virus font leur apparition chaque jour. Pour cette raison, nous vous conseillons de sélectionner la mise à jour automatique afin que l'application dispose des informations les plus récentes.

- *Gestion de l'application localement* via la ligne de commande ou la console d'administration ou *à distance* via le système d'administration centralisé **Kaspersky Administration Kit 5.0**.

1.1. Nouveautés de la version 5.0

Par rapport aux versions 4.x, **Kaspersky Anti-Virus 5.0 for Windows File Servers** contient les améliorations suivantes :

- Utilisation d'un nouveau moteur antivirus qui réduit condisérablement la quantité de mémoire vive requise par rapport à la version 4.0.
- L'utilisation des nouvelles technologies iChecker™ et iStreams™ renforce l'efficacité de la protection antivirus par rapport à la version 4.0.
- L'accélération de la vitesse des mises à jour des bases antivirus grâce à la sélection automatique du serveur de mise à jour de Kaspersky Lab le moins sollicité ; ajout d'un algorithme assurant la réception du reste de la mise à jour en cas de déconnexion ; possibilité de placer les mises à jour téléchargées dans une source de mise à jour locale;
- Possibilité de configurer la protection antivirus à l'aide de l'un des trois niveaux de protection dont les paramètres ont été prédéfinis par les experts de Kaspersky Lab : *Sécurité maximale, Recommandé et Vitesse maximale* ;
- Possibilité d'analyser et de traiter les riskwares en mode protection en temps réel ou analyse à la demande
- Possibilité de réparer les fichiers dans les archives ZIP, ARJ, CAB et RAR.
- Le composant Control Centre a été remplacé par une interface administrateur plus conviviale et plus simple qui offre une plus grande souplesse d'administration des paramètres de l'application.
- Possibilité de procéder à la suppression simultanée de l'application sur quelques serveurs de fichiers grâce à **Kaspersky Administration Kit 5.0**

et possibilité d'installation à distance sur les postes du réseau avec enregistrement automatique sur le *Serveur d'administration*.

- Amélioration du fonctionnement de la quarantaine : possibilité de limiter la durée de conservation des objets suspects placés dans le dossier de quarantaine.
- Création d'un dossier de sauvegarde pour les copies des objets suspects et infectés créées avant la réparation ou la suppression de ces derniers.
- Le journal des événements contient une fonction de filtrage des événements enregistrés permettant de réaliser les actions suivantes : *enregistrement dans le Windows Event Log, notification par courrier électronique, notification à l'aide de NET SEND, exécution de la commande du système d'exploitation*.
- Possibilité de créer des listes de processus de confiance dont l'activité n'est pas contrôlée par Kaspersky Anti-Virus en mode d'analyse en temps réel.
- Possibilité de copier les mises en jour en entier ou en partie : pour tous les logiciels de Kaspersky Lab ou uniquement pour Kaspersky Anti-Virus 5.0 for Windows Workstations et Kaspersky Anti-Virus 5.0 for Windows File Servers.

1.2. Configurations matérielle et logicielle requises

Pour garantir le fonctionnement optimal de l'application, le serveur doit répondre aux conditions suivantes :

- Microsoft Windows® NT 4.0 Server avec le Service Pack 6a ou suivant :
    - Intel Pentium® ou suivant ;
    - 32 Mo de RAM disponible ;
    - 30 Mo d'espace disque.
- Microsoft Windows® 2000 Server/Advanced Server avec Service Pack 2 ou suivant:
    - Intel Pentium® ou suivant ;
    - 64 Mo de RAM disponible ;
    - 30 Mo d'espace disque.
- Microsoft Windows® 2003 Server:

- Intel Pentium® ou suivant ;
- 128 Mo de RAM disponible ;
- 30 Mo d'espace disque.

Sous Microsoft Windows® 2003, la version 64 bit du système d'exploitation pour la plate-forme IA-64 n'est pas prise en charge.

1.3. Contenu du pack logiciel

Vous pouvez acquérir ce logiciel chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr – rubrique **E-Store / Particuliers**).

Le pack logiciel en boite contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés; la clé de licence 365 jours est inclue et présente sur le CDROM, séparément ou incluse dans le fichier executable.
- Le manuel de l'utilisateur avec le contrat de licence utilisateur imprimé à la fin de ce manuel.

Si vous achetez ce logiciel en ligne, et dés la réception de votre paiement, vous recevrez un email contenant des liens personnels pointants sur le site Web de Kaspersky Lab pour télécharger :

- le fichier d'installation contenant votre clé de licence d'un an,
- votre clé de licence un an seule (utile dans le cas où vous auriez déja installé une version avec une clé d'essai),
- la version électronique de ce manuel (format Adobe PDF).

La licence utilisateur constitue l'accord juridique passé entre vous et Kaspersky Lab, stipulant les conditions d'utilisation du progiciel que vous avez acquis. Lisez la attentivement !

1.4. Services réservés aux utilisateurs enregistrés

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

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

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

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

1.5. Notations conventionnelles

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

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

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

CHAPITRE 2. INSTALLATION ET DESINSTALLATION DU PROGRAMME

Il existe deux modes d'installation de Kaspersky Anti-Virus 5.0 for Windows File Servers : locale ou à distance (via le système d'administration centralisée de Kaspersky Administration Kit 5.0). Ce manuel aborde uniquement l'installation locale de Kaspersky Anti-Virus. Pour obtenir de plus amples informations sur l'installation à distance, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

En fonction de l'utilisation prévue de Kaspersky Anti-Virus 5.0 for Windows File Servers, vous pouvez envisager l'une des installations suivantes :

- **Administration via la ligne de commande :** installez Kaspersky Anti-Virus 5.0 for Windows File Servers sur l'ordinateur-serveur. Dans ce cas, l'interface graphique est absente et l'administration de l'application s'opère via la ligne de commande à l'aide de l'utilitaire *kavshell.exe.*
- **Administration via la *Console d'administration*** : installez Kaspersky Anti-Virus 5.0 for Windows File Servers sur l'ordinateur-serveur, ainsi que *l'Agent d'administration* et la *Console* d'administration qui font partie de Kaspersky Administration Kit. Dans ce cas, l'administration s'opère localement via la *Console d'administration*.

  

  Si vous avez l'intention à l'avenir d'administrer Kaspersky Anti-Virus à l'aide de Kaspersky Administration Kit 5.0, veillez, lors de l'installation de l'*Agent d'administration*, à ce que l'adresse (nom et port) du *Serveur d'administration* soit défini correctement.

- **Administration centralisée du logiciel via Kaspersky Administration Kit** :
  - Installez Kaspersky Anti-Virus 5.0 for Windows File Servers ainsi que l'*Agent d'administration* sur l'ordinateur-serveur ;
  - Déployez le *Serveur d'administration* dans le réseau, installez la *Console d'administration* sur le poste de travail de l'administrateur (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

2.1. Installation de l'application

Afin d'installer le logiciel, lancez le fichier exécutable *setup.exe* repris dans la distribution. Le programme d'installation se compose d'une succession de boîtes de dialogue. Chacune de ces boîtes présente différents boutons destinés à contrôler la procédure. Voici une brève description de chacun d'entre eux :

- **OK** : validation des actions ;
- **Annuler** : annulation des actions ;
- **Suivant** : passage au point suivant ;
- **Précédent** : retour à l'étape précédente.

Etape 1. Lecture du contrat de licence

La boîte de dialogue **Contrat de licence** contient le texte du contrat de licence. Lisez le texte du contrat de licence et si vous en acceptez les conditions, cliquez sur **Oui**. Pour interrompre l'installation de l'application, cliquez sur **Non**.

Etape 2. Saisie des données concernant l'utilisateur

Saisissez dans la boîte de dialogue **Informations utilisateur** les données requises. Saisissez le nom de l'utilisateur dans le champ **Nom de l'utilisateur** et celui de la société dans le champ **Organisation**. Ces champs reprennent par défaut les données de la base du registre de Microsoft Windows.

Etape 3. Choix du dossier d'installation

Dans la boîte de dialogue **Sélection du dossier d'installation**, indiquez le nom du dossier dans lequel Kaspersky Anti-Virus sera installé. Par défaut, il s'agit du dossier **Program Files\Kaspersky Lab\Kaspersky Anti-Virus for File Servers 5**.

Cliquez sur **Parcourir** pour sélectionner un autre dossier.

Etape 4. Lecture des informations importantes relatives à l'application

Avant d'utiliser l'application, il est recommandé de lire les informations importantes reprises dans cette fenêtre. Vous y découvrirez les principales fonctions de Kaspersky Anti-Virus, les particularités de son fonctionnement, etc.

Cliquez sur **Suivant >** lorsque vous aurez lu ces renseignements.

Etape 5. Activation de la clé de licence

Vous devez absolument indiquer dans la boîte de dialogue **Clé de licence** la clé de licence que Kaspersky Anti-Virus utilisera pour vérifier la présence du contrat de licence et définir sa durée de validité.

Cette clé est votre clé personnelle qui reprend toutes les informations fonctionnelles indispensables au fonctionnement de Kaspersky Anti-Virus ainsi que des informations complémentaires, à savoir :

- Les informations sur l'assistance technique (qui l'assure et comment l'obtenir) ;
- Le nom et le numéro de licence ainsi que sa date d'expiration.

L'apparence de la fenêtre **Clé de licence** varie selon que la clé de licence a été livrée en même temps que la distribution ou si elle doit être téléchargée depuis Internet.

Dans le premier cas, le programme d'installation ajoute le fichier de la clé de licence, pour autant qu'il se trouve sur le disque d'installation ou dans le répertoire où l'application est installée. Les renseignements relatifs à la clé de licence ajoutée sont alors affichés.

Dans le deuxième cas, vous aurez le choix entre l'une des deux options suivantes :

- **Clé de licence locale** : activation de la clé de licence reprise sur l'ordinateur.
- **Clé de licence téléchargée depuis Internet** : pour l'obtention de la clé via Internet, depuis le site de Kaspersky Lab.

Le choix de la première option entraîne l'ouverture d'une boîte de dialogue avec un bouton **Parcourir** permettant de localiser sur le disque le fichier de la clé de licence avec l'extension *.key*.

Le choix de l'option **Clé de licence téléchargée depuis Internet** entraîne l'ouverture d'une boîte de dialogue dans laquelle il conviendra de saisir les informations requises ainsi que le code d'activation de la clé (ce code est octroyé lors de l'achat du logiciel). Cliquez sur **Suivant** lorsque vous aurez saisi les données.

Etape 6. Fin de l'installation

La fenêtre **L'installation/la suppression du logiciel est terminée** reprend des informations relatives à la fin de l'installation de Kaspersky Anti-Virus sur votre ordinateur.

Il n'est pas nécessaire de redémarrer l'ordinateur pour terminer l'installation. Décochez la case **Lancer Kaspersky Anti-Virus 5.0 for Windows File Servers**

si vous ne souhaitez pas activer la protection antivirus de votre ordinateur directement après la fin de l'installation. Cliquez sur **Terminer.**

Si vous décochez cette case, la protection antivirus de votre ordinateur sera lancée automatiquement uniquement après le redémarrage celui-ci.

2.2. Suppression de l'application

Si pour une raison quelconque, vous devez supprimer Kaspersky Anti-Virus, utilisez la commande **Démarrer→Programmes→Kaspersky Anti-Virus 5.0 for Windows File Servers→Kaspersky Anti-Virus Uninstall** ou utiliser la fonction standard **Ajout/Suppression de programmes** dans Microsoft Windows.

Une demande de confirmation de la suppression de l'application apparaîtra à l'écran. Pour lancer la procédure de désinstallation, cliquez sur **OK**. La procédure de suppression du programme se terminera par l'affichage d'une boîte de dialogue vous invitant à redémarrer l'ordinateur. Reportez, si nécessaire, le redémarrage et cliquez sur **Terminer** pour quitter l'Assistant.

2.3. Mise à jour de la version 4.x à la version 5.0

Avant de procéder à la mise à jour de Kaspersky Anti-Virus, il est recommandé de traiter les objets qui se trouvent dans le dossier de quarantaine ou dans le dossier de sauvegarde.

Afin de procéder à la mise à niveau de la version 4.x de Kaspersky Anti-Virus for Windows File Servers à la version 5.0, lancez le fichier de l'application *setup.exe*. La version antérieure de l'application sera supprimée pendant l'installation.

Il faudra redémarrer le système d'exploitation à la fin de l'installation.

En cas d'administration à distance via Kaspersky Administration Kit (pour de plus amples informations, consultez le manuel de « Kaspersky Administration Kit 5.0 »), la mise à jour de la version 4.x à la version 5.0 s'opère automatiquement : la version antérieure de Kaspersky Anti-Virus sera supprimée et l'ordinateur distant sera redémarré.

Veuillez noter que les paramètres de la version 4.x seront supprimés lors de la mise à niveau de Kaspersky Anti-Virus. Vous pouvez utiliser les paramètres recommandés définis par défaut ou reconfigurer l'application.

CHAPITRE 3. CONCEPT D'ADMINISTRATION DE L'APPLICATION

Kaspersky Anti-Virus for Windows File Servers s'installe sur le serveur et peut être administré localement ou à distance grâce au programme Kaspersky Administration Kit (pour autant que l'ordinateur soit inclus dans le système d'administration centralisée à distance).

Il existe plusieurs catégories de personnes qui peuvent être amenées à utiliser Kaspersky Anti-Virus :

- *L'administrateur de la sécurité antivirus* (ci-après, l'administrateur), c.-à-d. la personne chargée de l'administration locale de Kaspersky Anti-Virus ;
- *L'administrateur du réseau logique*, c.-à-d. la personne chargée de l'administration du fonctionnement de Kaspersky Anti-Virus via Kaspersky Administration Kit, le système d'administration centralisée.

Par défaut, les administrateurs locaux de l'ordinateur sont les administrateurs de la protection antivirus.

En cas d'administration locale, l'application est installée sur le serveur et est administrée soit via la ligne de commande, soit via la *Console d'administration*. Dans ce cas, l'administrateur peut réaliser les tâches suivantes :

- Administration de l'application via les paramètresConfiguration des paramètres de l'application ;
- Configuration et lancement des tâches antivirus ;
- Mise à jour des bases antivirus et des modules de l'application ;
- Activation de la clé de licence des clés de licence;
- Examen du contenu du dossier de quarantaine ou de sauvegarde ;
- Obtention de rapport sur l'activité de l'application.

Le programme d'administration centralisée Kaspersky Administration Kit permet l'administration à distance depuis l'ordinateur sur lequel la *console d'administration* a été installée lorsque le *Serveur d'administration* est présent dans le réseau.

Dans ce cas, l'administrateur du réseau logique peut, en plus des tâches mentionnées ci-dessus, réaliser les tâches suivantes :

- Installation à distance de Kaspersky Anti-Virus sur les ordinateurs client ;
- Application des stratégies et administration des tâches sur les ordinateurs client Configuration à distance de Kaspersky Anti-Virus;
- Activation et suppression des clés de licence sur les ordinateurs client ;
- Examen des rapports d'activité des informations relatives à l'activité du programme sur les ordinateurs client.

Pour obtenir de plus amples informations sur le concept d'administration centralisée, consultez le Manuel de l'administrateur de « Kaspersky Administration Kit 5.0 ».

3.1. Principes de base du concept d'administration

En cas d'administration locale de Kaspersky Anti-Virus, la protection est définie par l'administrateur qui configure les paramètres des tâches et de l'application dans le cadre de la configuration.

Une **Tâche** est une action exécutée par Kaspersky Anti-Virus. Les tâches sont réparties en différents types selon leurs fonctions. On distingue ainsi la tâche d'analyse complète, la tâche de mise à jour des bases antivirus et des modules de l'application, etc.). A chaque tâche correspond un groupe de paramètres de fonctionnement de Kaspersky Anti-Virus pendant ld'exécution de la tâche. Il s'agit des *paramètres de la tâche*.

Paramètres de l'application : ensemble de paramètres de fonctionnement complémentaires comprenant les paramètres de la quarantaine, du dossier de sauvegarde, de réception des rapports, etc.

En cas d'administration centralisée via Kaspersky Administration Kit, l'administrateur détermine également la configuration des tâches et de l'application, mais uniquement pour les copies de Kaspersky Anti-Virus installées sur les ordinateurs distants du réseau.

Parmi les particularités de l'administration centralisée, citons la répartition des ordinateurs distants en groupe et l'administration de ceux-ci des paramètres via la création et la définition de stratégies de groupe.

La **stratégie** est un ensemble de paramètres de fonctionnement de l'application dans le groupe de l'application pour un groupe d'ordinateurs du réseau logique ainsi qu'un ensemble de restrictions sur la redéfinition des les paramètres lors de la configuration de l'application et des tâches sur des ordinateurs clients distincts.

La stratégie intègre la configuration complète de toutes les fonctions de l'application. Elle reprend donc les paramètres de l'application et ceux de tous les types de tâches, à l'exception des paramètres spécifiques à un type de tâche particulier qu'il faut définir directement au moment du lancement de la tâche.

Pour interdire la redéfinition des paramètres de la stratégie, il faut les « verrouiller » :  . L'icône  indique les paramètres qui peuvent être modifiés.

3.2. Conception de l'interface utilisateur

L'interface graphique d'administration est fournie par un composant au sein de Kaspersky Administration Kit 5.0 : la *Console d'administration*. Il s'agit d'un élément spécialisé autonome intégré à la Microsoft Management Console (MMC). Pour cette raison, l'interface de Kaspersky Administration Kit est standard pour MMC.

Cette rubrique est consacrée à ses principaux éléments, à savoir : la fenêtre principale, l'arborescence de la console et le menu contextuel.

3.2.1. Fenêtre principale de l'application

La fenêtre principale de l'application (cf. ill. 1) contient :

- **Le menu** : fonctions principales d'administration des fichiers et des fenêtres et accès aux fichiers d'aide.
- **La barre d'outils** : ensembles des boutons offrant un accès direct aux actions les plus souvent exécutées.
- **Le panneau d'affichage** : liste des objets du système antivirus représentés sous la forme d'une arborescence.
- **Le panneau des résultats** : liste des éléments de l'objet sélectionné dans l'arborescence.

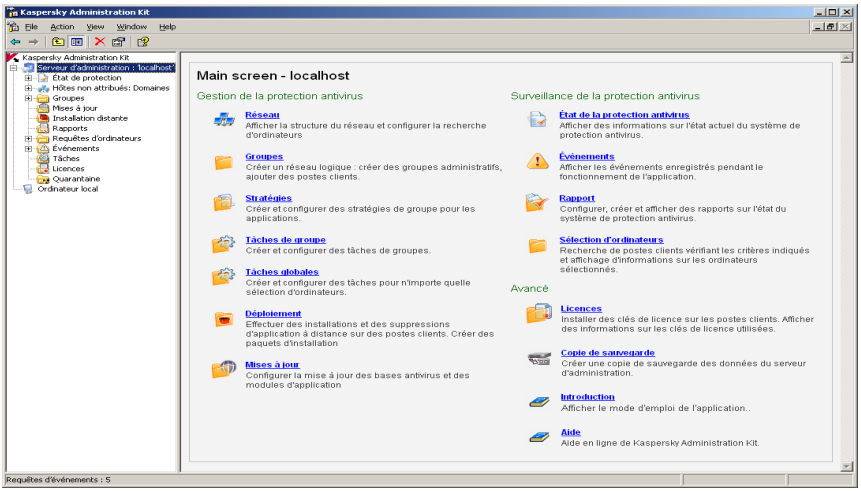

Illustration 1. Console d'administration

3.2.2. Arborescence de la console

L'arborescence de la console permet de représenter les réseaux logiques du réseau de l'entreprise et les propriétés de l'ordinateur local sur lequel est installé la *Console d'administration.*

L'espace intitulé **Kaspersky Administration Kit** peut contenir plusieurs nœuds avec les noms des *Serveurs d'administration* du réseau ainsi que l'objet **Ordinateur local**.

L'objet **Ordinateur local** sert à l'administration locale de la copie de Kaspersky Anti-Virus 5.0 for Windows File Servers installée sur l'ordinateur-serveur. Au départ de la commande correspondante du menu contextuel, il est possible d'ouvrir la fenêtre de configuration des paramètres de l'application et d'administration des tâches du serveur localde cet ordinateur.

Lorsqu'un *Serveur d'administration* existe dans le réseau, vous pouvez administrer la copie de Kaspersky Anti-Virus 5.0 for Windows File Servers installée sur les serveurs distants. Lors de la connexion au Serveur d'administration, le nœud **<Nom du serveur>** contiendra plusieurs dossiers (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0).

Suite à la sélection d'un dossier dans l'arborescence de la console, le panneau des résultats en affichera le contenu. L'administration des objets repris dans le dossier s'opère à l'aide des commandes du menu contextuel.

Les dossiers **Stratégies** et **Tâches**, dans le dossier **Groupes**, sont prévus pour l'administration des stratégies de groupes (cf. Chapitre 7, p. 74) et des tâches (cf. point 7.2, p. 78) de Kaspersky Anti-Virus. Pour tous les ordinateurs distants repris dans le dossier **Groupes** et sur lesquels Kaspersky Anti-Virus 5.0 for Windows File Servers a été installé, il est possible de modifier la configuration les paramètres de l'application (cf. point 7.3, p 82) et les paramètres des tâches locales (cf. point 7.2, p. 78).

3.2.3. Menu contextuel

Dans l'arborescence de la console, chaque catégorie d'objet de l'espace intitulé **Kaspersky Administration Kit** dispose d'un menu contextuel qui lui est propre. En plus des commandes standard du menu contextuel de Microsoft Management Console, on y retrouve des commandes qui permettent de manipuler l'objet en question.

Le panneau des résultats de chaque élément de l'objet sélectionné dans l'arborescence possède également son propre menu contextuel à l'aide duquel il est possible de réaliser des actions sur l'élément en question.

CHAPITRE 4. PROTECTION DU SERVEUR SANS CONFIGURATION COMPLEMENTAIRE

La protection antivirus, appliquant les paramètres par défaut, est activée directement après l'installation du programme sur l'ordinateur. Ces paramètres ont été définis par les experts de Kaspersky Lab afin de garantir au maximum la sécurité de votre ordinateur.

Il est possible également de modifier rapidement les paramètres en choisissant l'un des trois niveaux définis par les experts de Kaspersky Lab : *Sécurité maximale, Recommandé ou Vitesse maximale.*

4.1. Niveau de protection antivirus

Afin de faciliter la configuration des paramètres de la protection antivirus, l'application propose trois niveaux avec des paramètres prédéfinis préconfigurés (cf. Tableau 1. Configuration des paramètres des niveaux de protection) :

- **Sécurité maximale** : niveau de protection de l'ordinateur correspondant au niveau de protection maximum, au détriment d'un léger recul des performances du système.
- **Niveau recommandé** : niveau de protection antivirus qui repose sur les paramètres recommandés par les experts de Kaspersky Lab et qui assure la protection optimale de votre ordinateur.
- **Vitesse maximale** : niveau de protection de l'ordinateur correspondant à la vitesse maximale de fonctionnement, au détriment d'un léger recul de la protection.

En cas de modification des paramètres de n'importe lequel de ces niveaux, le niveau est renommé **Paramètres utilisateur**. Il s'agit du quatrième niveau de protection antivirus reposant sur les paramètres définis par l'utilisateur.

Le tableau ci-après reprend la valeur des paramètres des niveaux prédéfinis pour la protection en temps réel (**protection**) et l'analyse à la demande (**analyse**).

Valeurs conventionnelles :

- **+** paramètre activé ;
- **–** paramètre désactivé ;
- **x** aucune configuration prévue pour cette tâche.

Tableau 1. Configuration des paramètres des niveaux de protection

Paramètre	Sécurité maximale		Recommandé		Vitesse maximale	
	Protection	Analyse	Protection	Analyse	Protection	Analyse
Utiliser iChecker	+	+	+	+	+	+
Utiliser iStreams	+	+	+	+	+	+
Niveau d'analyse	Fichier en fonction du format	Tous les fichiers	Fichier en fonction du format	Tous les fichiers	Fichiers en fonction de l'extension	Fichier en fonction du format
Taille maximale de l'objet analysé (Mo)	x	–	x	–	x	8
Durée maximale de l'analyse de l'objet (s.)	60	–	60	–	60	60
Disques durs	+	x	+	x	+	x
Disques amovibles	+	x	+	x	+	x
Disques de réseau	+	x	+	x	–	x
Flux NTFS	+	+	+	+	+	+
Secteurs d'amorçage des disques	+	+	+	+	+	+
Fichiers compactés	+	+	+	+	+	+
Archives	x	+	x	+	x	–
Archives auto-extractibles	+	+	–	+	–	+
Bases de données de messagerie électronique	x	+	x	–	x	–

Paramètre	Sécurité maximale		Recommandé		Vitesse maximale	
	Protection	Analyse	Protection	Analyse	Protection	Analyse
Messages individuels	x	+	x	–	x	–
Objets OLE	+	+	+	+	–	+

4.2. Paramètres par défaut

La protection antivirus, appliquant les paramètres par défaut, est activée directement après l'installation de l'application sur le serveur.

Ces paramètres sont définis pour chacune des tâches spécifiques à la protection antivirus :

PROTECTION EN TEMPS REEL EN MODE SURVEILLANCE

Le *niveau recommandé*, avec les paramètres suivants, est appliqué par défaut à la protection en temps réel :

- Analyse des fichiers soupçonnés d'être infectés en lecture, écriture et exécution, à savoir :
    - Les fichiers des disques durs, amovibles et de réseau, les secteurs d'amorçage ;
    - Les fichiers compactés et les objets OLE ;
- Les archives, les bases de données de messagerie et les fichiers aux formats de messagerie ne sont pas analysés ;
- Utilisation des technologies iChecker™ et iStreams™ ;
- En cas de découverte d'un objet infecté, l'application tente de le réparer. Si la réparation est impossible, elle supprime l'objet. En cas de découverte d'un objet suspect, elle le met en quarantaine ;
- En cas de découverte d'un riskware, Kaspersky Anti-Virus empêche l'exécution de celui-ci et consigne les informations dans le rapport ;
- Analyse des scripts dynamiques VBScript et JavaScript, traités par le module de traitement des scripts du système d'exploitation ; en cas de découverte d'un script suspect, son exécution est bloquée ;
- Limitation de la durée d'analyse des objets complexes (max. 60 s)

ANALYSE ANTIVIRUS A LA DEMANDE

Le *niveau recommandé*, avec les paramètres suivants, est appliqué par défaut à l'analyse complète de l'ordinateur :

- L'analyse complète programmée est réalisée chaque vendredi à 20h00 ;
- L'analyse porte sur les fichiers suivants :
    - Les archives et les archives auto-extractibles ;
    - Les fichiers compactés et les objets OLE ;
    - Les secteurs d'amorçage des disques et les flux supplémentaires NTFS ;
    - Les objets de démarrage ;
    - Les objets situés dans les ressources de la mémoire vive ;
- Les bases de données de messagerie et les fichiers aux formats de messagerie ne sont pas analysés ;
- Utilisation des technologies iChecker™ et iStreams™ ;
- En cas de découverte d'un riskware, Kaspersky Anti-Virus le laisse passer et consigne les informations dans le rapport.
- En cas de découverte d'un objet infecté, l'application tente de le réparer. Si la réparation est impossible, elle supprime l'objet. En cas de découverte d'un objet suspect, elle le met en quarantaine ;

MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES LOGICIELS DE L'APPLICATION

La configuration par défaut suivante est prévue pour la mise à jour des bases antivirus :

- La mise à jour des bases antivirus a lieu toutes les heures à partir de l'installation de Kaspersky Anti-Virus ;
- La mise à jour des bases antivirus et les mises à niveau urgentes de l'application sont autorisées ;
- Impossibilité de recevoir toutes les mises à jour accessibles de l'application.

ISOLEMENT DES OBJETS SUSPECTS

Les paramètres par défaut suivants sont appliqués à la mise en quarantaine des objets :

- Les objets en quarantaine sont analysés après chaque mise à jour des bases antivirus ;

- La taille du dossier de quarantaine n'est pas limitée ;
- La durée de conservation des objets en quarantaine est de 90 jours.

CONSERVATION D'UNE COPIE DE L'OBJET INFECTE

Avant la réparation ou la suppression d'un objet, une copie de celui-ci est créée dans le dossier de sauvegarde. Les paramètres suivants sont appliqués par défaut :

- La taille du dossier de sauvegarde n'est pas limitée ;
- La durée de conservation des objets dans le dossier de sauvegarde est de 90 jours.

CHAPITRE 5. RECOMMANDATIONS SUR LA DEFINITION DES PARAMETRES EN FONCTION DE LA CONFIGURATION DU SERVEUR

L'ordinateur peut remplir plusieurs fonctions : il peut être à la fois serveur de messagerie, serveur de fichiers et serveur d'applications travaillant avec des bases de données, etc.

Lors de la configuration de l'antivirus, nous vous recommandons de tenir compte de la configuration de votre serveur et de suivre les conseils repris ci-après :

- Si vous utilisez des bases de données volumineuses et d'un format particulier, il est recommandé de les exclure de la zone d'analyse. L'analyse des bases pourrait entraîner un ralentissement de l'accès des applications client ou la perte de la connexion entre l'application client et le serveur.
- Si le package antivirus est installé sur le serveur qui assure le contrôle du domaine, il est recommandé d'exclure de la zone d'analyse les dossiers renfermant les données auxquelles le service de contrôle du domaine doit avoir accès en permanence (fichiers journal, fichiers d'initialisation, etc.)
- Il est recommandé d'éviter la double d'analyse d'une même objet à l'aide de deux solutions antivirus différentes. La double analyse ralentit le fonctionnement de l'application. Ceci concerne principalement les données transmises par les applications client-serveur.

CHAPITRE 6. ADMINISTRATION LOCALE

6.1. Administration via la ligne de commande

L'administration de Kaspersky Anti-Virus 5.0 for Windows File Servers peut s'opérer via la ligne de commande. Les tâches suivantes peuvent être exécutées au départ de la ligne de commande :

SCAN	Analyse des objets sélectionnés
FULLSCAN	Analyse complète de l'ordinateur
UPDATE	Mise à jour des bases antivirus et des modules de l'application
ROLLBACK	Annulation de la dernière mise à jour réalisée des base antivirus
RTP	Administration du mode d'analyse en temps réel de l'ordinateur
START	Lancement de Kaspersky Anti-Virus
STOP	Arrêt de Kaspersky Anti-Virus
TASK	Administration des tâches de Kaspersky Anti-Virus
CONVERT	Conversion du rapport dans un format plus aisé à lire
IMPORT	Importation de la configuration des paramètres de Kaspersky Anti-Virus depuis le fichier

EXPORT	Exportation de la configuration des paramètres de Kaspersky Anti-Virus vers le fichier

Pour étudier la syntaxe des commandes, utilisez :

```
KAVSHELL HELP commande
KAVSHELL commande /?
```

Exemple:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

Pour consulter cette rubrique d'aide :

```
KAVSHELL [ /? | HELP ]
```

6.1.1. Analyse des objets sélectionnés

Syntaxe de la commande :

```
KAVSHELL SCAN [objects] [/L[!]:fichier_objet] [/F(A|E|C)]
[/DISINFECT|/DELETE] [/W[A]:fichier_journal]
```

objets	[files] [directories] [PREDIFINED] Dresse la liste d'un ou de plusieurs fichiers, répertoires, d'objets prédéfinis (PREDEFINED) ou de problèmes distincts. Remarques : - Si le nom de l'objet contient un espace, il devrait être écrit entre guillemets ; - Il est possible d'avoir recours aux masques pour analyser plusieurs fichiers (des exemples de masque sont repris au point 6.2.1.2.1 ,à la page 39); - Lorsqu'un catalogue précis est indiqué, tous les fichiers qu'il contient sont analysés..
PREDEFINED	[/MEMORY] – Analyse tous les objets de la mémoire vive; [/STARTUP] – Analyse les objets lancés automatiquement ;

	[/REMDRIVES] – Analyse tous les disques amovibles ; [/FIXDRIVES] – Analyse tous les disques locaux : [/NETDRIVES] – Analyse tous les disques de réseau.
/L[!]:fichier_objet	Dresse la liste des objets à analyser, un objet par ligne. Le symbole « ! » détermine la suppression du fichier de la liste après l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
[/F(A|E|C)] /FA /FC /FE	Typtes de fichiers analysés : – Tous les fichiers. – Les fichiers infectés en fonction du format. – Les fichiers infectés en fonction de l'extension.
/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/DISINFECT /DELETE	Actions réalisées sur les objets infectés : Réparer ; si la réparation est impossible, supprimer. Supprimer tous les objets infectés. Remarques : - Si l'action n'est pas précisée, l'objet sera ignoré et les informations relatives à sa découverte seront consignées dans le rapport ; - Les objets complexes ne seront pas supprimés.

Exemple:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt
```

6.1.2. Analyse complète

Syntaxe de la commande :

```
KAVSHELL FULLSCAN [/W[A]:fichier_journal]
```

/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.

Exemple:

```
KAVSHELL FULLSCAN
KAVSHELL FULLSCAN /WA:fullscan.log
```

6.1.3. Lancement de la mise à jour

Syntaxe de la commande :

```
KAVSHELL UPDATE [source de la mise à jour]
[/W[A]:fichier_journal] [/APP]
```

[source de la mise à jour]	Serveur http, serveur FTP ou répertoire du réseau pour le téléchargement des mises à jour. Si aucun chemin n'est indiqué, la source de la mise à jour sera celle indiquée dans les paramètres la configuration de la mise à jour des bases antivirus et des modules de l'application.

/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
/APP	Procède à la mise à jour des modules de l'application.

Exemple:

```
KAVSHELL UPDATE ftp://ftp.kaspersky.ru/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP
```

6.1.4. Annulation de la dernière mise à jour

Syntaxe de la commande :

```
KAVSHELL ROLLBACK [/W[A]:fichier_journal]
```

/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace

Exemple:

```
KAVSHELL ROLLBACK /WA:rollback.log
```

6.1.5. Mode de protection en temps réel

Syntaxe de la commande :

```
KAVSHELL RTP [taskid] { /START [/W[A]:fichier_journal] |
                        /STOP }
```

/START	Active la protection en temps réel ou l'une de ses tâches définies.
/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace.
/STOP	Arrête la protection en temps réel ou l'une de ses tâches.
taskid	Identifiant de la tâche de protection en temps réel. Si l'identifiant (taskid) n'est pas repris, toutes les commandes sont appliquées à toutes les tâches de la protection en temps réel. Valeurs possibles : on-access : protection en temps réel des fichiers script-checker : analyse en temps réel des scripts

Exemple:

```
KAVSHELL RTP /START /W:rtp.log
KAVSHELL RTP on-access /START /WA:oas.log
KAVSHELL RTP script-checker /STOP
```

6.1.6. Lancement de l'application

Syntaxe de la commande :

```
KAVSHELL START
```

Cette commande est uniquement accessible à l'administrateur local de l'ordinateur.

6.1.7. Arrêt de l'application

Syntaxe de la commande :

```
KAVSHELL STOP
```

Cette commande est uniquement accessible à l'administrateur local de l'ordinateur.

6.1.8. Administration des tâches

Syntaxe de la commande :

```
KAVSHELL TASK [taskid { /START [/W[A]:fichier_journal] |
                        /STOP |
                        /PAUSE |
                        /RESUME |
                        /DELETE} ]
```

Sans paramètres	Donne toutes les tâches accessibles avec l'identifiant unique, le nom et l'état.
/START	Lance la tâche correspondant à l'identifiant spécifié.
/W:fichier_journal	Consigne uniquement les événements importants dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/WA:fichier_journal	Consigne tous les événements dans le fichier journal. La saisie d'un chemin relatif ou absolu est autorisée.

	Le chemin doit être saisi entre guillemets s'il contient un espace
/STOP	Arrête la tâche correspondant à l'identifiant spécifié.
/PAUSE	Suspend l'exécution de la tâche correspondant à l'identifiant spécifié.
/RESUME	Reprend l'exécution de la tâche correspondant à l'identifiant spécifié.
/DELETE	Supprime la tâche correspondant à l'identifiant spécifié.
taskid	Identifiant unique de la tâche. Pour consulter les identifiants, utilisez la commande KAVSHELL TASK sans paramètres. Les tâches système peuvent être administrées via les identifiants standard suivants : • scan-computer : analyse complète de l'ordinateur • scan-critical : analyse des secteurs de démarrage, de la mémoire et des objets de démarrage • update-bases : mise à jour des bases antivirus • update-app : mise à jour des modules de l'application • rollback : annulation de la dernière mise à jour des bases antivirus • on-access : protection en temps réel des fichiers • script-checker : analyse en temps réel des scripts.

Exemple:

```
KAVSHELL TASK
KAVSHELL TASK update-app /START /WA:update_ applica-
tion.log
```

```
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/START /WA:task.log
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE
```

6.1.9. Conversion du rapport dans un format plus commode à lire

Syntaxe de la commande :

```
KAVSHELL CONVERT /I:fichier_journal
/O:fichier_journal_prêt
```

/I:fichier_journal	Fichier journal source, constitué des tâches, au format optimalisé. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/O:fichier_journal_prêt	Fichier journal dans un format facile à lire. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace

Exemple:

```
KAVSHELL CONVERT /I:scan.log /O:scan.txt
```

6.1.10. Importation/exportation des paramètres de la configuration

Syntaxe des commandes:

```
KAVSHELL IMPORT fichier_de_configuration
KAVSHELL EXPORT fichier_de_configuration
```

fichier_de_configuration	Nom du fichier depuis lequel ou vers lequel l'importation ou l'exportation des paramètres de Kaspersky Anti-Virus est réalisée.

Exemple:

```
KAVSHELL IMPORT c:\kav50settings.xml
KAVSHELL EXPORT c:\kav50settings.xml
```

6.2. Administration via la console d'administration

En cas d'administration locale de Kaspersky Anti-Virus via la *Console d'administration*, vous travaillez uniquement avec l'objet **Ordinateur local** de l'arborescence de la console.

Ce mode vous permet d'administrer les tâches et les paramètres de l'application Kaspersky Anti-Virus 5.0 for Windows File Servers installée sur l'ordinateur-serveur en question.

6.2.1. Administration des tâches

Une série de tâches système est créée lors de l'installation de l'application. Cette liste reprend les tâches liées à la protection en temps réel (protection des fichiers et analyse des scripts), une série de tâches liées à l'analyse à la demande (analyse de Mon poste de travail, analyse automatique lors du lancement de Kaspersky Anti-Virus) et les tâches de mise à jour (mise à jour des bases antivirus, mise à jour des composants de l'application et annulation de la mise à jour des bases antivirus).

Les tâches liées à la protection en temps réel sont uniques et sont exécutées en arrière-plan. Les tâches système liées à l'analyse à la demande et à la mise à jour des bases antivirus sont programmées.

Vous pouvez lancer les tâches système, configurer les paramètres et les programmer. La suppression de ces tâches, par contre, est impossible.

L'administrateur peut également créer ses propres tâches, les configurer et les administrer.

Afin d'afficher la liste de l'ensemble des tâches de Kaspersky Anti-Virus 5.0 for Windows File Servers :

Cliquez sur l'objet **Ordinateur local** de l'arborescence et sélectionnez le point **Propriétés** du menu contextuel. Ouvrez l'onglet **Tâches** (cf. ill. 2) de la fenêtre **Propriétés de Ordinateur local**.

Les boutons **Ajouter** et **Supprimer** vous permettent de modifier le contenu de la liste. Le bouton **Propriétés** ouvre une fenêtre dans laquelle vous pouvez modifier les propriétés de la tâche sélectionnée.

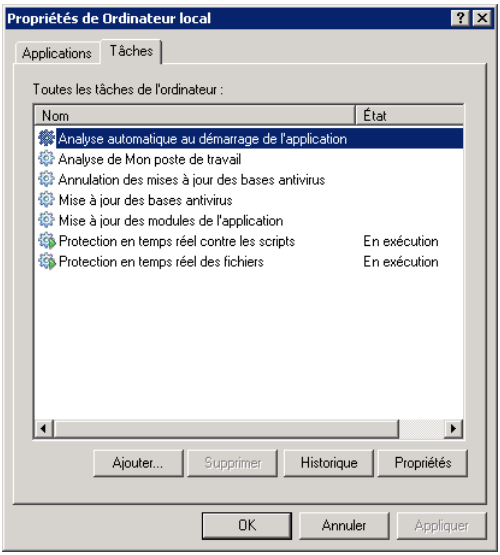

Illustration 2. Liste des tâches de Kaspersky Anti-Virus

6.2.1.1. Lancement et arrêt des tâches

Le lancement d'une tâche sur l'ordinateur est possible uniquement si l'application correspondante est lancée. En cas d'arrêt de l'application, l'exécution des tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide de la commande du menu contextuel ou depuis la fenêtre d'examen des paramètres de la tâche). Vous pouvez suspendre l'exécution d'une tâche puis la reprendre.

Afin de lancer /arrêter/interrompre/reprendre manuellement une tâche :

Sélectionnez la tâche dans la liste (cf. ill. 2), ouvrez le menu contextuel et exécutez la commande :
Démarrer / Stopper / Pause / Continuer.

Les mêmes actions peuvent être réalisées au départ de la fenêtre des paramètres de la tâches, dans l'onglet **Général** (cf. ill. 3) à l'aide des boutons identiques.

6.2.1.2. Examen et modification des paramètres des tâches

Pour vérifier les paramètres d'une tâche et / ou les modifier :

1. Sélectionnez l'objet **Ordinateur local**. Sélectionnez l'élément **Propriétés** dans le menu contextuel.
2. Ouvrez l'onglet **Tâches** (cf. ill. 2) de la fenêtre **Propriétés de Ordinateur local**. L'examen et la modification des paramètres de la tâche sélectionnée s'opèrent dans la fenêtre ouverte après avoir cliqué sur le bouton **Propriétés**.

La fenêtre **Propriétés de la tâche « nom de la tâche »** (cf. ill. 3) contient les onglets suivants : **Général**, **Paramètres**, **Compte**, **Planification, Notification**.

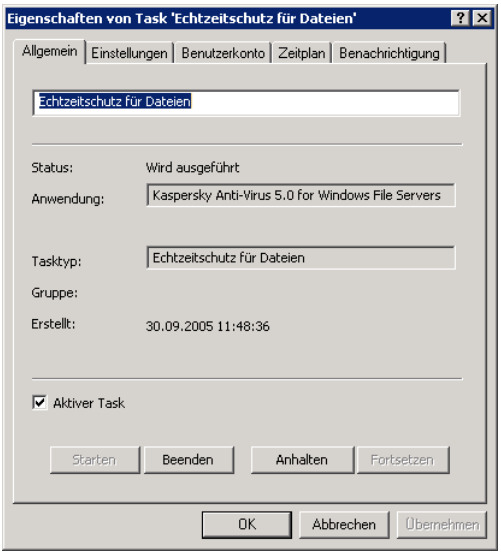

Illustration 3. Onglet **Général**

Tous les onglets (à l'exception de l'onglet **Paramètres** et **Compte**) sont des onglets standard de Kaspersky Administration Kit 5.0. Ils sont décrits en détail dans le manuel de l'administrateur de Kaspersky Administration Kit.

L'onglet **Compte** vous permet de configurer le lancement des tâches sous un autre compte (cf. point 6.2.1.3 à la page. 55). L'onglet **Paramètres** reprend les paramètres spécifiques des tâches de Kaspersky Anti-Virus 5.0 for Windows File Servers. Le contenu de cet onglet varie en fonction du type de tâche sélectionné (la description détaillée est fournie dans les pages ci-après).

6.2.1.2.1. Analyse à la demande

La fenêtre **Paramètres** (cf. ill. 4) vous permet de définir les paramètres des tâches liées à l'analyse à la demande.

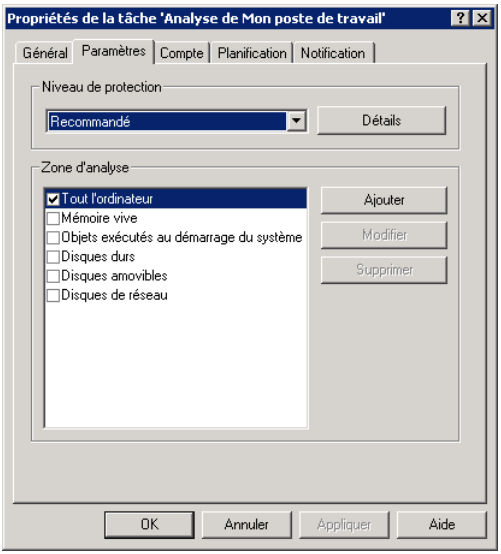

Illustration 4. Configuration de la tâche d'analyse à la demande

Le champ **Zone d'analyse** reprend la liste des objets qui seront analysés lors de l'exécution de la tâche. Il est possible d'ajouter un objet (disque, dossier ou fichier) à analyser dans la fenêtre ouverte après avoir cliqué sur le bouton **Ajouter**. Pour modifier la liste, cliquez sur **Modifier** et pour supprimer certains objets, cliquez sur **Supprimer**.

Sélectionnez dans la liste déroulante **Niveau de protection** l'un des trois niveaux prédéfinis de protection antivirus (cf. 4.1, p. 21)

Le bouton **Détails** ouvre une fenêtre qui présente les paramètres du niveau sélectionné et au départ de laquelle il est possible de procéder à une configuration personnalisée. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**.

La fenêtre de configuration détaillée de la tâche renferme les onglets **Zone d'analyse**, **Action** et **Complémentaire**.

L'onglet **Zone d'analyse** (cf. ill. 5) vous permet de définir les objets à analyser et leur type ainsi que de rédiger la liste des exclusions.

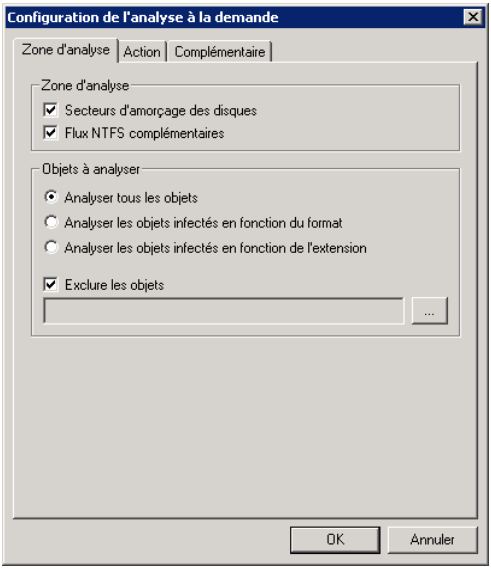

Illustration 5. Onglet **Zone d'analyse**

Vous pouvez définir dans la **Zone d'analyse** les ressources qui seront analysées lors de l'exécution de la tâche. Pour ce faire, cochez la case en regard des objets qui doivent être inclus dans l'analyse.

Sélectionnez, dans le champ **Objets à analyser**, les types d'objets qui seront soumis à l'analyse :

- *Analyser tous les objets* : analyse tous les objets du système de fichiers.
- *Analyser les objets infectés en fonction du format* : analyse porte tous les objets qui présentent un risque d'infection. Le contenu interne du fichier est pris en compte pour l'analyse, à savoir : l'identificateur du format dans son entête.

- *Analyser les objets infectés en fonction de l'extension*: l'analyse porte sur tous les objets qui présentent un risque d'infection. L'extension du fichier est prise en compte pour l'analyse.

Dans la section **Exclure les objets**, vous pouvez définir les exclusions pour l'analyse à la demande. Afin d'ajouter de nouvelles exclusions, cochez la case **Exclure les objets**. Cliquez sur le bouton à droite du champ et dans la fenêtre qui s'ouvre, modifiez la liste des exclusions à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

Vous pouvez définir des masques pour les objets à exclure : Voici quelques exemples de masques admis :

- Masques sans chemin :
    - ***.exe** : tous les fichiers avec le masque **.exe*
    - ***.exe?** : tous les fichiers avec le masque **.ex?*
    - **test** : tous les fichiers portant le nom *test*
- Masques avec un chemin absolu :
    - **C:\dir*.*** : tous les fichiers du répertoire C:\dir\
    - **C:\dir*.exe** : tous les fichiers avec le masque *.exe du répertoire *C:\dir*\
    - **C:\dir*.ex?** tous les fichiers avec le masque *.ex ? du répertoire *C:\dir*\
    - **C:\dir\test** : uniquement le fichier C:\dir\test
    - **C:\dir**\: tous les fichiers du répertoire C:\dir\ et de ses sous-répertoires
- Masques avec un chemin relatif :
    - **dir*.*** : tous les fichiers dans tous les répertoires *dir*\
    - **dir\test** : tous les fichiers test dans tous les répertoires *dir*\
    - **dir*.exe** : tous les fichiers correspondant au masque **.exe* dans tous les répertoires *dir*\
    - **dir*.ex?** : tous les fichiers correspondant au masque **.ex?* dans tous les répertoires *dir*\
    - **dir*.*** : tous les fichiers dans tous les répertoires dir\ et leurs sous-répertoires

Il est interdit de saisir un masque contenant uniquement le caractère **?** et *.

L'onglet **Action** (cf. ill. 6) permet de définir l'action qui serales actions qui seront exécutées suite à la découverte d'un objet infecté ou suspect :

- *Réparer, supprimer si la réparation est impossible* : répare l'objet infecté. Si l'objet ne peut être réparé, il sera supprimé.
- *Mettre en quarantaine* : place l'objet suspect dans le dossier de quarantaine en vue d'une analyse ultérieure à l'aide des bases antivirus mises à jour ou en vue d'une restauration.
- *Supprimer* : supprime l'objet infecté ou suspect. Le choix de cette action entraîne la création d'une copie de sauvegarde de l'objet qui sera placée dans le répertoire de sauvegarde. Cette copie pourra servir à la restauration du fichier ou pourra être envoyée à Kaspersky Lab pour examen.
- *Consigner les informations dans le rapport* : aucune action n'est exécutée sur les objets suspects ou infectés. Seule leur découverte est consignée dans le rapport (pour de plus amples informations sur le service de réception des rapports, consultez le point 6.2.2.8 à la page 71). Ce mode n'est pas recommandé car il ne débarrasse pas votre ordinateur des objets infectés et suspects, ce qui conduira inévitablement à l'infection de celui-ci.

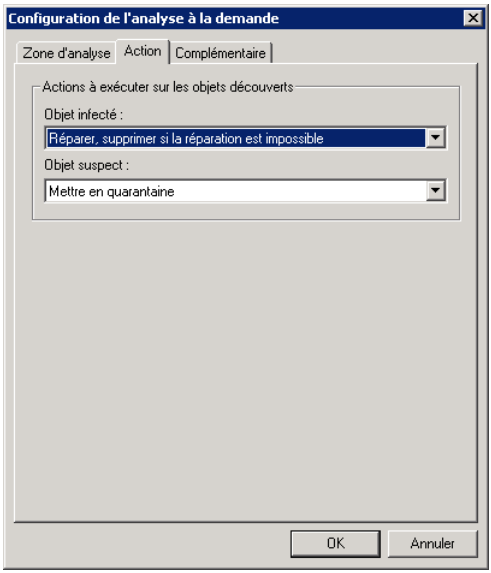

Illustration 6. Onglet **Action**

L'onglet **Complémentaire** (cf. ill. 7) vous permet d'activer/désactiver l'analyse de différents types de fichiers complexes, d'exclure de l'analyse les riskwares de confiance et d'imposer certaines limites à l'analyse.

Pour exclure de l'analyse les riskwares autorisés sur votre ordinateur, cochez la case ☑ **Ne pas détecter les riskwares de confiance**(Pour de plus amples informations, consultez le point 6.2.2.3 à la page 63).

Saisissez dans le champ **Arrêter si l'analyse dure plus de… s** la durée maximale (en secondes) au-delà de laquelle l'analyse sera interrompue. Saisissez dans le champ **Analyser les objets composés d'une taille max. de, Mo** la taille maximale des objets complexes à analyser.

- ☑ **Utiliser la technologie iChecker™**, **Utiliser la technologie iStreams™** : utilise les technologies permettant d'accélérer l'analyse antivirus.

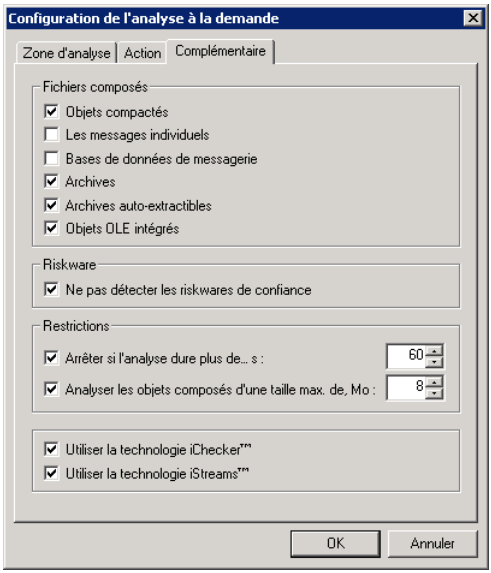

Illustration 7. Onglet **Complémantaire**

6.2.1.2.2. Protection en temps réel des fichiers

L'onglet **Paramètres** (cf. Illustration 8) vous permet de définir les paramètres des tâches liées à la protection en temps réel des objets du système de fichiers.

Le champ **Zone d'analyse** reprend la liste des objets qui seront analysés lors de l'exécution de la tâche. Il est possible d'ajouter un objet (disque, dossier ou fichier) à analyser dans la fenêtre qui s'ouvre après avoir cliqué sur **Ajouter**. Pour modifier la liste, cliquez sur **Modifier** et pour supprimer certains objets de l'analyse, cliquez sur **Supprimer**.

Sélectionnez dans la liste déroulante **Niveau de protection** l'un des trois niveaux prédéfinis de protection antivirus (cf. 4.1, p. 21).

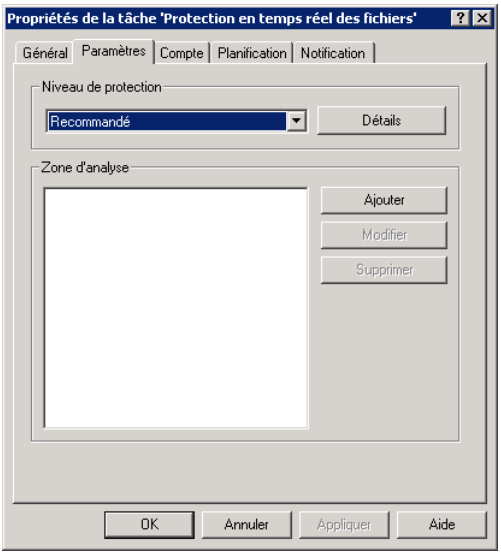

Illustration 8. Configuration de la tâche liée à la protection en temps réel des fichiers

Le bouton **Détails** ouvre la fenêtre des paramètres détaillés dans laquelle vous pouvez examiner les paramètres correspondant au niveau sélectionné et procéder à une configuration personnalisée. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**.

La fenêtre de configuration détaillée renferme les onglets **Zone de protection**, **Action** et **Complémentaire**.

L'onglet **Zone de protection** (cf. ill. 9) vous permet de définir les objets à analyser et de rédiger la liste des exclusions. Les paramètres repris sur cet onglet sont identiques à ceux de l'onglet du même nom dans le cadre de l'analyse à la demande (pour de plus amples informations, consultez le point 6.2.1.2.1 à la page 39).

L'analyse des secteurs de démarrage s'opère uniquement lorsque les cases suivantes sont cochées : **Secteurs d'amorçage des disques/ Disques durs** ou **Secteurs d'amorçages des disques / Disques amovibles**.

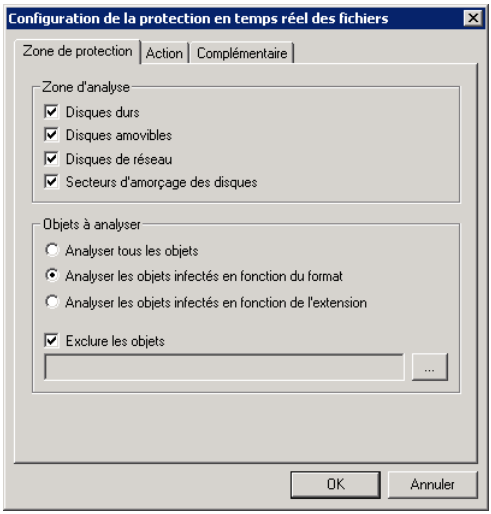

Illustration 9. Onglet **Zone de protection**

L'onglet **Action** (cf. ill. 10) permet de définir les actions qui seront exécutées suite à la découverte d'un objet infecté ou suspect :

- *Interdire l'accès et réparer, supprimer si la réparation est impossible* : répare l'objet à l'aide des définitions des bases antivirus. Si l'objet ne peut être réparé, il sera supprimé.
- *Interdire l'accès et mettre en quarantaine* : place l'objet suspect en quarantaine en vue d'une analyse ultérieure à l'aide des bases antivirus mises à jour ou en vue d'une restauration.
- *Interdire l'accès et supprimer* : supprime l'objet. Le choix de cette action entraîne la création d'une copie de sauvegarde de l'objet qui sera placée dans le répertoire de sauvegarde. Cette copie pourra servir à la restauration du fichier ou pourra être envoyée à Kaspersky Lab pour examen.
- *Interdire l'accès* : empêche les applications d'accéder aux objets suspects ou infectés.

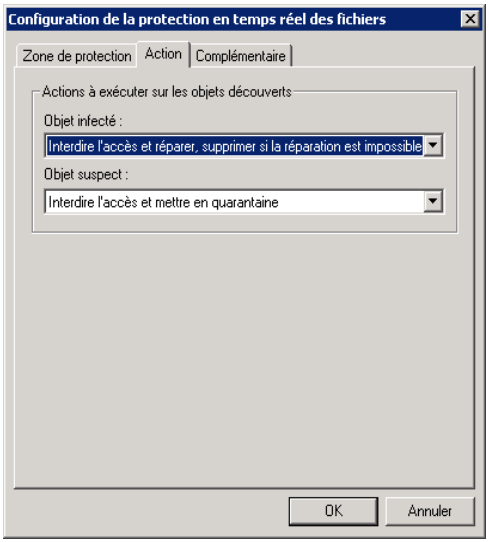

Illustration 10. Onglet **Action**

L'onglet **Complémentaire** (cf. ill. 11) vous permet d'activer/désactiver l'analyse de différents types de fichiers complexes d'exclure de l'analyse les riskwares de confiance et d'imposer certaines limites à l'analyse.

Pour exclure de l'analyse les riskwares autorisés sur votre ordinateur, cochez la case ☑ **Ne pas détecter les riskwares de confiance**(Pour de plus amples informations, consultez le point 6.2.2.3 à la page 63).

Saisissez dans le champ **Arrêter si l'analyse dure plus de… s** la durée maximale (en secondes) au-delà de laquelle l'analyse sera interrompue.

- ☑ **Utiliser la technologie iChecker™**, **Utiliser la technologie iStreams™** : utilise les technologies permettant d'accélérer l'analyse antivirus.

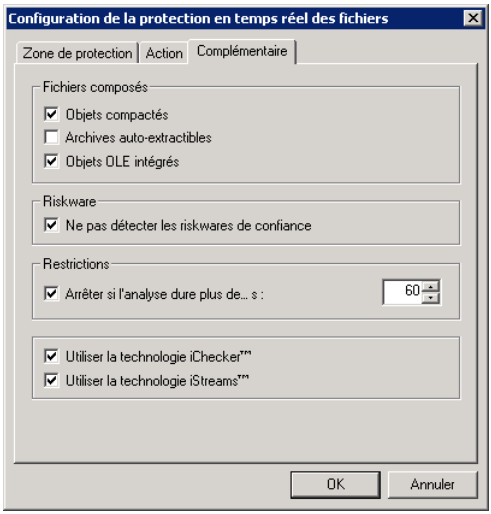

Illustration 11. Onglet **Complémentaire**

6.2.1.2.3. Protection en temps réel contre les scripts

L'onglet **Paramètres** vous permet de définir les paramètres des tâches liées à la protection en temps réel contre les scripts VBScript et Java Script dangereux.

La sélection du niveau de protection et l'ouverture de la fenêtre de configuration détaillée sont identiques à la protection en temps réel des fichiers (cf. point 6.2.1.2.2, p. 44).

Dans la fenêtre de configuration détaillée (cf. ill. 12), l'action **Bloquer l'exécution** est sélectionnée pour tous les niveaux de protection. En cas de sélection de l'action **Autoriser l'exécution**, le niveau de protection deviendra **Paramètres utilisateur**.

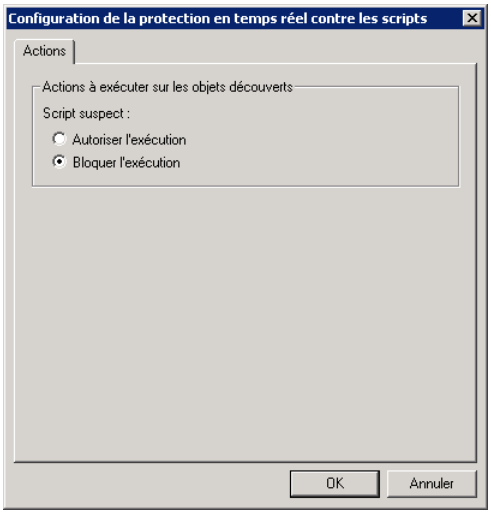

Illustration 12. Onglet **Actions**

6.2.1.2.4. Mise à jour des bases antivirus et des composants du logiciel

Les fenêtres **Paramètres** (cf. ill. 13) pour la mise à jour des bases antivirus et des modules de l'application sont identiques. La tâche liée au rejet de la mise à jour des bases antivirus ne dispose pas de paramètres particuliers.

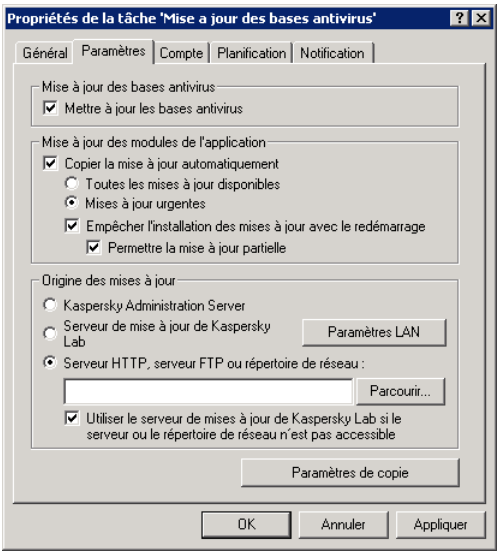

Illustration 13. Configuration de la tâche liée à la mise à jour des bases antivirus et des composants de l'application

- **Mettre à jour les bases antivirus** : obtenir la mise à jour des bases antivirus.
- **Copier la mise à jour automatiquement** : télécharger et installer automatiquement les mises à jour des modules de l'application :
  - **Toutes les mises à jour disponibles** : toutes les mises à jour de l'application disponibles.
  - **Mises à jour urgentes** : uniquement les mises à jour urgentes (critiques) des modules de l'application.

Empêcher l'installation des mises à jour avec le redémarrage. Si cette case n'est pas cochée, l'ordinateur/serveur sera redémarré automatiquement après le téléchargement et l'installation de mises à jour nécessitant le redémarrage.

Lorsque la case est cochée et que le redémarrage n'est pas possible, l'installation des mises à jour dépend du statut de la case **Permettre la mise à jour partielle**.

- *La case n'est pas cochée :* les mises à jour seront copiées dans le dossier des mises à jour mais elles ne seront pas installées.
- *La case est cochée* : les mises à jour seront copiées dans le dossier des mises à jour. Les correctifs repris dans cet ensemble seront classés dans

un certain ordre. Lors de la mise à jour, tous les fichiers seront installés à partir du début de la chaîne jusqu'au premier fichier qui requiert le redémarrage de l'ordinateur.

Dans la section **Origine des mises à jour**, définissez l'origine de la mise à jour et ses paramètres :

- **Kaspersky Administration Server** : emplacement central, sur le serveur d'administration de Kaspersky Administration Kit, reprenant les mises à jour.
- **Serveur de mise à jour de Kaspersky Lab** : serveurs HTTP ou FTP de Kaspersky Lab où les nouvelles mises à jour sont publiées quotidiennement.
- **Serveur HTTP, serveur FTP ou répertoire de réseau** : serveur ou répertoire local dans lequel l'administrateur de la sécurité place les mises à jour téléchargées sur Internet. Saisissez dans le champ en-dessous le chemin d'accès au répertoire de mise à jour.

En cas d'erreur lors de la mise à jour via le serveur d'administration de Kaspersky Administration Kit ou via le serveur ou le répertoire local, vous pouvez configurer la mise jour automatique au départ des serveurs Internet de Kaspersky Lab. Pour ce faire, cochez la case ☑ **Utiliser le serveur de mises à jour de Kaspersky Lab si le serveur ou le répertoire de réseau n'est pas accessible**.

Cliquez sur **Paramètres LAN** (cf. ill. 14) afin d'ouvrir la fenêtre permettant la configuration de la connexion au réseau.

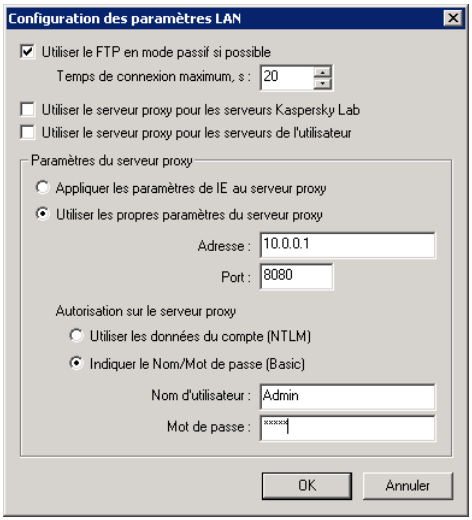

Illustration 14. Configuration des paramètres du réseau

- **Utiliser le FTP en mode passif si possible**. Il est recommandé de cocher cette case si votre serveur est équipé d'un pare-feu et que vous n'êtes pas en mesure de vous connecter au site FTP en mode actif.

Saisissez dans le champ **Temps de connexion maximum, s**. la durée maximale de la connexion au serveur de mises à jour de Kaspersky Lab.

Si l'accès à la source de la mise à jour s'opère via un serveur proxy, activez l'utilisation du serveur proxy et configurez les paramètres de connexion :

- **Utiliser le serveur proxy pour les serveurs Kaspersky Lab** : configure la réception des mises à jour de Kaspersky Lab via le serveur proxy.
- **Utiliser le serveur proxy pour les serveurs de l'utilisateur:** configure la réception de la mise à jour depuis un serveur/répertoire local via le serveur proxy.
  - **Appliquer les paramètres de IE au serveur proxy** : les paramètres de Microsoft Internet Explorer sont utilisés par le proxy.
  - **Utiliser les propres paramètres du serveur proxy**. Si vous avez décidé d'utiliser les propres paramètres du proxy, saisissez les informations requises dans les champs **Adresse** et **Port**.

Dans la section **Autorisation sur le serveur proxy**, sélectionnez le type d'autorisation utilisé : **NTLM** ou **Basic**. Si vous choisissez le mode Basic, vous devrez saisir un **Nom d'utilisateur** ainsi qu'un **Mot de passe**.

En cliquant sur **Paramètres de copie** vous ouvrirez une fenêtre (cf. ill. 15) vous permettant de configurer le service de copie des mises à jour. Ce service vous permet de conserver, dans un répertoire local, les mises à jour des bases antivirus et des modules logiciels de l'application obtenues sur le serveur de Kaspersky Lab afin de les distribuer aux autres ordinateurs du réseau et de réduire ainsi le trafic de données.

Cochez la case ☑ **Copier dans la source locale de la mise à jour** afin d'activer le service. Précisez ensuite le type de mise à jour qui sera placé dans le répertoire source local :

- ☑ **Copier la mise à jour des bases antivirus** : place les mises à jour des bases antivirus dans le répertoire.
- ☑ **Copier les mises à jour des modules de l'application** : place les mises à jour des modules de l'application dans le répertoire :
  - ◉ **Toutes les mises à jour disponibles** : toutes les mises à jour de l'application.
  - ◉ **Les mises à jour urgentes** : uniquement les mises à jour urgentes (critiques) des modules de l'application.

De plus, vous pouvez sélectionner le mode de copie de la mise à jour :

- *complet*, : copie les bases antivirus, les bases de filtrage en fonction du contenu et la mise à jour des modules de tous les logiciels de Kaspersky Lab. Pour choisir la mise à jour complète, cochez la case ☑ **Copier la mise à jour pour toutes les applications**.
- *Partiel :* copie les bases antivirus et la mise à jour des modules uniquement pour Kaspersky Anti-Virus 5.0 for Windows Workstations et Kaspersky Anti-Virus for Windows File Servers. Pour sélectionner ce mode, désélectionnez la case **Copier la mise à jour pour toutes les applications** (cette case est cochée par défaut).

Saisissez dans le champ **Répertoire pour la source locale** le chemin d'accès au répertoire.

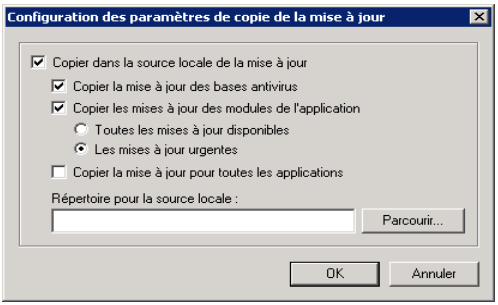

Illustration 15. Configuration du service de copie des mises à jour

Afin de permettre aux autres ordinateurs du réseau d'accéder au répertoire pour la source locale, réalisez les opérations suivantes :

1. Activez l'accès total au répertoire local où sont stockées les mises à jour.
2. Sur l'ordinateur client, indiquez le chemin d'accès au répertoire pour la source locale dans les paramètres de la mise à jour des bases antivirus et des modules de l'application.

6.2.1.2.5. Activation de la clé de licence

Cette tâche est une tâche système. Elle peut être définie par l'administrateur pour ajouter une nouvelle clé de licence.

Dans la fenêtre **Paramètres** (cf. ill. 16) de la tâche d'ajout d'une clé de licence, indiquez le chemin d'accès au fichier à l'aide du bouton **Parcourir**.

Afin que la clé ajoutée devienne la clé actuelle, cochez la case **Utiliser en tant que clé de licence actuelle**.

Si la clé installée est une clé de réserve, il n'est pas nécessaire de cocher cette case. La clé de licence de réserve prendra la place de la clé actuelle dès que cette dernière sera arrivée à l'échéance.

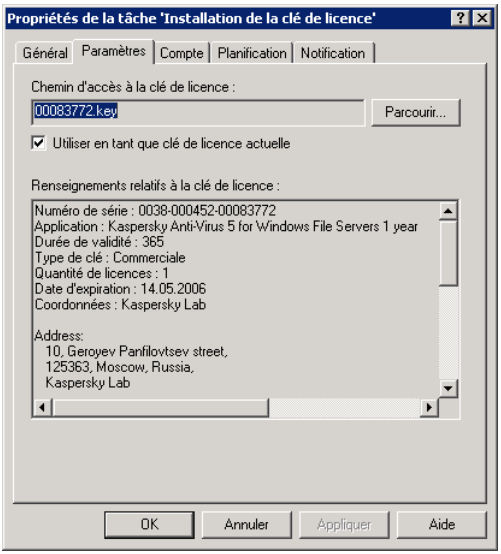

Illustration 16. Ajout d'une clé de licence

6.2.1.3. Lancement d'une tâche au nom d'un utilisateur sélectionné

Kaspersky Anti-Virus offre la possibilité de lancer une tâche utilisateur au nom d'un autre utilisateur (représentation).

Cette option est désactivée par défaut et les tâches sont exécutées sous le compte ouvert. Lorsque cette option est activée, l'administrateur saisit les données du compte jouissant des privilèges adéquats pour accéder à l'objet : par exemple, pour l'analyse à la demande, il est indispensable de jouir du privilège d'accès à l'objet et pour la mise à jour, il faut pouvoir accéder au répertoire local où se trouvent les mises à jour ou être autorisé à utiliser le serveur proxy.

Ceci évite les erreurs pendant l'exécution de l'analyse à la demande ou des mises à jour qui surviennent lorsque l'utilisateur qui lance la tâche ne jouit pas des privilèges adéquats.

La configuration de l'exécution des tâches au nom d'un autre compte s'opère dans l'onglet **Compte** (cf. ill.17).

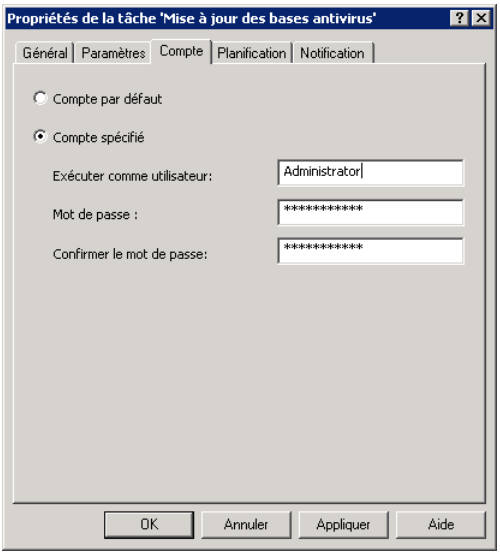

Illustration 17. Onglet **Compte**

- **Compte par défaut**. Utilise le compte actuel.
- **Compte specifié**. Saisie des paramètres d'un autre compte. Une fois que vous aurez choisi cette variante, remplissez les champs **Exécuter comme utilisateur**, **Mot de passe** et **Confirmer le mot de passe**.

6.2.1.4. Création d'une tâche

Pour créer une tâche, exécutez les opérations suivantes :

1. Sélectionnez l'objet **Ordinateur local** dans l'arborescence de la console. Sélectionnez l'élément **Propriétés** dans le menu contextuel.
2. Ouvrez l'onglet **Tâches** (cf. ill. 2) où sont reprises les tâches de l'application.
3. Cliquez sur **Ajouter**. Cette action entraîne l'ouverture de la fenêtre de création d'une nouvelle tâche. L'interface se présente sous la forme d'un Assistant Microsoft Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur

Terminer. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Etape 1. Saisie des données générales sur la tâche

Le première fenêtre de l'Assistant est destinée à la saisie d'informations. il faut saisir ici le nom de la tâche (champ **Nom**).

Etape 2. Sélection de l'application et du type de tâche

Sélectionnez **Kaspersky Anti-Virus 5.0 for Windows File Servers** dans la liste des applications de Kaspersky Lab installées sur l'ordinateur**.** La sélection du type de tâche s'opère dans la liste suivante. Pour Kaspersky Anti-Virus 5.0 for Windows File Servers, vous avez le choix entre les tâches suivantes :

- **Mise à jour des bases antivirus et des modules de l'application**
- **Annulation de la mise à jour des bases antivirus**
- **Analyse à la demande**
- **Installation de la clé de licence**

Etape 3. Configuration des paramètres du type de tâche sélectionné

Le contenu des fenêtres suivantes varie en fonction du type de tâche sélectionné à l'étape précédente. Pour obtenir de plus amples informations sur les paramètres de chaque type de tâche, consultez le point 6.2.1.2 à la page 38.

L'annulation de la mise à jour ne possède pas de paramètres propres.

Etape 4. Configuration du lancement d'une tâche au nom d'un utilisateur sélectionné

Cette étape (cf. Ill. 18) vous offre la possibilité de configurer le lancement de tâches définies sous un autre compte jouissant des privilèges d'accès adéquats à l'objet à analyser ou à la source de la mise à jour (pour de plus amples informations, consultez le point 6.2.1.3 à la page 55).

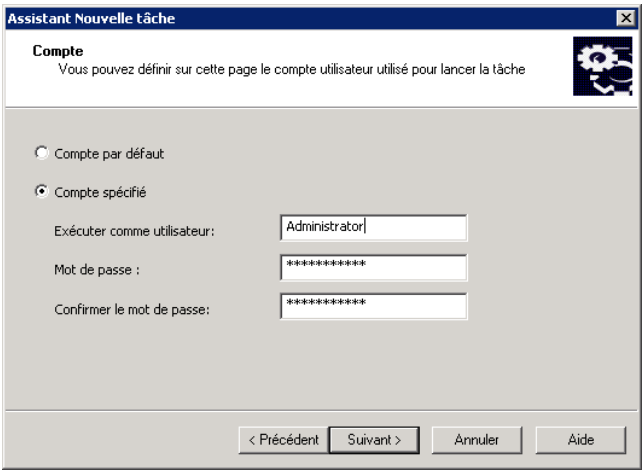

Illustration 18. Configuration du lancement d'une tâche au nom d'un autre compte

Etape 5. Programmation de la tâche

Une fois que vous aurez configuré le type de tâche sélectionné, l'Assistant passera à la fenêtre **Paramètres de programmation de la tâche** (cf. ill. 19) où il est indispensable de définir l'horaire selon lequel la tâche sera exécutée.

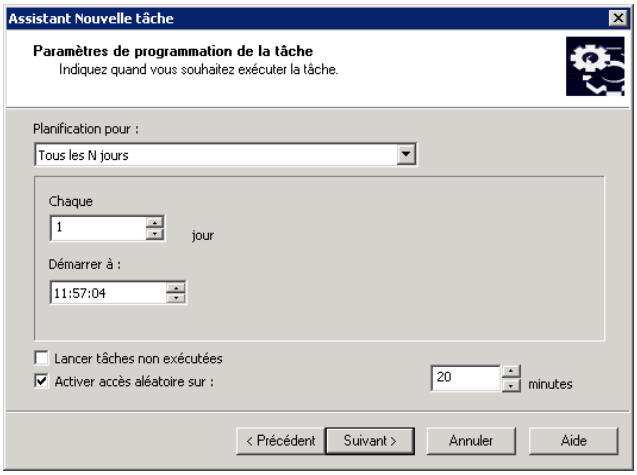

Illustration 19. Paramètres de programmation d'une tâche

Sélectionnez dans la liste déroulante **Planification pour** la fréquence d'exécution de la tâche. Vous avez le choix entre : *Toutes les N heures, Tous les N jours, Toutes les N semaines, Mode manuel, Au lancement de l'application.* La partie centrale avec les champs de saisie des données changera en fonction de la fréquence sélectionnée.

Seul le lancement manuel est possible pour l'annulation de la mise à jour des bases antivirus et pour l'activation de la clé de licence.

Pour obtenir de plus amples informations sur la programmation de l'exécution automatique des tâches, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

Etape 6. Fin de la création d'une tâche

La dernière étape de l'Assistant vous informe de la réussite de la création de la tâche.

6.2.2. Administration de l'application via les paramètres

Afin de consulter ou de modifier les paramètres de l'application :

1. Sélectionnez l'objet **Ordinateur local** dans l'arborescence de la console. Sélectionnez l'élément **Propriétés** dans le menu contextuel.
2. Ouvrez l'onglet **Applications** (cf. ill. 20) de la fenêtre **Propriétés de Ordinateur local**. Cet onglet reprend la liste des applications de Kaspersky Lab installées sur l'ordinateur.

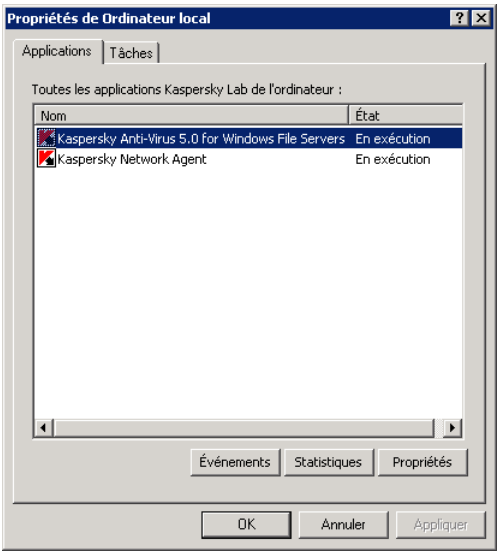

Illustration 20. Liste des applications de Kaspersky Lab

3. Sélectionnez l'application **Kaspersky Anti-Virus 5.0 for Windows File Servers.** En bas de cette liste se trouvent les boutons d'administration (**Evénements**, **Statistiques** et **Propriétés)** qui remplissent les fonctions suivantes :

   - Examen de la liste des événements survenus sur l'ordinateur pendant l'utilisation de l'application (pour de plus amples informations sur l'utilisation des rapports, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0).
   - Examen des statistiques actuelles sur l'activité de l'application.
   - Configuration des paramètres de l'application. En cliquant sur **Propriétés**, vous ouvrez une fenêtre contenant les onglets suivants : **Général, Complémentaires, Riskware, Processus de confiance, Quarantaine, Dossier de sauvegarde, Objets des dossiers, Licences** et **Traitement des événements**. Ces onglets sont décrits en détail ci-après.

6.2.2.1. Informations générales sur l'application

L'onglet **Général** (cf. ill. 21) reprend des informations d'ordre général sur Kaspersky Anti-Virus 5.0 for Windows File Server et vous permet de lancer ou d'arrêter l'application.

La partie supérieure de la fenêtre indique le nom de l'application, la version, la date d'installation, le statut (application lancée ou arrêtée sur l'ordinateur local) et l'état des bases antivirus.

Vous pouvez lancer/arrêter l'application à l'aide des boutons prévus à cet effet.

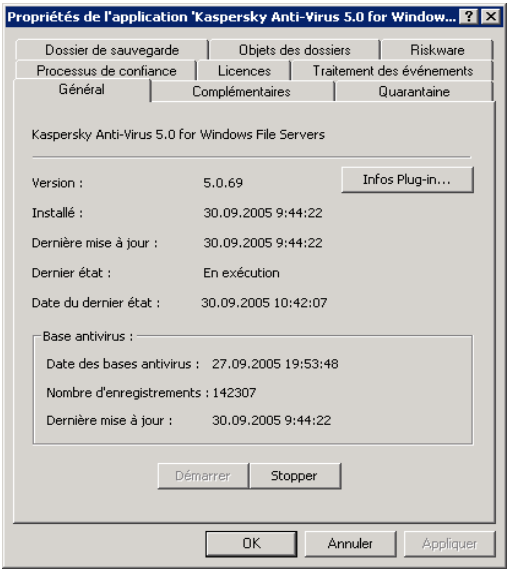

Illustration 21. Fenêtre des propriétés de l'application. Onglet **Général**

6.2.2.2. Configuration des paramètres supplémentaires de l'application

L'onglet **Complémentaires** (cf. ill. 22) reprend la configuration des paramètres de service :

Cochez la case ☑ **Lancer le logiciel après le redémarrage de l'ordinateur** pour autoriser le démarrage automatique de Kaspersky Anti-Virus lors du démarrage du système d'exploitation.

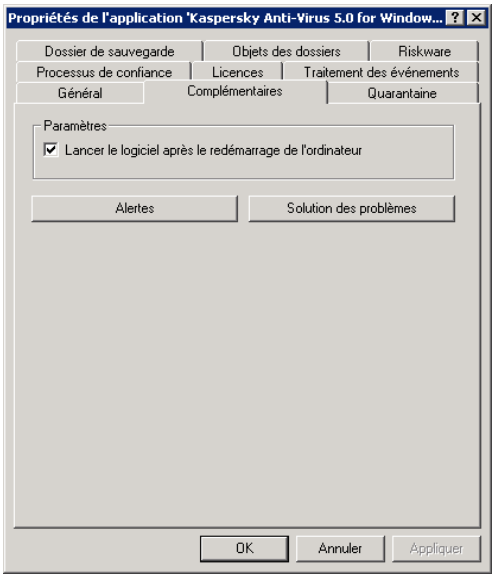

Illustration 22. Onglet **Complémentaires**

Dans la fenêtre (cf. ill. 23), qui s'ouvre si vous cliquez sur **Solution des problèmes**, vous pouvez également régler la charge du système lors de l'exécution de l'analyse à la demande. Pour ce faire, cochez la case ☑ **Définir une limite sur la charge du système** et à l'aide du curseur ou du champ situé à droite, indiquez a valeur limite (en pour cent). La valeur optimale, obtenue dans le cadre de tests, est de 30%. Une réduction de la valeur se traduit par une durée d'analyse plus longue et un transfert des ressources aux applications de l'utilisateur.

Afin d'augmenter la vitesse de l'analyse antivirus, il est possible de lancer simultanément plusieurs exemplaires du moteur antivirus. Ce nombre est défini automatiquement pendant l'installation sur la base des informations relatives au nombre de processeurs de l'ordinateur.

Afin de modifier le nombre d'exemplaires du moteur antivirus exécutés, modifiez la valeur du champ **Exemplaires du moteur antivirus**. Le nombre maximum d'exemplaires qui peuvent être lancés simultanément ne peut pas dépasser le nombre de processeurs de l'ordinateur.

Ce paramètres est utilisé uniquement en cas de configuration de l'application sur un ordinateur particulier. Il est impossible d'utiliser ce paramètre lors de la configuration d'une stratégie car les ordinateurs repris dans le groupe du réseau logique peuvent avoir des configurations matérielles différentes.

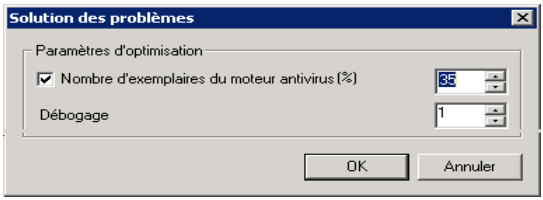

Illustration 23. Fenêtre **Solution des problèmes**

La fenêtre (cf. ill. 24) qui s'ouvre en cliquant sur le bouton **Alertes** vous permet de configurer les conditions de réception des alertes relatives à la mise à jour des bases antivirus et à l'analyse complète de l'ordinateur. Pour chacune de ces tâches, il existe deux niveaux d'événements : **Avertissement** et **Evénement critique**.

Dans le champ situé à droite de chacun des événements, définissez la période (en jours) après laquelle la notification correspondante sera envoyée chaque jour au démarrage de l'application. Cette période débute à partir de la date de la dernière exécution de la tâche en question.

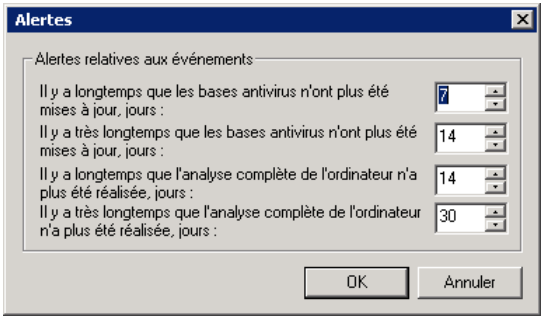

Illustration 24. Onglet **Alertes**

6.2.2.3. Configuration des paramètres de découverte des riskwares

Kaspersky Anti-Virus identifie les riskwares exécutés sur l'ordinateur ou téléchargés depuis Internet, de même que ceux qui se trouvent sur les disques amovibles ou les disques durs.

Les riskwares sont des logiciels qui peuvent nuire à votre ordinateur : il peut s'agir de programmes légaux contenant des failles et des erreurs, des programmes d'administration à distance, de programme enregistrant les frappes

de clavier, de programmes servant à déchiffrer les mots de passe ou de programmes réalisant des connexions à des sites payant, etc.

De tels programmes ne sont pas considérés comme des virus. Ils sont néanmoins scindés en plusieurs familles : adware, jokeware, spyware, riskware, hack tools etc. (pour de plus amples informations sur les riskwares découverts par Kaspersky Anti-Virus, consultez l'encyclopédie des virus sur http://www.viruslist.com/fr). Kaspersky Anti-Virus peut découvrir ces programmes grâce à l'utilisation d'un large éventail de bases antivirus.

La recherche des riskware est activée par défaut. En mode protection en temps réel, Kaspersky Anti-Virus bloque l'exécution de tout riskware dès que celui est découvert et consigne l'incident dans le rapport. En mode analyse à la demande, il ignore le riskware et consigne les informations dans le rapport.

Pour modifier les critères d'identification des riskwares, ouvrez la fenêtre **Riskwares** (cf. ill. 25). Vous pourrez également y constituer la liste des riskwares de confiance qui pourront être utilisés sur les ordinateurs du réseau.

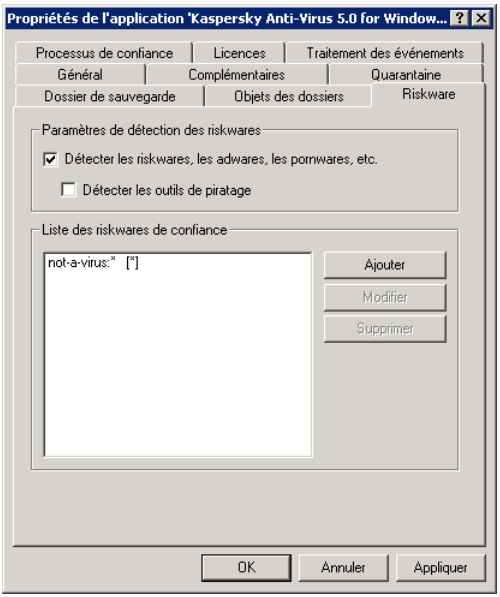

Illustration 25. Riskwares

Afin que Kaspersky Anti-Virus puisse analyser les fichiers d'un programme et déterminer s'ils appartiennent à une catégorie de riskware, cochez la case ☑ **Détecter les riskwares, les adwares, les pornwares, etc**.

Pour découvrir les programmes d'attaque informatique, cochez la case ☑ **Détecter les outils de piratage**.

Dans le champ **Liste des riskwares de confiance**, composez la liste des exclusions de l'analyse des riskwares. Les programmes repris dans cette liste sont autorisés et peuvent être exécutés sur l'ordinateur. Les boutons situés à droite permettent de compléter ou de modifier la liste.

En cliquant sur **Ajouter/Modifier**, vous ouvrez une nouvelle fenêtre (cf. ill. 26). Pour ajouter un programme ou modifier un programme déjà repris, remplissez l'un des champs de la fenêtre.

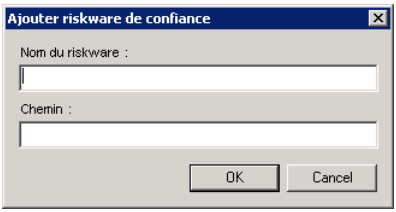

Illustration 26. Ajout d'un riskware de confiance

Dans le champ **Chemin**, indiquez le chemin d'accès au répertoire où sont stockés les fichiers du programme. Vous vous pouvez saisir, dans le champ **Nom du riskware** :

- Nom complet du programme, tel que repris dans l'encyclopédie des virus sur www.viruslist.com (ex. **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**);
- Nom du programme à l'aide d'un masque
  - **not-a-virus*** – exclut de l'analyse les riskwares licites, ainsi que les jokewares;
  - ***Riskware.*** – exclut de l'analyse tous les riskware ;
  - ***RemoteAdmin.*** – exclut de l'analyse toutes les versions des programmes d'administration à distance.

Les caractères * et **?**peuvent être repris dans le masque

Au lieu du masque du riskware, il est possible de saisir le chemin d'accès au répertoire où le masque saisi ne serait pas découvert.

Ainsi, en saisissant à la fois le masque "*Riskware.*" et le chemin d'accès "C:\Program Files\", les riskwares des sous-répertoires du répertoire "C:\Program Files\" seront ignorés.

6.2.2.4. Contrôle de l'activité des processus logiciels

Kaspersky Anti-Virus vous permet de constituer une liste de processus logiciels dont l'activité ne sera pas contrôlée par le logiciel antivirus.

Vous estimez par exemple que les objets utilisés par le **Bloc-Notes** de Windows sont inoffensifs et ne doivent pas être soumis à la protection en temps réel. En d'autres termes, vous faites confiance aux processus de ce logiciel. Pour exclure les objets utilisés par ce programme de l'analyse, ajoutez le **Bloc-Notes** à la liste des processus de confiance.

La constitution de la liste des processus de confiance s'opère dans l'onglet **Processus de confiance** (cf. ill. 27).

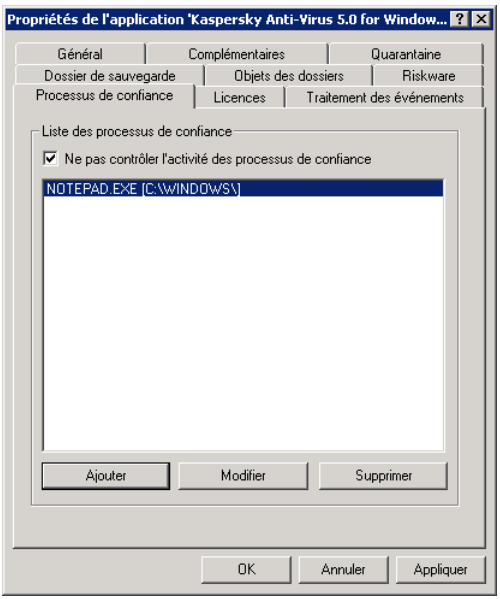

Illustration 27. Onglet **Processus de confiance**

Kaspersky Anti-Virus analyse par défaut les objets ouverts, exécutés ou enregistrés par n'importe quel processus logiciel. Pour désactiver le contrôle de l'activité des processus de confiance sur les fichiers, cochez la case ☑ **Ne pas contrôler l'activité des processus de confiance**.

Composez la liste des processus dont les objets ne seront pas analysés lors de l'exécution dans la section **Liste des processus de confiance**. Utilisez les boutons situés à droite de la liste pour la modifier ou l'allonger.

Une nouvelle fenêtre s'ouvre lorsque vous cliquez sur **Ajouter/Modifier** (cf. ill. 28).

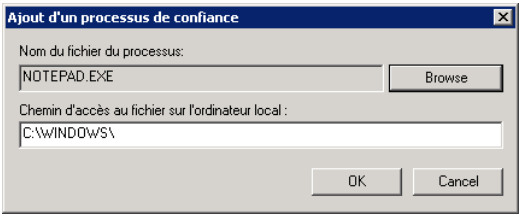

Illustration 28. Ajout d'un processus de confiance

Vous pouvez choisir le nom du processus à l'aide du bouton **Parcourir**. Lorsque le nom est sélectionné, Kaspersky Anti-Virus enregistre les attributs internes du fichier du processus grâce auxquels il pourra identifier le processus comme un processus de confiance lors de l'analyse antivirus.

Le chemin d'accès au fichier est saisi automatiquement lors de la sélection du nom. Vous pouvez le modifier manuellement ou saisir un chemin sous la forme d'un masque

En cas d'administration à distance via la *Console d'administration* il faut indiquer le chemin d'accès au processus sur l'ordinateur distant.

6.2.2.5. Configuration des paramètres de *Quarantaine* et *Dossier de sauvegarde*

Kaspersky Anti-Virus permet d'isoler les objets suspects dans un dossier de quarantaine et de conserver une copie des objets infectés avant de les réparer ou de les supprimer.

En cas de découverte d'un objet suspect, l'application l'isole dans le répertoire de quarantaine. Là, il pourra être à nouveau analysé, supprimé ou restauré.

La copie de sauvegarde est créée lors de la première suppression ou réparation après la découverte de l'objet. Elle est placée dans le dossier de sauvegarde. L'objet pourra être restauré s'il renferme des informations capitales.

Les onglets **Quarantaine** (cf. ill. 29) et **Dossier de sauvegarde** permettent la configuration des dossiers correspondant.

Les paramètres sont identiques pour les deux dossiers. Pour cette raison, ce manuel mentionne uniquement les paramètres du dossier de quarantaine.

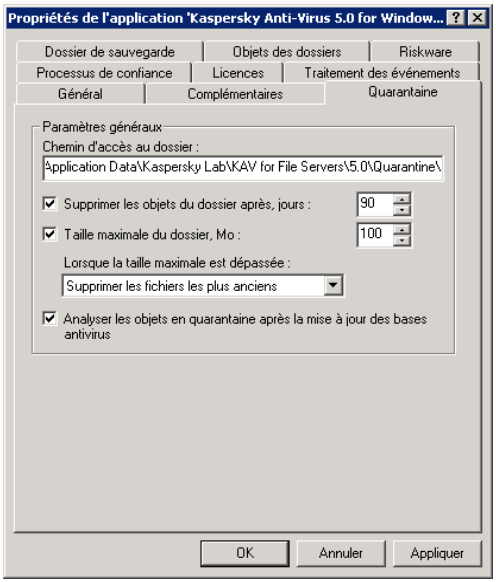

Illustration 29. Onglet **Quarantaine**

Indiquez dans le champ **Chemin d'accès au dossier** le chemin d'accès au dossier de quarantaine.

- **Supprimer les objets du dossier après, jours** : limite la durée de conservation des objets. Par défaut, les fichiers sont conservés pendant 90 jours. Vous pouvez modifier cette durée en saisissant une nouvelle valeur dans le champ situé à droite.
- **Taille maximale du dossier, Mo** : limite la taille totale des fichiers qui se trouvent dans le dossier. Une fois la limite atteinte, les fichiers les plus anciens seront supprimés.
- **Analyser les objets en quarantaine après la mise à jour des bases antivirus** : cochez cette case pour procéder à l'analyse automatique des objets suspects de la quarantaine après chaque mise à jour des bases antivirus.

6.2.2.6. Utilisation de la quarantaine et du dossier de sauvegarde

Pour examiner les objets situés dans le dossier de quarantaine ou de sauvegarde de l'ordinateur, utilisez l'onglet **Objets des dossiers** (cf. ill. 30).

Pour ce faire, cliquez sur **Liste des objets** de la section **Quarantaine** ou **Dossier de sauvegarde**.

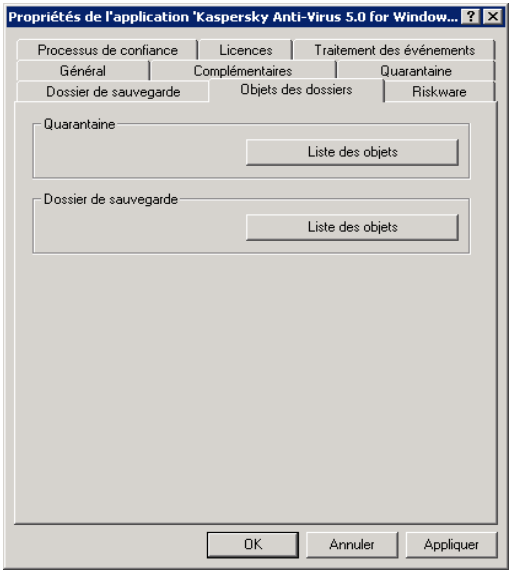

Illustration 30. Onglet **Objets des dossiers**

Les fenêtres des deux dossiers se ressemblent (cf.ill. 31). La partie centrale reprend la liste des objets mis en quarantaine ou des copies de sauvegarde. Les informations suivantes accompagnent chaque objet : nom, état de l'objet, date du placement dans le dossier et emplacement d'origine.

Au dessus de la liste, vous trouverez une barre d'administration des objets proposant les boutons suivants :

: restaure l'objet. En cliquant sur ce bouton, vous ferez apparaître la fenêtre dans laquelle il faudra saisir le chemin d'accès au répertoire souhaité pour la restauration de l'objet.

En cas d'administration à distance via Kaspersky Administration Kit, la restauration des objets a lieu uniquement sur l'ordinateur au départ duquel l'administration est réalisée.

: supprime l'objet du dossier.

: rafraîchit le contenu du dossier.

: lance l'analyse des objets (uniquement pour la quarantaine).

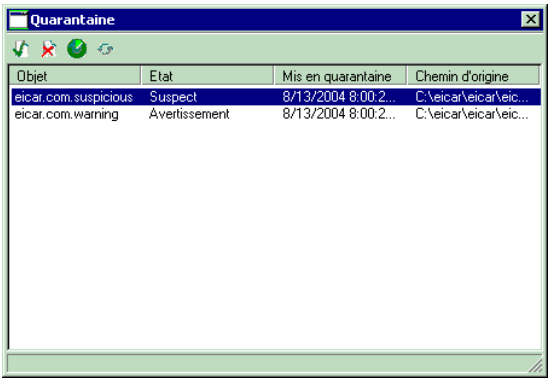

Illustration 31. Quarantaine

6.2.2.7. Informations sur les clés de licence

L'onglet **Licences** (cf. ill. 32) reprend uniquement des informations. Ces informations portent sur les clés de licence actuelles ou de réserve installées sur cet ordinateur particulier.

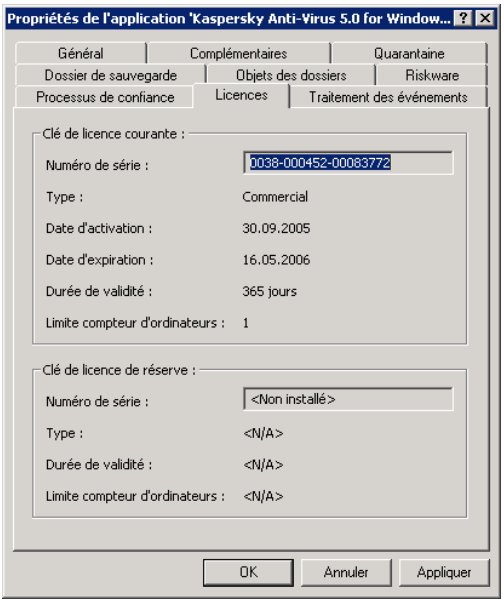

Illustration 32. Onglet **Licences**

6.2.2.8. Configuration des paramètres de la formation des rapports

L'onglet **Traitement des événements** (cf. ill. 33) reprend tous les événements survenus pendant l'utilisation de l'application et consignés dans le rapport, de même que l'emplacement du rapport et le mode d'avertissement de l'administrateur et/ou des autres utilisateurs.

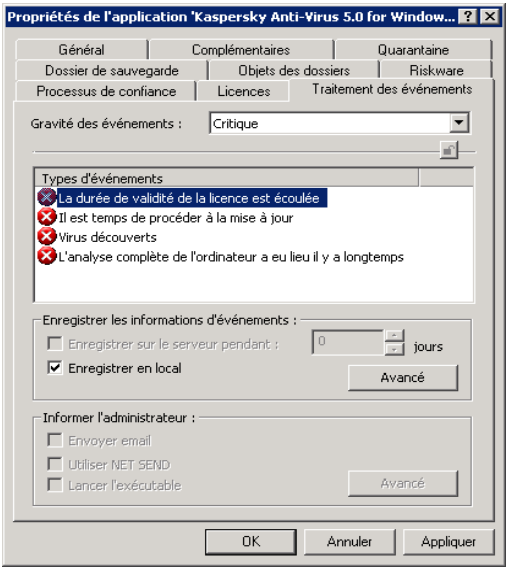

Illustration 33. Modification d'une stratégie. Onglet **Traitement des événements**

Kaspersky Anti-Virus 5.0 for Windows File Servers génère un ensemble défini d'événements pendant son utilisation (cf. Tableau 2). Chaque événement est accompagné d'une caractéristique qui reflète son degré d'importance. Il existe quatre degrés :

- **Critique – evénement critique**
- **Erreur – refus de fonctionnement**
- **Avertissement**
- **Info – message d'information**

Les événements d'un même type peuvent avoir différents niveaux d'importance. Tout dépend de la situation dans laquelle l'événement s'est produit.

Sélectionnez le degré d'importance de l'événement dans la liste déroulante **Gravité des événements**. Le champ en dessous reprend les types d'événements pour le degré sélectionné.

Tableau 2. Evénements de l'application

Type d'événement	Degré d'importance
Objet réparé	**Avertissement**
Objet infecté supprimé	**Avertissement**
Modification du niveau de protection en temps réel	**Message d'information**
La licence arrive en fin de validité (deux semaines avant la fin)	**Avertissement**
La durée de validité de la licence est écoulée	**Evénement critique**
L'analyse de la licence a échoué	**Refus de fonctionnement**
Découverte d'un objet suspect	**Avertissement**
Erreur de fonctionnement	**Avertissement** **Refus de fonctionnement**
Il est temps de procéder à la mise à jour : - une semaine* - deux semaines*	 **Avertissement** **Evénement critique**
Virus découvert	**Evénement critique**
Erreur interne	**Refus de fonctionnement**
Le système d'exploitation a redémarré après l'installation de l'application	**Avertissement**
Découverte d'une archive protégée par un mot de passe	**Avertissement**

Type d'événement	Degré d'importance
Objet non réparé	**Avertissement**
L'analyse complète de l'ordinateur a eu lieu il y a longtemps : - il y a deux semaines* - il y a un mois*	**Avertissement** **Evénement critique**

*Ces valeurs existent par défaut. Vous pouvez les modifier dans la fenêtre Avertissement (cf. point 6.2.2.2, page 61).

Pour chaque événement, vous pouvez décider de l'inclure ou non dans le rapport et définir les paramètres de notification de l'administrateur lorsque l'événement se produit.

Pour obtenir de plus amples informations sur les autres paramètres de l'onglet **Traitement des événements**, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

CHAPITRE 7. ADMINISTRATION A DISTANCE

L'administration centralisée de Kaspersky Anti-Virus via Kaspersky Administration Kit vous permet d'administrer les stratégies, les tâches ainsi que les paramètres de l'application Kaspersky Anti-Virus 5.0 for Windows File Servers installée sur les ordinateurs distants du réseau.

7.1. Administration des stratégies

Cette rubrique est consacrée à la création et à la configuration de stratégies pour Kaspersky Anti-Virus 5.0 for Windows File Servers. Pour obtenir de plus amples informations sur le concept d'administration des stratégies, consultez le Manuel de l'administrateur de « Kaspersky Administration Kit 5.0 ».

7.1.1. Création d'une stratégies

Pour créer une stratégies, exécutez les opérations suivantes :

1. Dans l'arborescence de la console du dossier **Groupes**, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez créer la stratégie.
2. Sélectionnez le dossier **Stratégie** appartenant au groupe sélectionné, ouvrez le menu contextuel et cliquez sur **Créer→Stratégie** La fenêtre de création d'une nouvelle stratégie apparaîtra à l'écran.

L'interface du programme de création des stratégies se présente sous la forme d'un Assistant Microsoft Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Lors de la création d'une stratégie, vous pouvez bloquer la modification des paramètres des stratégies des sous-groupes, des paramètres de l'application et des paramètres des tâches.

Etape 1. Saisie des données générales sur la stratégie

Les premières fenêtres de l'Assistant sont destinées à la saisie d'informations. Il faut à ce stade définir le nom de la stratégie (champ **Nom**) et sélectionner l'application **Kaspersky Anti-Virus 5.0 for Windows File Servers** dans la liste déroulante **Nom de l'application**.

Afin que les paramètres de la stratégie entrent en vigueur directement après sa création, cochez la case **Activer la politique**.

Une seule stratégie active de groupe peut être définie pour l'application. Si l'application possède déjà une stratégie de groupe d'un niveau hiérarchique supérieur, vous pourrez uniquement modifier les paramètres de la stratégie du groupe qui correspondent aux paramètres modifiables de la stratégie du niveau supérieur.

Etape 2. Choix du niveau de protection en temps réel

Sélectionnez à ce stade le niveau de protection antivirus (cf. point 4.1, p. 21) selon lequel la protection en temps réel sera organisée.

Etape 3. Choix du niveau de protection pour l'analyse à la demande

Sélectionnez à ce stade le niveau de protection antivirus (cf. point 4.1, p. 21) selon lequel la protection pour l'analyse à la demande sera organisée.

Le bouton **Détails** ouvre une fenêtre qui vous permettra de définir les paramètres de l'analyse à la demande (cf. ill. 5). Si vous modifiez les paramètres de l'un des niveaux prédéfinis, vous passerez automatiquement au mode **Paramètres utilisateur**.

Etape 4. Sélection de l'origine des mises à jour

Vous devez sélectionner à ce stade (cf. ill. 34) l'origine des mises à jour des bases antivirus et des modules de l'application et configurer également les paramètres du réseau local (pour de plus amples informations, consultez le point 6.2.1.2.4 à la page 49).

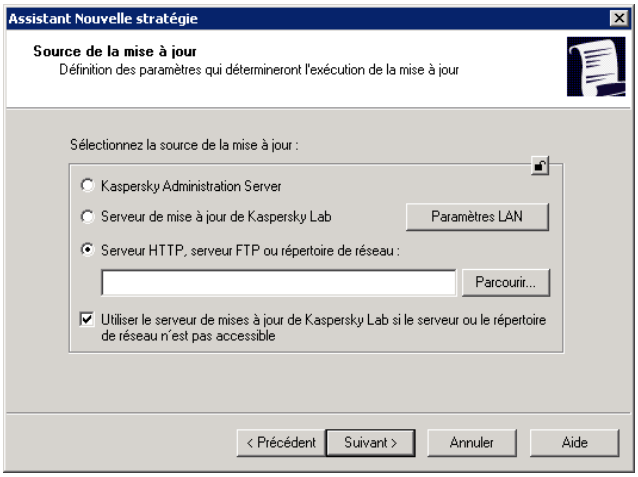

Illustration 34. Sélection de l'origine de la mise à jour

Etape 5. Sélection des paramètres de service de mise à jour

Définissez dans cette fenêtre (cf. ill. 35) les paramètres du service de mise à jour des bases antivirus et des modules de l'application (pour de plus amples informations, consultez le point 6.2.1.2.4 à la page 49).

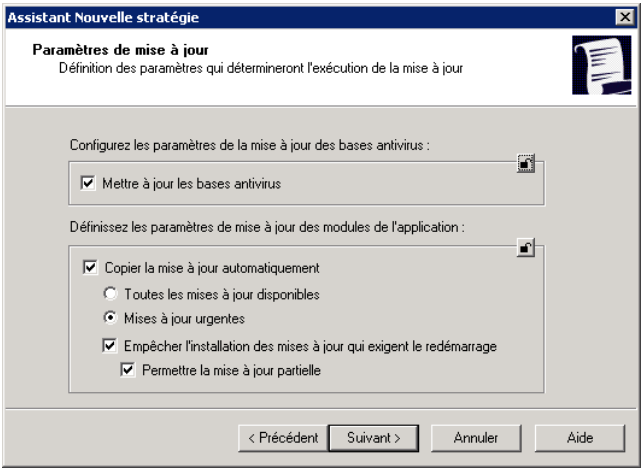

Illustration 35. Sélection des paramètres du service de mise à jour

Etape 6. Fin de la création d'une stratégie

La dernière fenêtre de l'Assistant vous informe sur la réussite de la création de la stratégie.

Lorsque vous quittez l'Assistant de création de stratégie pour l'application sélectionnée, le dossier **Stratégie** du groupe correspondant sera ajouté et repris dans le panneau des résultats.

Pour appliquer une stratégie, modifiez ses paramètres et imposez des restrictions quant à la modification des paramètres si cela n'a pas été fait lors de la création de la stratégie. La stratégie sera diffusée sur les ordinateurs client lors de la première synchronisation des clients avec le serveur.

L'application de la stratégie s'opère de la manière suivante : si des tâches résidentes (tâches liées à la protection en temps réel) sont exécutées sur l'ordinateur client, elles seront exécutées selon les nouveaux paramètres. Les tâches exécutées périodiquement (analyse à la demande, mise à jour des bases antivirus) seront toujours exécutées selon les anciens paramètres. Toute nouvelle tâche sera réalisée selon les paramètres modifiés. Vous pouvez examiner la valeur des paramètres de fonctionnement de l'application suite à l'application de la stratégie dans les onglets **Applications** et **Tâches** (cf. point 7.3, p. 82) dans la fenêtre des propriétés de l'ordinateur client distant.

Vous pouvez copier et déplacer les stratégies d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Action**. Le déplacement peut également être réalisé à l'aide de la souris.

7.1.2. Examen et modification des paramètres de la stratégie

A cette étape, vous pouvez introduire des modifications dans la stratégie ou interdire la modification de certains paramètres des stratégies des sous-groupes, de l'application et des tâches.

Pour interdire la redéfinition des paramètres, il faut les « verrouiller » :  . L'icône  indique les paramètres qui peuvent être modifiés.

Pour examiner la valeur des paramètres de la stratégie et / ou introduire des modifications :

1. Dans l'arborescence de la console, dans le dossier **Groupes**, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez modifier les paramètres.

2. Sélectionnez le dossier **Stratégies** faisant partie de ce groupe. Toutes les stratégies définies pour ce groupe seront reprises dans le panneau des résultats.
3. Sélectionnez dans la liste la stratégie pour l'application **Kaspersky Anti-Virus 5.0 for Windows File Servers** (le nom de l'application est indiqué dans le schéma **Application**).
4. Affichez le menu contextuel pour la stratégie sélectionnée et utilisez la commande **Propriétés**. La fenêtre des paramètres de la stratégie de **Kaspersky Anti-Virus 5.0 for Windows File Servers** apparaîtra à l'écran. Elle reprend plusieurs onglets.

Les onglets **Général, Contrôle** et **Traitement des événements** sont standard pour l'application Kaspersky Administration Kit (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit).

Les autres onglets contiennent les **paramètres** de Kaspersky Anti-Virus 5.0 for Windows File Servers et correspondent aux onglets des paramètres des tâches (cf. point 6.2.1.2, p. 38) et aux onglets des paramètres de l'application (cf. point 6.2.2, p. 59).

7.2. Administration des tâches

Cette rubrique est consacrée à la création et à la configuration des paramètres des tâches pour Kaspersky Anti-Virus 5.0 for Windows File Servers.

7.2.1. Création d'une tâche

Lors de l'utilisation de Kaspersky Anti-Virus 5.0 for Windows File Servers via Kaspersky Administration Kit, vous pouvez créer :

- Des tâches locales : définies pour un ordinateur client distinct.
- Des tâches de groupe : pour un groupe d'ordinateurs client.
- Des tâches globales : définies pour un ensemble d'ordinateurs clients issus de groupes du réseau local.

Vous pouvez modifier les paramètres des tâches, observer leur exécution, copier et déplacer les tâches d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Action**.

Les paramètres de fonctionnement de l'application lors de l'exécution des tâches sur chaque ordinateur client sont définis conformément à la stratégie du groupe,

à la configuration des tâches et à la configuration de cette application sur l'ordinateur client.

Les tâches sont exécutées conformément à l'horaire établi. Vous pouvez suspendre temporairement certaines des tâches programmées. Dans ce cas la tâche n'est pas supprimée. Elle n'est simplement pas exécutée selon l'horaire défini.

Vous pouvez lancer une tâche, l'arrêter, la suspendre ou la reprendre manuellement grâce aux commandes du menu contextuel **Démarrer/Stopper/Pause/Continuer** ou aux éléments correspondants du menu **Action.**

7.2.1.1. Création d'une tâche locale

Afin de créer une tâche locale pour Kaspersky Anti-Virus 5.0 for Windows File Servers, réalisez les opérations suivantes :

1. Dans le dossier **Groupes**, sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.
2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez créer la tâche locale. Utilisez la commande **Propriétés** du menu contextuel ou l'élément correspondant du menu **Action**. Ceci entraîne l'ouverture dans la fenêtre principale de l'application de la fenêtre d'examen des propriétés de l'ordinateur client **Propriétés de <nom de l'ordinateur>**.
3. Sélectionnez l'onglet **Tâches** (cf. Ill. 36). Il reprend toutes les tâches créées pour cet ordinateur client. Pour créer une nouvelle tâche, cliquez sur **Ajouter**.

Cette action entraîne l'ouverture d'un Assistant semblable à celui utilisé pour la création d'une tâche en cas d'administration locale de l'application (pour de plus amples informations, consultez le point 6.2.1.3 à la page 55). Suivez les instructions affichées à l'écran.

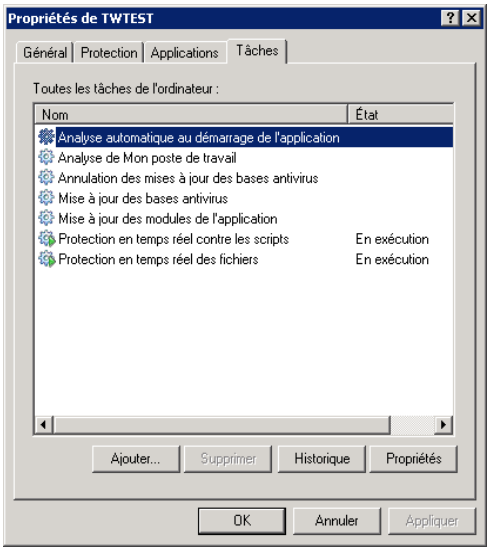

Illustration 36. Création d'une tâche locale.
Onglet **Tâches**

7.2.1.2. Création d'une tâche de groupe

Afin de créer une tâche de groupe pour Kaspersky Anti-Virus 5.0 for Windows File Servers, réalisez les opérations suivantes :

1. Sélectionnez le groupe pour lequel vous souhaitez créer la tâche dans l'arborescence de la console.
2. Sélectionnez le répertoire **Tâche** qui en fait partie, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Action**. Cette action entraîne l'ouverture d'un Assistant semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 6.2.1.3 à la page 55). Suivez les instructions affichées à l'écran.

Une fois que vous aurez quitté l'Assistant, la tâche sera ajoutée au dossier **Tâche** du groupe correspondant et de tous les groupes inclus dans ce groupe et reprise dans le panneau des résultats.

7.2.1.3. Création d'une tâche globale

Afin de créer une tâche globale pour Kaspersky Anti-Virus 5.0 for Windows File Servers, réalisez les opérations suivantes :

1. Sélectionnez le nœud **Tâche** dans l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Action**.
2. Cette action entraîne l'ouverture d'un Assistant semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 6.2.1.3 à la page 55). La seule différence se situe au niveau de l'existence d'une étape permettant de dresser la liste des ordinateurs clients du réseau logique pour lesquels vous créez la tâche globale.
3. Sélectionnez les ordinateurs du réseau logique sur lesquels la tâche sera exécutée. Il est possible de sélectionner des ordinateurs de différents répertoires ou des répertoires complets (pour de plus amples informations, consultez le manuel de l'administrateur de « Kaspersky Administration Kit 5.0 »).

Les tâches globales sont exécutées uniquement sur le groupe d'ordinateurs sélectionné. Lorsque de nouveaux ordinateurs clients sont ajoutés au groupe, la tâche ne sera pas exécutée sur ces ordinateurs. Il faudra donc créer une nouvelle tâche ou modifier comme il se doit les paramètres de la tâche existante.

A la fin de la création de la tâche, la nouvelle tâche globale sera reprise dans le nœud **Tâches** de l'arborescence de la console et apparaîtra dans le panneau des résultats.

7.2.2. Examen et modification des paramètres d'une tâche

Pour vérifier les paramètres d'une tâche et les modifier :

- Pour une tâche locale, sélectionnez, dans le dossier **Groupes,** le dossier portant le nom du groupe dont l'ordinateur client fait partie. Sélectionnez l'ordinateur dans le panneau des résultats et utilisez la commande **Propriétés** du menu contextuel. Ouvrez l'onglet **Tâches** (cf.ill. 36) de la fenêtre **Propriétés de <nom de l'ordinateur>**. L'examen et la

modification des paramètres de la tâche sélectionnée s'opère dans la fenêtre ouverte après avoir cliqué sur le bouton **Propriétés**.

L'onglet **Tâche** reprend la liste de toutes les tâches définies pour l'ordinateur local (y compris les tâches globales et de groupe). Les tâches globales et de groupe sont signalées par une icône représentant un « dossier ». Vous pouvez consulter les paramètres de toutes les tâches. Toutefois, vous ne pourrez modifier que ceux des tâches locales.

- Pour les tâches de groupe, sélectionnez le groupe dans l'arborescence de la console et choisissez le dossier **Tâches** qui en fait partie. Ceci entraînera l'affichage dans le panneau des résultats de toutes les tâches définies pour ce groupe. Sélectionnez la tâche qui vous intéresse puis, ouvrez le menu contextuel afin de choisir le point **Propriétés** ou sélectionnez l'élément équivalent dans le menu **Action**.
- Si vous devez absolument modifier les paramètres d'une tâche globale, sélectionnez le nœud **Tâches** dans l'arborescence de la console, sélectionnez la tâche qui vous intéresse dans le panneau des résultats puis, ouvrez le menu contextuel afin de choisir le point **Propriétés** ou sélectionnez l'élément équivalent dans le menu **Action**.

Cela entraînera l'ouverture de la fenêtre **Propriétés de «nom de la tâche»** avec les onglets suivants : **Général, Paramètres, Compte, Planification, Notification**. La fenêtre de configuration de la tâche globale contient également l'onglet intitulé **Ordinateurs client**.

Ces onglets (à l'exception de l'onglet **Paramètres** et **Compte**) sont des onglets standard pour la configuration des tâches dans Kaspersky Administration Kit 5.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit.

L'onglet **Compte** vous permet de configurer le lancement des tâches sous un autre compte (cf. point 6.2.1.3 à la page. 55) L'onglet **Paramètres** reprend les paramètres propres à Kaspersky Anti-Virus 5.0 for Windows File Servers. Le contenu de l'onglet varie en fonction du type de tâche sélectionné (pour de plus amples informations, consultez le point 6.2.1.2 à la page 38).

7.3. Administration de l'application via les paramètres

Les paramètres de l'application vous permettent de modifier les paramètres de fonctionnement de celle-ci pour des ordinateurs clients distincts. Seuls les paramètres dont la modification n'est pas interdite par la stratégie développée pour cette application peuvent être changés (cf. point 7.1.2, p. 77).

Afin de modifier les paramètres de l'application :

1. Dans le dossier **Groupes**, sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.
2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez modifier les paramètres de l'application. Utilisez la commande **Propriétés** du menu contextuel ou l'élément correspondant du menu **Action**.
3. Cette action entraîne l'ouverture de la fenêtre **Propriétés de <nom de l'ordinateur>** dans la fenêtre principale. Sélectionnez l'onglet **Applications** (cf. ill. 37). Cet onglet reprend la liste des applications de Kaspersky Lab installées sur l'ordinateur client.

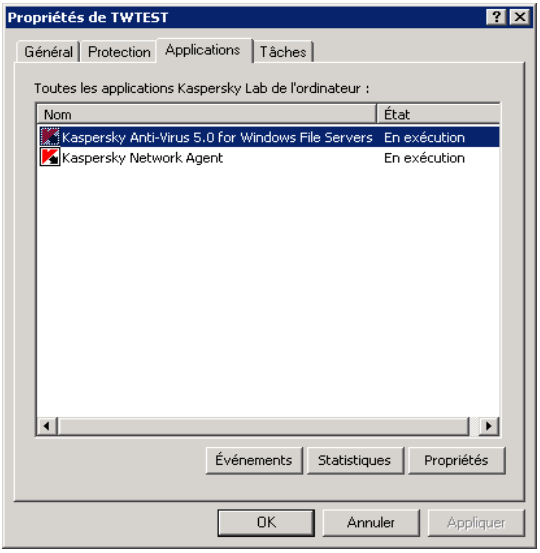

Illustration 37. Liste des applications de Kaspersky Lab

4. Sélectionnez l'application **Kaspersky Anti-Virus 5.0 for Windows File Servers** et cliquez sur **Propriétés**.

L'administration des paramètres de l'application en situation d'administration à distance est identique à l'administration en situation d'administration locale (pour de plus amples informations, consultez le point 6.2.2 à la page 59).

CHAPITRE 8. VERIFICATION DU BON FONCTIONNEMENT DU LOGICIEL ANTIVIRUS

8.1. Virus d'essai EICAR et ses modifications

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

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

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

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

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

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

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

Afin de vérifier le comportement de Kaspersky Anti-Virus lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du « virus » d'essai standard en ajoutant un des préfixes repris au Tableau 3.

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

Tableau 3. Modifications du « virus » d'essai

Préfixe	Type d'objet
Pas de préfixe, « virus » d'essai standard	**Infecté**. Une erreur se produit pendant la réparation ; l'objet est supprimé.
CORR–	**Corrompu**.
SUSP-	**Suspect** (code d'un virus inconnu).
WARN-	**Suspect** (code modifié d'un virusconnu).
ERRO-	**Non analysé suite a un échec**.
CURE-	**Infecté**. L'objet sera réparé et le texte du corps du « virus » sera remplacé par CURE.
DELE-	**Infecté**. L'objet sera effacé automatiquement.

La première colonne reprend les préfixes qu'il faudra ajouter au début de la ligne de code du « virus »d'essai standard (par exemple : `DELE-X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`).

Une fois que vous aurez ajouté le préfixe, enregistrez le fichier sous le nom *eicar_dele.com* par exemple (utilisez la même convention pour toutes les modifications du virus).

La deuxième colonne reprend la description des types d'objet identifiés par l'antivirus suite à l'ajout des différents préfixes. Les actions exécutées sur chacun de ces objets dépendent des paramètres de l'antivirus définis par l'administrateur.

8.2. Essai de Kaspersky Anti-Virus

Afin de vérifier l'exactitude des paramètres et le bon fonctionnement de Kaspersky Anti-Virus 5.0 for Windows File Servers :

- Créez un nouveau répertoire dans lequel vous enregistrerez tous les virus d'essai que vous avez créés.
- Créez une tâche pour l'analyse à la demande de ce répertoire (cf. point 6.2.1.3, p. 55) :
- Afin de bien consigner les événements survenus pendant l'utilisation de l'application, veillez à cocher les cases adéquates dans l'onglet **Traitement des événements** (cf. point 6.2.2.8**,** p. 71)
- Lancez la tâche.
- Vérifiez l'exactitude de la description de l'événements ainsi que la présence d'objets dans le dossier de quarantaine ou de sauvegarde au cas où la configuration prévoyait le déplacement des objets dans l'un de ces dossiers (cf. point 6.2.2.6, p. 68).

CHAPITRE 9. PROTECTION ANTIVIRUS PENDANT L'ENTRETIEN DU SERVEUR

Lors de la réalisation de tâches d'entretien sur le serveur, il est indispensable de tenir compte des recommandations de l'éditeur du système d'exploitation et de désactiver la protection antivirus dans les cas suivants :

- *Défragmentation du disque*.
- *Installation de nouveaux périphériques de données*. En cas d'ajout d'un disque dur ou d'un disque amovible contenant déjà certaines données, nous vous recommandons de procéder comme suit :
    - Lancez l'analyse à la demande du nouveau disque directement après son installation ;
    - Assurez-vous que ce disque est inclus dans l'analyse aussi bien pour l'analyse à la demande que pour la protection en temps réel.
- *Réalisation d'une copie de sauvegarde ou restauration des données*. Lors de la réalisation de ces opérations, nous vous recommandons de lancer la recherche d'un éventuel code malicieux dans les données dont une copie de sauvegarde sera créée directement avant d'entamer cette opération.
- *Mise à niveau du système d'exploitation.*

Il n'est pas nécessaire d'arrêter le logiciel antivirus lors des opérations qui ne sont pas liées à la nécessité d'un accès rapide à un grand volume de données (par exemple, lors de la réplication sur le serveur).

Kaspersky Anti-Virus for Windows File Servers fonctionne correctement avec les autres applications développées pour le système d'exploitation Windows.

Il n'est pas possible d'installer sur une même machine des logiciels antivirus de Kaspersky Lab et des logiciels d'autres éditeurs. Nous ne pouvons garantir, dans ce cas de figure, le fonctionnement correct de l'application et du système d'exploitation dans son ensemble.

CHAPITRE 10. QUESTIONS FREQUEMMENT POSEES

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

Question : L'utilisation simultanée de Kaspersky Anti-Virus 5.0 for Windows File Servers avec des logiciels antivirus d'autres éditeurs est-elle possible ?

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

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

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

Et cela, grâce aux nouvelles technologies iChecker™ et iStreams™. Ces technologies reposent sur l'utilisation d'une base de données des sommes de contrôle des objets et la conservation des sommes de contrôle dans les flux NTFS complémentaires.

Question : Est-il possible de configurer l'analyse de tout le trafic de messagerie à l'aide de Kaspersky Anti-Virus 5.0 for Windows File Servers comme cela est le cas avec Kaspersky Anti-Virus Personal 5.0 ?

Kaspersky Anti-Virus 5.0 for Windows File Server a été conçu pour la protection des objets du système de fichiers du serveur. Pour obtenir de plus amples informations sur les logiciels assurant la protection des serveurs de messagerie, contactez Kaspersky Lab.

Question : Faut-il installer Kaspersky Administration Kit 5.0 afin d'administrer Kaspersky Anti-Virus 5.0 for Windows File Servers ?

Kaspersky Anti-Virus 5.0 for Windows File Servers ne dispose pas de sa propre interface graphique et est administré soit via la ligne de

commande, soit via la *Console d'administration* qui fait partie de Kaspersky Administration Kit.

En cas d'administration via la *Console d'administration*, il n'est pas nécessaire d'installer Kaspersky Administration Kit 5.0 dans son ensemble : il suffit en effet d'installer la *Console d'administration* et *l'Agent d'administration.*

Question : Est-il possible de recevoir des notifications (courrier électronique, net send) relatives aux événements survenus lors de l'utilisation de Kaspersky Anti-Virus 5.0 for Windows File Servers ?

Vous pouvez recevoir les notifications relatives aux événements survenus pendant l'utilisation de Kaspersky Anti-Virus via le serveur de messagerie, via le réseau par l'intermédiaire de NET Send ou par le biais de l'exécution d'un programme ou d'un fichier exécutable tiers lorsque l'événement survient (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0).

Question : J'ai l'intention d'administrer Kaspersky Anti-Virus via la ligne de commande. Comment peut-on déterminer l'état de Kaspersky Anti-Virus à un moment donné ?

Il est généralement admis que Kaspersky Anti-Virus est activé en permanence.

Si l'application est arrêtée, le message « Unable to connect to Kaspersky Anti-Virus » apparaîtra après la saisie de n'importe quelle commande. Pour lancer l'application, exécutez la commande KAVSHELL START.

Question : Pourquoi les répertoires raccordés en tant que disque réseau ne sont-ils pas couverts par la protection en temps réel ?

Pour analyser un répertoire monté en tant que disque de réseau dans l'**Assistant** ou à l'aide de la commande **Net Use**, il convient de cocher les cases **Disques durs**, **Disques amovibles** de l'onglet **Zone d'analyse** (cf. 6.2.1.2.2 p. 44) des tâches liées à la protection en temps réel.

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

La détection des virus est une tâche mathématique liée à l'analyse de la structure, de la somme de contrôle et des données mathématiques. Pour cette raison, la principale ressource utilisée Kaspersky Anti-Virus

est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse.

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

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

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

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

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

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

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

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

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

Question : Mon antivirus ne fonctionne pas.

Que puis-je faire ?

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

Si vous ne trouvez pas la solution à vos problèmes dans ces ressources ou dans la base de solutions, nous vous conseillons de contacter le service d'assistance technique de Kaspersky Lab.

Pour les questions urgentes, composez le numéro de téléphone repris dans la rubrique. L'assistance technique par téléphone est offerte 24h/24 en russe, en anglais, en français et en allemand. N'oubliez pas que pour pouvoir bénéficier de l'assistance, vous devez être un utilisateur enregistré et vous devrez transmettre votre numéro d'inscription à l'opérateur (en cas d'achat du logiciel dans une boîte) ou les informations relatives à votre commande (en cas d'achat en ligne).

Vous pouvez également envoyer votre demande via le formulaire publié sur le site Internet de Kaspersky Lab dans la rubrique **Services/ Centre de support/ Résoudre un problème**.

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

- Le type de requête. Sélectionnez la catégorie à laquelle appartient votre requête.
- Le nom du logiciel de Kaspersky Lab que vous utilisez (par exemple, **Kaspersky Anti-Virus for Windows File Servers**).
- Le texte de la requête. Décrivez le problème survenu pendant l'utilisation du logiciel de Kaspersky Lab.
- Les données d'enregistrement. Sélectionnez le type d'enregistrement du programme en choisissant **Clé de licence** si vous avez achetez le logiciel dans un magasin ou si vous avez installé la licence depuis une disquette ou **commande en ligne** si vous avez acheté le logiciel en ligne. En fonction du type d'enregistrement, saisissez le numéro de la clé ou le numéro de la commande dans le champ situé en dessous.

  Les informations relatives au numéro de série de Kaspersky Anti-Virus 5.0 for Windows File Servers sont accessibles sur l'onglet **Licence** (cf. ill 32).

- L'adresse électronique à laquelle le représentant du service d'assistance technique pourra vous joindre.

A la page suivante du formulaire, saisissez vos coordonnées, le code de protection contre les envois automatiques et cliquez **Отправить Soumettre**. Les experts du service d'assistance technique étudieront votre problème et vous répondront dans les plus brefs délais.

Question : À quoi servent les mises à jour quotidiennes ?

Il y a encore quelques années, les virus étaient transmis via disquette et afin de protéger l'ordinateur, il suffisait d'installer un logiciel antivirus et de procéder de temps à autre à la mise à jour des bases antivirus. Les épidémies les plus récentes se sont répandues à travers le monde entier en quelques heures uniquement et dans ces conditions, un logiciel antivirus équipé d'anciennes bases antivirus est impuissant face aux nouvelles menaces. Afin de ne pas devenir victime de la prochaine épidémie de virus, il est indispensable de mettre à jour les bases antivirus quotidiennement.

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

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

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

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

Voici les avantages du nouveau système de mise à jour :

- Fin du téléchargement des fichiers en cas de déconnexion : désormais, il n'est plus nécessaire de télécharger à nouveau les données obtenues avant la déconnexion.
- *Réduction de moitié de la taille de la mise à jour cumulée.* La mise à jour cumulée contient toute la base antivirus, ce qui

explique pourquoi la taille de la mise à jour cumulée est de loin supérieur à la taille de la mise à jour traditionnelle. Le nouveau service introduit une nouvelle technologie qui permet d'utiliser les bases antivirus qui existent déjà pour la mise à jour cumulée.

- *Accélération du téléchargement depuis Internet.* Kaspersky Anti-Virus sélectionne le serveur de mise à jour situé dans votre région. De plus, la charge du serveur est répartie en fonction de ses performances. Autrement dit, vous ne serez pas connecté à un serveur surchargé pendant qu'un autre n'est pas sollicité.

- *Application des « listes noires » des clés.* Ceci permet d'exclure des mises à jour les utilisateurs qui ne disposent pas de la licence d'utilisation de Kaspersky Anti-Virus. Ainsi, les utilisateurs qui possèdent une licence ne sont pas pénalisés à cause de serveurs surchargés.

- Les logiciels destinés aux entreprises autorisent la création d'un répertoire local pour la mise à jour des bases antivirus. Cette fonction est prévue pour les entreprises où les ordinateurs, protégés par les applications de Kaspersky Lab, sont regroupés au sein d'un réseau. N'importe quel ordinateur peut jouer le rôle de serveur de mise à jour. C'est lui qui recevra les mises à jour depuis Internet. Elles seront enregistrées dans un répertoire local accessible aux autres ordinateurs du réseau.

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

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

Question : Comment configurer la mise à jour pour un ordinateur via Internet afin qu'il devienne ensuite le serveur de mise à jour pour les autres ordinateurs du réseau ?

Le serveur sera l'ordinateur mis à jour via Internet tandis que les autres ordinateurs du réseau seront les clients de ce serveur.

Il est possible de configurer la mise à jour via le réseau local de l'une des manières suivantes :

- Activer l'utilisation de la source de mise à jour locale sur le serveur Kaspersky Administration Kit 5.0.

Kaspersky Administration Kit est équipé d'un outil de diffusion des mises à jour via le réseau de l'entreprise. Il peut, selon l'horaire défini, mettre à jour les ressources d'accès commun et lancer la mise à jour des autres ordinateurs. Kaspersky Administration Kit veillera à ce que le volume de données téléchargées ne dépasse les besoins des applications installées. Il est possible de voir sur le serveur la liste des correctifs disponibles. La procédure de configuration est décrite en détail dans le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

- Activer l'utilisation de la source de mise à jour locale dans l'un des logiciels de Kaspersky Lab.

  Cette méthode doit être suivie lorsque l'utilisation de Kaspersky Administration Kit est impossible ou lorsqu'il faut obtenir une structure du réseau des serveurs de mise à jour plus complexe. Pour ce faire :

  - Sélectionnez les ordinateurs qui serviront de serveur de mise à jour. La version 5.0[1] des applications de Kaspersky Lab devront être installées sur cet ordinateur.
  - Il faut absolument créer sur chaque ordinateur sélectionné une ressource de réseau qui servira à la diffusion de la mise à jour. Il peut s'agir d'un répertoire de réseau sur un ordinateur Windows, un serveur FTP ou un serveur HTTP. Il convient d'octroyer les privilèges d'accès (lecture de ce répertoire.
  - Créez la tâche de mise à jour ou modifiez la tâche existante. Activez l'utilisation de la mise à jour depuis la source locale et indiquez le chemin d'accès au répertoire.
  - Précisez le répertoire de source locale de la mise à jour du serveur sur tous les ordinateurs qui devront être mis à jour au départ de ce serveur.

Question : J'utilise un serveur proxy et la mise à jour ne fonctionne pas. Que faire ?

[1] Autre que Kaspersky Anti-Virus 5.0 Personal et Kaspersky Anti-Virus 5.0 for Microsoft ISA Server

L'échec de la réception des mises à jour en cas d'utilisation d'un serveur proxy peut provenir de l'une des causes suivantes :

- Configuration incorrecte des paramètres du réseau.

  Lors de la configuration du service de mise à jour, il est possible de configurer les paramètres du réseau de deux manières : soit en utilisant les paramètres de Microsoft Internet Explorer, soit en utilisant des paramètres individuels. Le service de mise à jour n'utilise pas toujours correctement les paramètres de Microsoft Internet Explorer, surtout dans les cas suivants :

  - La connexion Internet n'est pas configurée sur l'ordinateur ;
  - Les paramètres de Microsoft Internet Explorer ne sont pas accessibles lorsqu'aucun utilisateur n'est enregistré dans le système d'exploitation.
  - Le serveur proxy requiert une autorisation.

  Dans tous ces cas, il est nécessaire de définir les paramètres du réseau directement dans les paramètres du service de mise à jour.

- Utilisation d'un serveur proxy qui n'est pas compatible avec le service de mise à jour de Kaspersky Anti-Virus.

  Le service de mise à jour ne fonctionne pas avec Kerio WinRoute car WinRoute ne résout pas entièrement le protocole http 1.0. Dans ce cas, nous vous recommandons d'utiliser n'importe quel autre serveur proxy.

  De même, le service de mise à jour ne fonctionne pas via le protocole FTP avec Microsoft ISA Server. Dans ce cas, il est conseillée de procéder à la mise à jour au départ des serveurs de Kaspersky Lab via le protocole HTTP.

Question : Comment obtenir le fichier journal du service de mise à jour ?

Kaspersky Anti-Virus vous permet d'obtenir les fichiers journal de la mise à jour. Vous pouvez obtenir un rapport plus détaillé en activant l'option de consignation de tous les événements dans le journal dans les options avancées.

Si le Service d'assistance technique vous a demandé de lui envoyer le journal de la mise à jour, vous devrez réaliser les opérations suivantes :

- Lancez regedit

- Créez la section HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Fileserver\5.0.0.0\Debug
- Dans cette section, créez la clé « TraceLevel » e type DWORD et donnez lui la valeur 10.
- Lancez la mise à jour. Le fichier journal intitulé $Up2Date-Fileserver.log sera constitué dans le dossier de l'application.
- Compressez ce fichier et envoyez-le au Service d'assistance technique.

Cet exemple convient à Kaspersky Anti-Virus 5.0 for Windows File Servers. Pour les autres applications, il convient de choisir la section comportant le nom de l'application.

APPENDICE A. GLOSSAIRE

Ce manuel reprend des termes et des notions propres à la lutte contre les virus informatiques. Ce glossaire vise à vous offrir une définition de ces différents termes. Les termes sont présentés par ordre alphabétiques.

A

Administrateur (sécurité) : personne en charge de l'administration locale de l'application via la ligne de commande ou la *Console d'administration*.

Administrateur du réseau logique :personne en charge de l'administration du fonctionnement de Kaspersky Anti-Virus via Kaspersky Administration Kit, le système d'administration centralisée.

Administration centralisée de l'application : administration à distance de l'application à l'aide des services d'administration proposés par Kaspersky Administration Kit 5.0.

Adware : programme introduit dans des applications à l'insu de l'utilisateur et dont l'objectif est d'afficher des publicités. Ces programmes sont diffusés gratuitement. Les publicités s'affichent sur l'interface de travail. Bien souvent, ces programmes recueillent des données personnelles sur l'utilisateur et les transmettent à l'auteur du programme, modifient les paramètres du navigateur (page d'ouverture, paramètres de sécurité, etc.) et créent un trafic non contrôlé par l'utilisateur. Tout ceci peut entraîner une violation de la sécurité, voire des pertes financières.

Agent d'administration : application spéciale garantissant l'interaction entre le serveur d'administration et les applications faisant partie des solutions pour entreprises de Kaspersky Lab. Elle fait partie de Kaspersky Administration Kit 5.0.

Analyse complète : mode de fonctionnement qui permet à l'administrateur de sécurité de rechercher quand il le souhaite la présence d'éventuels virus dans tout l'ordinateur et de réparer ou de supprimer les objets suspects ou infectés découverts.

Analyser les fichiers pouvant être infectés, en fonction de l'extension : l'extension du fichier est prise en compte pour l'analyse.

Analyser les fichiers pouvant être infectés, en fonction du format : l'analyse porte sur les fichiers en fonction du format, c'est-à-dire que le contenu du fichier est analysé, à savoir l'identificateur de format dans l'entête.

B

Bases antivirus : il s'agit des bases de données développées par les experts de Kaspersky Lab. Elles reprennent une description détaillée de tous les virus connus à l'heure actuelle ainsi que des méthodes utilisées

pour les identifier et réparer les dégâts qu'ils causent. Elles sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouveaux virus apparaissent. Afin d'accroître l'efficacité de la découverte des virus, nous vous recommandons de procéder à la mise à jour régulière des bases antivirus.

Bases de données de messagerie électronique : bases de données qui reprennent les messages électroniques sauvegardés sur votre ordinateur. Chaque message entrant/sortant est repris dans la base après son envoi ou sa réception. Ces bases sont couvertes par la protection en temps réel de votre ordinateur.

Bloquer l'objet : empêcher les applications externes d'accéder à l'objet. L'objet bloqué ne peut être ni lu, ni exécuté, ni modifié, ni supprimé.

C

Clé de licence actuelle : clé de licence installée et utilisée actuellement par Kaspersky Anti-Virus. Elle définit la durée de validité de la licence et la politique de licence par rapport au logiciel. Il ne peut pas y avoir plus de deux clés « actuelles » activées.

Clé de licence de réserve : clé de licence installée, mais pas encore activée pour Kaspersky Anti-Virus. La clé de licence de réserve entrera en vigueur dès la fin de la période de validité de la clé de licence actuelle.

Clé de licence : fichier avec une extension **.key* qui représente votre clé personnelle, indispensable à l'utilisation de Kaspersky Anti-Virus. La clé de licence est reprise dans le pack logiciel lorsque vous achetez celui-ci chez un revendeur Kaspersky Lab. Par contre, elle vous sera envoyée par courrier électronique si vous achetez le logiciel en ligne. Kaspersky Anti-Virus ne peut fonctionner sans la clé de licence.

Console d'administration : composant offrant une interface graphique pour l'administration de Kaspersky Anti-Virus5.0 for Windows File Servers. Elle fait partie de Kaspersky Administration Kit 5.0.

Copie de sauvegarde : création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et mise de cette copie dans le dossier de sauvegarde. Le fichier pourra être restauré, par exemple pour l'analyse avec des bases antivirus actualisées.

D

Dossier de sauvegarde : dossier spécial prévu pour la conservation des copies de sauvegarde des objets avant leur réparation ou leur suppression.

Durée de validité de la licence : période pendant laquelle vous pouvez utiliser toutes les fonctions de Kaspersky Anti-Virus. Cette durée est définie par la clé de licence et est égale à une année calendaire à partir du jour d'activation de la clé de licence. Lorsque la licence est arrivée à

échéance, les fonctions du logiciel sont réduites : il n'est plus possible de mettre à jour les *bases antivirus et les modules de l'application*.

E

Etat de la protection antivirus : état actuel de la protection antivirus, caractérisé par le niveau de protection de l'ordinateur.

Exclusions : ensemble de paramètres qui permettent d'exclure certains objets de l'analyse. Vous pouvez configurer ces exclusions aussi bien pour la *protection en temps réel* que pour *l'analyse complète*. Par exemple, vous pouvez exclure les *archives* de l'analyse complète de votre ordinateur ou définir les masques des fichiers que vous ne souhaitez pas analyser.

F

Flux NTFS complémentaires (flux NTFS) : flux de données du disque en provenance du système de fichier NTFS qui viennent en complément du flux principal où se trouve son contenu.

G

Groupe d'administration : groupe d'ordinateurs réunis pour la facilité de l'administration du groupe. Le groupe est administré comme un tout. Il est possible de lui appliquer une stratégie de groupe, de l'inclure dans d'autres groupes et d'appliquer des commandes d'administration.

H

Hack Tools : programme utilisé par des personnes malveillantes pour s'instroduire dans l'ordinateur d'autrui. Cette catégorie comprend les dispositifs de balayage, les programmes de déchiffrage de mot de passe et tout autre programme qui vise à pénétrer dans les ressources d'un réseau.

K

Kaspersky Administration Kit 5.0 : application faisant partie des logiciels Kaspersky Business Optimal et Kaspersky Corporate. Elle sert à l'exécution centralisée des principales tâches d'administration pour la gestion du système de protection antivirus du réseau de l'entreprise utilisant les solutions de Kaspersky Lab.

L

Liste noire : base de données reprenant les informations relatives aux clés de licence dont les détenteur ont violé les conditions d'utilisation ou aux clés qui ont été livrées mais qui pour une raison quelconque n'ont pas été vendues. Le contenu de la « liste noire » est mis à jour en même temps que les bases antivirus et sans celui-ci, Kaspersky Anti-Virus ne fonctionnera pas.

M

Masque de fichier : il s'agit de la représentation du nom et de l'extension d'un fichier à l'aide de caractères généraux. Les deux principaux

caractères utilisés à cette fin sont * et ? (* représente une chaîne de caractères quelconques et ? représente un caractère quelconque. Ces caractères permettent de représenter n'importe quel fichier. N'oubliez que le nom du fichier et son extension sont toujours séparés par un point.

Mise à jour : procédure de remplacement/d'ajout de nouveaux fichiers (bases antivirus ou modules logiciels de l'application) depuis les serveurs de mises à jour de Kaspersky Lab.

Mise en quarantaine des objets : mode de traitement d'un objet *suspect* qui consiste à bloquer l'accès et à le mettre en quarantaine pour la suite du traitement.

Mises à jour disponibles : Service Packs contenant l'ensemble des mises à jour urgentes recueillies sur une certaine période ainsi que les modifications apportées à l'architecture de l'application.

Mises à jour urgente : mises à jour critiques des composants de l'application.

Modules de l'application : fichiers faisant partie de la distribution de Kaspersky Anti-Virus for Windows Workstations et responsables de l'exécution des principales fonctions de l'application. A chaque tâche exécutée par Kaspersky Anti-Virus (protection en temps réel, analyse à la demande et mise à jour) correspond un module exécutable distinct. En lançant la tâche depuis la fenêtre principale de l'application, vous lancez le module correspondant à cette application.

N

Niveau recommandé : niveau de protection antivirus qui repose sur les paramètres recommandés par les experts de Kaspersky Lab et qui assure la protection optimale de votre ordinateur. Ce niveau est sélectionné par défaut.

O

Objet infecté : objet qui renferme un code malicieux. Nous vous conseillons vivement de ne pas travailler avec de tels objets car cela pourrait entraîner une infection de votre ordinateur.

Objet OLE : objets ou documents intégrés à d'autres fichiers via la technologie OLE.

Objet suspect : objet dont le code renferme une modification du code d'un virus connu ou d'un code qui évoque celui d'un virus qui n'a pas encore été découvert par Kaspersky Lab.

Objets de démarrage : ensemble des programmes indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont lancés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter de tels objets, ce qui peut par exemple bloquer le lancement du système d'exploitation.

P

Plug-in d'administration de l'application : composant spécial servant d'interface pour l'administration à distance de l'utilisation de l'application via la *Console d'administration*. Le plug-in d'administration est propre à chaque application et fait partie de toutes les applications de Kaspersky Lab qui peuvent être administrées par Kaspersky Administration Kit 5.0.

Pornware : programme établissant une connexion par modem vers un site Internet payant, généralement à contenu pornographique.

Processus de confiance : liste des processus logiciels dont l'activité sur les fichiers n'est pas contrôlée par Kaspersky Anti-Virus en mode de protection en temps réel. Autrement dit, tous les objets exécutés, ouverts et enregistrés par le processus de confiance ne sont pas analysés.

Protection en temps réel : mode de fonctionnement pendant lequel l'application se trouve en permanence dans la mémoire vive de l'ordinateur et surveille les requêtes adressées aux objets des systèmes de fichiers. Avant d'autoriser l'accès à l'objet, l'application vérifie que l'objet est exempt de virus. S'il en détecte un, il propose soit de réparer l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction des paramètres définis).

Q

Quarantaine : dossier spécial prévu pour l'isolement des objets suspects et infectés.

R

Réparation des objets : ensemble des moyens de traitement appliqués aux *objets infectés* qui débouchent sur une restauration complète ou partielle des données ou sur un constat d'incapacité à réparer l'objet en question La réparation des objets s'opère sur la base des enregistrements contenus dans les *bases antivirus*. Lorsque la réparation est la première action prévue pour un objet (autrement dit, la première action exercée sur cet objet directement après sa découverte), une *copie de sauvegarde* de l'objet sera créée avant de procéder à la réparation. En effet, une partie des données peut être perdue pendant la réparation. La copie vous donne la possibilité de restaurer l'objet à l'état antérieur à la réparation.

Réparation des objets au redémarrage : mode de traitement des objets infectés, utilisés par d'autres applications au moment de la réparation. Ce mode consiste à créer une copie du fichier infecté, à réparer la copie et remplace, au redémarrage, le fichier original infecté par la copie réparée.

Restauration : rétablissement de l'objet en *quarantaine* ou dans le *dossier de sauvegarde* vers son répertoire d'origine, c'est-à-dire le répertoire où il se trouvait avant sa mise en quarantaine, sa réparation ou sa

suppression. En cas d'administration à distance, les objets sont restaurés sur l'ordinateur où la *Console d'administration* est installée.

Riskwares : logiciels n'ont pas de fonctions malfaisantes mais qui peuvent être utilisés par des personnes mal intentionnées en qualité de complément à un programme malfaisant car ils contiennent des failles. Cette catégorie reprend les programmes d'administration à distance, les clients IRC, les serveurs FTP et tous les utilitaires servant à arrêter des processus ou à dissimuler des activités.

S

Sécurité maximale : niveau de protection de l'ordinateur correspondant au niveau de protection antivirus maximum, au détriment d'un léger recul des performances du système.

Serveur d'administration : application spéciale assurant les fonctions de centre d'information centralisé sur les applications de Kaspersky Lab installées sur les machines du réseau de l'entreprise et permettant de les administrer. Il fait partie de Kaspersky Administration Kit 5.0.

Serveurs de mises à jour de Kaspersky Lab : liste des serveur http et ftp de Kaspersky Lab à partir desquels Kaspersky Anti-Virus copie les bases antivirus sur votre ordinateur.

Spyware : programme qui vise à accéder de manière illicite aux données de l'utilisateur, de suivre les actions réalisées avec l'ordinateur et de recueillir les informations stockées sur le disque dur. Ce type de programme permet non seulement à son auteur de recueillir des informations, mais également de prendre les commandes des ordinateurs. Le spywares sont diffusés au sein d'applications gratuites et sont installés à l'insu de l'utilisateur. Les programmes de suivi de frappe de clavier, les programmes de déchiffrage de mot de passe et les programmes qui recueillent les informations confidentielles (comme les numéros de carte de crédit) appartiennent à cette catégorie.

Stratégie de groupe : ensemble de paramètres de fonctionnement de l'application dans le groupe d'administration en cas de gestion via Kaspersky Administration Kit 5.0.

Suppression d'un objet : mode de traitement d'un objet qui consiste à le supprimer de votre ordinateur. Ce traitement doit être appliqué aux objets infectés. Lorsque la suppression est la première action prévue, le logiciel crée d'abord une copie de *sauvegarde de l'objet*. Cette copie vous permettra de restaurer l'objet original.

T

Tâche : action exécutée par l'application de Kaspersky Lab.

Technologie iChecker™ : technologie permettant d'exclure de l'analyse les objets qui n'ont pas été modifiés depuis la dernière analyse. Cette technologie repose sur l'utilisation de bases de données avec les sommes de contrôle des objets.

Technologie iStreams™ : cette technologie exclut de l'analyse les fichiers situés sur le disque avec un système de fichiers NTFS et qui n'ont pas changé depuis la dernière analyse. Cette technologie repose sur la technologie de conservation des sommes de contrôle des fichiers dans les flux complémentaires NTFS.

V

Virus inconnu : nouveau virus au sujet duquel il n'existe aucune information dans les *bases antivirus*. En règle générale, les virus inconnus peuvent être malgré tout identifiés par Kaspersky Anti-Virus grâce à *l'analyse heuristique* et ces objets reçoivent le statut de *suspects*

Vitesse maximale : niveau de protection de l'ordinateur correspondant à la vitesse maximale de fonctionnement, au détriment d'un léger recul de la protection antivirus.

APPENDICE B. CODE DE RETOUR LIGNE DE COMMANDE

Les codes de retour de commande sont classés en deux catégories. Les codes de réussite ont une valeur positive, tandis que les codes d'échec ont une valeur négative.

B.1. Codes de retour généraux

Les codes de retour généraux peuvent être produits par n'importe quelle commande

Code	Description
0	Réussite de l'opération
1	Annulation de l'opération
-1	Erreur lors de l'initialisation de l'application
-2	Service inaccessible
-3	Erreur de privilège
-4	Objet introuvable
-5	Syntaxe incorrecte
-6	Action incorrect (tentative de lancement d'une tâche dont l'exécution est déjà en cours)
-99	Erreur interne

B.2. Code de retour pour l'analyse à la demande

Les codes de retour généraux (cf. Appendice B ; p. 104) et les codes de retour spécifiques suivant appartiennent à cette catégorie:

Code	Description
101	Tous les objets suspects ou infectés n'ont pas été supprimés
102	Tous les objets infectés ont été réparés
103	Toutes les variantes des objets infectés ou suspects ont été mises en quarantaine
104	Tous les objets suspects ou infectés ont été supprimés
105	Découverte d'objets infectés
106	Découverte de variantes d'objets infectés
107	Découverte d'objets suspects
108	Tous les objets n'ont pas été traités

B.3. Code de retour de la mise à jour

Les codes de retour généraux (cf. Appendice B, p. 104) et les codes spécifiques suivants appartiennent à cette catégorie :

Code	Descriptiion
200	Tous les fichiers sont à jour. La mise à jour n'est pas nécessaire
201	Toutes les mises à jour n'ont pas été appliquées (ex. :les mises à jour nécessitant le redémarrage du serveur n'ont pas été installées (cf. point 6.2.1.2.4 à la page 49)

Code	Descriptiion
-2xx	Erreru du service de mise à jour où **xx** représente un code particulier: **04** – Les fichiers manquent ou son corrompus **06** – Le fichier est introuvalbe **07** – La source de la mise à jour est bloquée; les fichiers y sont mis à jour **08**, **11**, **12**, **15**, **27**, **31** – Erreur interne de l'application **09** – Erreur de connexion à la liste de serveurs autorisés **17** – Erreur de signature de l'un des fichiers **18** – Erreur lors de l'opération sur le fichier **20** – Erreur de mise à jour vers une version antérieure **21** – Annulation impossible (la copie de sauvegarde des fichiers est absente) **22** – Fichier d'index corrompu **28**– Chargement des fichiers impossible **32** – Erreur d'autorisation sur le serveur proxy **33** – Erreur de DNS **34** – Erreur de connexion au serveur d'administration de Kaspersky Administration Kit

B.4. Code de retour de la licence

Les codes de retour généraux (cf. Appendice B, p. 104) et les codes spécifiques suivants appartiennent à cette catégorie:

Code	Description
-301	La vérification de la licence a échoué (licence manquante, licence reprise dans la liste noire.)
-302	Fin de validité de la licence.

APPENDICE A. KASPERSKY LAB

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

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

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

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

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

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

B.5. Autres produits antivirus

Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

Kaspersky Anti-Virus® Personal Pro

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

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

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

Kaspersky® Anti-Hacker

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

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

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

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

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

Kaspersky® Personal Security Suite

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

Kaspersky® Personal Security Suite possède les fonctions suivantes :

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

Kaspersky Lab News Agent

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

News Agent permet également de:

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

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

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

Kaspersky OnLine Scanner

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

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

Kaspersky Anti-Virus 6.0

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

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et

SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.

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

La défense proactive permet de :

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

Kaspersky® Internet Security 6.0

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

Les fonctions antivirus proposées sont les suivantes :

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

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

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

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

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

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

Kaspersky® Security for PDA

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

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

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

Kaspersky Anti-Virus® 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[2] 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, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 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

[2] En fonction du type de livraison

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, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition ;
- *Ordinateurs de poche* sous 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.

B.6. Coordonnées

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

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

APPENDICE C. CONTRAT DE LICENCE

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

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

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

CONFORMÉMENT À LA LÉGISLATION, LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) ACHETÉS EN LIGNE VIA INTERNET CHEZ KASPERSKY LAB BÉNÉFICIENT D'UN DÉLAI DE RÉTRACTATION DE 7 JOURS FRANCS À COMPTER DE LA RÉCEPTION DES BIEN ACHETÉS, SI CES LOGICIELS N'ONT PAS ÉTÉ DESCELLÉS.

CONCERNANT LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NON ACHETÉS EN LIGNE VIA INTERNET, ILS NE SERONT NI REPRIS NI ÉCHANGÉS SAUF DISPOSITIONS CONTRAIRES PROPRES AU PARTENAIRE CHEZ QUI LE PRODUIT A ÉTÉ ACHETÉ. DANS CE CAS, KASPERSKY LAB N'EST EN AUCUN CAS ENGAGÉ PAR LES CLAUSES DES PARTENAIRES.

LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

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

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser une copie de cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer une copie du Logiciel sur un ordinateur, poste de travail, assistant digital personnel, ou tout autre appareil électronique pour lequel le Logiciel a été conçu (un "Système Client"). Si le Logiciel est inscrit en tant que suite ou paquet avec plus d'un seul Logiciel, cette licence s'applique à tous les Logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée sur le tarif en vigueur ou l'emballage du produit qui concerne chacun de ces Logiciels.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un Système Client ou par plus d'un utilisateur à la fois, sauf comme décrit ci-dessous dans cette section.

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

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

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

1.1.4 Il est interdit de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

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

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

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur ("Serveur") dans un environnement multi-utilisateurs ou en réseau ("Mode-Serveur") uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est exigée pour chaque Système Client ou "siège" pouvant se connecter au Serveur à tout moment, indifféremment du fait que de tels Systèmes Clients inscrits ou sièges sont connectés en même temps au Logiciel, y accèdent ou l'utilisent. L'utilisation d'un logiciel ou de matériel réduisant le nombre de Systèmes Clients ou sièges qui accèdent au Logiciel ou l'utilisent directement (e.g., un logiciel ou matériel de "multiplexage" ou de "regroupement") ne réduit pas le nombre de licences exigées (i.e., le nombre requis de licences égalerait le nombre d'entrées distinctes au logiciel ou matériel de multiplexage ou de regroupement frontal). Si le nombre de Systèmes Clients ou sièges pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. Cette licence vous permet d'effectuer ou de télécharger autant de copies de la Documentation que le réseau compte de Systèmes Clients ou sièges possédant une licence d'utilisation du Logiciel, et pourvu que chaque copie contienne les notes de propriété de la Documentation.

1.3 Licences de volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en oeuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous permet d'effectuer ou de télécharger une copie de la Documentation pour chaque copie additionnelle autorisée par la licence de volume, pourvu que chaque copie contienne toutes les notes de propriété de la Documentation.

2. *Durée*. Ce Contrat est valable pour la période indiquée dans le Fichier Clé d'Identification (Ce fichier est unique et est nécessaire à l'activation complète du Logiciel, voir Aide/ sur Logiciel ou " à propos de ", pour les versions Unix/Linux du Logiciel voir les notifications sur la date d'expiration du Fichier Clé) à moins

que celle-ci n'arrive à terme avant pour l'une des raisons notées ci-après. Ce contrat se terminera automatiquement si vous n'en respectez les termes, limites ou conditions décrites. Au-delà du terme ou expiration de ce Contrat, vous devez immédiatement détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez mettre un terme à ce Contrat à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. Assistance technique.

(i) Kaspersky Lab vous fournira une assistance technique ("Assistance Technique") comme décrit ci-dessous pour une période d'un an à condition que:

(a) le paiement des frais de l'assistance technique en cours ait été fait; et

(b) le Formulaire d'Inscription à l'Assistance Technique fourni avec ce Contrat ou disponible sur le site web de Kaspersky Lab ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Lab avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Lab de juger si vous remplissez les conditions nécessaires pour un accès aux services d'Assistance Technique.

(ii) L'Assistance technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Politique de Confidentialité de Kaspersky Lab déposée sur www.kapersky.com/privacy, et vous consentez explicitement au transfert de données vers d'autres pays que le votre en accord avec les termes de la Politique de Confidentialité.

(iv) "Assistance Technique" signifie:

(a) Mises à jour quotidiennes des bases antivirus;

(b) Mises à jour gratuites du logiciel, incluant des mises à niveau de versions;

(c) Assistance Technique étendue par E-mail et assistance téléphonique fournie par votre Vendeur et/ou Distributeur;

(d) Mises à jour de détection et désinfection de virus sous 24 heures.

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

5. *Confidentialité*. Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez,

fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

6. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de six (6) mois suivant le téléchargement ou l'installation du logiciel, acheté de manière physique, ce dernier fonctionnera correctement comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

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

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

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

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

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

7. *Limites de Responsabilité.*

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

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

(a) Perte de revenus;

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

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

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

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

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

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

(i) Rien dans ce Contrat n'engagera la responsabilité de Kaspersky Lab pour toute Fausse Représentation faite en connaissance de cause.

(ii) La responsabilité de Kaspersky Lab pour Fausse Déclaration quant à une question fondamentale pour la capacité du créateur à exécuter ses engagements envers ce Contrat, sera sujette à la limitation de responsabilité décrite dans le paragraphe 7 (iii).