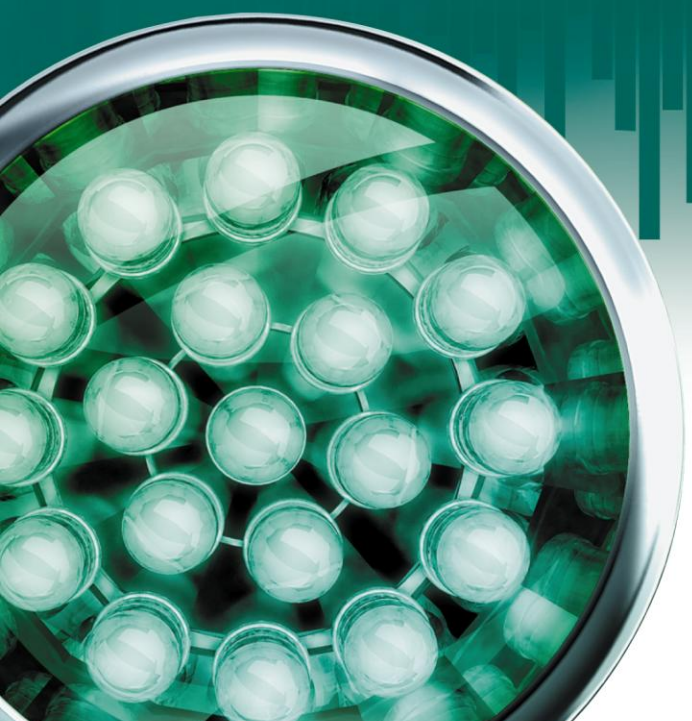
Kaspersky Anti-Virus 8.0 for Linux File Server

MANUEL D'ADMINISTRATEUR

VERSION DU LOGICIEL : 8.0



KASPERSKY lab

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que le présent manuel vous sera utile dans votre travail et qu'il fournir des réponses à la plupart de vos questions.

Ce manuel peut être modifié sans préavis. La version plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.fr/docs.

Date d'édition du document : le 18/10/10

http://www.kaspersky.fr
http://support.kaspersky.fr

TABLE DES MATIERES

INTRODUCTION

Kaspersky Anti-Virus protège des serveurs administrés par le système d'exploitation Linux contre les programmes malveillants qui pénètrent par l'échange de fichiers.

Kaspersky Anti-Virus analyse les disques du serveur et d'autres périphériques montés. Il est capable d'analyser des répertoires particuliers accessibles via les protocoles SMB/CIFS et NFS, ainsi que les répertoires distants montés sur le serveur à l'aide des protocoles SMB/CIFS et NFS.

DANS CETTE SECTION

INFORMATIONS GENERALES SUR KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus 8.0 for Linux File Server (ci-après Kaspersky Anti-Virus ou l'application) protège les serveurs tournant sous le système d'exploitation Linux contre les programmes malveillants qui s'introduisent dans le système de fichiers via les canaux de transfert de données du réseau ou via des supports amovibles.

L'application permet de :

- Analyser les objets du système de fichiers situés sur les disques locaux du serveur ainsi que sur les disques montés et les ressources partagées accessibles via les protocoles SMB/CIFS et NFS.

  L'analyse des objets du système de fichiers s'opère aussi bien en temps réel (protection en temps réel) qu'à la demande.

- Découvrir des objets infectés et suspects.

  Kaspersky Anti-Virus attribue l'état infecté à un objet si le code d'un virus connu a été découvert dans celui-ci. S'il est impossible d'affirmer avec certitude si l'objet est infecté ou non, l'objet est considéré comme suspect.

- Neutraliser les menaces découvertes dans les fichiers.

  En fonction du type de menace, l'application choisit automatiquement l'action à exécuter pour neutraliser la menace : réparer l'objet infecté, placer l'objet suspect en quarantaine, supprimer l'objet ou l'ignorer, à savoir laisser l'objet tel quel.

- Placer les objets suspects en quarantaine.

  Kaspersky Anti-Virus fait isoler des objets qu'il reconnaît comme suspects. Il met de tels objets en quarantaine – les transfère depuis l'endroit d'origine dans le répertoire de sauvegarde spécial dans lequel aux fins de sécurité ils sont conservés sous forme codée. Après chaque mise à jour des bases, Kaspersky Anti-Virus lance automatiquement l'analyse des objets en quarantaine. Certains d'entre eux peuvent être considérés comme sains et seront restaurés.

- Enregistrer des copies de sauvegarde des fichiers avant le traitement antivirus. Restaurer les fichiers depuis les copies de sauvegarde.

- Administrer les tâches et configurer les paramètres.

L'application propose quatre types de tâches gérables par l'utilisateur : la protection en temps réel, l'analyse à la demande, l'analyse des objets en quarantaine et la mise à jour. Les tâches des autres types sont des tâches prédéfinies et ne peuvent être gérées par l'utilisateur.

- Alerter l'administrateur des événements qui indiquent une modification de l'état de la protection du serveur contre les virus et de Kaspersky Anti-Virus dans son ensemble.
- Configurer les actions, via les scripts Shell, qui seront exécutées automatiquement quand un événement déterminé se produit.
- Composer les statistiques et les rapports sur les résultats de l'utilisation.
- Surveiller l'état de la protection du serveur sur le protocole SMTP.
- Actualiser, selon un horaire défini ou à la demande, les bases antivirus depuis l'ordinateur de mise à jour de Kaspersky Lab ou depuis une source indiquée par l'utilisateur.

  Les bases interviennent dans la recherche et la réparation des fichiers infectés. Sur la base des entrées contenues dans ces bases, chaque fichier est soumis à la recherche d'une menace éventuelle : le code du fichier est comparé au code caractéristique d'une menace ou d'une autre.
- Configurer les paramètres de l'application et gérer son utilisation localement, via les outils standard du système d'exploitation, ou à distance depuis n'importe quel ordinateur du réseau local ou via Internet.

  Vous pouvez administrer Kaspersky Anti-Virus :

  - Via la ligne de commande et les instructions d'administration de l'application ;
  - Via la modification du fichier de configuration de l'application ;
  - Via la console Web ;
  - Via Kaspersky Administration Kit.

PROTECTION EN TEMPS REEL ET ANALYSE A LA DEMANDE

Pour sécuriser les serveurs, vous pouvez utiliser les fonctionnalités de *protection en temps réel* et d'*analyse à la demande*.

Protection en temps réel des fichiers

Par défaut, la tâche de protection en temps réel est lancée automatiquement en même temps que Kaspersky Anti-Virus lors du démarrage du serveur et elle est en service en continu. Kaspersky Anti-Virus analyse les fichiers à l'accès.

Kaspersky Anti-Virus vérifie qu'il n'y ait pas dans des fichiers de programmes malveillants de plusieurs types (cf. section " Menaces détectées par Kaspersky Anti-Virus " à la page 11). Lorsqu'un programme fait requête à un fichier du serveur (par exemple, l'enregistre et le lit), Kaspersky Anti-Virus intercepte la requête à ce fichier. À l'aide de ses bases, il vérifie que ce fichier ne contient pas de programmes malveillants (cf. section " À propos des objets infectés ou suspects possédant le statut " Avertissement " " à la page 10). Lorsque Kaspersky Anti-Virus détecte dans le fichier un programme malveillant, celui-là effectue pour ce fichier les actions que vous avez spécifiées, par exemple, il essaie de le réparer et le supprime. Le programme qui a sollicité le fichier ne peut l'utiliser que s'il n'est pas infecté ou si les virus ont bien été neutralisés.

Analyse à la demande

L'analyse à la demande consiste à effectuer une seule analyse complète ou à analyser une sélection de fichiers pour y détecter des menaces éventuelles.

PARTICULARITES DE L'ANALYSE DES LIENS SYMBOLIQUES ET MATERIELS

Lors de l'analyse des liens matériels et symboliques par Kaspersky Anti-Virus, il faut tenir compte des particularités suivantes.

Analyse des liens symboliques

La tâche de protection en temps réel et les tâches d'analyse à la demande de Kaspersky Anti-Virus n'analysent des liens symboliques que si le fichier qui fait l'objet du lien symbolique fait partie de la zone à analyser.

Si le fichier, auquel l'appel se passe à l'aide du lien symbolique, ne fait pas partie de la zone de protection, l'appel vers lui ne sera pas analysé. Si un tel fichier contient un code malveillant, la sécurité du serveur sera en danger !

Analyse des liens matériels

Quand Kaspersky Anti-Virus traite le fichier qui possède plus d'un lien matériel, les scénarios suivants sont possibles selon l'action indiquée sur les objets :

- si l'action **Quarantaine** (placer en quarantaine) a été sélectionnée : le lien matériel traité sera placé en quarantaine, les autres liens matériels ne seront pas traités ;
- Si l'action **Remove** (supprimer) a été sélectionnée : le lien matériel traité sera supprimé. Les autres liens matériels ne seront pas traités ;
- Si l'action **Cure** (réparer) a été sélectionnée : le fichier d'origine sera réparé, ou le lien matériel sera supprimé. A sa place, la copie réparée du fichier d'origine avec le nom du lien matériel supprimé sera créée.

Lors de la restauration du fichier de la quarantaine ou du dossier de sauvegarde, une copie du fichier d'origine avec le nom du lien matériel qui a été placé en quarantaine (dossier de sauvegarde) sera créée. Les rapports avec d'autres liens matériels ne seront pas restaurés.

A PROPOS DES OBJETS INFECTES, SUSPECTS ET POSSEDANT LE STATUT " AVERTISSEMENT "

Kaspersky Anti-Virus contient l'ensemble des bases. Les bases sont des fichiers contenant des signatures qui permettent de détecter dans les objets analysés le code malveillant de centaines de milliers de menaces connues. Ces signatures contiennent des informations sur les segments de contrôle du code des programmes malveillants et des algorithmes de réparation des objets qui contiennent ces programmes.

Lorsque Kaspersky Anti-Virus détecte dans l'objet analysé un segment du code qui correspond parfaitement à un segment de contrôle du code d'une menace malveillante connue selon les informations reprises dans la base, il considère cet objet comme étant *infecté*.

Lorsqu'un objet contient un segment de code qui correspond partiellement au segment de contrôle d'une menace connue (selon les informations déterminées), Kaspersky Anti-Virus attribue à l'objet infecté le statut " Avertissement ". La possibilité de faux-positif existe.

Kaspersky Administration Kit attribue le statut *suspect* aux objets qui sont détectés par l'analyseur heuristique (Heuristic Analyzer). L'analyseur heuristique reconnaît les objets malveillants sur la base de leur comportement. Il est impossible d'affirmer que le code de cet objet correspond parfaitement ou partiellement au code d'une menace connue mais il contient une série d'instructions propres aux menaces.

À PROPOS DE LA MISE EN QUARANTAINE ET DE LA COPIE DE SAUVEGARDE DES OBJETS

Kaspersky Anti-Virus isole des objets infectés et suspects détectés afin de protéger le serveur contre une éventuelle action malveillante.

Placement des objets en quarantaine

Kaspersky Anti-Virus déplace les objets infectés et suspects détectés depuis leur emplacement d'origine vers la quarantaine / le dossier de sauvegarde. Dans ce répertoire, les objets sont sauvegardés sous forme chiffrée. Kaspersky Anti-Virus analyse à nouveau les objets mis en quarantaine après chaque mise à jour des bases de Kaspersky Anti-Virus. Après avoir analysé les objets mis en quarantaine, Kaspersky Anti-Virus peut reconnaître certains d'entre eux comme étant non infectés. Les autres objets peuvent être reconnus par Kaspersky Anti-Virus comme étant infectés.

Si le comportement d'un fichier vous permet de soupçonner qu'il renferme une menace alors que Kaspersky Anti-Virus le considère comme sain, vous pouvez vous-même le mettre en quarantaine pour ensuite l'analyser à l'aide des bases actualisées.

Copie de sauvegarde des objets avant leur traitement ou suppression

Kaspersky Anti-Virus place la copie des objets infectés ou suspects dans le dossier de la quarantaine / de sauvegarde avant de les réparer ou de les supprimer. Ces objets peuvent ne pas se trouver dans l'emplacement d'origine s'ils ont été supprimés ou ils peuvent être sauvegardés sous forme modifiée si Kaspersky Anti-Virus les a réparé.

Vous pouvez restaurer à tout moment l'objet depuis la quarantaine / le dossier de sauvegarde vers son emplacement d'origine ou vers n'importe quel autre répertoire indiqué sur le serveur. Il peut s'avérer nécessaire de restaurer un objet depuis le dossier de sauvegarde, par exemple, si le fichier infecté d'origine contenait des informations importantes que Kaspersky Anti-Virus n'a pas pu préserver lors de la réparation, les rendant inaccessibles.

La restauration des objets infectés et suspects peut entraîner l'infection du serveur.

PROGRAMMES DETECTES PAR KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus est capable de détecter dans le système de fichiers du serveur beaucoup de programmes différents qui peuvent constituer une menace pour la sécurité de l'ordinateur. Certains de ces programmes sont très dangereux pour l'utilisateur ; les autres ne sont dangereux que sous certaines conditions. Après avoir détecté un programme malveillant dans un objet, Kaspersky Anti-Virus le rajoute à une catégorie déterminée possédant son propre niveau de sécurité (élevé, moyen ou bas).

Kaspersky Anti-Virus distingue les catégories de programmes suivantes :

- virus et vers (Virware) ;
- chevaux de Troie (Trojware) ;
- autres programmes malveillants (Malware) ;
- logiciels à caractère pornographique (Pornware) ;
- logiciels publicitaires (Adware) ;
- applications présentant un risque potentiel (Riskware).

L'exposé sommaire des menaces est donné ci-après. Pour en savoir plus sur les programmes malveillants et leur classification, consultez le site de l'" Encyclopédie des virus " de Kaspersky Lab (http://www.viruslist.com/ru/viruses/encyclopedia).

Virus et vers (Virware)

Niveau de danger : élevé

Cette catégorie comprend des virus classiques et des vers de réseau.

Le virus classique infecte les fichiers des autres logiciels ou les données. Il y ajoute son code pour pouvoir les gérer lors de leur lancement. Une fois que le virus classique s'est introduit dans le système, il infecte un fichier, s'y active et exécute son action malveillante.

Les virus classiques se distinguent par leur environnement et le procédé d'infection.

Par environnement, il faut entendre divers secteurs de l'ordinateur, les systèmes d'exploitation ou les applications dans lesquels le code du virus s'introduit. On distingue les virus de fichier, les virus de démarrage, les virus de macro et les virus de script.

Par le procédé d'infection, on sous-entend de divers procédés d'introduction d'un code malveillants dans les objets infectés. Plusieurs types de virus peuvent être identifiés sur la base du mode d'infection. Les virus écraseurs (overwriting) remplacent le code du fichier infecté par leur propre code et suppriment ainsi le contenu du fichier. Le fichier infecté n'est plus exploitable et il ne peut être restauré. Les virus parasites (Parasitic) modifient le code des fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les virus compagnons (Companion) ne modifient pas les fichiers mais créent leurs copies. Lorsque le fichier infecté est exécuté, les commandes passent à son double, à savoir le virus. Il existe également des virus-liens (Link), des virus qui infectent les modules objets (OBJ), des virus qui infectent les bibliothèques de compilateur (LIB), les virus qui infectent les textes source des programmes et d'autres.

Le code des vers de réseau, à l'instar du code des virus classiques, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Toutefois, le ver doit son nom à sa capacité à " ramper " d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

La principale caractéristique qui distingue les vers entre eux c'est le mode de diffusion. Les vers de types différents peuvent se propager avec l'utilisation du courrier, de la messagerie instantanée, des canaux IRC, des réseaux d'échange de fichiers, etc. Parmi les autres vers de réseau, on distingue les vers qui diffusent leur copie via les ressources de réseau. Les programmes malveillants s'introduisent dans les systèmes d'exploitation via les vulnérabilités des systèmes ou des applications, ceux qui pénètrent dans les ressources de réseau publiques ou ceux qui viennent parasiter d'autres menaces.

Plusieurs vers de réseau jouissent d'une très grande vitesse de diffusion.

Ces programmes malveillants nuisent à l'ordinateur infecté mais ils nuisent également à l'utilisateur en le faisant payer davantage pour le trafic de réseau et en surchargeant les canaux Internet.

Chevaux de Troie (Trojware)

Niveau de danger : élevé

Les chevaux de Troie (classes Trojan, Backdoor, Rootkit et autres) exécutent des actions qui ne sont pas sanctionnées par l'utilisateur de l'ordinateur, par exemple, ils volent des mots de passe, sollicitent des ressources Internet et téléchargent et installent d'autres programmes malveillants.

À la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie en s'infiltrant dans les fichiers et en les infectant. Ils s'infiltrent sur les ordinateurs via le courrier Internet ou via le navigateur lorsque l'internaute visite un site web " infecté ". Les chevaux de Troie sont exécutés sur intervention de l'utilisateur. Ils entament leur action malveillante au démarrage.

Les dommages causés par les chevaux de Troie peuvent s'avérer beaucoup plus graves que ceux causés par une attaque de virus traditionnelle.

Les chevaux de Troie Backdoor sont considérés comme les plus dangereux de tous les chevaux de Troie. Leurs fonctions évoquent celles des applications d'administration à distance : s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu mal intentionné d'administrer l'ordinateur à distance.

Parmi les chevaux de Troie, on distingue les outils de dissimulation d'activité (Rootkit). À l'instar des autres chevaux de Troie, les Rootkits s'infiltrent dans le système sans que l'utilisateur ne s'en aperçoive. Ils n'exécutent pas d'actions

malveillantes mais ils cachent les autres programmes malveillants et leurs activités et ce faisant, ils prolongent la présence de ceux-ci dans le système infecté. Les Rootkits peuvent dissimuler des fichiers et des processus dans la mémoire de l'ordinateur infecté ou dissimuler les requêtes des personnes mal intentionnées adressées au système.

Autres programmes malveillants (Malware)

Niveau de danger : moyen

Les autres programmes malveillants ne présentent pas de danger pour l'ordinateur sur lequel ils sont exécutés, mais ils peuvent être utilisés pour l'organisation d'attaques de réseau sur des ordinateurs distants, l'intrusion dans des ordinateurs ou la création d'autres virus et chevaux de Troie.

Les applications malveillantes de cette catégorie sont fort variées. Il s'agit notamment *des attaques de réseau* (catégorie DoS (Denial-of-Service)). Ils envoient de nombreuses requêtes vers des ordinateurs distants ce qui provoque la défaillance de ces derniers. *Des blagues de mauvais goût* (types BadJoke, Hoax) effraient l'utilisateur à l'aide des messages semblables à ceux que pourrait produire un virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu. *Des encodeurs* (classes FileCryptor, PolyCryptor) encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus. *Des constructeurs* (classe Constructor) permettent de créer de nouveau virus, des modules d'objet et des fichiers infectés. *Des utilitaires spam* (classe SpamTool) collectent sur l'ordinateur infecté des adresses électroniques ou le transforment en une machine de diffusion du spam.

Logiciels à caractère pornographique (Pornware)

Niveau de danger : moyen

Les logiciels à caractère pornographique appartiennent à la catégorie des programmes présentant un danger potentiel (not-a-virus). Ils possèdent des fonctions qui nuiront à l'utilisateur uniquement si certaines conditions sont satisfaites.

Ces logiciels servent à afficher du contenu pornographique. En fonction de leur comportement, on distingue trois types : numéroteurs automatiques (Porn-Dialer), programmes pour le téléchargement de fichiers depuis Internet (Porn-Downloader) et outils (Porn-Tool). Les numéroteurs automatiques établissent une connexion avec des ressources Internet pornographiques payantes par téléphone tandis que les logiciels de téléchargement de fichiers depuis Internet téléchargent du contenu pornographique sur l'ordinateur. Les outils sont les programmes liés à la recherche et à l'affichage du contenu pornographique (par exemple, des barres d'outils spéciales pour les navigateurs et des lecteurs vidéo spécifiques).

Logiciels publicitaires (Adware)

Niveau de danger : moyen

Les logiciels publicitaires sont considérés comme potentiellement dangereux (classe not-a-virus). Ils s'intègrent sans autorisation dans les autres logiciels pour afficher des annonces publicitaires. Plusieurs de ces logiciels affichent des publicités, mais ils recueillent également des informations personnelles sur l'utilisateur et les transmettent à leur auteur, modifient des paramètres du navigateur (pages de démarrage et de recherche, niveaux de sécurité, etc.) ou créent un trafic qui n'est pas soumis au contrôle de l'utilisateur. Les actions des logiciels publicitaires peuvent compromettre la politique de sécurité et provoquer également des pertes financières directes.

Applications présentant un risque potentiel (Riskware)

Niveau de danger : bas

Les applications qui présentent un risque potentiel appartiennent à la catégorie des programmes dangereux (classe not-a-virus). Ces programmes peuvent être vendus légalement et être utilisés tous les jours, par exemple, par les administrateurs de réseau.

Les programmes potentiellement dangereux sont certains programmes d'administration à distance tels que Remote Administrator, programmes de réception des informations sur le réseau.

OBTENTION DES INFORMATIONS SUR KASPERSKY ANTI-VIRUS

Kaspersky Lab fournit de différentes sources d'information sur Kaspersky Anti-Virus. Sélectionnez la question qui vous convient le mieux en fonction d'importance et d'urgence.

Si vous avez déjà acheté Kaspersky Anti-Virus vous pouvez vous adresser au Service d'assistance technique. Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum au http://forum.kaspersky.fr.

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources d'informations suivantes sur Kaspersky Anti-Virus :

- la page de Kaspersky Anti-Virus sur le site Web de Kaspersky Lab
- documentation
- manual pages

La page sur le site Web de Kaspersky Lab

http://www.kaspersky.fr/kaspersky_anti-virus_file_server

Sur cette page, vous allez retrouver les informations générales sur l'application, ses possibilités et ses particularités. Vous pouvez acheter Kaspersky Anti-Virus ou prolonger sa durée d'utilisation dans notre magasin en ligne.

Documentation

Le **Manuel d'installation** décrit la fonction et l'utilisation de Kaspersky Anti-Virus, la configuration requise de l'ordinateur pour pouvoir installer Kaspersky Anti-Virus, les instructions d'installation, la vérification du bon fonctionnement et la configuration initiale.

Le **Manuel d'administrateur** contient les informations sur l'administration de Kaspersky Anti-Virus via l'utilitaire de la ligne de commande, Kaspersky Web Management Console et Kaspersky Administration Kit.

Cette documentation au format PDF sont fournis avec Kaspersky Anti-Virus. Vous pouvez télécharger les fichiers contenant les documents depuis la page de Anti-Virus sur le site de Kaspersky Lab.

Manual pages

Vous pouvez consulter les fichiers manual pages suivants pour obtenir les renseignements sur Kaspersky Anti-Virus :

- administration de Kaspersky Anti-Virus à l'aide de la ligne de commande :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-control.1.gz*;
  - pour FreeBSD – */usr/local/man/man1/kav4fs-control.1.gz;*
- configuration des paramètres généraux de Kaspersky Anti-Virus :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs.conf.5.gz*;

  - pour FreeBSD – */usr/local/man/man5/kav4fs.conf.5.gz;*

- configuration de la tâche de protection en temps réel :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-oas.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-oas.conf.5.gz;*
- configuration des tâches d'analyse à la demande :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-ods.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-ods.conf.5.gz;*
- configuration des tâches de mise à jour :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-update.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-update.conf.5.gz;*
- configuration des paramètres du dossier de quarantaine et des objets réservés avant leur réparation ou suppression :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-quarantine.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-quarantine.conf.5.gz;*
- configuration des notifications :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-notifier.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-notifier.conf.5.gz;*
- configuration des paramètres de l'agent SNMP :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-snmp.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-snmp.conf.5.gz;*
- configuration des paramètres du référentiel des événements :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-events.conf.5.gz*;
  - pour FreeBSD – */usr/local/man/man5/kav4fs-events.conf.5.gz;*
- description de l'utilitaire qui modifie le mot de passe de l'utilisateur Web Management Console :
  - pour Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-wmconsole-passwd.1.gz*;
  - pour FreeBSD – */usr/local/man/man1/kav4fs-wmconsole-passwd.1.gz;*
- description de l'utilitaire qui modifie les paramètres de connexion avec le Serveur d'administration Kaspersky Administration Kit :
  - pour Linux – */opt/kaspersky/klnagent/share/man/man1/klmover.1.gz*;
- description de l'utilitaire qui modifie les paramètres de connexion avec le Serveur d'administration Kaspersky Administration Kit :
  - pour Linux – */opt/kaspersky/klnagent/share/man/man1/klnagchk.1.gz*;

APPEL AU SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez déjà acheté Kaspersky Anti-Virus, vous pouvez obtenir des renseignements sur celle-ci auprès des opérateurs du Service du Support Technique, par téléphone ou via Internet.

Avant de contacter le service d'assistance technique veuillez prendre connaissance des règles de l'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Requête électronique adressée au Service d'assistance technique

Vous pouvez poser vos questions aux experts du service d'assistance technique en remplissant le formulaire en ligne dans le système de traitement des demandes des clients (http://support.kaspersky.com/fr/helpdesk.html).

Vous pouvez envoyer vos messages en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une requête par voie électronique, vous devez indiquer **le numéro de client** obtenu lors de l'enregistrement sur le site Internet du service d'assistance technique ainsi que **le mot de passe**.

Si vous n'êtes pas encore un utilisateur enregistré des applications de Kaspersky Lab, vous pouvez remplir le formulaire d'inscription (https://support.kaspersky.com/fr/PersonalCabinet/Registration/Form/). Lors de l'enregistrement, veuillez spécifier le nom du fichier de clé.

L'opérateur du service d'assistance technique vous enverra sa réponse dans votre Espace personnel(https://support.kaspersky.com/ru/PersonalCabinet) , ainsi que à l'adresse électronique que vous avez indiquée dans votre demande.

Décrivez le plus exactement possible le problème que vous rencontrez. Dans les champs obligatoires, indiquez :

- **Le type de la requête**. Sélectionnez le sujet qui correspond le mieux au problème rencontré, par exemple, " Problème d'installation / de suppression du logiciel " ou " Problème de recherche / de neutralisation de virus ".
- **Nom et numéro de version de Kaspersky Anti-Virus**.
- **Texte de la demande**. Décrivez en détails le problème rencontré.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenus lors de l'enregistrement sur le site du Service d'assistance technique.
- **Adresse de messagerie**. Il s'agit de l'adresse à laquelle les experts du Service d'assistance technique enverront la réponse à votre question.

Assistance technique par téléphone

Si le problème est urgent, vous pouvez toujours téléphoner au Service d'assistance technique dans votre ville. Lorsque vous contactez les experts du Service d'assistance technique russe (http://support.kaspersky.ru/support/support_local) ou internationale (http://support.kaspersky.ru/support/international) n'oubliez pas de fournir les informations relatives à Kaspersky Anti-Virus (http://support.kaspersky.ru/support/details), pour que nos experts puissent vous aider dans les délais les plus courts.

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum au http://forum.kaspersky.fr.

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

UTILISATION DE LA CONSOLE WEB DE KASPERSKY ANTI-VIRUS

La console Web de Kaspersky Anti-Virus (ci-après, la console Web) est un moyen d'administration de Kaspersky Anti-Virus via le browser web.

Sur la console Web, vous pouvez exécutez les actions suivantes :

- afficher l'état de la protection du serveur sur lequel est installé Kaspersky Anti-Virus, créer les rapports sur l'état de la protection et sur le fonctionnement de Kaspersky Anti-Virus ;
- administrer Kaspersky Anti-Virus et le configurer.

La console Web est fournie avec Kaspersky Anti-Virus. Les actions nécessaires à la configuration et au lancement de la console Web sont décrites dans le manuel *Kaspersky Anti-Virus 8.0 for Linux File Server. Manuel d'installation*.

Un compte **admin** est requis pour accéder à la console Web de Kaspersky Anti-Virus. Le mot de passe de ce compte est donné pendant la configuration initiale de Kaspersky Anti-Virus. Ce compte peut être utilisé pour l'accès simultané dans la console Web depuis des postes différents.

Si deux utilisateurs, qui ont ouvert au même moment la fenêtre de la console Web depuis des ordinateurs différents, modifient un paramètre quelconque de Kaspersky Anti-Virus, Kaspersky Anti-Virus appliquera la valeur du dernier paramètre sauvegardé.

LANCEMENT DE LA CONSOLE WEB

Vous pouvez lancer la console Web dans le navigateur Internet de l'ordinateur protégé ou d'un autre ordinateur qui se trouve dans le même segment de réseau que le serveur et qui satisfait les configurations matérielles et logicielles.

Pour ouvrir la console Web de Kaspersky Anti-Virus, procédez comme suit :

1. Saisissez l'URL suivant dans la ligne d'adresse du navigateur Internet :

   ```
   http://<Adresse IP ou nom de domaine du serveur à protéger>:9080
   ```

2. Sur la page **Lancement**, saisissez le mot de passe d'utilisateur de la console Web et cliquez sur le bouton **Lancer**.

   Lors du premier lancement de la console Web, vous devez saisir le mot de passe d'utilisateur donné pendant la configuration initiale de Kaspersky Anti-Virus.

Si vous n'avez pas défini le mot de passe d'accès à Web Management Console pendant la configuration initiale de Kaspersky Anti-Virus, vous pouvez le faire plus tard à l'aide de l'utilitaire /opt/kaspersky/kav4fs/bin/kav4fs-wmconsole-passwd.

CHANGEMENT DU MOT DE PASSE DE L'UTILISATEUR DE LA CONSOLE WEB

Le compte utilisateur sous les privilèges duquel la console Web sera utilisée possède par défaut les paramètres suivants :

- Nom d'utilisateur : **admin**.

- Mot de passe de l'utilisateur : donné pendant la configuration initiale de Kaspersky Anti-Virus.

Le cas échéant, vous pouvez modifier le mot de passe de l'utilisateur.

Pour modifier le mot de passe de l'utilisateur de la console Web, procédez comme suit :

1. A gauche dans la fenêtre de la console Web de Kaspersky Anti-Virus sélectionnez la section **Paramètres généraux**.

2. Saisissez le mot de passe de l'utilisateur employé pour l'instant dans le champ **Mot de passe actuel**.

3. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe de l'utilisateur et confirmez-le dans le champ **Confirmation du nouveau mot de passe**.

4. Cliquez sur le bouton **Changer de mot de passe**.

DEMARRAGE ET ARRET DE KASPERSKY ANTI-VIRUS

Attention ! Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kav4fs-supervisor est lancé sur l'ordinateur.

Par défaut, Kaspersky Anti-Virus est lancé automatiquement lors du démarrage du système d'exploitation (aux niveaux d'exécution par défaut adoptés pour chaque système d'exploitation). Kaspersky Anti-Virus lance toutes les tâches système ainsi que les tâches définies par l'utilisateur dont la planification contient la règle d'exécution PS (cf. page 156).

Si vous arrêtez Kaspersky Anti-Virus, toutes les tâches en cours d'exécution seront arrêtées. Après le lancement réitéré de Kaspersky Anti-Virus, ces tâches ne reprendront pas automatiquement. Seules les tâches définies par l'utilisateur dont la planification contient la règle d'exécution PS (cf. page 156) seront à nouveau lancées.

- *Pour lancer Kaspersky Anti-Virus, exécutez la commande :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --start-app
  ```

- Pour arrêter *Kaspersky Anti-Virus*, exécutez la commande :

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --stop-app
  ```

- *Pour redémarrer Kaspersky Anti-Virus, exécutez la commande :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --restart-app
  ```

ADMINISTRATION DES TACHES DE KASPERSKY ANTI-VIRUS

Tâche : composant de Kaspersky Anti-Virus qui réalise une partie des fonctions de l'application. Par exemple, la tâche de protection en temps réel protège les fichiers en temps réel, la tâche de mise à jour télécharge et installe les mises à jour des bases de Kaspersky Anti-Virus, etc.

- *Pour obtenir la liste des tâches de Kaspersky Anti-Virus, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-task-list
```

L'utilisateur peut gérer (cf. page 21) la protection à l'aide des tâches suivantes :

- **OAS** – tâche de protection en temps réel ;
- **ODS** – tâche d'analyse à la demande ;
- **QS** – tâche de l'analyse des objets mis en quarantaine ;
- **Update** – tâches de mise à jour.

Les tâches des autres types sont des tâches prédéfinies et ne peuvent être gérées par l'utilisateur. Vous pouvez uniquement modifier les paramètres de fonctionnement.

DANS CETTE SECTION

CREATION D'UNE TACHE D'ANALYSE A LA DEMANDE OU DE MISE A JOUR

Une tâche de chaque type est créée lors de l'installation de Kaspersky Anti-Virus. Vous pouvez créer des tâches d'analyse à la demande et des tâches de mise à jour définies par l'utilisateur.

- *Pour créer une tâche d'analyse à la demande, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \

--create-task <nom de la tâche> --use-task-type=ODS
```

La tâche créée sera exécutée selon les paramètres par défaut :

- tous les objets locaux et montés seront repris dans la couverture d'analyse ;
- l'analyse sera réalisée conformément au niveau de sécurité **recommandé** (cf. page 46).

Vous pouvez créer une tâche d'analyse à la demande avec les paramètres requis. Pour ce faire, saisissez le chemin d'accès complet au fichier contenant les paramètres de la tâche à l'aide de l'argument **--file** de l'instruction **--create-task**.

Pour créer une tâche de mise à jour, procédez comme suit :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--create-task <nom de la tâche> --use-task-type=Update \
--file=<chemin d'accès au fichier contenant les paramètres de la tâche>
```

La création de la tâche de mise à jour réussira uniquement si le chemin d'accès au fichier contenant les paramètres de la tâche est défini.

SUPPRESSION DE LA TACHE D'ANALYSE A LA DEMANDE OU DE MISE A JOUR

Vous pouvez supprimer les tâches de mise à jour, ainsi que les tâches d'analyse à la demande (sauf la tâche **Analyse des objets en quarantaine** (ID=10) et **On-Demand Scan** (ID=9)).

Vous ne pouvez pas supprimer la tâche de protection en temps réel.

Pour supprimer une tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --delete-task <ID de la tâche>
```

ADMINISTRATION DE LA TACHE EN MODE MANUEL

Les actions décrites dans cette rubrique sont accessibles pour les types de tâche OAS, ODS, QS et Update.

Vous pouvez suspendre et relancer toutes les tâches, sauf les tâches de mise à jour.

Vous pouvez lancer plusieurs tâches d'analyse à la demande simultanément.

Pour lancer une tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task <ID de la tâche>
```

Pour arrêter une tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --stop-task <ID de la tâche>
```

Pour suspendre une tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --suspend-task <ID de la tâche>
```

Pour reprendre une tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --resume-task <ID de la tâche>
```

L'ADMINISTRATION AUTOMATIQUE DES TACHES

Outre l'administration manuelle des tâches de Kaspersky Anti-Virus, il est possible d'utiliser l'administration automatique. Pour ce faire, planifiez la tâche.

Planification d'une tâche : ensemble de règles qui définissent l'heure de lancement, de suspension ou d'arrêt d'une tâche.

L'administration automatique est supportée pour les tâches de types suivants :

- protection en temps réel – les règles de lancement, d'arrêt et de suspension sont accessible pour ce type de tâches ;
- analyse à la demande – les règles de lancement, d'arrêt et de suspension sont accessible pour ce type de tâches ;
- mise à jour des bases – uniquement les règles de lancement sont accessible pour ce type de tâches.

Pour configurer la planification de la tâche à l'aide du fichier de configuration, procédez comme suit :

1. Enregistrez les paramètres de la planification de la tâche dans le fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control -T --get-schedule <ID de la tâche> \
   --file=<chemin d'accès complet au fichier>
   ```

2. Attribuez la valeur **yes** au paramètre **Enabled**.
3. Spécifiez les paramètres de la planification (cf. page 155).
4. Importez les paramètres de planification dans la tâche :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control --set-schedule <ID de la tâche> \
   --file=<chemin d'accès complet au fichier>
   ```

CONSULTATION DE L'ETAT DE LA TACHE

Un des aspects de l'administration des tâches est le contrôle de l'état des tâches.

Les tâches de Kaspersky Anti-Virus peuvent avoir un des états suivants :

- **Started** – en cours d'exécution ;
- **Starting** – en cours de lancement ;
- **Stopped** – arrêtée ;
- **Stopping** – en cours d'arrêt ;
- **Suspended** – suspendue ;
- **Suspending** – en cours de suspension ;
- **Resumed** – reprise ;
- **Resuming** – en cours de reprise ;
- **Failed** – terminée par une erreur ;

- **Interrupted by user** – l'utilisateur a interrompu l'exécution de la tâche.

Pour afficher l'état de la tâche de mise à jour, saisissez l'instruction,

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-task-state <ID  de la tâche>
```

Exemple d'instruction :

```
Name: On-demand scan

Id: 9

Class: ODS

State: Stopped
```

CONSULTATION DES STATISTIQUES DE LA TACHE

Vous pouvez obtenir les statistiques du fonctionnement des tâches de Kaspersky Anti-Virus. Il est possible de consulter les statistiques pour les tâches suivantes :

- **Application** : statistiques générales de Kaspersky Anti-Virus ;
- **Quarantine** : statistiques de la quarantaine ;
- **OAS** : statistiques de la tâche de protection en temps réel ;
- **ODS** : statistiques de la tâche d'analyse à la demande ;
- **Backup** : statistiques du dossier de sauvegarde ;
- **Update** : statistiques des mises à jour.

Les indicateurs de tâche sont indispensables pour les tâches de type ODS et Update. Si l'identificateur n'apparaît pas, ce sont les statistiques générales pour la tâche du type indiqué qui seront présentées.

Pour afficher les statistiques de la tâche, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-stat <type de la tâche> [--task-id <ID de la tâche>]
```

Vous pouvez limiter l'intervalle de temps à afficher les statistiques.

La date et l'heure de début et de fin d'une période sont saisies au format **[YYYY-MM-DD] [HH24:MI:SS]**.

Pour afficher les statistiques après un certain temps, exécutez la commande suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-stat <type de la tâche> \
--from=<début d'une période> --to=<fin d'une période>
```

Si la valeur de la variable `<début d'une période>` n'est pas indiquée, les statistiques sont récoltées depuis le lancement de la tâche. Si la valeur de la variable `<fin d'une période>` n'est pas indiquée, les statistiques sont récoltées jusqu'au moment en cours.

Vous pouvez sauvegarder les statistiques des tâches dans les fichiers de deux formats : HTML et CSV. Par défaut, le format du fichier est indiqué par l'extension du fichier.

- *Afin d'enregistrer les statistiques dans un fichier, exécutez la commande suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \

--get-stat <type de la tâche> [--task-id <ID de la tâche>]

--export-report=<chemin d'accès complet au fichier>
```

MISE A JOUR DE KASPERSKY ANTI-VIRUS

Durant la validité de la licence, vous pouvez obtenir les mises à jour des bases de Kaspersky Anti-Virus.

Les bases sont des fichiers contenant des signatures qui permettent de détecter dans les objets analysés le code malveillant de menaces connues. Ces signatures contiennent des informations sur les segments de contrôle du code des programmes malveillants et des algorithmes de réparation des objets qui contiennent ces programmes.

Des analystes spécialisés en virus de Kaspersky Lab détectent tous les jours un grand nombre de nouvelles menaces et créent pour ces dernières des signatures d'identification qu'ils intègrent à la mise à jour des bases. (*La mise à jour des bases* reprend un ou plusieurs fichiers contenant les signatures qui identifient les menaces détectées depuis la dernière mise à jour). Pour réduire le risque d'infection du serveur au minimum, téléchargez les mises à jour régulièrement.

Kaspersky Lab peut diffuser des paquets de mises à jour des modules logiciels de Kaspersky Anti-Virus. Les paquets de mise à jour sont répartis entre les paquets urgents (critiques) et les paquets ordinaires. Les paquets de mise à jour urgents supprimer les vulnérabilités et les erreurs tandis que les paquets ordinaires ajoutent de nouvelles fonctions ou améliorent les fonctions existantes.

Durant la validité de la licence, vous pouvez installer ces mises à jour manuellement après les avoir téléchargées depuis le site Web de Kaspersky Lab.

Cependant, vous pouvez installer automatiquement les mises à jour des modules des autres applications de Kaspersky Lab.

Mise à jour des bases

Lors de l'installation, Kaspersky Anti-Virus a reçu les bases actuelles depuis un des serveurs http de mises à jour de Kaspersky Lab et si vous avez configuré la mise à jour automatique des bases, Kaspersky Anti-Virus l'exécutera selon la planification, toutes les 30 minute ou à l'aide de la tâche de mise à jour préconfigurée (ID=6).

Vous pouvez configurer la tâche de mise à jour préconfigurée et créer des tâches de mise à jour définies par l'utilisateur.

Si le téléchargement des mises à jour échoue ou termine par une erreur, Kaspersky Anti-Virus continuera d'utiliser les bases actualisées la dernière fois. Si les bases de Kaspersky Anti-Virus sont corrompues, vous pourrez revenir aux bases antérieures à la mise à jour.

Par défaut, si les bases de Kaspersky Anti-Virus ne sont pas mises à jour durant une semaine à partir de la dernière publication des mises à jour par Kaspersky Lab, Kaspersky Anti-Virus consigne l'événement *Les bases sont dépassées* (AVBasesAreOutOfDate) dans le journal. Si les bases ne sont pas mises à jour durant deux semaines, il consigne l'événement *Les bases sont fortement dépassées* (AVBasesAreTotallyOutOfDate).

Copie des mises à jour des bases et des modules de l'application Distribution des mises à jour

Vous pouvez télécharger les mises à jour sur chacun des ordinateurs protégés ou utiliser un seul ordinateur en tant qu'intermédiaire en copiant les mises à jour sur celui-ci et en les distribuant après sur les ordinateurs. Si vous utilisez l'application Kaspersky Administration Kit pour l'administration centralisée de la protection des ordinateurs au sein d'une entreprise, vous pouvez utiliser le Serveur d'administration Kaspersky Administration Kit en tant qu'intermédiaire pour distribuer les mises à jour.

Pour enregistrer les mises à jour des bases sur l'ordinateur intermédiaire sans les utiliser, configurez *la copie des mises à jour* dans la tâche de mise à jour.

DANS CETTE SECTION

SELECTION DE LA SOURCE DES MISES A JOUR

La source des mises à jour (cf. page 190) est la source qui contient les mises à jour des bases de Kaspersky Anti-Virus. Les serveurs HTTP ou FTP, les répertoires locaux ou de réseau peuvent être utilisés en tant que source de mise à jour.

Les serveurs de mises à jour de Kaspersky Lab sont une source principale de mises à jour. Il s'agit de sites Internet spéciaux qui hébergent les mises à jour des bases et des modules de programme pour tous les logiciels de Kaspersky Lab.

- *Pour sélectionner les serveurs de Kaspersky Lab en tant que source des mises à jour, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.SourceType=KLServers
```

- *Pour désigner en tant que source des mises à jour le Serveur d'administration Kaspersky Administration Kit :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.SourceType=AKServer
```

Pour réduire le trafic Internet, vous pouvez configurer la mise à jour des bases de Kaspersky Anti-Virus depuis le répertoire local ou de réseau (cf. page 26).

MISE A JOUR DEPUIS LE REPERTOIRE LOCAL OU DE RESEAU

La procédure de récupération des mises à jour depuis le répertoire local est la suivante :

1. Un des ordinateurs du réseau reçoit le paquet des mises à jour de Kaspersky Anti-Virus depuis les serveurs de mises à jour de Kaspersky Lab sur Internet ou depuis toute autre ressource Web contenant l'ensemble des mises à jour actualisé. Les mises à jour récupérées de la sorte sont placées dans un répertoire partagé.

2. Les autres ordinateurs sollicitent le réservoir partager afin d'obtenir les mises à jour des bases de Kaspersky Anti-Virus.

- *Pour recevoir les mises à jour des bases de Kaspersky Anti-Virus dans le répertoire partagé d'un des ordinateurs du réseau, exécutez les actions suivantes :*

1. Créez un répertoire où seront enregistrées les mises à jour des bases de Kaspersky Anti-Virus.

2. Partagez le répertoire ainsi créé.

3. Créez le fichier de configuration contenant les paramètres avec les valeurs suivantes :

```
UpdateType="RetranslateProductComponents"
[CommonSettings]
SourceType="KLServers"
UseKLServersWhenUnavailable=yes
UseProxyForKLServers=no
UseProxyForCustomSources=no
PreferredCountry=""
ProxyServer=""
ProxyPort=3128
ProxyBypassLocalAddresses=yes
ProxyAuthType="NotRequired"
ProxyAuthUser=""
ProxyAuthPassword=""
UseFtpPassiveMode=yes
ConnectionTimeout=10
[UpdateComponentsSettings]
Action="DownloadAndApply"
[RetranslateUpdatesSettings]
RetranslationFolder="<chemin d'accès complet au répertoire créé>"
```

4. Importez les paramètres depuis le fichier de configuration dans la tâche à l'aide de l'instruction :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
--file=<chemin d'accès complet au fichier>
```

5. Lancez la tâche de mise à jour à l'aide l'instruction :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task <ID de la tâche de mise à jour>
```

Les bases de Kaspersky Anti-Virus seront chargées dans le répertoire partagé.

➧ *Pour désigner le répertoire partagé en tant que source des mises à jour pour les autres ordinateurs du réseau, exécutez les actions suivantes :*

1. Créez le fichier de configuration contenant les paramètres avec les valeurs suivantes :

```
UpdateType="AllBases"
[CommonSettings]
SourceType="Custom"
UseKLServersWhenUnavailable=yes
UseProxyForKLServers=no
UseProxyForCustomSources=no
PreferredCountry=""
ProxyServer=""
ProxyPort=3128
ProxyBypassLocalAddresses=yes
ProxyAuthType="NotRequired"
```

```
ProxyAuthUser=""
ProxyAuthPassword=""
UseFtpPassiveMode=yes
ConnectionTimeout=10
[CommonSettings:CustomSources]
Url="/home/bases"
Enabled=yes
[UpdateComponentsSettings]
Action="DownloadAndApply"
```

2. Importez les paramètres depuis le fichier de configuration dans la tâche à l'aide de l'instruction :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
--file=<chemin d'accès complet au fichier>
```

UTILISATION DU SERVEUR PROXY

Si le serveur proxy est utilisé pour accéder à Internet, il faudra configurer ses paramètres.

- *Pour activer l'utilisation du serveur proxy lors de l'accès aux serveurs de mises à jour deKaspersky Lab, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.UseProxyForKLServers=yes \
CommonSettings.ProxyBypassLocalAddresses=yes \
CommonSettings.ProxyServer=proxy.company.com \
CommonSettings.ProxyPort=3128
```

- *Pour activer l'utilisation du serveur proxy lors de l'accès aux sources de mises à jour définies par l'utilisateur, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.UseProxyForCustomSources=yes \
CommonSettings.ProxyBypassLocalAddresses=yes \
CommonSettings.ProxyServer=proxy.company.com \
CommonSettings.ProxyPort=3128
```

- *Pour configurer les paramètres de l'authentification sur le serveur proxy, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.ProxyAuthType=Plain \
CommonSettings.ProxyAuthUser=user \
CommonSettings.ProxyAuthPassword=password
```

RETOUR A LA VERSION ANTERIEURE DES BASES

Avant d'appliquer les mises à jour des bases, Anti-Virus crée des copies de réserve des bases utilisées jusqu'à présent. Si la mise à jour échoue ou se solde par un échec, Anti-Virus revient automatiquement aux bases en vigueur avant la dernière mise à jour.

Si des problèmes se présentent après la mise à jour, vous pouvez utiliser les mises à jour installées antérieurement. La tâche de remise à la version précédente des bases a été développée à cette fin.

- *Pour lancer la tâche de remise à l'état antérieur à la mise à jour, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 14
```

PROTECTION EN TEMPS REEL DES FICHIERS

La tâche de protection en temps réel permet de prévenir l'infection du système de fichiers de l'ordinateur. Par défaut, la tâche de protection en temps réel est lancée automatiquement au démarrage de Kaspersky Anti-Virus. La tâche demeure dans la mémoire vive de l'ordinateur et analyse tous les fichiers qui sont ouverts, enregistrés et lancés. Vous pouvez l'arrêter, la lancer, la suspendre et la reprendre.

Vous ne pouvez pas créer de tâches de protection en temps réel définies par l'utilisateur.

DANS CETTE SECTION

COMPOSITION DES NIVEAUX DE SECURITE PREDEFINIS DANS LA TACHE DE PROTECTION EN TEMPS REEL

Les experts de Kaspersky Lab ont configuré trois niveaux de protection. Vous devez choisir le niveau qui correspond le mieux aux conditions de travail et à la situation en vigueur. Vous avez le choix entre les niveaux de sécurité suivants :

- **Faible**

Le niveau de sécurité **Faible** peut être spécifié sur le serveur si le réseau est doté de mesures de sécurité en plus de l'utilisation d'Anti-Virus sur les serveurs et postes de travail. Par exemple, des pare-feu sont configurés, des stratégies de sécurité pour les utilisateurs de réseau sont en vigueur.

Au niveau de sécurité **Faible**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]

ScanArchived=no
```

```
ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=yes

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Cure"

InfectedSecondAction="Skip"

SuspiciousFirstAction="Quarantine"

SuspiciousSecondAction="Skip"

UseAdvancedActions=no

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no
```

- **Recommandé**

Le niveau de sécurité **Recommandé** est installé par défaut. Les experts de Kaspersky Lab estiment qu'il suffit pour protéger les serveurs de fichiers dans la plupart des réseaux. Ce niveau assure l'équilibre optimum entre la qualité de la protection et l'impact sur les performances du serveur à protéger.

Au niveau de sécurité **Recommandé**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]

ScanArchived=no

ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=no

SizeLimit=0
```

```
ScanByAccessType="SmartCheck"
InfectedFirstAction="Recommended"
InfectedSecondAction="Skip"
SuspiciousFirstAction="Recommended"
SuspiciousSecondAction="Skip"
UseAdvancedActions=no
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
ReportPackedObjects=no
```

- **Elevé**

Utilisez le niveau de sécurité **Elevé**, si vos exigences en matière de sécurité informatique du réseau sont strictes.

Au niveau de sécurité **Elevé**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=yes
ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=no
SizeLimit=0
ScanByAccessType="SmartCheck"
InfectedFirstAction="Cure"
InfectedSecondAction="Skip"
SuspiciousFirstAction="Quarantine"
SuspiciousSecondAction="Skip"
UseAdvancedActions=no
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
```

```
ReportPackedObjects=no
```

CREATION DE LA ZONE DE PROTECTION

Faites attention aux particularités (cf. page 10) de l'analyse des liens matériels et symboliques.

Par défaut, la tâche de protection en temps réel analyse tous les objets lancés, modifiés et enregistrés qui se trouvent dans le système de fichiers local du serveur.

Vous pouvez élargir ou restreindre la zone de protection en ajoutant / en supprimant des objets d'analyse ou en modifiant le type des fichiers analysés (cf. page 34).

Kaspersky Anti-Virus analysera les objets dans les zones indiquées dans l'ordre d'énumération de celles-ci dans le fichier de configuration ou dans la liste des zones de la console Web de Kaspersky Anti-Virus. Si vous voulez configurer des paramètres de sécurité pour le répertoire enfant différents de ceux du répertoire parent, placez le répertoire enfant dans la liste avant le répertoire parent.

Pour élargir la zone de protection, exécutez les actions suivantes :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ajoutez dans le fichier créé les sections suivantes :

   - `[ScanScope]`, secteur contenant les paramètres suivants :
     - **AreaMask**, qui précise le masque du nom des objets à analyser ;
     - **UseAccessUser**, qui comprend le mode d'analyse en fonction des droits d'accès aux objets (cf. page 39) ;
     - **AreaDesc**, qui précise le nom de la zone de protection.
   - `[ScanScope:AreaPath]`, section contenant le paramètre **Path.**
   - `[ScanScope:AccessUser]`, section contenant les paramètres spécifiant les droits d'accès aux objets lors des opérations au cours desquelles ces objets seront analysés par la tâche de protection en temps réel.
   - `[ScanScope:ScanSettings]`, section contenant les paramètres de l'analyse de la zone ajoutée.

   Dans la section `[ScanScope:ScanSettings]`, les valeurs de tous les paramètres doivent être définies.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

Pour réduire la zone de protection, exécutez les actions suivantes :

1. Enregistrez les paramètres de la tâche de protection en temps rée l à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Dans le fichier créé, supprimez les sections suivantes qui définissent la zone de protection :

   - `[ScanScope]` ;
   - `[ScanScope:AreaPath]` ;
   - `[ScanScope:AccessUser]`;
   - `[ScanScope:ScanSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

RESTRICTION DE LA ZONE DE PROTECTION A L'AIDE DE MASQUES ET D'EXPRESSIONS REGULIERES

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone de protection.

Vous pouvez configurer les modèles des noms ou des chemins d'accès aux fichiers à analyser. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone de protection que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier pour l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire qui définit la zone d'analyse ou de protection.

Pour configurer les modèles des noms ou des chemins d'accès aux fichiers à analyser, exécutez les actions suivantes :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Spécifiez la valeur du paramètre **AreaMask** dans la section `[ScanScope]` qui décrit la zone de protection.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

EXCLUSION DES OBJETS DE LA PROTECTION

Par défaut, la tâche de protection en temps réel analyse tous les objets qui font partie des zones de protection définies pour cette tâche.

Vous pouvez exclure certains objets de l'analyse. Créez pour ce faire quatre types d'exclusion :

- exclusion des objets de la zone de protection : dans ce cas, les objets seront exclus uniquement de la zone de protection sélectionnée ;

- exclusion globale d'objets : dans ce cas, les objets indiqués seront exclus de tous les zones de protection configurées pour la tâche ;
- exclusion des objets en fonction des privilèges d'accès : dans ce cas, les objets seront exclus de la zone de protection en fonction des privilèges avec lesquels ils sont manipulés ;
- exclusion des objets en fonction du nom de la menace qu'ils contiennent.

DANS CETTE SECTION

CREATION D'UNE ZONE D'EXCLUSION GLOBALE

Vous pouvez créer une zone d'exclusion globale. Les objets qui font partie de cette zone seront exclus de toutes les zones de protection définies pour la tâche de protection en temps réel.

Pour créer une zone d'exclusion globale, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ajoutez dans le fichier créé les sections suivantes :

   - `[ExcludedFromScanScope]`, secteur contenant les paramètres suivants :
     - **AreaMask**, qui définit les modèles du nom des objets à exclure de l'analyse ;
     - **UseAccessUser** qui active le mode d'exclusion des objets en fonction des droits d'accès à ceux-ci ;
     - **AreaDesc**, qui définit le nom unique de la zone d'exclusion ;
   - `[ExcludedFromScanScope:AreaPath]`, section contenant le paramètre **Path**, qui définit le chemin d'accès aux objets à exclure de l'analyse.
   - `[ExcludedFromScanScope:AccessUser]`, section contenant les paramètres spécifiant les droits d'accès aux objets lors des opérations au cours desquelles ces objets seront exclus de l'analyse.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

EXCLUSION DES OBJETS DE LA ZONE DE PROTECTION

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone de protection.

Vous pouvez indiquer les modèles des noms ou des chemins d'accès exclus de la zone de protection. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone de protection que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire contenant l'objet à exclure.

Pour exclure les objets de la zone de protection, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.

3. Assignez la valeur **yes** au paramètre **UseExcludeMasks** dans la section `[ScanScope:ScanSettings]`.

4. Précisez le modèle des noms ou des chemins d'accès à l'aide du paramètre **ExcludeMasks** dans la section `[ScanScope:ScanSettings]`.

   Pour définir plusieurs modèles ou chemins d'accès, répétez la valeur du paramètre **ExcludeMasks** le nombre de fois approprié.

5. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

EXCLUSION DES OBJETS EN FONCTION DES DROITS D'ACCES

Kaspersky Anti-Virus permet d'exclure des objets de la zone de protection en cas de tentative d'accès à ceux-ci avec les droits des utilisateurs ou des groupes définis.

Pour exclure des objets de la zone de protection en fonction des droits d'accès à ceux-ci, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.

3. Attribuez la valeur **yes** au paramètre **UseAccessUser** dans la section `[ExcludedFromScanScope]` ;

4. Indiquez le nom de l'utilisateur dont les privilèges seront appliqués aux opérations qui ne seront pas analysées à l'aide du paramètre **UserName** dans la section `[ExcludedFromScanScope:AccessUser]` ;

5. Indiquez le nom du groupe dont les privilèges seront appliqués aux opérations qui ne seront pas analysées à l'aide du paramètre **UserGroup** dans la section `[ExcludedFromScanScope:AccessUser]`.

   Si vous voulez spécifier plusieurs noms d'utilisateurs ou de groupes, définissez les valeurs des paramètres **UserName** et **UserGroup** autant de fois que nécessaire dans une section.

6. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

EXCLUSION DES OBJETS EN FONCTION DU NOM DE LA MENACE DECOUVERTE

Si Kaspersky Anti-Virus considère que l'objet analysé est infecté ou qu'il est suspect, l'action définie sera exécutée. Si vous estimez que cet objet ne présente aucun danger pour l'ordinateur protégé, vous pouvez l'exclure de l'analyse en fonction du nom de la menace découverte. Dans ce cas, Kaspersky Anti-Virus considère ces objets comme étant sains et ne les traite pas.

Le nom complet de la menace peut contenir les informations suivantes :

<classe de la menace>:<type de la menace>.<nom abrégé du système d'exploitation>.<nom de la menace>.<code de la modification de la menace>. Par exemple : **not-a-virus:NetTool.Linux.SynScan.a**.

Vous pouvez trouver le nom complet de la menace détectée dans l'objet, dans le registre de Kaspersky Anti-Virus.

Vous pouvez également trouver le nom complet de la menace détectée dans le logiciel sur le site de l'Encyclopédie des virus (cf. rubrique l'Encyclopédie des virus – http://www.viruslist.com/fr). Pour trouver le type de menace, saisissez le nom du logiciel dans le champ **Recherche**.

Lors de la définition des modèles de nom de menaces, vous pouvez utiliser les masques Shell ou les expressions régulières étendues POSIX.

Pour exclure des objets en fonction du nom de la menace détectée, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Ouvrez le fichier créé pour le modifier.

3. Assignez la valeur **yes** au paramètre **UseExcludeThreats** dans la section `[ScanScope:ScanSettings]`.

4. Précisez le modèle des noms de menaces d'accès à l'aide du paramètre **ExcludeThreats** dans la section `[ScanScope:ScanSettings]`.

   Pour définir plusieurs modèles de menaces, répétez la valeur du paramètre **ExcludeThreats** le nombre de fois approprié.

5. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

SELECTION DU MODE D'INTERCEPTION

Kaspersky Anti-Virus contient deux composants qui interceptent les requêtes aux fichiers et qui les analyse. Il s'agit de l'intercepteur Samba (il sert à analyser les objets des ordinateurs distants lorsqu'ils sont sollicités via le protocole SMB / CIFS) et l'intercepteur du niveau du noyau (il analyse les objets lorsqu'ils sont sollicités via d'autres moyens).

En tant que informations supplémentaires sur l'objet, l'intercepteur Samba permet de recevoir l'adresse IP de l'ordinateur distant depuis lequel l'application a fait appel à l'objet au moment de son interception par Kaspersky Anti-Virus.

- *Pour activer l'intercepteur du niveau du noyau, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=KernelOnly
```

- *Pour permettre l'interception des opérations Samba, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=SambaOnly
```

- *Pour activer les deux intercepteurs, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=Full
```

Si seul l'intercepteur Samba est activé, Kaspersky Anti-Virus n'analysera pas les objets sollicités des moyens autres que l'appel via le protocole SMB / CIFS.

SELECTION DU MODE DE PROTECTION DES OBJETS

Par mode de protection (cf. page 185), il faut entendre la condition de l'activation de la tâche de protection en temps réel. Kaspersky Anti-Virus utilise par défaut le mode intelligent dans lequel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Par exemple, lors du travail avec un document Microsoft Office, Kaspersky Anti-Virus analyse le fichier à sa première ouverture et à sa dernière fermeture. Toutes les opérations intermédiaires visant à écraser le fichier ne sont pas analysées.

- *Pour changer le mode de protection des objets, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Ouvrez le fichier créé pour l'éditer et attribuez au paramètre **ScanByAccessType** de la section `[ScanScope:ScanSettings]` une des valeurs suivantes :

   - **SmartCheck** pour activer le mode de protection intelligent ;
   - **Open** pour activer le mode de protection en cas de tentative d'ouverture du fichier ;
   - **OpenAndModify** pour activer le mode de protection en cas de tentative d'ouverture et de modification du fichier.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Anti-Virus compare l'objet trouvé aux entrées des bases, ce qui permet d'affirmer sans faute si l'objet analysé est malveillant ou non et d'identifier la catégorie d'applications dangereuses à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. *L'analyse heuristique* permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Par conséquent, les nouvelles menaces peuvent être détectées avant qu'elles ne soient connues des analystes de virus.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :

   - assignez la valeur **yes** au paramètre **UseAnalyzer** dans la section `[ScanScope:ScanSettings]` ;
   - assignez une des valeurs suivantes : **Light**, **Medium** ou **Deep** au paramètre **HeuristicLevel** dans la section `[ScanScope:ScanSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

UTILISATION DU MODE D'ANALYSE EN FONCTION DES DROITS D'ACCES AUX OBJETS

Kaspersky Anti-Virus permet d'analyser les objets en cas de tentative d'accès à ceux-ci avec les droits d'utilisateurs ou de groupes spécifiés.

Pour activer le mode d'analyse des objets en fonction des droits d'accès à ceux-ci, procédez de la manière suivant :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :

   - valeur **yes** au paramètre **UseAccessUser** dans la section `[ScanScope]` ;
   - nom de l'utilisateur, dont les privilèges seront appliqués à l'analyse des opérations au paramètre **UserName** dans la section `[ScanScope:AccessUser]` ;
   - nom du groupe dont les privilèges seront appliqués à l'analyse des opérations au paramètre **UserGroup** dans la section `[ScanScope:AccessUser]`.

   Si vous voulez spécifier plusieurs noms d'utilisateurs ou de groupes, définissez les valeurs des paramètres **UserName** et **UserGroup** autant de fois que nécessaire dans une section.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

SELECTION DE L'ACTION A REALISER SUR LES OBJETS DETECTES

Kaspersky Anti-Virus bloque l'accès au fichier découvert, quelle que soit l'action sélectionnée.

Suite à l'analyse, Kaspersky Anti-Virus attribue un des états suivants à l'objet :

- *infecté* si le code d'un virus connu est détecté dans l'objet ;
- *suspect* s'il s'avère impossible de dire avec certitude si l'objet est infecté ou non. Cela signifie qu'une séquence de code inconnu ou que code modifié d'un virus connu a été détecté dans le fichier.

Vous pouvez configurer deux actions pour les objets de n'importe quel statut. La deuxième action sera exécutée si l'exécution de la première action échoue.

Les objets découverts peuvent être soumis aux actions suivantes :

- **Recommended**. Kaspersky Anti-Virus sélectionne automatiquement l'action et l'exécute sur la base du danger que représente la menace détectée et des possibilités de réparation. Par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie car ils ne s'intègrent pas aux autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés.
- **Cure**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Anti-Virus place les objets en quarantaine sous forme cryptée.
- **Remove**. Kaspersky Anti-Virus supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Anti-Virus laisse l'objet inchangé.

L'action **Recommended** ne peut être sélectionnée qu'en tant que première action.

Si vous avez choisi **Skip** en tant que première action, la deuxième action ne peut être que **Skip**.

Si vous avez choisi **Recommended** ou **Remove** en tant que première action, la deuxième action ne pourra être que **Quarantine**.

➧ *Pour configurer les actions à effectuer sur les objets infectés, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - **InfectedFirstAction** dans la section `[ScanScope:ScanSettings]` ;
   - **InfectedSecondAction** dans la section `[ScanScope:ScanSettings]` ;
3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

Pour configurer les actions à effectuer sur les objets suspects, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :

   - **SuspiciousFirstAction** dans la section `[ScanScope:ScanSettings]` ;
   - **SuspiciousSecondAction** dans la section `[ScanScope:ScanSettings]` ;

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

SELECTION DES ACTIONS A EXECUTER EN FONCTION DU TYPE DE MENACE

Kaspersky Anti-Virus bloque l'accès au fichier découvert, quelle que soit l'action sélectionnée.

Vous pouvez déterminer les actions pour les types des menaces suivants :

- **Virware** – virus ;
- **Trojware** – chevaux de Troie ;
- **Malware** – programmes qui ne peuvent pas nuire directement à votre ordinateur mais qui peuvent être utilisés par les auteurs du code malveillant ou par d'autres programmes malveillants ;
- **Adware** – logiciels publicitaires ;
- **Pornware** – programmes qui téléchargent du contenu à caractère pornographique ou qui visitent des sites pornographiques sans l'autorisation de l'utilisateur ;
- **Riskware** – programmes ne présentant pas de menace mais qui peuvent éventuellement être utilisés dans des fins illégales. Citons par l'exemple les utilitaires d'administration à distance.

Pour les menaces de chaque type, vous pouvez configurer deux actions. La deuxième action sera exécutée si l'exécution de la première action échoue.

Vous pouvez définir les actions suivantes :

- **Recommended**. Kaspersky Anti-Virus sélectionne automatiquement l'action et l'exécute sur la base du danger que représente la menace détectée et des possibilités de réparation. Par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie car ils ne s'intègrent pas aux autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés.
- **Cure**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.

- **Quarantine**. Kaspersky Anti-Virus place les objets en quarantaine sous forme cryptée.
- **Remove**. Kaspersky Anti-Virus supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Anti-Virus laisse l'objet inchangé.

L'action **Recommended** ne peut être sélectionnée qu'en tant que première action.

Si vous avez choisi **Skip** en tant que première action, la deuxième action ne peut être que **Skip**.

Si vous avez choisi **Recommended** ou **Remove** en tant que première action, la deuxième action ne pourra être que **Quarantine**.

Pour configurer les actions à exécuter sur des menaces de type bien précis, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.
3. Assignez la valeur **yes** au paramètre **UseAdvancedActions** dans la section `[ScanScope:ScanSettings]`.
4. Ajoutez au fichier de configuration la section `[ScanScope:ScanSettings:AdvancedActions]`.
5. Indiquez le type de menace à l'aide du paramètre **Verdict** dans la section `[ScanScope:ScanSettings:AdvancedActions]`.
6. Indiquez les actions à effectuer pour la menace de type choisi à l'aide des paramètres **FirstAction** et **SecondAction** dans la section `[ScanScope:ScanSettings:AdvancedActions]`.
7. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée de l'analyse et augmenter la vitesse de fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut définir deux types de restrictions :

- restriction sur la longueur de l'analyse : à l'issue du délai défini, l'analyse de l'objet sera interrompue ;
- restriction sur la taille maximale de l'objet à analyser : les objets dont la taille dépasse la valeur maximale seront ignorés durant l'analyse.

Pour activer la restriction sur la durée de l'analyse d'un objet, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - assignez la valeur **yes** au paramètre **UseTimeLimit** dans la section `[ScanScope:ScanSettings]` ;

- durée maximum de l'analyse d'un objet (en secondes) **–** au paramètre **TimeLimit** dans la section `[ScanScope:ScanSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

Pour activer la restriction selon la taille maximum d'un objet à analyser, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :

   - assignez la valeur **yes** au paramètre **UseSizeLimit** dans la section `[ScanScope:ScanSettings]` ;
   - taille maximum de l'objet à analyser (en octets) **–** au paramètre **SizeLimit** dans la section `[ScanScope:ScanSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

COMPATIBILITE ENTRE KASPERSKY ANTI-VIRUS ET D'AUTRES APPLICATIONS DE KASPERSKY LAB

Pour garantir la compatibilité de Kaspersky Anti-Virus 8.0 avec Kaspersky Anti-Virus for Linux Mail Server, Kaspersky Anti-Spam et Kaspersky Mail Gateway, il est nécessaire d'exclure les répertoires de service de ces applications de l'analyse par la tâche de protection en temps réel.

Pour configurer la compatibilité entre Kaspersky Anti-Virus 8.0 et Kaspersky Anti-Virus for Mail Server, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Ajoutez dans le fichier créé la section suivante :

```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path=<chemin d'accès au répertoire d'une suite de messagerie de l'agent de
messagerie intégré avec Kaspersky Anti-Virus for Linux Mail Server>
[ExcludedFromScanScope:AccessUser]
UserName=<nom d'utilisateur : propriétaire du répertoire d'une suite de
messagerie>
```

3. Répéter la section indiquée ci-dessus pour tous les agents de messagerie intégrés avec Kaspersky Anti-Virus for Linux Mail Server.

4. Pour exclure de l'analyse le répertoire temporaire des filtres et des services de Kaspersky Anti-Virus for Linux Mail Server, ajoutez dans le fichier créé la section suivante :

```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path="/var/tmp"
[ExcludedFromScanScope:AccessUser]
UserName="kluser"
```

5. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

Pour configurer la compatibilité entre Kaspersky Anti-Virus 8.0 et Kaspersky Anti-Spam, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Ajoutez dans le fichier créé la section suivante :

```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path=<chemin d'accès au répertoire d'une suite de messagerie de l'agent de
messagerie intégré avec Kaspersky Anti-Spam>
[ExcludedFromScanScope:AccessUser]
UserName=<nom d'utilisateur : propriétaire du répertoire d'une suite de
messagerie>
```

3. Répéter la section indiquée ci-dessus pour tous les agents de messagerie intégrés avec Kaspersky Anti-Spam.

4. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

Pour configurer la compatibilité entre Kaspersky Anti-Virus 8.0 et Kaspersky Mail Gateway, procédez comme suit :

1. Enregistrez les paramètres de la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

2. Pour exclure de l'analyse le répertoire d'une suite Kaspersky Mail Gateway, ajoutez dans le fichier créé la section suivante :

```
[ExcludedFromScanScope]
```

```
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path="/var/spool/kaspersky/mailgw"
[ExcludedFromScanScope:AccessUser]
UserName="kluser"
```

3. Importez les paramètres depuis le fichier dans la tâche de protection en temps réel à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

ANALYSE A LA DEMANDE

L'analyse à la demande consiste à effectuer une seule analyse complète à analyser une sélection des objets sur l'ordinateur pour y détecter des programmes malveillants.

Kaspersky Anti-Virus peut exécuter plusieurs tâches d'analyse à la demande à la fois.

Kaspersky Anti-Virus propose trois tâches prédéfinies d'analyse à la demande :

- **Analyse complète de l'ordinateur**. Tous les objets locaux de l'ordinateur sont analysés selon les paramètres de protection recommandés.
- **Analyse de tous les objets partagés**. Tous les objets partagés sont analysés indépendamment du protocole d'accès.
- **Analyse des objets en quarantaine**. Les objets en quarantaine sont analysés. Cette tâche est lancée par défaut après chaque mise à jour des bases.

Kaspersky Anti-Virus permet également d'analyser rapidement les fichiers et les répertoires (cf. section "Analyse rapide des fichiers et des répertoires" à la page 49) depuis la ligne de commande.

Vous pouvez créer des tâches d'analyse à la demande.

DANS CETTE SECTION

COMPOSITION DES NIVEAUX DE PROTECTION PREDEFINIS DE LA TACHE D'ANALYSE A LA DEMANDE

Les experts de Kaspersky Lab ont configuré trois niveaux de protection. Vous devez choisir le niveau qui correspond le mieux aux conditions de travail et à la situation en vigueur. Vous avez le choix entre les niveaux de sécurité suivants :

- **Faible**

Le niveau de sécurité **Faible** peut être spécifié sur le serveur si le réseau est doté de mesures de sécurité en plus de l'utilisation d'Anti-Virus sur les serveurs et postes de travail. Par exemple, des pare-feu sont configurés, des stratégies de sécurité pour les utilisateurs de réseau sont en vigueur.

Au niveau de sécurité **Faible**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]

ScanArchived=no

ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=yes

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Cure"

InfectedSecondAction="Remove"

SuspiciousFirstAction="Quarantine"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Light"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

- **Recommandé**

  Le niveau de sécurité **Recommandé** est installé par défaut. Les experts de Kaspersky Lab estiment qu'il suffit pour protéger les serveurs de fichiers dans la plupart des réseaux. Ce niveau assure l'équilibre optimum entre la qualité de la protection et l'impact sur les performances du serveur à protéger.

Au niveau de sécurité **Recommandé**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]

ScanArchived=no

ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=no

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Recommended"

InfectedSecondAction="Skip"

SuspiciousFirstAction="Recommended"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Light"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

- **Elevé**

  Utilisez le niveau de sécurité **Elevé**, si vos exigences en matière de sécurité informatique du réseau sont strictes.

  Au niveau de sécurité **Elevé**, les paramètres suivants sont appliqués à l'analyse :

```
[ScanScope:ScanSettings]
```

```
ScanArchived=no

ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=no

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Recommended"

InfectedSecondAction="Skip"

SuspiciousFirstAction="Recommended"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Light"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

ANALYSE RAPIDE DES FICHIERS ET DES REPERTOIRES

Kaspersky Anti-Virus permet d'analyser rapidement les fichiers et les répertoires sans avoir à configurer une zone d'analyse. Vous pouvez définir les modèles des noms des fichiers et des répertoires à analyser ou le chemin d'accès à ceux-ci à l'aide de masques Shell.

Les masques Shell permettent de spécifier le modèle du nom de fichier ou de répertoire pour l'analyse par Kaspersky Anti-Virus.

- *Pour analyser un fichier ou un répertoire, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --scan-file <chemin d'accès au fichier ou au répertoire>
```

- *Pour analyser plusieurs fichiers ou répertoires, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --scan-file <chemin d'accès au fichier ou au répertoire> <chemin d'accès au fichier ou au répertoire>, etc.
```

Paramètres selon lesquels l'analyse des fichiers et des répertoires est lancée à l'aide de l'instruction --scan-file :

```
ScanPriority="System"

[ScanScope]

AreaMask="*"

AreaDesc="Scan one file"

[ScanScope:AreaPath]

Path="<chemin d'accès aux fichiers ou aux répertoires à analyser>"

[ScanScope:ScanSettings]

ScanArchived=yes

ScanSfxArchived=yes

ScanMailBases=yes

ScanPlainMail=yes

ScanPacked=yes

UseTimeLimit=no

TimeLimit=120

UseSizeLimit=no

SizeLimit=0

InfectedFirstAction="Skip"

InfectedSecondAction="Skip"

SuspiciousFirstAction="Skip"

SuspiciousSecondAction="Skip"

UseAdvancedActions=no

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=no
```

```
HeuristicLevel="Medium"
```

Par défaut, tous les objets découverts seront ignorés et les informations relatives à ceux-ci seront consignées dans le rapport. Il est possible de définir une des actions suivantes à exécuter sur les objets découverts : **Recommended**, **Cure**, **Quarantine**, **Remove**, **Skip**.

- *Pour définir les actions à exécuter sur les objets découverts, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --action <action> --scan-file <chemin
d'accès au fichier ou au répertoire>
```

COMPOSITION DE LA ZONE D'ANALYSE

Faites attention aux particularités (cf. page 10) de l'analyse des liens matériels et symboliques.

La tâche d'analyse à la demande analyse les objets du système de fichiers du serveur qui figurent dans la *zone d'analyse*. Vous pouvez élargir ou restreindre la zone d'analyse en ajoutant / en supprimant des objets d'analyse ou en modifiant le type des fichiers analysés (cf. page 52).

Kaspersky Anti-Virus analysera les objets dans les zones indiquées dans l'ordre d'énumération de celles-ci dans le fichier de configuration ou dans la liste des zones de la console Web de Kaspersky Anti-Virus. Si vous voulez configurer des paramètres de sécurité pour le répertoire enfant différents de ceux du répertoire parent, placez le répertoire enfant dans la liste avant le répertoire parent.

- *Pour élargir la zone d'analyse, exécutez les actions suivantes :*

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Ajoutez dans le fichier créé les sections suivantes :

   - `[ScanScope]`, secteur contenant les paramètres suivants :
     - **AreaMask**, qui précise le masque du nom des objets à analyser ;
     - **AreaDesc**; qui précise le nom de la zone de protection.
   - `[ScanScope:AreaPath]`, section contenant le paramètre **Path**.
   - `[ScanScope:ScanSettings]`, section contenant les paramètres de l'analyse de la zone ajoutée.

   Dans la section `[ScanScope:ScanSettings]`, les valeurs de tous les paramètres doivent être définies.

3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

- *Pour réduire la zone d'analyse, exécutez les actions suivantes :*

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
```

```
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Dans le fichier créé, supprimez les sections suivantes qui définissent la zone de protection :
   - `[ScanScope]` ;
   - `[ScanScope:AreaPath]` ;
   - `[ScanScope:ScanSettings]`.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

RESTRICTION DE LA ZONE D'ANALYSE A L'AIDE DE MASQUES ET D'EXPRESSIONS REGULIERES

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone de protection.

Vous pouvez configurer les modèles des noms ou des chemins d'accès aux fichiers à analyser. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone de protection que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier pour l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire qui définit la zone d'analyse ou de protection.

Pour configurer les modèles des noms ou des chemins d'accès aux fichiers à analyser, exécutez les actions suivantes :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Spécifiez la valeur du paramètre **AreaMask** dans la section `[ScanScope]` qui décrit la zone de protection.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

EXCLUSION DES OBJETS DE L'ANALYSE

La tâche d'analyse à la demande analyse par défaut tous les objets qui figurent dans la zone d'analyse définie pour cette tâche.

Vous pouvez exclure certains objets de l'analyse. Créez pour ce faire trois types d'exclusion :

- exclusion des objets de la zone d'analyse : dans ce cas, les objets seront exclus uniquement de la zone d'analyse sélectionnée ;

- exclusion globale d'objets : dans ce cas, les objets indiqués seront exclus de tous les zones d'analyse configurées pour la tâche ;
- exclusion des objets en fonction du nom de la menace qu'ils contiennent.

DANS CETTE SECTION

CREATION D'UNE ZONE D'EXCLUSION GLOBALE

Vous pouvez créer une zone d'exclusion globale. Les objets repris dans cette zone seront exclus de toutes les zones d'analyse définies pour la tâche d'analyse à la demande.

Pour créer une zone d'exclusion globale, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ajoutez dans le fichier créé les sections suivantes :

   - `[ExcludedFromScanScope]`, secteur contenant les paramètres suivants :
     - **AreaMask**, qui définit les modèles du nom des objets à exclure de l'analyse ;
     - **AreaDesc** qui définit le nom unique de la zone d'exclusion.
   - `[ExcludedFromScanScope:AreaPath]`, section contenant le paramètre **Path**, qui définit le chemin d'accès aux objets à exclure de l'analyse.

3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

EXCLUSION DES OBJETS DE LA ZONE D'ANALYSE

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone d'analyse.

Vous pouvez indiquer les modèles des noms ou des chemins d'accès exclus de la zone d'analyse. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone d'analyse que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire contenant l'objet à exclure.

Pour exclure les objets de la zone d'analyse, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.

3. Assignez la valeur **yes** au paramètre **UseExcludeMasks** dans la section `[ScanScope:ScanSettings]`.

4. Précisez le modèle des noms ou des chemins d'accès à l'aide du paramètre **ExcludeMasks** dans la section `[ScanScope:ScanSettings]`.

   Pour définir plusieurs modèles ou chemins d'accès, répétez la valeur du paramètre **ExcludeMasks** le nombre de fois approprié.

5. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

EXCLUSION DES OBJETS EN FONCTION DU NOM DE LA MENACE DECOUVERTE

Si Kaspersky Anti-Virus considère que l'objet analysé est infecté ou qu'il est suspect, l'action définie sera exécutée. Si vous estimez que cet objet ne présente aucun danger pour l'ordinateur protégé, vous pouvez l'exclure de l'analyse en fonction du nom de la menace découverte. Dans ce cas, Kaspersky Anti-Virus considère ces objets comme étant sains et ne les traite pas.

Le nom complet de la menace peut contenir les informations suivantes :

<classe de la menace>:<type de la menace>.<nom abrégé du système d'exploitation>.<nom de la menace>.<code de la modification de la menace>. Par exemple : **not-a-virus:NetTool.Linux.SynScan.a**.

Vous pouvez trouver le nom complet de la menace détectée dans l'objet, dans le registre de Kaspersky Anti-Virus.

Vous pouvez également trouver le nom complet de la menace détectée dans le logiciel sur le site de l'Encyclopédie des virus (cf. rubrique l'Encyclopédie des virus – http://www.viruslist.com/fr). Pour trouver le type de menace, saisissez le nom du logiciel dans le champ **Recherche**.

Lors de la définition des modèles de nom de menaces, vous pouvez utiliser les masques Shell ou les expressions régulières étendues POSIX.

Pour exclure des objets en fonction du nom de la menace détectée, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.

3. Assignez la valeur **yes** au paramètre **UseExcludeThreats** dans la section `[ScanScope:ScanSettings]`.

4. Précisez le modèle des noms de menaces d'accès à l'aide du paramètre **ExcludeThreats** dans la section `[ScanScope:ScanSettings]`.

Pour définir plusieurs modèles de menaces, répétez la valeur du paramètre **ExcludeThreats** le nombre de fois approprié.

5. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Anti-Virus compare l'objet trouvé aux entrées des bases, ce qui permet d'affirmer sans faute si l'objet analysé est malveillant ou non et d'identifier la catégorie d'applications dangereuses à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. *L'analyse heuristique* permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Par conséquent, les nouvelles menaces peuvent être détectées avant qu'elles ne soient connues des analystes de virus.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :

   - assignez la valeur **yes** au paramètre **UseAnalyzer** dans la section `[ScanScope:ScanSettings]` ;
   - assignez une des valeurs suivantes : **Light**, **Medium** ou **Deep** au paramètre **HeuristicLevel** dans la section `[ScanScope:ScanSettings]`.

3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

SELECTION DE L'ACTION A REALISER SUR LES OBJETS DETECTES

Suite à l'analyse, Kaspersky Anti-Virus attribue un des états suivants à l'objet :

- *infecté* si le code d'un virus connu est détecté dans l'objet ;
- *suspect* s'il s'avère impossible de dire avec certitude si l'objet est infecté ou non. Cela signifie qu'une séquence de code inconnu ou que code modifié d'un virus connu a été détecté dans le fichier.

Vous pouvez configurer deux actions pour les objets de n'importe quel statut. La deuxième action sera exécutée si l'exécution de la première action échoue.

Les objets découverts peuvent être soumis aux actions suivantes :

- **Recommended**. Kaspersky Anti-Virus sélectionne automatiquement l'action et l'exécute sur la base du danger que représente la menace détectée et des possibilités de réparation. Par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie car ils ne s'intègrent pas aux autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés.
- **Cure**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Anti-Virus place les objets en quarantaine sous forme cryptée.
- **Remove**. Kaspersky Anti-Virus supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Anti-Virus laisse l'objet inchangé.

L'action **Recommended** ne peut être sélectionnée qu'en tant que première action.

Si vous avez choisi **Skip** en tant que première action, la deuxième action ne peut être que **Skip**.

Si vous avez choisi **Recommended** ou **Remove** en tant que première action, la deuxième action ne pourra être que **Quarantine**.

Pour configurer les actions à effectuer sur les objets infectés, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - **InfectedFirstAction** dans la section `[ScanScope:ScanSettings]` ;
   - **InfectedSecondAction** dans la section `[ScanScope:ScanSettings]`.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

Pour configurer les actions à effectuer sur les objets suspects, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - **SuspiciousFirstAction** dans la section `[ScanScope:ScanSettings]` ;
   - **SuspiciousSecondAction** dans la section `[ScanScope:ScanSettings]`.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

SELECTION DES ACTIONS A EXECUTER EN FONCTION DU TYPE DE MENACE

Vous pouvez déterminer les actions pour les types des menaces suivants :

- **Virware** – virus ;
- **Trojware** – chevaux de Troie ;
- **Malware** – programmes qui ne peuvent pas nuire directement à votre ordinateur mais qui peuvent être utilisés par les auteurs du code malveillant ou par d'autres programmes malveillants ;
- **Adware** – logiciels publicitaires ;
- **Pornware** – programmes qui téléchargent du contenu à caractère pornographique ou qui visitent des sites pornographiques sans l'autorisation de l'utilisateur ;
- **Riskware** – programmes ne présentant pas de menace mais qui peuvent éventuellement être utilisés dans des fins illégales. Citons par l'exemple les utilitaires d'administration à distance.

Pour les menaces de chaque type, vous pouvez configurer deux actions. La deuxième action sera exécutée si l'exécution de la première action échoue.

Vous pouvez définir les actions suivantes :

- **Recommended**. Kaspersky Anti-Virus sélectionne automatiquement l'action et l'exécute sur la base du danger que représente la menace détectée et des possibilités de réparation. Par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie car ils ne s'intègrent pas aux autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés.
- **Cure**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Anti-Virus place les objets en quarantaine sous forme cryptée.
- **Remove**. Kaspersky Anti-Virus supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Anti-Virus laisse l'objet inchangé.

L'action **Recommended** ne peut être sélectionnée qu'en tant que première action.

Si vous avez choisi **Skip** en tant que première action, la deuxième action ne peut être que **Skip**.

Si vous avez choisi **Recommended** ou **Remove** en tant que première action, la deuxième action ne pourra être que **Quarantine**.

Pour configurer les actions à exécuter sur des menaces de type bien précis, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier.
3. Assignez la valeur **yes** au paramètre **UseAdvancedActions** dans la section `[ScanScope:ScanSettings]`.
4. Ajoutez au fichier de configuration la section `[ScanScope:ScanSettings:AdvancedActions]`.

5. Indiquez le type de menace à l'aide du paramètre **Verdict** dans la section `[ScanScope:ScanSettings:AdvancedActions]`.

6. Indiquez les actions à effectuer pour la menace de type choisi à l'aide des paramètres **FirstAction** et **SecondAction** dans la section `[ScanScope:ScanSettings:AdvancedActions]`.

7. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée de l'analyse et augmenter la vitesse de fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut définir deux types de restrictions :

- restriction sur la longueur de l'analyse : à l'issue du délai défini, l'analyse de l'objet sera interrompue ;
- restriction sur la taille maximale de l'objet à analyser : les objets dont la taille dépasse la valeur maximale seront ignorés durant l'analyse.

Pour activer la restriction sur la durée de l'analyse d'un objet, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - assignez la valeur **yes** au paramètre **UseTimeLimit** dans la section `[ScanScope:ScanSettings]` ;
   - durée maximum de l'analyse d'un objet (en secondes) **–** au paramètre **TimeLimit** dans la section `[ScanScope:ScanSettings]`.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

Pour activer la restriction selon la taille maximum d'un objet à analyser, procédez comme suit :

1. Enregistrez les paramètres de la tâche d'analyse à la demande dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

2. Ouvrez le fichier créé et attribuez les valeurs suivantes aux paramètres :
   - assignez la valeur **yes** au paramètre **UseSizeLimit** dans la section `[ScanScope:ScanSettings]` ;
   - taille maximum de l'objet à analyser (en octets) **–** au paramètre **SizeLimit** dans la section `[ScanScope:ScanSettings]`.
3. Importez les paramètres du fichier dans la tâche d'analyse à la demande à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

SELECTION DE LA PRIORITE DE LA TACHE

Toutes les tâches d'analyse à la demande sont exécutées par défaut selon la priorité définie par le système au lancement de la tâche. Vous pouvez attribuer une des priorités suivantes à la tâche :

- **System**. La priorité du processus est déterminée par le système d'exploitation.
- **High**. Accélère l'exécution de la tâche mais, en même temps, elle peut ralentir la vitesse d'exécution des processus des autres applications actives.

  Choisissez cette option si la tâche doit être exécutée le plus rapidement possible, malgré la charge éventuelle sur le serveur à protéger.
- **Medium**. La priorité du processus passe de la valeur système à la valeur recommandée par Kaspersky Lab.
- **Low**. Ralentit l'exécution de la tâche mais, en même temps, elle peut augmenter la vitesse d'exécution des processus des autres applications actives.

  Sélectionnez cette option s'il faut diminuer la charge sur le serveur à protéger durant l'exécution de la tâche.

Pour modifier la priorité de la tâche d'analyse à la demande, saisissez l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <ID de la tâche> ScanPriority=<priorité>
```

ISOLATION DES OBJETS SUSPECTS. COPIE DE SAUVEGARDE

Kaspersky Anti-Virus fait isoler des objets qu'il reconnaît comme suspects. Il met de tels objets en quarantaine – les transfère depuis l'endroit d'origine dans le répertoire de sauvegarde spécial dans lequel aux fins de sécurité ils sont conservés sous forme codée.

L'espace dans le référentiel est limité à 1 Go. Une fois cette limite atteinte, aucun nouvel objet n'est ajouté au référentiel.

Après chaque mise à jour, Kaspersky Anti-Virus analyse automatiquement tous les objets en quarantaine. Certains d'entre eux peuvent être considérés comme sains et seront restaurés. De plus, vous pouvez restaurer les objets manuellement depuis la quarantaine.

La restauration des objets infectés et suspects peut entraîner l'infection de l'ordinateur.

Kaspersky Anti-Virus enregistre dans le référentiel des copies cryptées des objets avant de tenter de les réparer ou de les supprimer.

Si l'objet fait partie d'un objet conteneur, Kaspersky Anti-Virus enregistre l'objet conteneur entier dans le répertoire de sauvegarde de réserve. Par exemple, si Kaspersky Anti-Virus a reconnu comme étant infecté un des objets conteneurs de la base de messagerie, il fait réserver la totalité de la base de messagerie.

Les objets qui se trouvent en quarantaine ou dans le dossier de sauvegarde sont décrit à l'aide des paramètres suivants (cf. page 123).

DANS CETTE SECTION

CONSULTATION DE LA STATISTIQUE DES OBJETS MIS EN QUARANTAINE

Vous pouvez recevoir la statistique brève ou détaillée des objets mis en quarantaine.

- *Pour afficher des statistiques succinctes, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --get-stat --query
"(OrigType!=s'Backup')"
```

Sont affichés le nombre des objets mis en quarantaine au moment actuel et le volume total de mémoire qu'ils occupent.

➧ *Pour afficher des statistiques détaillées, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -S --get-stat Quarantine
```

Si les dates de début et de fin du rapport ne sont pas définies (cf. page 92), les statistiques seront proposées à partir de l'installation de Kaspersky Anti-Virus.

Tableau 1. Champs de la statistique des objets mis en quarantaine

CHAMP	DESCRIPTION
Quarantined objects	Nombre total d'objets mis en quarantaine.
Auto saved objects	Nombre d'objets mis en quarantaine par Kaspersky Anti-Virus.
Manually saved objects	Nombre d'objets placés par l'utilisateur en quarantaine.
Restored objects	Nombre d'objets restaurés de la quarantaine.
Removed objects	Nombre d'objets supprimés de la quarantaine.
Infected objects	Nombre d'objets infectés (cf. rubrique "A propos des objets infectés et suspects portant l'état 'Avertissement'" à la page 10) : a) qui ont reçu l'état Infecté après l'analyse des objets mis en quarantaine et b) que Kaspersky Anti-Virus a mis en quarantaine selon la valeur du paramètre Action en fonction du type de la menace.
Suspicious objects	Nombre d'objets suspects (cf. rubrique " À propos des objets infectés, suspects et possédant le statut "Avertissement" " à la page 10).
Curable objects	Nombre d'objets dans le répertoire de sauvegarde que Kaspersky Anti-Virus a reconnus comme étant infectés et pouvant être réparés.
Password protected objects	Nombre d'objet protégés par un mot de passe.
Corrupted objects	Nombre d'objets endommagés.
False detected objects	Nombre d'objets qui ont reçu le statut Faux positif qu'après avoir analysé les objets mis en quarantaine avec utilisation des bases actualisées ont été reconnus comme étant non infectés.

ANALYSE DES OBJETS MIS EN QUARANTAINE

Par défaut, après chaque mise à jour des bases, Kaspersky Anti-Virus effectue la tâche **Analyse des objets en quarantaine**. Les paramètres de la tâche sont donnés dans le tableau ci-dessous. Vous ne pouvez pas les modifier.

Après l'analyse des objets en quarantaine suite à la mise à jour des bases antivirus, Kaspersky Anti-Virus peut considérer certains d'entre eux comme étant sains (la valeur du champ **Type** (cf. page 123) pour ces objets devient **Clean**). Les autres objets peuvent être reconnus par Kaspersky Anti-Virus comme étant infectés.

Vous pouvez lancer la tâche **Analyse des objets en quarantaine** manuellement.

➧ *Pour lancer la tâche **Analyse des objets en quarantaine**, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 10
```

*Tableau 2. Paramètres de la tâche **Analyse des objets en quarantaine***

PARAMETRES DE LA TACHE " ANALYSE DES OBJETS EN QUARANTAINE "	VALEUR
ID	10
Secteur d'analyse	Objets mis en quarantaine
Planification par défaut	Après la mise à jour des bases
Paramètres de sécurité	Uniques pour tout le secteur d'analyse. Vous ne pouvez pas les modifier. Les valeurs des paramètres sont reprises dans le tableau suivant.

*Tableau 3. Paramètres de sécurité dans la tâche **Analyse des objets en quarantaine***

PARAMÈTRES DE SÉCURITÉ	VALEUR
Action à exécuter sur les objets infectés	Sauter
Action à exécuter sur les objets suspects	Sauter
Exclusion des objets selon le nom	Non
Exclusion des objets selon la signature de la menace	Non
Durée maximum d'analyse d'un objet	600 s
Taille maximum de l'objet analysé	Non configuré
Analyse des objets composés	• Archives • Archives SFX • Objets archivés

MISE DES FICHIERS EN QUARANTAINE MANUELLEMENT

Si vous pensez que le fichier est infecté, vous pouvez le placer manuellement en quarantaine. Le fichier, placé en quarantaine, ne présente aucun danger.

- *Pour placer manuellement l'objet en quarantaine, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--add-object <chemin d'accès complet>
```

CONSULTATION DE L'IDENTIFICATEUR DES OBJETS

L'utilisation de la clé **-Q** dans les commandes, décrites dans cette section, est obligatoire.

Quand Kaspersky Anti-Virus place les objets dans le référentiel, il lui attribue un identificateur numérique. Celui-ci est utilisé durant les opérations sur les objets en quarantaine ou dans le dossier de sauvegarde.

- *Pour obtenir les identificateurs des objets en quarantaine, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType!=s'Backup')"
```

Exemple d'instruction :

```
Objects returned: 1

Object ID: 1

    Filename: /home/corr/eicar.com

    Object type: UserAdded

    Compound object: no

    UID: 0

    GID: 0

    Mode: 644

    AddTime: 2009-03-29 21:20:32

    Size: 73
```

- *Pour obtenir l'identificateur des objets dans le dossier de sauvegarde, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType==s'Backup')"
```

Exemple d'instruction :

```
Objects returned: 2

Object ID: 1

    Filename: /home/cur/eicar.com

    Object type: Backup

    Compound object: no

    UID: 0

    GID: 0

    Mode: 644

    AddTime: 2009-03-29 22:24:50

    Size: 73
```

Lors des manipulations d'objets, utilisez la valeur du champ **Object ID**.

RESTAURATION DES OBJETS

La restauration des objets infectés et suspects peut entraîner l'infection du serveur.

Kaspersky Anti-Virus conserve les objets en quarantaine / dans le répertoire de sauvegarde de réserve sous forme codée pour préserver le serveur à protéger contre leur action malveillante potentielle.

Vous pouvez restaurer tout objet de la quarantaine ou du dossier de sauvegarde. Cela peut s'avérer nécessaire dans les cas suivants :

- Si le fichier d'origine qui s'est avéré infecté, contenait des informations importantes, lors du traitement du fichier, Kaspersky Anti-Virus n'a pas réussi à garder son intégrité et les informations qu'il contenait sont devenues inaccessibles.

- Si après l'analyse des objets en quarantaine suite à la mise à jour des bases antivirus, l'objet est considéré comme étant sain (la valeur du champ **Type** (cf. page 123) pour ces objets devient **Clean**).

- si vous considérez l'objet comme ne représente aucun danger pour le serveur et que vous voulez l'utiliser. Pour que Kaspersky Anti-Virus n'isole pas cet objet lors de futures analyses, vous pouvez l'exclure de l'analyse dans la tâche de protection en temps réel ainsi que dans les tâches d'analyse à la demande. Pour cela, spécifier l'objet en tant que valeur du paramètre de sécurité **Exclure les objets selon un masque** (cf. page 188) ou **Exclure les objets selon le nom de la menace** (cf. page 188) dans ces tâches.

Vous pouvez choisir l'emplacement dans lequel sera sauvegardé le fichier restauré : dans l'emplacement d'origine ou dans le répertoire que vous spécifiez.

Il est possible d'enregistrer l'objet restauré sous un autre nom.

La date et l'heure de création du fichier restauré depuis la quarantaine diffère de la date et de l'heure de création du fichier original.

- *Pour restaurer un objet depuis la quarantaine ou le dossier de sauvegarde vers son emplacement d'origine, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --restore <ID de l'objet>
```

- *Pour restaurer un objet depuis la quarantaine ou le dossier de sauvegarde vers un répertoire défini, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--restore <ID de l'objet> -F <nom du fichier et son chemin d'accès>
```

SUPPRESSION DES OBJETS

L'utilisation de la clé **-Q** dans les commandes, décrites dans cette section, est obligatoire.

Si vous êtes persuadé que l'objet en quarantaine / dans le dossier de sauvegarde ne constitue aucun danger pour le serveur, vous pouvez le supprimer de la quarantaine / du dossier de sauvegarde.

- *Pour supprimer un objet de la quarantaine / du dossier de sauvegarde, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--remove <ID de l'objet>
```

Il est possible également de supprimer tous les objets de la quarantaine / du dossier de sauvegarde.

- *Pour supprimer tous les objets de la quarantaine, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--mass-remove --query "(OrigType!=s'Backup')"
```

- *Pour supprimer tous les objets du dossier de sauvegarde, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--mass-remove --query "(OrigType==s'Backup')"
```

Vous pouvez faire la purge partielle de la quarantaine/du dossier de sauvegarde à l'aide des arguments spéciaux de l'instruction -Q --mass-remove (cf. page 118).

ADMINISTRATION DES LICENCES

Il est primordial de comprendre les notions suivantes dans le cadre de l'octroi des licences pour les applications de Kaspersky Lab :

- le contrat de licence ;
- la licence ;
- le fichier de licence ;
- code d'activation ;
- l'activation de l'application.

Ces trois notions sont étroitement liées et forment un modèle unique de licence.

Examinons chacune d'entre elles en détail.

PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un contrat entre une personne physique ou juridique possédant une copie de Kaspersky Anti-Virus et Kaspersky Lab, Ltd. Ce contrat accompagne chaque application de Kaspersky Lab. Il détaille les droits et les limites d'utilisation de Kaspersky Anti-Virus.

Conformément au contrat de licence, en achetant et en installant l'application de Kaspersky Lab, vous obtenez le droit de posséder pour une durée indéterminée une copie.

Kaspersky Lab est également ravi de vous offrir des services complémentaires :

- assistance technique ;
- mise à jour des bases de Kaspersky Anti-Virus ;
- mise à jour des modules logiciels de Kaspersky Anti-Virus.

Pour en profiter, vous devez acheter et activer une licence (cf. rubrique " Présentation des licences de Kaspersky Anti-Virus " à la page 65).

A PROPOS DES LICENCES DE KASPERSKY ANTI-VIRUS

La licence est le droit d'utilisation de Kaspersky Anti-Virus et des services complémentaires que vous confère Kaspersky Lab ou ses partenaires.

Chaque licence est caractérisée par sa durée de validité et son type.

La durée de validité de la licence est la période au cours de laquelle vous pouvez bénéficier des services complémentaires (cf. rubrique "Présentation du contrat de licence" à la page 65). Le type de services dépend du type de licence.

Il existe différents types de licence :

- *Évaluation* : licence gratuite à durée de validité limitée, par exemple 30 jours. Elle permet de découvrir Kaspersky Anti-Virus.

La licence d'évaluation ne peut être utilisée qu'une seule fois !

Elle est fournie avec la version d'évaluation de l'application. La licence d'évaluation ne vous permet pas de contacter le service d'assistance technique de Kaspersky Lab. Une fois que la licence arrive à échéance, toutes les fonctions de Kaspersky Anti-Virus deviennent inopérationnelles.

- *Commerciale* : licence payante avec une durée de validité d'un an par exemple, octroyée à l'achat de Kaspersky Anti-Virus. Cette licence impose des restrictions, par exemple sur le nombre d'ordinateurs protégés ou sur le volume du trafic analysé par jour.

Conformément au point 3.6 du contrat de licence, en cas d'achat de Kaspersky Anti-Virus pour protéger plus d'un ordinateur, la durée de validité de la licence commencera à courir à dater de l'activation ou de l'installation du fichier de licence sur le premier ordinateur.

Tant que la licence commerciale est valide, toutes les fonctions de Kaspersky Anti-Virus sont accessibles, ainsi que les services complémentaires.

Une fois la durée de validité de la licence commerciale écoulée, Kaspersky Anti-Virus continue à fonctionner mais la mise à jour des bases antivirus n'est plus réalisée. Vous pouvez continuer à réaliser des analyses antivirus de l'ordinateur ou à utiliser les composants de la protection, mais uniquement à l'aide des bases qui étaient d'actualité à la date de fin de validité de la licence. Par conséquent, Kaspersky Lab ne peut garantir une protection à 100 % contre les nouveaux virus après l'échéance de la licence.

Pour pouvoir continuer à utiliser l'application et les services complémentaires, il faut acheter une licence commerciale et l'activer.

L'activation de la licence s'opère en installant le fichier de licence (cf. rubrique " Présentation du fichier de licence de Kaspersky Anti-Virus " à la page 66) associé à la licence.

PRESENTATION DES FICHIERS DE LICENCE DE KASPERSKY ANTI-VIRUS

Le fichier de licence est le moyen technique qui permet d'activer la licence associée (cf. rubrique "A propos des licences de Kaspersky Anti-Virus" à la page 65), et constitue de ce fait votre droit d'utiliser l'application et les services complémentaires (cf. page 65).

Le fichier de licence est livré avec le fichier d'installation de l'application si vous acheter l'application chez un revendeur ou vous le recevez par courrier électronique en cas d'achat en ligne.

Le fichier de licence reprend les informations suivantes :

- Durée de validité de la licence.
- Type de licence (évaluation ou commerciale).
- Restrictions imposées par la licence (par exemple, le nombre d'ordinateurs couverts par la licence ou le volume de trafic de messagerie protégé).
- Coordonnées pour l'assistance technique.
- Durée de validité du fichier de licence.

La durée de validité du fichier de licence désigne comme son nom l'indique la durée de validité à partir de sa date de diffusion. Il s'agit de la période à l'issue de laquelle le fichier n'est plus valide et n'est plus en mesure d'activer la licence associée.

Voici un exemple qui illustre le lien entre la durée de validité du fichier de licence et la durée de validité de la licence.

Exemple :

Durée de validité de la licence : 300 jours

Date d'édition du fichier de licence : 01/09/2010

Durée de validité du fichier de licence : 300 jours

Date d'installation du fichier de licence (activation de la licence) : 10/09/2010, soit 9 jours après sa diffusion.

Durée:

Durée de validité calculée de la licence : 300 jours - 9 jours = 291 jours.

INSTALLATION DU FICHIER DE LICENCE

Vous pouvez installer directement deux fichiers de licence (cf. page 66) : actif ou de réserve. Le fichier de licence actif entre en vigueur dès son installation. Le fichier de licence de réserve est utilisé automatiquement à l'échéance de la période de validité du fichier actif.

Si vous installez un fichier de licence en tant que fichier actif, alors qu'il existe déjà un fichier de licence actif pour Kaspersky Anti-Virus, le nouveau fichier remplace le fichier existant. Le fichier antérieur sera supprimé.

Si vous installez un fichier de licence en tant que fichier de réserve, alors qu'il existe déjà un fichier de licence de réserve pour Kaspersky Anti-Virus, le nouveau fichier remplace le fichier existant. Le fichier antérieur sera supprimé.

- *Pour installer un fichier de licence en tant que fichier actif, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \

--install-active-key <nom du fichier de licence>
```

- *Pour installer un fichier de licence en tant que fichier de réserve, saisissez l'instruction suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--install-suppl-key <nom du fichier de licence>
```

CONSULTATION DES INFORMATIONS RELATIVES A LA LICENCE AVANT L'INSTALLATION DU FICHIER DE LICENCE

Vous pouvez consulter les informations relatives à la licence reprises dans le fichier de licence avant de l'installer.

- *Pour consulter l'information sur la licence (cf. page 65), exécutez la commande suivante :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \

--show-license-info <chemin d'accès complet au fichier de licence>
```

L'exécution de cette instruction entraîne l'affichage des informations suivantes (cf. tableau ci-après).

Tableau 4. Informations sur la licence

CHAMP	DESCRIPTION
Application name	Nom de l'application pour laquelle le fichier de licence est prévu.
Key file creation date	Date de création du fichier de licence (cf. page 66).
Key file expiration date	Date de fin de validité de la licence.
License number	Numéro de série de la licence.
License type	Type de licence : évaluation ou commerciale.
Usage restriction	Nombre de restrictions. Il existe des restrictions imposées par la licence sur l'utilisation de Kaspersky Anti-Virus.
License period	Durée de validité de la licence (cf. page 65).

Exemple d'instruction :

```
License info :

Application name:                Kaspersky BusinessSpace Security International Edition.
10-14 User 1 year NFR License: Kaspersky Anti-Virus Suite for WS and FS

Key file creation date:            2009-05-28

Key file expiration date:          2010-08-27

License number:                    0038-000451-05B74DD4

License type:                      Commercial

Usage restriction:                 10

License period:                    365
```

SUPPRESSION DU FICHIER DE LICENCE

Vous pouvez supprimer le fichier de licence. Si vous supprimerez le fichier de licence actif, le fichier de réserve deviendra automatiquement actif.

- *Pour supprimer le fichier de licence, saisissez l'instruction suivante :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --revoke-active-key
  ```

- *Pour supprimer le fichier de licence de réserve, saisissez l'instruction suivante :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --revoke-suppl-key
  ```

CONSULTATION DE LA CONVENTION DE LICENCE

Le contrat de licence est un contrat entre une personne physique ou juridique possédant une copie de Kaspersky Anti-Virus et Kaspersky Lab, Ltd. Ce contrat accompagne chaque application de Kaspersky Lab. Il détaille les droits et les limites d'utilisation de Kaspersky Anti-Virus.

Conformément au contrat de licence, en achetant et en installant l'application de Kaspersky Lab, vous obtenez le droit de posséder pour une durée indéterminée une copie.

- *Pour connaître les conditions d'utilisation définies dans le contrat de licence,*

  ouvrez un éditeur de texte pour lire le fichier `/opt/kaspersky/kav4fs/share/doc/LICENSE`.

NOTIFICATIONS DE L'ADMINISTRATEUR. ACTIONS EN CAS D'EVENEMENT

Différents types d'événement (cf. page 126) peuvent survenir durant l'utilisation de Kaspersky Anti-Virus. Ils illustrent des modifications au niveau de l'état de la protection antivirus du serveur et de Kaspersky Anti-Virus dans son ensemble. Vous pouvez configurer l'envoi de notifications à l'administrateur via courrier électronique lorsque ces événements surviennent.

De plus, les scripts Shell permettent de définir l'action qui sera exécutée quand un événement défini survient.

L'envoi de notification et l'exécution d'actions est disponible pour les événements suivants :

- **ApplicationStarted** qui correspond au lancement de Kaspersky Anti-Virus ;
- **ApplicationShutdown** qui correspond à l'arrêt de Kaspersky Anti-Virus ;
- **ThreatDetected** qui correspond à la découverte d'un objet malveillant ;
- **LicenseExpired** qui correspond à l'expiration de la durée de validité de la licence ;
- **LicenseExpiresSoon** qui correspond à l'expiration prochaine de la durée de validité de la licence ;
- **LicenseError** qui correspond à une erreur dans le sous-système de licence ;
- **AVBasesAttached** qui correspond à la réussite de la mise à jour des bases de Kaspersky Anti-Virus ;
- **AVBasesAreOutOfDate** qui correspond à l'état dépassé des bases de Kaspersky Anti-Virus ;
- **AVBasesAreTotallyOutOfDate** qui correspond à l'état fortement dépassé des bases de Kaspersky Anti-Virus ;
- **UpdateError** qui correspond à une erreur survenue lors de la mise à jour des bases de Kaspersky Anti-Virus ;
- **RetranslationError** qui correspond à une erreur survenue lors de la copie des bases de Kaspersky Anti-Virus ;
- **LicenseInstalled** qui correspond à la réussite de l'installation du fichier de licence ;
- **LicenseRevoked** qui correspond à la suppression du fichier de licence ;
- **AVBasesIntegrityCheckFailed** qui correspond à une erreur survenue lors de la vérification de l'intégrité des bases de Kaspersky Anti-Virus ;
- **ObjectNotProcessed** qui correspond au nombre d'objets non traités ;
- **ObjectProcessingError** qui correspond à une erreur survenue durant le traitement d'un objet ;
- **ObjectDisinfected** qui correspond à la réussite de la réparation d'un objet ;
- **ObjectDeleted** qui correspond à la réussite de la suppression d'un objet ;
- **QuarantineSizeLimitReached** qui correspond au volume maximal de la quarantaine ou du dossier de sauvegarde atteint ;
- **QuarantineSoftSizeLimitReached** qui correspond au volume recommandé de la quarantaine ou du dossier de sauvegarde atteint ;
- **QuarantineObjectAddFailed** qui correspond à l'échec de l'ajout d'un objet en quarantaine ;

- **QuarantineObjectAdded** qui correspond à la réussite de l'ajout d'un objet en quarantaine ;
- **QuarantineObjectRemoved** qui correspond à la réussite de la suppression d'un objet de la quarantaine ;
- **QuarantineObjectRestored** qui correspond à la réussite de la restauration d'un objet en quarantaine ;
- **QuarantineThreatDetected** qui correspond à la détection d'un objet malveillant dans un objet en quarantaine ;
- **QuarantineObjectProcessingError** qui correspond à une erreur survenue durant le traitement d'un objet en quarantaine ;
- **QuarantineObjectCurable** qui correspond à un objet en quarantaine qui peut être réparé ;
- **QuarantineFalseDetect** qui correspond à un faux positif pour un objet placé en quarantaine et considéré comme sain suite à l'analyse des objets en quarantaine (cf. page 61).

DANS CETTE SECTION

UTILISATION DU CLIENT DE MESSAGERIE DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus possède un client de messagerie intégré pour l'envoi des notifications.

Pour utiliser le client de messagerie intégré pour l'envoi des notifications, procédez comme suit :

1. Enregistrez les paramètres de la notification dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 7 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier et saisissez les modifications suivantes :

   - Attribuez la valeur **yes** au paramètre **EnableSmtp**.
   - Attribuez la valeur **Internal** au paramètre **Mailer** dans la rubrique `[CommonSmtpSettings]`.
   - Composez la liste des destinataires via le paramètre **DefaultRecipients** dans la rubrique `[CommonSmtpSettings]`.
   - Indiquez l'adresse du serveur SMTP à l'aide du paramètre **SmtpServer** dans la rubrique `[CommonSmtpSettings:InternalMailerSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 7 --file=<chemin d'accès au fichier>
   ```

La description détaillée des paramètres de notification figure dans la rubrique " Paramètres de notification et actions en fonction des événements " (cf. page 166).

UTILISATION DU CLIENT DE MESSAGERIE SENDMAIL

Si vous utilisez l'application Sendmail pour envoyer le courrier électronique, vous pouvez l'utiliser également pour envoyer les notifications de Kaspersky Anti-Virus.

Pour garantir l'envoi des notifications, Sendmail doit être configuré correctement.

Pour utiliser l'application Sendmail afin d'envoyer les notifications, procédez comme suit :

1. Enregistrez les paramètres de la notification dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 7 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier et saisissez les modifications suivantes :

   - Attribuez la valeur **yes** au paramètre **EnableSmtp**.
   - Attribuez la valeur **Sendmail** au paramètre **Mailer** dans la rubrique `[CommonSmtpSettings]`.
   - Composez la liste des destinataires via le paramètre **DefaultRecipients** dans la rubrique `[CommonSmtpSettings]`.
   - Indiquez le chemin d'accès au fichier exécutable de Sendmail à l'aide du paramètre **SendmailPath** dans la rubrique `[CommonSmtpSettings]`.

3. Importez les paramètres depuis le fichier dans la tâche à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --set-settings 7 --file=<chemin d'accès au fichier>
   ```

La description détaillée des paramètres de notification figure dans la rubrique " Paramètres de notification et actions en fonction des événements " (cf. page 166).

COMPOSITION DES NOTIFICATIONS

Avant d'envoyer des notifications, il faut rédiger le texte du message et indiquer l'adresse électronique du destinataire. Le texte du message peut contenir des macros (cf. page 73).

Pour rédiger le texte de la notification, procédez comme suit :

1. Enregistrez les paramètres de la notification dans un fichier à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \
   --get-settings 7 --file=<chemin d'accès au fichier>
   ```

2. Ouvrez le fichier créé pour le modifier et saisissez les modifications suivantes :

   a. Ajoutez la section `[SmtpNotifies]` au fichier. Elle contient les paramètres suivants :

   - **Recepients** : définit le destinataire de la notification en cas d'utilisation d'une liste locale de destinataires. Répétez le paramètre le nombre de fois nécessaire pour créer la liste des destinataires ;
   - **UseRecipientList** : définit la liste des destinataires de la notification ;

- **Subject** : définit l'objet de la notification ;
- **Body** : contient le corps du texte de la notification ;
- **EventName** : désigne le nom de l'événement pour lequel la notification est envoyée ;
- **Enable** ; active ou désactive l'application.

b. Répétez la rubrique `[SmtpNotifies]` pour tous les événements pour lesquels une notification sera envoyée.

3. Enregistrez les modifications faites.

4. Importez les paramètres depuis le fichier dans la tâche à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 7 --file=<chemin d'accès au fichier>
```

CONFIGURATION DES ACTIONS

Vous pouvez créer des scripts Shell afin d'exécuter certaines actions suite à un événement en particulier. Le texte du script peut contenir des macros (cf. page 73).

Pour créer le script qui sera exécuté suite à l'événement, procédez comme suit :

1. Enregistrez les paramètres de la notification dans un fichier à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 7 --file=<chemin d'accès au fichier>
```

2. Ouvrez le fichier créé pour le modifier et saisissez les modifications suivantes :

a. Ajoutez la section `[Actions]` au fichier. Elle contient les paramètres suivants :

- **Command** : définit le texte du script ;
- **EventName** : désigne le nom de l'événement pour lequel le script est exécuté ;
- **Enable** : active / désactive l'exécution du script.

b. Répétez la rubrique `[Actions]` pour tous les événements pour lesquels des scripts seront exécutés.

3. Enregistrez les modifications faites.

4. Importez les paramètres depuis le fichier dans la tâche à l'aide de l'instruction suivante :

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 7 --file=<chemin d'accès au fichier>
```

UTILISATION DES MACROS

Le texte des notifications et des scripts peut contenir les macros décrites dans le tableau suivant.

Tableau 5. Macros

MACRO	DESCRIPTION	ÉVÉNEMENT
%NOW%	Heure à laquelle l'événement s'est produit	Utilisée pour tous les événements
%HOST_NAME%	Nom du serveur où l'événement s'est produit	Utilisée pour tous les événements
%OBJECT%	Nom de l'objet infecté	Une menace a été découverte, L'objet n'a pas été traité, Erreur lors du traitement de l'objet, L'objet a été réparé, L'objet a été supprimé, La taille maximale du dossier de la quarantaine et de la sauvegarde est atteinte, Erreur lors du traitement de l'objet en quarantaine, Objet placé en quarantaine, L'objet a été supprimé de la quarantaine ou de la sauvegarde, L'objet a été restauré depuis la quarantaine ou la sauvegarde, Une menace a été découverte lors de l'analyse de l'objet en quarantaine, Erreur lors du traitement de l'objet en quarantaine, L'objet en quarantaine est considéré comme réparé, Faux positif : l'objet en quarantaine est considéré comme sain
%SOURCE%	Nom de l'ordinateur-source d'un objet infecté	Une menace a été découverte, L'objet n'a pas été traité, Erreur lors du traitement de l'objet, L'objet a été réparé, L'objet a été supprimé
%VERDICT%	État de l'objet découvert	Une menace a été découverte, Objet placé en quarantaine, Une menace a été découverte lors de l'analyse de l'objet en quarantaine
%THREAT_NAME%	Nom de la menace	Une menace a été découverte, Une menace a été découverte lors de l'analyse de l'objet en quarantaine
%DANGER%	Niveau de danger	Une menace a été découverte, Objet placé en quarantaine, Une menace a été découverte lors de l'analyse de l'objet en quarantaine
%RECORDS%	Nombre d'enregistrement dans les bases	Les bases ont été actualisées
%DAYS_LEFT%	Nombre de jours restant avant l'expiration de la licence.	La licence arrive bientôt à échéance
%REASON%	Cause de l'erreur	Erreur de licence, Erreur de mise à jour, Erreur de copie des mises à jour, L'analyse de l'intégrité des bases s'est soldée sur une erreur, L'objet n'a pas été traité, Erreur lors du traitement de l'objet, Erreur lors du traitement de l'objet en quarantaine
%DAYS_PASSED%	Nombre de jours écoulés depuis la dernière mise à jour	Les bases sont dépassées, Les bases sont fortement dépassées
%SERIAL%	Numéro de série de la licence	La licence est installée, la licence a été supprimée
%OBJECT_SIZE%	Taille de l'objet	La taille maximale du dossier de la quarantaine et de la sauvegarde est atteinte, L'objet a été placé en quarantaine, L'objet a été supprimé de la quarantaine ou de la sauvegarde, L'objet a été restauré depuis la quarantaine ou la sauvegarde
%SIZE_LIMIT%	Taille maximale de la quarantaine et du dossier de sauvegarde	La taille recommandée du dossier de la quarantaine et de la sauvegarde est atteinte
%ACTUAL_SIZE%	Taille actuelle de la quarantaine et du dossier de sauvegarde	La taille recommandée du dossier de la quarantaine et de la sauvegarde est atteinte
%DESCRIPTION%	Description	Erreur lors du traitement de l'objet en quarantaine

MACRO	DESCRIPTION	ÉVÉNEMENT
%OBJECT_TYPE%	Type d'objet	L'objet a été placé en quarantaine, L'objet a été supprimé de la quarantaine ou de la sauvegarde, L'objet a été restauré depuis la quarantaine ou la sauvegarde

CREATION DES RAPPORTS

Vous avez la possibilité de créer les rapports suivants :

- rapports sur les programmes malveillants détectés dans le plus grand nombre d'objets sur l'ordinateur (cf. page 94);
- rapports sur le fonctionnement des composants de Kaspersky Anti-Virus (cf. page 92).

  La ligne de commande vous permet d'obtenir les rapports sur le fonctionnement de composants particuliers. La console Web vous permet d'obtenir des rapports contenant les informations générales sur les composants **Protection en temps réel** et **Analyse à la demande**.

Vous pouvez exécuter les opérations suivantes :

- créer des rapports sur les périodes de temps spécifiées ;
- afficher les rapports dans des fenêtres séparées de la console Web ;
- enregistrer les rapports créés dans les formats suivants :
  - en cas d'utilisation de la ligne de commande : HTML ou CSV ;
  - en cas d'utilisation de la console Web : PDF ou XLS.

CONSULTATION DE L'ETAT DE LA PROTECTION VIA LE PROTOCOLE SNMP

Le protocole SNMP donne accès aux catégories d'informations suivantes sur Kaspersky Anti-Virus :

- informations générales ;
- statistiques de fonctionnement récoltées depuis l'installation de Kaspersky Anti-Virus ;
- informations sur les événements survenus durant l'utilisation de Kaspersky Anti-Virus.

Ces informations sont accessibles uniquement en lecture.

L'interaction via le protocole SNMP dans Kaspersky Anti-Virus est à charge de l'agent SNMP. N'importe quel agent SNMP compatible avec le protocole AgentX peut servir de gestionnaire SNMP.

L'application fonctionne avec les gestionnaires SNMP qui prennent en charge les protocoles SNMP v2, v2c, v3. L'agent SNMP proposé dans l'application est compatible avec le protocole AgentX version 1.

DANS CETTE SECTION

CONFIGURATION DE L'INTERACTION VIA LE PROTOCOLE SNMP

Pour activer l'échange d'informations via le protocole SNMP, procédez comme suit :

1. Indiquez l'adresse du serveur, où fonctionne le gestionnaire SNMP à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control \

   --set-settings 12 \

   MasterAgentXAddress=tcp:<adresse_IP_ou_nom_DNS_du_gestionnaire_SNMP>:705
   ```

   Cette adresse figure dans le fichier de configuration de l'agent SNMP maître.

2. Lancez la tâche de Kaspersky Anti-Virus **SNMP plugin** (ID=12), si elle avait été suspendue, à l'aide de l'instruction suivante :

   ```
   /opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 12
   ```

Ensuite, il est possible de contacter les objets MIB de Kaspersky Anti-Virus et d'obtenir des informations sur le protocole SNMP à l'aide des objets OID. Kaspersky Anti-Virus est livré avec des fichiers MIB qui contiennent les noms

symboliques des objets, les événements et leurs paramètres. Après l'installation de Kaspersky Anti-Virus, les fichiers MIB se trouvent dans le répertoire */opt/kaspersky/kav4fs/share/snmp-mibs*.

- *Pour utiliser les noms symboliques pour contacter les objets MIB de Kaspersky Anti-Virus,*

  SNMP maître l'accès aux fichiers MIB de Kaspersky Anti-Virus.

Pour consulter la structure MIB de Kaspersky Anti-Virus à l'aide de l'instruction *snmpwalk*, ajoutez la ligne suivante au fichier de configuration *snmpd.conf* :

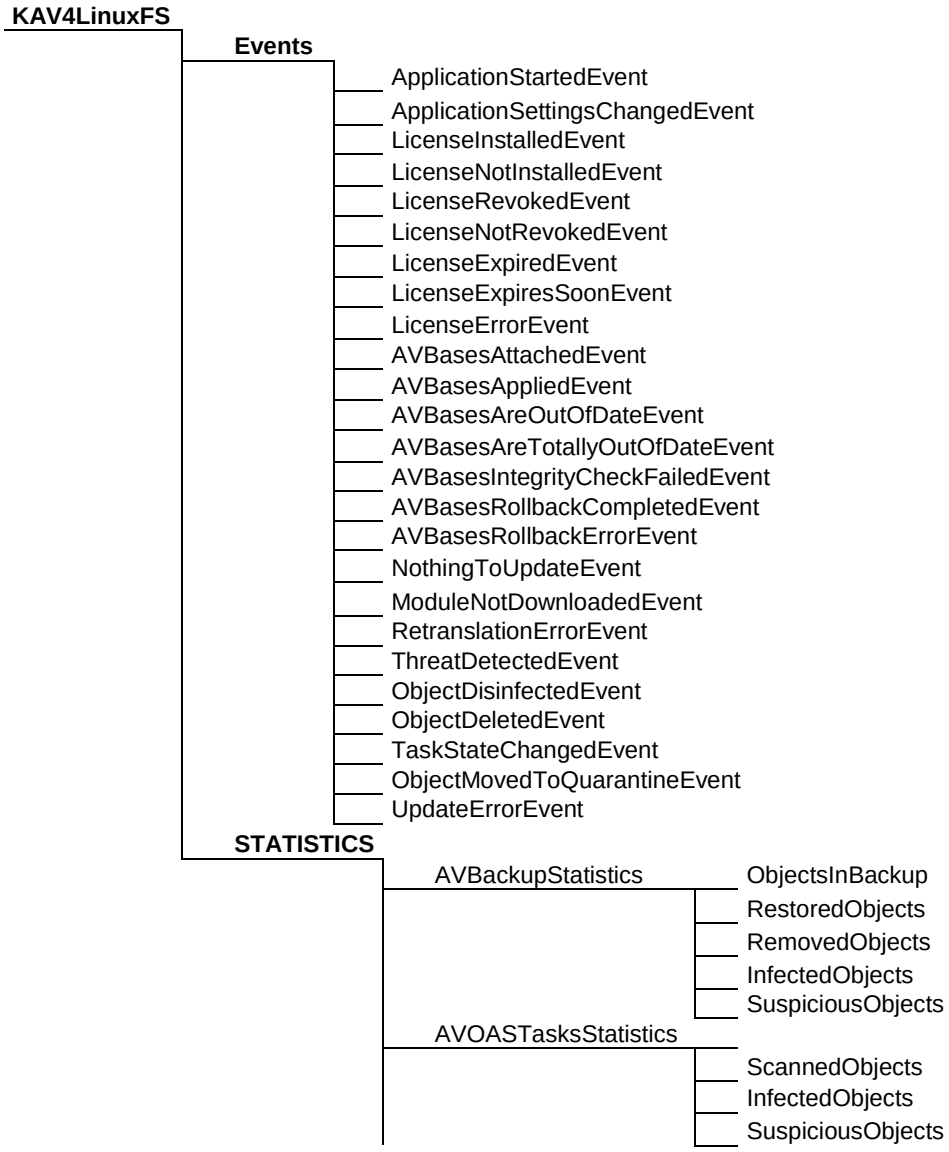
```
view systemview included .1.3.6.1.4.1.23668.1046
```

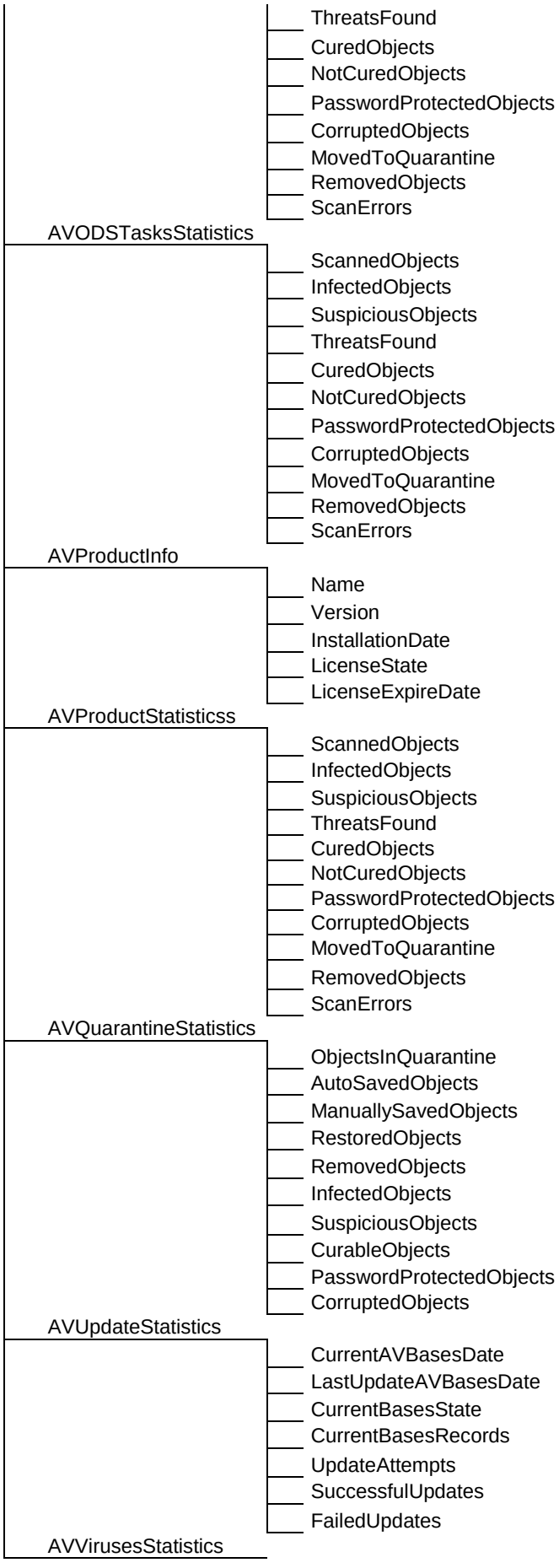
Le protocole SNMP permet d'accéder aux statistiques de fonctionnement et aux pièges d'événements survenus durant le fonctionnement de Kaspersky Anti-Virus. Vous pouvez activer / désactiver les pièges de Kaspersky Anti-Virus.

- *Pour activer / désactiver les pièges d'événements de Kaspersky Anti-Virus,*

  attribuez la valeur **yes/no** au paramètre **TrapsEnable**.

LA STRUCTURE MIB DE KASPERSKY ANTI-VIRUS




ThreatsFound
CuredObjects
NotCuredObjects
PasswordProtectedObjects
CorruptedObjects
MovedToQuarantine
RemovedObjects
ScanErrors
AVODSTasksStatistics
ScannedObjects
InfectedObjects
SuspiciousObjects
ThreatsFound
CuredObjects
NotCuredObjects
PasswordProtectedObjects
CorruptedObjects
MovedToQuarantine
RemovedObjects
ScanErrors
AVProductInfo
Name
Version
InstallationDate
LicenseState
LicenseExpireDate
AVProductStatisticss
ScannedObjects
InfectedObjects
SuspiciousObjects
ThreatsFound
CuredObjects
NotCuredObjects
PasswordProtectedObjects
CorruptedObjects
MovedToQuarantine
RemovedObjects
ScanErrors
AVQuarantineStatistics
ObjectsInQuarantine
AutoSavedObjects
ManuallySavedObjects
RestoredObjects
RemovedObjects
InfectedObjects
SuspiciousObjects
CurableObjects
PasswordProtectedObjects
CorruptedObjects
AVUpdateStatistics
CurrentAVBasesDate
LastUpdateAVBasesDate
CurrentBasesState
CurrentBasesRecords
UpdateAttempts
SuccessfulUpdates
FailedUpdates
AVVirusesStatistics

AVVirusesStatisticsTable
VirusName
InfectedObjects

LA DESCRIPTION DES OBJETS MIB DE KASPERSKY ANTI-VIRUS

La base des objets de Kaspersky Anti-Virus dans l'arborescence SNMP reçoit le nom symbolique suivant : *iso.org.dod.internet.private.enterprises.kaspersky.kav4LinuxFS*. Les noms symboliques des objets MIB de Kaspersky Anti-Virus sont affichés dans les tableaux ci-dessous.

Les noms symboliques sont indiqués par rapport à l'identificateur de Kaspersky Anti-Virus.

Evénements de Kaspersky Anti-Virus

Tableau 6. Evénements de Kaspersky Anti-Virus

NOM SYMBOLIQUE	DESCRIPTION
Events.ApplicationStartedEvent	Kaspersky Anti-Virus est lancé ; cet événement survient une fois que tous les services nécessaires pour le fonctionnement de Kaspersky Anti-Virus ont été lancées.
Events.ApplicationSettingsChangedEvent	Les paramètres généraux de Kaspersky Anti-Virus ont été modifiés.
Events.LicenseInstalledEvent	Le fichier de licence est installé.
Events.LicenseNotInstalledEvent	Le fichier de licence n'est pas installé.
Events.LicenseRevokedEvent	Le fichier de licence est supprimé avec succès.
Events.LicenseNotRevokedEvent	Le fichier de licence n'est pas supprimé.
Events.LicenseExpiredEvent	Licence a expiré.
Events.LicenseExpiresSoonEvent	Délai de validité de la licence va bientôt expirer.
Events.LicenseErrorEvent	Erreur du système de délivrance de licences.
Events.AVBasesAttachedEvent	Les bases de Kaspersky Anti-Virus sont téléchargées sur le serveur avec succès.
Events.AVBasesAppliedEvent	Les bases de Kaspersky Anti-Virus sont connectées et utilisées avec succès.
Events.AVBasesAreOutOfDateEvent	Les bases de Kaspersky Anti-Virus sont dépassées.
Events.AVBasesAreTotallyOutOfDateEvent	Les bases de Kaspersky Anti-Virus sont fortement dépassées.
Events.AVBasesIntegrityCheckFailedEvent	L'intégrité des bases de Kaspersky Anti-Virus a été violée.
Events.AVBasesRollbackCompletedEvent	La remise à la version précédente des bases de Kaspersky Anti-Virus a réussi.
Events.AVBasesRollbackErrorEvent	L'erreur pendant la remise à la version précédente des bases de Kaspersky Anti-Virus.
Events.NothingToUpdateEvent	La mise à jour n'est pas requise.
Events.UpdateErrorEvent	Une erreur s'est produite lors de la mise à jour.
Events.ModuleNotDownloadedEvent	Erreur de téléchargement du module actualisé de programme.
Events.RetranslationErrorEvent	Erreur de retransmission.
Events.TaskStateChangedEvent	L'état de la tâche a été modifié.
Events.ThreatDetectedEvent	Une menace a été détectée.
Events.ObjectDeletedEvent	Objet supprimé.
Events.ObjectDisinfectedEvent	Objet réparé.
Events.ObjectMovedToQuarantineEvent	Objet est placé en quarantaine.

Toutes les statistiques sont récoltées depuis l'installation de Kaspersky Anti-Virus.

Statistiques du dossier de sauvegarde

Tableau 7. Statistiques du dossier de sauvegarde

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVBackupStatistics.ObjectsInBackup	Nombre d'objets dans le stockage.
Statistics.AVBackupStatistics.RestoredObjects	Nombre d'objets restaurés du stockage.
Statistics.AVBackupStatistics.RemovedObjects	Nombre d'objets supprimés du stockage.
Statistics.AVBackupStatistics.InfectedObjects	Nombre d'objets infectés dans le stockage.
Statistics.AVBackupStatistics.SuspuciousObjects	Nombre d'objets suspects dans le stockage.

Le nombre d'objets dans le stockage ne désigne pas les objets qui s'y trouvent, qui ont été supprimés ou restaurés à ce moment, mais bien le nombre d'objets qui s'y trouvent, qui ont été supprimés ou restaurés tout au long de la période de collecte des statistiques.

Statistiques de la tâche de protection en temps réel

Tableau 8. Statistiques du fonctionnement de la tâche de protection en temps réel

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVOASTasksStatistics.ScannedObjects	Nombre d'objets analysés.
Statistics.AVOASTasksStatistics.ThreatsFound	Nombre de programmes malveillants détectés.
Statistics.AVOASTasksStatistics.InfectedObjects	Nombre d'objets infectés.
Statistics.AVOASTasksStatistics.SuspiciousObjects	Nombre d'objets suspects.
Statistics.AVOASTasksStatistics.CuredObjects	Nombre d'objets réparés.
Statistics.AVOASTasksStatistics.MovedToQuarantine	Nombre d'objets placés en quarantaine.
Statistics.AVOASTasksStatistics.RemovedObjects	Nombre d'objets supprimés.
Statistics.AVOASTasksStatistics.NotCuredObjects	Nombre d'objets non-réparés.
Statistics.AVOASTasksStatistics.ScanErrors	Nombre d'erreurs pendant l'analyse.
Statistics.AVOASTasksStatistics.PasswordProtectedObjects	Nombre d'objet protégés par un mot de passe.
Statistics.AVOASTasksStatistics.CorruptedObjects	Nombre d'objets endommagés

Configuration des tâches d'analyse à la demande

Statistiques du fonctionnement de la tâche d'analyse à la demande sont récoltées pour toutes les tâches.

Tableau 9. Statistiques du fonctionnement des tâches d'analyse à la demande

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVODSTasksStatistics.ScannedObjects	Nombre d'objets analysés.
Statistics.AVODSTasksStatistics.ThreatsFound	Nombre de programmes malveillants détectés.
Statistics.AVODSTasksStatistics.InfectedObjects	Nombre d'objets infectés.
Statistics.AVODSTasksStatistics.SuspiciousObjects	Nombre d'objets suspects.
Statistics.AVODSTasksStatistics.CuredObjects	Nombre d'objets réparés.
Statistics.AVODSTasksStatistics.MovedToQuarantine	Nombre d'objets placés en quarantaine.
Statistics.AVODSTasksStatistics.RemovedObjects	Nombre d'objets supprimés.
Statistics.AVODSTasksStatistics.NotCuredObjects	Nombre d'objets non-réparés.
Statistics.AVODSTasksStatistics.ScanErrors	Nombre d'erreurs pendant l'analyse.
Statistics.AVODSTasksStatistics.PasswordProtectedObjects	Nombre d'objet protégés par un mot de passe.
Statistics.AVODSTasksStatistics.CorruptedObjects	Nombre d'objets endommagés

Statistiques de Kaspersky Anti-Virus

Tableau 10. Informations générales sur le logiciel

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVProductInfo.Name	Nom de l'application.
Statistics.AVProductInfo.Version	Version du logiciel.
Statistics.AVProductInfo.InstallDate	Date d'installation de l'application.
Statistics.AVProductInfo.LicenseState	Statut de la licence.
Statistics.AVProductInfo.LicenseExpireDate	Date de fin de validité de la licence.

Statistiques du fonctionnement de Kaspersky Anti-Virus

Tableau 11. Statistiques du fonctionnement de l'application

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVProductStatistics.ScannedObjects	Nombre d'objets analysés.
Statistics.AVProductStatistics.ThreatsFound	Nombre de programmes malveillants détectés.
Statistics.AVProductStatistics.InfectedObjects	Nombre d'objets infectés.
Statistics.AVProductStatistics.SuspiciousObjects	Nombre d'objets suspects.
Statistics.AVProductStatistics.CuredObjects	Nombre d'objets réparés.
Statistics.AVProductStatistics.MovedToQuarantine	Nombre d'objets placés en quarantaine.
Statistics.AVProductStatistics.RemovedObjects	Nombre d'objets supprimés.
Statistics.AVProductStatistics.NotCuredObjects	Nombre d'objets non-réparés.
Statistics.AVProductStatistics.ScanErrors	Nombre d'erreurs pendant l'analyse.
Statistics.AVProductStatistics.PasswordProtectedObjects	Nombre d'objet protégés par un mot de passe.
Statistics.AVProductStatistics.CorruptedObjects	Nombre d'objets endommagés

Statistiques de la quarantaine

Tableau 12. Statistiques de la quarantaine

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVQuarantineStatistic.ObjectsInQuarantine	Nombre d'objets mis en quarantaine.
Statistics.AVQuarantineStatistic.AutoSavedObjects	Nombre d'objets placés automatiquement en quarantaine.
Statistics.AVQuarantineStatistic.ManuallySavedObjects	Nombre d'objets placés manuellement en quarantaine.
Statistics.AVQuarantineStatistic.RestoredObjects	Nombre d'objets restaurés de la quarantaine.
Statistics.AVQuarantineStatistic.RemovedObjects	Nombre d'objets supprimés de la quarantaine.
Statistics.AVQuarantineStatistic.InfectedObjects	Nombre d'objets infectés mis en quarantaine.
Statistics.AVQuarantineStatistic.SuspiciousObjects	Nombre d'objets suspects mis en quarantaine.
Statistics.AVQuarantineStatistic.CuredObjects	Nombre d'objets réparés mis en quarantaine.
Statistics.AVQuarantineStatistic.PasswordProtectedObjects	Nombre d'objets en quarantaine, protégés par un mot de passe.
Statistics.AVQuarantineStatistic.CorruptedObjects	Nombre d'objets endommagés mis en quarantaine.
Statistics.AVQuarantineStatistic.FalseDetectedObjects	Nombre d'objets faux discernés en quarantaine.

Le nombre d'objets en quarantaine ne désigne pas les objets qui s'y trouvent, qui ont été supprimés ou restaurés à ce moment, mais bien le nombre d'objets qui s'y trouvent, qui ont été supprimés ou restaurés tout au long de la période de collecte des statistiques.

Statistiques des mises à jour

Tableau 13. Statistiques des mises à jour

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVUpdateStatistics.CurrentAVBasesDate	Date d'édition de la version actuelle des bases de Kaspersky Anti-Virus.
Statistics.AVUpdateStatistics.LastUpdateAVBasesDate	Date de la dernière mise à jour des bases de Kaspersky Anti-Virus.
Statistics.AVUpdateStatistics.CurrentBasesState	Etat des bases de Kaspersky Anti-Virus.
Statistics.AVUpdateStatistics.CurrentBasesRecords	Nombre de signatures dans les bases de Kaspersky Anti-Virus.
Statistics.AVUpdateStatistics.UpdateAttempts	Nombre de tentatives de mises à jour.
Statistics.AVUpdateStatistics.SuccessfulUpdates	Nombre de tentatives réussies de mises à jour.
Statistics.AVUpdateStatistics.UpdateManualStops	Nombre d'arrêts manuels des mises à jour.
Statistics.AVUpdateStatistics.FailedUpdates	Nombres de mises à jour terminées avec des erreurs.

Statistiques de l'activité virale

Tableau 14. Statistiques de l'activité virale

NOM SYMBOLIQUE	DESCRIPTION
Statistics.AVVirusesStatistics.AVVirusesStatisticsTable.AVVirusName	Nom d'un virus.
Statistics.AVVirusesStatistics.LastUpdateAVBasesDate	Nombre d'objets où le virus a été découvert.

LES COMMANDES D'ADMINISTRATION DE KASPERSKY ANTI-VIRUS DEPUIS LA LIGNE DE COMMANDE

Lors de la saisie des commandes de Kaspersky Anti-Virus, appliquez les règles suivantes :

- Respectez le registre.
- Séparez les clés par le caractère " espace ".
- En utilisant le nom court (littéral) de la commande ou de la clé, saisissez la valeur immédiatement après la commande ou par espace. En utilisant le nom complet de la commande ou de la clé, saisissez la valeur avec le caractère " égal " (=) ou avec " espace ".

La liste des commandes de Kaspersky Anti-Virus est donnée dans le tableau suivant.

Tableau 15. Liste des commandes de Kaspersky Anti-Virus

COMMANDES	DESCRIPTION
--help (cf. page 89)	Affiche les renseignements sur les commandes de Kaspersky Anti-Virus.
Commandes d'administration de Kaspersky Anti-Virus	
--start-app (cf. page 89)	Lance Kaspersky Anti-Virus.
--restart-app (cf. page 90)	Redémarre Kaspersky Anti-Virus.
--stop-app (cf. page 89)	Arrête Kaspersky Anti-Virus.
--scan-file (cf. page 90)	Analyse fichiers ou répertoires.
Commandes de la réception de la statistique de Kaspersky Anti-Virus	
-S	Préfix ; désigne que la commande appartient au groupe des commandes de la réception de la statistique et des rapports (facultatif).
-S --app-info (cf. page 91)	Fait afficher les informations sur Kaspersky Anti-Virus.
-S --get-stat (cf. page 92)	Crée les rapports sur le fonctionnement de Kaspersky Anti-Virus et de ses composants.
-S --top-viruses (cf. page 94)	Crée les rapports sur les menaces les plus fréquentes sur le serveur.
Commandes de l'affichage des événements de Kaspersky Anti-Virus	
-W (cf. page 90)	Fait activer l'affichage des événements de Kaspersky Anti-Virus.
Commandes d'administration des paramètres de Kaspersky Anti-Virus et des tâches	

COMMANDES	DESCRIPTION
-T	Préfix ; désigne que la commande appartient au groupe des commandes d'administration des paramètres de Kaspersky Anti-Virus / d'administration des tâches (facultatif).
-T --get-app-settings (cf. page 96)	Fait afficher les paramètres généraux de Kaspersky Anti-Virus.
-T --set-app-settings (cf. page 97)	Installe les paramètres généraux de Kaspersky Anti-Virus.
-T --get-task-list (cf. page 98)	Reprend la liste des tâches en cours de Kaspersky Anti-Virus.
-T --get-task-state (cf. page 99)	Fait afficher l'état de la tâche spécifiée (par exemple, En cours, Arrêtée, Suspendue).
-T --start-task (cf. page 101)	Lance la tâche.
-T --stop-task (cf. page 102)	Arrête la tâche.
-T --suspend-task (cf. page 102)	Suspend la tâche.
-T --resume-task (cf. page 102)	Reprend la tâche.
-T --get-settings (cf. page 103)	Fait afficher les paramètres de la tâche.
-T --set-settings (cf. page 104)	Installe les paramètres de la tâche.
-T --create-task (cf. page 105)	Crée la tâche de type spécifié ; importe dans la tâche les paramètres depuis le fichier de configuration spécifié.
-T --delete-task	Supprime la tâche.
-T --set-schedule (cf. page 106)	Détermine les paramètres de l'horaire de la tâche / les importe dans la tâche depuis le fichier de configuration.
-T --get-schedule (cf. page 107)	Fait afficher les paramètres de l'horaire de la tâche.
-T --del-schedule	Supprime l'horaire de la tâche.
-T --show-schedule (cf. page 108)	Recherche les événements planifiés.
Commandes d'administration des licences	

COMMANDES	DESCRIPTION
-L	Préfix ; désigne que la commande appartient au groupe des commandes d'administration des licences (facultatif).
-L --validate-key (cf. page 110)	Vérifie l'authenticité de la licence suivant la base de Kaspersky Lab ; affiche les informations sur la licence depuis le fichier de clé sans installer la licence.
-L --show-license-info	Affiche les informations sur la licence depuis le fichier de clé sans installer la licence.
-L --get-installed-keys (cf. page 112)	Fait afficher les informations sur les licences installées.
-L --query-status (cf. page 110)	Fait afficher l'état des licences installées.
-L --install-active-key (cf. page 113)	Installe la licence active.
-L --install-suppl-key (cf. page 113)	Installe la licence supplémentaire.
-L --revoke-active-key (cf. page 114)	Supprime la licence active.
-L --revoke-suppl-key (cf. page 114)	Supprime la licence supplémentaire.
Commandes d'administration de la quarantaine et du répertoire de sauvegarde de réserve	
-Q	Préfix ; désigne que la commande appartient au groupe des commandes d'administration de la quarantaine et du répertoire de sauvegarde de réserve (facultatif).
-Q --get-stat (cf. page 114)	Fait afficher la courte statistique du répertoire de sauvegarde.
-Q --query (cf. page 115)	Fait afficher les informations sur les objets dans le répertoire de sauvegarde.
-Q --get-one (cf. page 115)	Fait afficher les informations sur un seul objet du répertoire de sauvegarde.
-Q --restore (cf. page 116)	Restaure les objets depuis le répertoire de sauvegarde.
-Q --add-object (cf. page 116)	Met la copie de l'objet en quarantaine.
-Q --remove (cf. page 117)	Supprime l'objet du répertoire de sauvegarde.
-Q --export (cf. page 117)	Exporte les objets depuis le répertoire de sauvegarde dans le répertoire spécifié.
-Q --import (cf. page 118)	Importe les objets dans le répertoire de sauvegarde depuis le répertoire spécifié dans lequel ils ont été exportés avant.
-Q --mass-remove (cf. page 118)	Purge le répertoire de sauvegarde complètement ou partiellement.
Instruction d'administration du journal des événements	
-E	Préfixe ; désigne que l'instruction appartient au groupe d'instructions d'administration du journal des événements (facultatif).
-E --count (cf. page 119)	Affiche le nombre d'événement filtrés du journal des événements ou du fichier de rotation indiqué.
-E --query (cf. page 120)	Affiche le nombre d'événement filtrés du journal des événements ou du fichier de rotation indiqué.
-E --period (cf. page 121)	Affiche l'intervalle de temps comprenant les événements enregistrés dans le journal des événements ou dans le fichier de rotation indiqué.
-E --rotate (cf. page 121)	Exécute la rotation du journal des événements.
-E --remove (cf. page 121)	Supprime les événements du journal des événements ou du fichier de rotation indiqué.

AFFICHAGE DES RENSEIGNEMENTS SUR LES COMMANDES DE KASPERSKY ANTI-VIRUS

L'instruction kav4fs-control avec l'argument --help <sélection d'instruction de Kaspersky Lab> affiche l'aide sur les instructions de Kaspersky Lab.

Syntaxe de la commande

```
kav4fs-control --help [<ensemble des commandes de Kaspersky Anti-Virus]
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<ensemble des commandes de Kaspersky Anti-Virus>	Spécifiez l'ensemble des commandes de Kaspersky Anti-Virus dont les renseignements vous voulez recevoir. Les valeurs possibles comprennent : -T [--task-and-settings] – commandes d'administration des tâches et des paramètres généraux de Kaspersky Anti-Virus ; -L [--licenser] – commandes d'administration des licences ; -Q [--quarantine-and-backup] – commandes d'administration de la quarantaine et du répertoire de sauvegarde de réserve ; -S [--statistics] – commandes d'administration de la statistique de Kaspersky Anti-Virus ; -E [--event-log] – commandes d'administration des événements de Kaspersky Anti-Virus.

LANCEMENT DE KASPERSKY ANTI-VIRUS

Attention ! Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kav4fs-supervisor est lancé sur l'ordinateur.

L'instruction kav4fs-control avec l'argument --start-app lance Kaspersky Anti-Virus.

Syntaxe de la commande

```
kav4fs-control --start-app
```

ARRET DE KASPERSKY ANTI-VIRUS

Attention ! Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kav4fs-supervisor est lancé sur l'ordinateur.

L'instruction kav4fs-control avec l'argument --stop-app arrête Kaspersky Anti-Virus.

Syntaxe de la commande

```
kav4fs-control --stop-app
```

REDEMARRAGE DE KASPERSKY ANTI-VIRUS

Attention ! Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kav4fs-supervisor est lancé sur l'ordinateur.

L'instruction kav4fs-control avec l'argument --start-app lance Kaspersky Anti-Virus.

Syntaxe de la commande

```
kav4fs-control --restart-app
```

ACTIVATION DE L'AFFICHAGE DES EVENEMENTS

La commande -W fait activer le mode d'affichage des événements de Kaspersky Anti-Virus. Vous pouvez utiliser cette commande toute seule pour afficher tous les événements de Kaspersky Anti-Virus, ainsi que ensemble avec la commande --start-task (cf. page 101) (lancer la tâche) pour afficher uniquement les événements sur la tâche en cours d'exécution.

La commande reprend le nom de l'événement et les informations supplémentaires sur l'événement.

Syntaxe de la commande

```
kav4fs-control -W [--file=<nom du fichier>]
```

Exemple de la commande

- *Activer le mode d'affichage des événements de Kaspersky Anti-Virus :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control -W
  ```

- *Activer le mode de sauvegarde des événements de Kaspersky Anti-Virus dans le fichier ; enregistrer les événements dans le fichier du registre 081808.xml du répertoire en cours :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  -W --file 081808.xml
  ```

CLÉ	SPÉCIFICATION ET VALEURS POSSIBLES
--file <nom du fichier>	Nom du fichier du registre dans lequel seront enregistrées les informations sur les événements de Kaspersky Anti-Virus. Le format du fichier du registre sauvegardé est XML.

ANALYSE RAPIDE DES FICHIERS ET DES REPERTOIRES

L'instruction kav4fs-control avec l'argument --scan-file réalise une analyse rapide des fichiers et des répertoires.

Syntaxe de la commande

```
kav4fs-control --action <action> --scan-file <chemin d'accès au fichier ou au
répertoire>[ <chemin d'accès au fichier ou au répertoire> ...]
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--scan-file <chemin d'accès au fichier ou au répertoire>	Nom des fichiers ou des répertoires qui seront analysés rapidement par Kaspersky Anti-Virus.
--action <action>	Clé facultative. Valeurs possibles : • **Recommended** – exécuter l'action recommandée. • **Cure** – réparer. • **Quarantine** – mettre en quarantaine. • **Remove** – supprimer. • **Skip** – ignorer.

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS

Avant d'appliquer les mises à jour des bases, Kaspersky Anti-Virus crée des copies de réserve des bases utilisées jusqu'à présent. Si la mise à jour échoue ou se solde par un échec, Kaspersky Anti-Virus revient automatiquement aux bases en vigueur avant la dernière mise à jour.

Si des problèmes se présentent après la mise à jour, vous pouvez utiliser les mises à jour installées antérieurement.

La tâche de remise à l'état antérieur à la mise à jour des bases restaure la copie de sauvegarde des bases de Kaspersky Anti-Virus.

Syntaxe d'exécution de la tâche

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 14
```

COMMANDES DE RECEPTION DE LA STATISTIQUE ET DES RAPPORTS

DANS CETTE SECTION

CONSULTATION DES INFORMATIONS SUR L'APPLICATION

La commande --app-info fait afficher les informations sur Kaspersky Anti-Virus.

Syntaxe de la commande

```
kav4fs-control [-S] --app-info
```

L'instruction affiche les informations suivantes:

CHAMP	DESCRIPTION
Name	Nom de Kaspersky Anti-Virus
Version	Version de Kaspersky Anti-Virus
Install date	Date et heure de la dernière installation de Kaspersky Anti-Virus
License state	Statut de la licence
License expire date	Date de fin de validité de la licence

CONSULTATION DES RAPPORTS SUR LE FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

La commande --get-stat fait afficher la statistique du fonctionnement de Kaspersky Anti-Virus ; permet de créer des rapports sur le fonctionnement de certains composants de Kaspersky Anti-Virus pour des périodes de temps spécifiées ; permet d'enregistrer les rapports dans les fichiers.

Syntaxe de la commande

```
kav4fs-control [-S] --get-stat <composant de Kaspersky Lab> \
[--from=<date de début>][--to=<date de fin>] \
[--task-id=<ID de la tâche (uniquement pour les tâches analyse à la demande et mise à jour)>] \
[--export-report=<nom du fichier de rapport>] [--report-type=<format du fichier de rapport>]
```

Exemple de la commande

- *Pour consulter la statistique du fonctionnement de Kaspersky Anti-Virus :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-stat Application
```

- *Pour afficher la statistique de la protection en temps réel pour janvier 2009 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-stat OAS --from=2009-01-01 --to=2009-01-31
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<composant de Kaspersky Anti-Virus>	Spécifiez le composant de Kaspersky Anti-Virus, dont la statistique du fonctionnement vous voulez recevoir. Les valeurs possibles comprennent : Application – application ; OAS – protection en temps réel ; ODS – analyse à la demande ; Quarantine – quarantaine ; Backup – répertoire de sauvegarde de réserve ; Update – mise à jour.
--from=<date de début>	Date de début du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – recevoir les informations depuis 0 heure de la date spécifiée ; • date et heure au format AAAA-MM-DD HH:MM:SS – recevoir les informations depuis l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – recevoir les informations depuis l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --from=<date de début>, le rapport comprendra les informations depuis l'installation de Kaspersky Anti-Virus.
--to=<date de fin>	Date de fin du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – recevoir les informations jusqu'à la date spécifiée inclus ; • date et heure au format AAAA-MM-DD HH:MM:SS – recevoir les informations jusqu'à l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – recevoir les informations jusqu'à l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --to=<date de fin>, le rapport comprendra les informations jusqu'au moment actuel.
--task-id=<ID de la tâche (uniquement pour les tâches d'analyse à la demande)>	Numéro d'identification de la tâche d'analyse à la demande dans Kaspersky Anti-Virus. Le rapport comprendra la statistique de la tâche d'analyse à la demande avec le numéro d'identification pour la période depuis le dernier lancement de la tâche. Cette clé n'est pas utilisée ensemble avec les clés --from=<date de début> et --to=<date de fin>.
--export-report=<nom du fichier du rapport>	Clé facultative. Nom du fichier dans lequel sera enregistré le rapport reçu. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent sur le disque, le fichier ne sera pas créé. Vous pouvez enregistrer le fichier du rapport au format HTML ou CSV. Vous pouvez attribuer au fichier l'extension HTML ou CSV, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --report-type, vous pouvez attribuer au fichier n'importe quelle extension.
--report-type=<format du fichier du rapport>	Clé facultative. Par défaut, le format du fichier indiqué par l'argument --export-report est défini par son extension. Indiquez cette clé si vous avez spécifié l'extension du fichier autre que HTML ou CSV. Valeurs possibles de la clé : HTML, CSV.

CONSULTATION DES RAPPORTS SUR LES MENACES LES PLUS FREQUENTES

La commande --top-viruses affiche les informations sur les programmes malveillants détectés dans la majorité des objets sur le serveur durant la période de temps spécifiée ; permet d'enregistrer le rapport dans le fichier.

Syntaxe de la commande

```
kav4fs-control [-S] --top-viruses <nombre de programmes malveillants> \
[--from=<date de début>][--to=<date de fin>][--export-report=<nom du fichier>] \
[--report-type=<format du fichier du rapport>]
```

Exemple de la commande

- *Pour recevoir les informations sur cinq programmes malveillants les plus fréquents sur le serveur pour janvier 2009, enregistrer le rapport dans le fichier /home/kavreports/2009_01_top_viruses.html :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--top-viruses 5 --from=2009-01-01 --to=2009-01-31 \
--export-report=/home/kavreports/2009_01_top_viruses.html
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<nombre de programmes malveillants>	Nombre de programmes malveillants ; le rapport ne comprendra que les informations sur le nombre spécifié des programmes malveillants les plus fréquents sur le serveur.
--from=<date de début>	Date de début du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – recevoir les informations depuis 0 heure de la date spécifiée ; • date et heure au format AAAA-MM-DD HH:MM:SS – recevoir les informations depuis l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – recevoir les informations depuis l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --to=<date de fin>, le rapport comprendra les informations jusqu'au moment actuel.
--to=<date de fin>	Date de fin du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – recevoir les informations jusqu'à la date spécifiée inclus ; • date et heure au format AAAA-MM-DD HH:MM:SS – recevoir les informations jusqu'à l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – recevoir les informations jusqu'à l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --from=<date de début>, le rapport comprendra les informations depuis l'installation de Kaspersky Anti-Virus.
--export-report=<nom du fichier du rapport>	Clé facultative. Nom du fichier dans lequel sera enregistré le rapport reçu. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent sur le disque, le fichier du rapport ne sera pas créé. Vous pouvez enregistrer le fichier du rapport au format HTML ou CSV. Vous pouvez attribuer au fichier l'extension HTML ou CSV, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --report-type, vous pouvez attribuer au fichier n'importe quelle extension.
--report-type=<format du fichier du rapport>	Clé facultative. Par défaut, le format du fichier indiqué par l'argument --export-report est défini par son extension. Indiquez cette clé si vous avez spécifié l'extension du fichier autre que HTML ou CSV. Valeurs possibles de la clé : HTML, CSV.

COMMANDES D'ADMINISTRATION DES PARAMETRES DE KASPERSKY ANTI-VIRUS ET DES TACHES

DANS CETTE SECTION

OBTENTION DES PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS

L'instruction --get-app-settings fait afficher les paramètres généraux de Kaspersky Anti-Virus (cf. page 160). Cette instruction permet également d'obtenir les paramètres généraux de Kaspersky Anti-Virus définis à l'aide des arguments de l'instruction.

Vous pouvez utiliser cette commande pour modifier les paramètres généraux de Kaspersky Anti-Virus installé sur le serveur :

1. Enregistrez les paramètres généraux de Kaspersky Anti-Virus dans le fichier de configuration à l'aide de l'instruction --get-app-settings.

2. Ouvrez le fichier de configuration créé, modifiez les paramètres voulus et enregistrez les modifications faites.

3. Importez les paramètres depuis le fichier de configuration dans Kaspersky Anti-Virus à l'aide de l'instruction --set-app-settings (cf. page 97). Kaspersky Anti-Virus utilisera les nouvelles valeurs des paramètres après que vous aurez arrêté et relancé le service Kaspersky Anti-Virus à l'aide des instructions --stop-app et --start-app.

Vous pouvez utiliser le fichier de configuration créé pour importer les paramètres dans Kaspersky Anti-Virus qui est installé sur un autre serveur.

Syntaxe de la commande

```
kav4fs-control [-T] \
--get-app-settings [--file=<nom du fichier de configuration>] \
 --file-format=<INI|XML>
kav4fs-control [-T] --get-app-settings <nom du paramètre>
```

Exemple de la commande

- *Exportez les paramètres généraux de Kaspersky Anti-Virus dans le fichier possédant le nom kav_config.xml. Enregistrer le fichier créé dans le répertoire en cours :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --get-app-settings -F kav_config.xml
  ```

- *Affiche la valeur du paramètre TraceLevel :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --get-app-settings TraceLevel
  ```

CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Nom du fichier de configuration dans lequel seront enregistrés les paramètres de Kaspersky Anti-Virus. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent sur le disque, le fichier de configuration ne sera pas créé. Vous pouvez enregistrer le fichier de configuration au format XML ou INI. Vous pouvez attribuer au fichier l'extension XML ou INI, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --file-format, vous pouvez attribuer au fichier n'importe quelle extension.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration indiqué par l'argument -F, est défini par son extension. Spécifiez cette clé si l'extension du fichier de configuration que vous avez spécifiée est différente de son format. Valeurs possibles de la clé : XML, INI.

MODIFICATION DES PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS

L'instruction --set-app-settings détermine à l'aide des arguments de l'instruction ou importe depuis le fichier de configuration spécifié les paramètres généraux de Kaspersky Anti-Virus (cf. page 160).

Vous pouvez utiliser cette commande pour modifier les paramètres généraux de Kaspersky Anti-Virus :

1. Enregistrez les paramètres généraux de Kaspersky Anti-Virus dans le fichier de configuration à l'aide de l'instruction --get-app-settings (cf. page 96).

2. Ouvrez le fichier de configuration créé, modifiez les paramètres voulus et enregistrez les modifications faites.

3. Importez les paramètres depuis le fichier de configuration dans Kaspersky Anti-Virus à l'aide de la commande --set-app-settings. Kaspersky Anti-Virus utilisera les nouvelles valeurs des paramètres après que vous aurez arrêté et relancé le service Kaspersky Anti-Virus à l'aide des commandes --stop-app et --start-app ou à l'aide de la commande --restart-app.

Syntaxe de la commande

```
kav4fs-control [-T] --set-app-settings \
```

```
--file=<nom du fichier de configuration> \
 --file-format=<INI|XML>
kav4fs-control [-T] \
--set-app-settings <nom du paramètre>=<valeur du paramètre> \
<nom du paramètre>=<valeur du paramètre>
```

Exemple de la commande

- *Importez dans Kaspersky Anti-Virus les paramètres généraux depuis le fichier de configuration possédant le nom /home/test/kav_config.xml :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --set-app-settings -F /home/test/kav_config.xml
  ```

- *Déterminer le niveau de détails dans le registre du tracé " Evénements importants " :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --set-app-settings TraceLevel=Warning
  ```

CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Le nom du fichier de configuration depuis lequel les paramètres seront importés dans Kaspersky Anti-Virus, comprend le chemin d'accès complet au fichier.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration indiqué par l'argument -F, est défini par son extension. Spécifiez cette clé si le format du fichier de configuration n'est pas conforme à son extension. Valeurs possibles de la clé : XML, INI.

CONSULTATION DE LA LISTE DES TACHES DE KASPERSKY ANTI-VIRUS

La commande --get-task-list reprend la liste des tâches disponibles de Kaspersky Anti-Virus.

Syntaxe de la commande

```
kav4fs-control [-T] --get-task-list
```

Les informations suivantes sur les tâches de Kaspersky Anti-Virus sont affichées :

CHAMP	DESCRIPTION
Name	Nom de la tâche ; le nom de la tâche d'utilisateur est attribué par l'utilisateur lors de sa création ; le nom des tâches de système est attribué par Kaspersky Anti-Virus.
Id	Le numéro d'identification de la tâche (nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création).
Class	Type de tâche de Kaspersky Anti-Virus. Il peut avoir les valeurs suivantes : • tâches que l'utilisateur peut administrer : Update : tâche prédéfinie de mise à jour (ID=6) ; OAS – tâche de protection en temps réel (ID=8) ; ODS : tâche prédéfinie d'analyse à la demande (ID=9) ; QS – tâche de l'analyse des objets mis en quarantaine (ID=10) ; • tâches qui assurent des fonctions de service : EventManager : assure l'échange des messages à l'intérieur de l'application (ID=1) ; AVS : assure le service d'analyse antivirus (ID=2) ; Quarantine : administre la quarantaine et le dossier de sauvegarde (ID=3) ; Statistics : récolte les statistiques (ID=4); License : réalise le " serveur de licence " (ID=5) ; Notifier : administre l'envoi de notifications et l'exécution des actions en fonction des événements (ID=7) ; EventStorage : assure le service du journal des événements (ID=11) ; Snmp plugin : assure le transfert des informations relatives au programme via le protocole SNMP (ID=12).
State	Etat de la tâche. Valeurs possibles : Stopped – arrêtée ; Stopping – en cours d'arrêt ; Started – en cours d'exécution ; Starting – en cours de lancement ; Suspended – suspendue ; Suspending – en cours de suspension ; Resumed – reprise ; Resuming – en cours de reprise ; Failed – terminée par une erreur.

CONSULTATION DE L'ETAT DE LA TACHE

La commande --get-task-state reprend l'état de la tâche spécifiée (par exemple, En cours d'exécution, Terminée, Suspendue).

Syntaxe de la commande

```
kav4fs-control [-T] --get-task-state <ID de la tâche>
```

Exemple de la commande

- *Obtenir l'état de la tâche avec ID=9 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-task-state 9
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez l'instruction kav4fs-control --get-task-list (cf. page 98).

Les informations sur la tâche suivantes sont affichées :

CHAMP	DESCRIPTION
Name	Nom de la tâche ; le nom de la tâche d'utilisateur est attribué par l'utilisateur lors de sa création ; le nom de la tâche de système est attribué par Kaspersky Anti-Virus.
Id	Le numéro d'identification de la tâche (nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création).
Class	Type de tâche de Kaspersky Anti-Virus. Il peut avoir les valeurs suivantes : • tâches que l'utilisateur peut administrer : Update : tâche prédéfinie de mise à jour (ID=6) ; OAS – tâche de protection en temps réel (ID=8) ; ODS : tâche prédéfinie d'analyse à la demande (ID=9) ; QS – tâche de l'analyse des objets mis en quarantaine (ID=10) ; • tâches qui assurent des fonctions de service : EventManager : assure l'échange des messages à l'intérieur de l'application (ID=1) ; AVS : assure le service d'analyse antivirus (ID=2) ; Quarantine : administre la quarantaine et le dossier de sauvegarde (ID=3) ; Statistics : récolte les statistiques (ID=4); License : réalise le " serveur de licence " (ID=5) ; Notifier : administre l'envoi de notifications et l'exécution des actions en fonction des événements (ID=7) ; EventStorage : assure le service du journal des événements (ID=11) ; Snmp plugin : assure le transfert des informations relatives au programme via le protocole SNMP (ID=12).
State	Etat de la tâche. Valeurs possibles : Complete – tâche s'est terminée sans échec ; Stopping – en cours d'arrêt ; Started – en cours d'exécution ; Starting – en cours de lancement ; Suspended – suspendue ; Suspending – en cours de suspension ; Resuming – en cours de reprise ; Failed – terminée par une erreur ; Interrupted by user – l'utilisateur a interrompu l'exécution de la tâche.

LANCEMENT D'UNE TACHE

La commande --start-task lance la tâche avec le numéro d'identification spécifié. Cette instruction peut être exécutée avec l'argument -W (cf. page 90) et les informations relatives aux événements survenus pendant l'exécution de la tâche seront affichées sur la console ou dans un fichier.

Syntaxe de la commande

```
kav4fs-control --start-task <ID de la tâche>
```

Exemple de la commande

- *Lancer la tâche avec ID=6 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 6
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande -T --get-task-list (cf. page 98).

ARRET D'UNE TACHE

La commande --stop-task lance la tâche avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kav4fs-control [-T] --stop-task <ID de la tâche>
```

Exemple de la commande

- *Arrêter la tâche avec ID=6 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --stop-task 6
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande kav4fs-control -T--get-task-list (cf. page 98).

SUSPENSION D'UNE TACHE

La commande --suspend-task lance la tâche avec le numéro d'identification spécifié. Vous pouvez suspendre la tâche de protection en temps réel et les tâches d'analyse à la demande. Vous ne pouvez pas suspendre les tâches de mise à jour.

Syntaxe de la commande

```
kav4fs-control [-T] --suspend-task <ID de la tâche>
```

Exemple de la commande

- *Suspendre la tâche avec ID=9 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --suspend-task 9
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande kav4fs-control -T--get-task-list (cf. page 98).

REPRISE D'UNE TACHE

La commande --resume-task reprend la tâche possédant le numéro d'identification spécifié qui a été suspendue à l'aide de la commande --suspend-task (cf. page 102).

Syntaxe de la commande

```
kav4fs-control [-T] --resume-task <ID de la tâche>
```

Exemple de la commande

- *Reprendre la tâche avec ID=9 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --resume-task 9
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande -T --get-task-list (cf. page 98).

OBTENTION DES PARAMETRES D'UNE TACHE

L'instruction --get-settings affiche tous les paramètres de la tâche définie ou les paramètres définis à l'aide des arguments de l'instruction.

Vous pouvez exporter les paramètres de la tâche dans un fichier de configuration sur un ordinateur et importer les paramètres (cf. la rubrique " Modification des paramètres de la tâche " cf. page 104) depuis ce fichier de configuration dans la tâche du type approprié sur un autre ordinateur.

Syntaxe de la commande

```
kav4fs-control [-T] --get-settings <ID de la tâche>
[--file=<nom du fichier de configuration>] --file-format=<INI|XML>
kav4fs-control [-T] --get-settings <ID de la tâche>
<nom de la rubrique du fichier INI>.<nom du paramètre>
```

Exemple de la commande

- *Exporter les paramètres de la tâche possédant ID=9 dans le fichier /home/test/configkavscanner.xml :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 9 -F /home/test/configkavscanner.xml
```

- *Exporter les paramètres de la tâche possédant ID=9 dans le fichier configkavscanner.xml situé dans le répertoire en cours :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 9 --file=configkavscanner.xml
```

- *Affiche la valeur du paramètre Path tiré de la sous-rubrique AreaPath de la rubrique ScanScope, définie dans la tâche d'analyse à la demande :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 9 ScanScope.AreaPath.Path
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--get-settings <ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande -T --get-task-list (cf. page 98).
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Nom du fichier de configuration dans lequel seront enregistrés les paramètres de la tâche. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent, le fichier de configuration ne sera pas créé. Vous pouvez enregistrer le fichier de configuration au format XML ou INI. Vous pouvez attribuer au fichier l'extension XML ou INI, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --file-format, vous pouvez attribuer au fichier n'importe quelle extension.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration indiqué par l'argument -F, est défini par son extension. Indiquez cette clé si vous avez spécifié l'extension du fichier autre que XML ou INI. Valeurs possibles de la clé : XML, INI.

MODIFICATION DES PARAMETRES DE LA TACHE

L'instruction --set-settings définit les paramètres de la tâche à l'aide des arguments de l'instruction ou les importe depuis le fichier de configuration désigné.

Vous pouvez importer les paramètres depuis le fichier de configuration dans la tâche exécutée du type correspondant. Kaspersky Anti-Virus utilisera de nouvelles valeurs des paramètres dans la tâche de protection en temps réel – immédiatement, dans les tâches des autres types – lors du prochain lancement de la tâche.

Syntaxe de la commande

```
kav4fs-control [-T] --set-settings <ID de la tâche>
--file=<nom du fichier de configuration> --file-format=<INI|XML>
kav4fs-control [-T] --set-settings <ID de la tâche>
<nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre>
```

Exemple de la commande

- *Importer dans la tâche avec ID=9 les paramètres depuis le fichier de configuration /home/test/config_fridayscan.xml :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --set-settings 9 \
--file=/home/test/config_fridayscan.xml
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--set-settings <ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande -T --get-task-list (cf. page 98).
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Le nom du fichier de configuration depuis lequel les paramètres seront importés dans la tâche, comprend le chemin d'accès complet au fichier.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration indiqué par l'argument -F, est défini par son extension. Spécifiez cette clé si l'extension du fichier spécifié n'est pas conforme à son format. Valeurs possibles de la clé : XML, INI.

CRÉATION D'UNE TÂCHE

La commande --create-task crée la tâche de Kaspersky Anti-Virus pour le composant spécifié ; importe dans la tâche les paramètres depuis le fichier de configuration spécifié. La commande reprend le numéro d'identification de la tâche créée.

Vous pouvez créer de nouvelles tâches d'analyse à la demande et de mise à jour.

Syntaxe de la commande

```
kav4fs-control [-T] --create-task <nom de la tâche> \
--use-task-type=<type de la tâche> --file=<nom du fichier de configuration> \
--file-format=<INI|XML>
```

Exemples de la commande

- *Créer la tâche d'analyse à la demande avec le nom Fridayscan ; importer dans la tâche les paramètres depuis le fichier de configuration /home/test/config_kavscanner.xml :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--create-task Fridayscan --use-task-type=ODS \
--file=/home/test/config_kavscanner.xml
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--create-task <nom de la tâche> -C <nom de la tâche>	Attribuez un nom à la tâche. Il peut contenir le nombre illimité de caractères ASCII.
--use-task-type=<type de la tâche>	Clé obligatoire. Spécifiez le type de la tâche à créer. Valeurs possibles : ODS – tâche d'analyse à la demande ; Update – tâche de mise à jour.
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Argument obligatoire pour créer une tâche de mise à jour de Kaspersky Anti-Virus. Spécifiez le chemin d'accès complet au fichier de configuration existant. Kaspersky Anti-Virus importe dans la tâche les paramètres spécifiés dans ce fichier.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration indiqué par l'argument -F, est défini par son extension. Spécifiez cette clé si l'extension du fichier de configuration spécifié n'est pas conforme à son format. Valeurs possibles de la clé : XML, INI.

SUPPRESSION D'UNE TÂCHE

La commande --delete-task supprime la tâche de Kaspersky Anti-Virus avec le numéro d'identification spécifié. Vous pouvez supprimer des tâches d'analyse à la demande (sauf la tâche **Analyse des objets en quarantaine**) ou des tâches de mise à jour.

Vous ne pouvez pas supprimer la tâche de protection en temps réel.

Syntaxe de la commande

```
kav4fs-control [-T] --delete-task <ID de la tâche>
```

Exemples de la commande

- *Supprimer la tâche avec ID=20 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --delete-task 20
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
--delete-task <ID de la tâche> -D <ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Anti-Virus attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Anti-Virus, utilisez la commande -T --get-task-list (cf. page 98).

OBTENTION DES PARAMETRES DE L'HORAIRE D'UNE TACHE

L'instruction --get-schedule fait afficher les paramètres de l'horaire de la tâche (cf. page 155). Cette instruction permet également d'obtenir les paramètres de planification de la tâche définis à l'aide des arguments de l'instruction.

Vous pouvez utiliser cette commande pour modifier l'horaire de la tâche :

1. Enregistrez les paramètres de planification dans un fichier de configuration à l'aide de l'instruction -T --get-schedule.
2. Ouvrez le fichier de configuration créé, modifiez les paramètres voulus et enregistrez les modifications faites.
3. Importez les paramètres depuis le fichier de configuration dans Kaspersky Anti-Virus à l'aide de l'instruction --set-schedule (cf. page 106). Kaspersky Anti-Virus utilisera de nouvelles valeurs des paramètres de l'horaire immédiatement.

Syntaxe de la commande

```
kav4fs-control [-T] --get-schedule <ID de la tâche>
[--file=<nom du fichier de configuration>] --file-format=<INI|XML>
kav4fs-control [-T] --get-schedule <ID de la tâche> <nom du paramètre>
```

Exemple de la commande

- *Enregistrer les paramètres de Kaspersky Anti-Virus dans le fichier appelé on_demand_schedule.xml. Enregistrer le fichier créé dans le répertoire en cours :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-schedule 9 -F on_demand_schedule.xml
```

- *Affiche la valeur du paramètre Strat Rules de la planification de la tâche de protection en temps réel :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-schedule 8 StartRules
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Le numéro d'identification de la tâche dans Kaspersky Anti-Virus.
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Nom du fichier de configuration dans lequel seront enregistrés les paramètres de l'horaire. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent sur le disque, le fichier de configuration ne sera pas créé. Vous pouvez enregistrer le fichier de configuration au format XML ou INI. Vous pouvez attribuer au fichier l'extension XML ou INI, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --file-format, vous pouvez attribuer au fichier n'importe quelle extension.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration spécifié par la clé -F, est déterminé par son extension. Spécifiez cette clé si l'extension du fichier de configuration que vous avez spécifiée est différente de son format. Valeurs possibles de la clé : XML, INI.

MODIFICATION DES PARAMETRES DE L'HORAIRE D'UNE TACHE

La commande -T --set-schedule détermine à l'aide des clés de la commande ou importe depuis le fichier de configuration spécifié les paramètres de l'horaire d'une tâche (cf. page 155).

Vous pouvez utiliser cette commande pour modifier les paramètres de Kaspersky Anti-Virus :

1. Enregistrez les paramètres de la planification dans le fichier de configuration à l'aide de l'instruction -T --get-schedule (cf. page 107).
2. Ouvrez le fichier de configuration créé, modifiez les paramètres voulus et enregistrez les modifications faites.
3. Importez les paramètres depuis le fichier de configuration dans Kaspersky Anti-Virus à l'aide de l'instruction-T --set-app-schedule. Kaspersky Anti-Virus utilisera de nouvelles valeurs des paramètres de l'horaire immédiatement.

Syntaxe de la commande

```
kav4fs-control -T --set-schedule <ID de la tâche> --file=<nom du fichier de
configuration> \
--file-format=<INI|XML>
kav4fs-control -T --set-schedule <ID de la tâche>
<nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre>
```

Exemple de la commande

- *Importer dans la tâche avec ID=9 les paramètres de l'horaire depuis le fichier de configuration avec le nom /home/test/on_demand_schedule.xml :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -T \
--set-schedule 9 -F /home/test/on_demand_schedule.xml
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Le numéro d'identification de la tâche dans Kaspersky Anti-Virus.
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Le nom du fichier de configuration depuis lequel les paramètres seront importés dans la tâche ; comprend le chemin d'accès complet au fichier.
--file-format=<INI|XML>	Clé facultative. Par défaut, le format du fichier de configuration spécifié par la clé -F, est déterminé par son extension. Spécifiez cette clé si l'extension du fichier de configuration que vous avez spécifiée est différente de son format. Valeurs possibles de la clé : XML, INI.

RECHERCHE D'ÉVÉNEMENTS SELON LA PLANIFICATION

La commande -T --show-schedule recherche les événements planifiés.

Syntaxe de la commande

```
kav4fs-control -T --show-schedule <type de règle> --from=<date de début> \
--to=<date> --action=<action> --task-id=<ID de la tâche>
```

Exemple de la commande

- *Recherche d'événements liés avec l'arrêt de la tâche, dont le temps exacte d'exécution est défini selon la planification et se trouve dans l'intervalle du 28/03/09 au 01/04/09 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--show-schedule Time --from=2009-03-28 \
--to=2009-04-01 --action=Stop
```

Exemple d'instruction :

```
Events number: 1

TaskId #9, Event: Stop, Date: 2009-03-30 12:00:00, Enabled, Stop Rule: [StopAt
2009/Mar/30:12:00 CanRunAfter 1800]
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<type de règle>	Type de règle de la planification. Valeurs possibles : • Time : des règles, contenant l'heure exacte (cf. page 159) de lancement, d'arrêt ou de suspension d'une tâche. • Startup : des règles, contenant la condition PS (au lancement de Kaspersky Anti-Virus). • Basereload : des règles, contenant la condition BR (après la mise à jour des bases).
--from=<date de début>	Date de début du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – recevoir les informations depuis 0 heure de la date spécifiée ; • date et heure au format AAAA-MM-DD HH:MM:SS – commencer le recherche depuis l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – commencer le recherche depuis l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --to=<date de fin>, la recherche sera exécutée pendant la semaine depuis le lancement de la commande.
--to=<date de fin>	Date de fin du rapport. Vous pouvez spécifier les valeurs suivantes : • date au format AAAA-MM-DD (ainsi que AAAA/MM/DD ou AAAA.MM.DD) – rechercher jusqu'à la date spécifiée inclus ; • date et heure au format AAAA-MM-DD HH:MM:SS – rechercher jusqu'à l'heure spécifiée de la date spécifiée ; • heure au format HH:MM:SS – rechercher jusqu'à l'heure spécifiée du jour en cours. Si vous ne spécifiez pas la clé --from=<date de debut>, la recherche sera exécutée depuis le moment du lancement de la commande.
--action=<action>	L'action exécutée par la règle. Valeurs possibles : • Start – règles de lancement d'une tâche. • Stop – règles d'arrêt d'une tâche. • Suspend – règles de suspension d'une tâche. • Resume – règles de reprise de l'exécution des tâches.
--task-id=<ID de la tâche>	Le numéro d'identification de la tâche à rechercher la planification.

COMMANDES D'ADMINISTRATION DES LICENCES

DANS CETTE SECTION

VERIFICATION DE L'AUTHENTICITE DU FICHIER DE LICENCE AVANT L'INSTALLATION

L'instruction kav4fs-control avec l'argument--validate-key vérifie dans les bases de données de Kaspersky Lab si le fichier de licence est authentique et s'il est prévu pour Kaspersky Anti-Virus. L'instruction affiche les informations relatives au fichier de licence sans l'installer.

Syntaxe de la commande

```
kav4fs-control [-L] --validate-key <chemin d'accès au fichier de licence>
```

Exemple de la commande

- *Vérifier l'authenticité du fichier de licence depuis le fichier de licence /home/test/00000001.key :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--validate-key /home/test/00000001.key
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<chemin d'accès au fichier de licence>	Chemin d'accès au fichier de licence ; si le fichier de licence se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

L'instruction fait afficher les informations suivantes relatives à la licence.

CHAMP	DESCRIPTION
Application name	Nom de Kaspersky Anti-Virus.
Key file creation date	Date de délivrance de la licence.
License expiration date	Date de fin de validité de la licence ; décompte réalisé par Kaspersky Anti-Virus. Correspond à la fin de l'activité de la licence, si elle n'est pas activée, mais ne peut être ultérieur à la date de fin de validité du fichier de licence.
License number	Numéro de la licence.
License type	Type de licence : évaluation ou commerciale.
Usage restriction	Éventuelles restrictions d'utilisation ; nombres d'objets soumis aux restrictions.
License period	La période de validité de la licence en jours est déterminée lors de la délivrance de la licence.

CONSULTATION DES INFORMATIONS RELATIVES A LA LICENCE AVANT L'INSTALLATION DU FICHIER DE LICENCE

L'instruction --show-license-info affiche les informations sur la licence sans le fichier.

Syntaxe de la commande

```
kav4fs-control [-L] --show-license-info <chemin d'accès au fichier de licence>
```

Exemple de la commande

- *Afficher les informations sur la licence depuis le fichier /home/test/00000001.key :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--show-license-info /home/test/00000001.key
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<chemin d'accès au fichier de licence>	Chemin d'accès au fichier de licence ; si le fichier de licence se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

L'instruction fait afficher les informations suivantes relatives à la licence.

CHAMP	DESCRIPTION
Application name	Nom de Kaspersky Anti-Virus.
Key file creation date	Date de délivrance de la licence.
Key file expiration date	" Délai de validité " du fichier de licence : date où le fichier de clé n'a plus de validité ; est installé lors de la délivrance de la licence.
License number	Numéro de la licence.
License type	Type de licence : évaluation ou commerciale.
Usage restriction	Éventuelles restrictions d'utilisation ; nombres d'objets soumis aux restrictions.
License period	La période de validité de la licence en jours est déterminée lors de la délivrance de la licence.

CONSULTATION DES INFORMATIONS RELATIVES AUX FICHIERS DE LICENCE INSTALLES

L'instruction kav4fs-control avec l'argument --get-installed-keys affiche les informations relatives aux fichiers de licence installé.

Syntaxe de la commande

```
kav4fs-control [-L] --get-installed-keys
```

L'instruction affiche les informations suivantes relatives aux fichiers de licence installés.

CHAMP	DESCRIPTION
Activation date	Date d'activation de la licence.
Expiration date	Date de fin de validité de la licence ; décompte réalisé par Kaspersky Anti-Virus. Correspond à la fin de l'activité de la licence depuis l'activation mais ne peut être ultérieure à la date de fin de validité du fichier de licence.
Aggregate expiration date	Date d'expiration de validité des licences active et supplémentaire.
Days remaining until aggregate expiration	Nombre de jours avant l'expiration de validité des licences active et supplémentaire.
License status	Etat de la licence ; peut avoir les valeurs suivantes : Valid – valide ; Expired – expirée ; Blacklisted – mise dans la liste noire ; Trial period is over – période d'essai expirée.
Functionality	Mode de fonctionnalité de Kaspersky Anti-Virus ; les valeurs possibles comprennent : Full functionality – fonctionnalité complète ; Functioning without updates – fonctionnalité sans la mise à jour ; est activée, une fois le délai de validité de la licence commerciale expirée ; No features – Kaspersky Anti-Virus arrête d'assurer toutes ses fonctions ; ce mode est activé, une fois le délai de validité de la licence d'essai expirée.
Informations détaillées sur la licence :	
Application name	Nom de Kaspersky Anti-Virus.
Key file creation date	Date de création du fichier de licence.
Key file expiration date	" Délai de validité " du fichier de licence : date où le fichier de clé n'a plus de validité ; est installé lors de la délivrance de la licence.
License number	Numéro de la licence.
License type	Type de licence : évaluation ou commerciale.
Usage restriction	Éventuelles restrictions d'utilisation ; nombres d'objets soumis aux restrictions.
License period	La période de validité de la licence en jours est déterminée lors de la délivrance de la licence.

CONSULTATION DE L'ETAT DES LICENCES INSTALLEES

L'instruction --query-status fait afficher l'état des licences installées.

Syntaxe de la commande

```
kav4fs-control [-L] --query-status
```

INSTALLATION D'UN FICHIER DE LICENCE ACTIF

L'instruction --install-active-key installe le fichier de licence actif. Pour plus d'informations sur les fichiers de licence, consultez la section " Présentation des fichiers de licence de Kaspersky Anti-Virus " (cf. page 65).

Syntaxe de la commande

```
kav4fs-control [-L] --install-active-key <chemin d'accès au fichier de licence>
```

Exemple de la commande

- *Installer la licence depuis le fichier /home/test/00000001.key en tant que licence active :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--install-active-key /home/test/00000001.key
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<chemin d'accès au fichier de licence>	Chemin d'accès au fichier de licence ; si le fichier de licence se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

INSTALLATION D'UN FICHIER DE LICENCE DE RESERVE

L'instruction --install-suppl-license installe le fichier de licence de réserve. Pour plus d'informations sur les fichiers de licence, consultez la section " Présentation des fichiers de licence de Kaspersky Anti-Virus " (cf. page 65).

Si le fichier de licence actif n'est pas installée, alors le fichier de licence de réserve deviendra le fichier principal.

Syntaxe de la commande

```
kav4fs-control [-L] --install-suppl-key <chemin d'accès au fichier de licence>
```

Exemple de la commande

- *Installer la licence supplémentaire depuis le fichier /home/test/00000002.key :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--install-suppl-key /home/test/00000002.key
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<chemin d'accès au fichier de licence>	Chemin d'accès au fichier de licence ; si le fichier de licence se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

SUPPRESSION D'UN FICHIER DE LICENCE ACTIF

L'instruction --revoke-active-key supprime le fichier de licence actif installé.

Syntaxe de la commande

```
kav4fs-control [-L] --revoke-active-key
```

SUPPRESSION D'UN FICHIER DE LICENCE DE RESERVE

L'instruction --revoke-suppl-key supprime le fichier de licence de réserve installé.

Syntaxe de la commande

```
kav4fs-control [-L] --revoke-suppl-key
```

COMMANDES D'ADMINISTRATION DE LA QUARANTAINE ET DU REPERTOIRE DE SAUVEGARDE DE RESERVE

DANS CETTE SECTION

OBTENTION DE LA STATISTIQUE BREVE DE LA QUARANTAINE / DU REPERTOIRE DE SAUVEGARDE DE RESERVE

La commande --get-stat fait afficher le nombre d'objets et le volume total des données dans le répertoire de sauvegarde au moment actuel.

Syntaxe de la commande

```
kav4fs-control [-Q] --get-stat [--query "<expression logique>"]
```

Exemple de la commande

- *Pour consulter la statistique brève de la quarantaine :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--get-stat --query "(OrigType!=s'Backup')"
```

- *Pour consulter la statistique brève du répertoire de sauvegarde de réserve :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--get-stat --query "(OrigType==s'Backup')"
```

OBTENTION DES INFORMATIONS SUR LES OBJETS DU REPERTOIRE DE SAUVEGARDE

La commande --query fait afficher les informations sur les objets dans le répertoire de sauvegarde au moment en cours. Vous pouvez utiliser des filtres.

Syntaxe de la commande

```
kav4fs-control [-Q] --query "<expression logique>" \
[--limit=<nombre d'entrées maximum>]
[--offset=<écart du début de la sélection>]
```

Exemple de la commande

- *Pour consulter les informations sur les objets du répertoire de sauvegarde :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query ""
  ```

- *Pour consulter les informations sur les objets mis en quarantaine, afficher 50 entrées à commencer par l'entrée 51 :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType!=s'Backup')" \
  --limit=50 --offset=50
  ```

- *Pour consulter les informations sur les objets du répertoire de sauvegarde de réserve :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType==s'Backup')"
  ```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre : expression logique (cf. page 122).
--limit=<nombre d'entrées maximum>	Met le filtre : nombre d'entrées maximum de la sélection à afficher.
--offset=<écart du début de la sélection>	Met le filtre : nombre d'entrées à s'écarter du début de la sélection.

OBTENTION DES INFORMATIONS SUR UN OBJET DU REPERTOIRE DE SAUVEGARDE

L'instruction --get-one affiche les informations sur un objet du référentiel avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kav4fs-control [-Q] --get-one <numéro d'identification de l'objet>
```

Exemple de la commande

- *Pour obtenir les informations sur l'objet avec ID=1 :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --get-one 1
  ```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<numéro d'identification de l'objet>	Pour avoir le numéro d'identification de l'objet, vous pouvez utiliser la commande -Q --query (cf. page 115).

RESTAURATION DES OBJETS DEPUIS LE REPERTOIRE DE SAUVEGARDE

La commande --restore restaure depuis le répertoire de sauvegarde l'objet avec le numéro d'identification spécifié.

La date et l'heure de création du fichier restauré depuis la quarantaine diffèrent de la date et de l'heure de création du fichier original.

Syntaxe de la commande

```
kav4fs-control [-Q] --restore <numéro d'identification de l'objet dans le référentiel> \
[--file=<nom du fichier et chemin d'accès au fichier>]
```

Exemple de la commande

- *Pour restaurer l'objet avec ID=1 dans l'emplacement d'origine :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --restore 1
  ```

- *Pour restaurer l'objet avec ID=1 dans le répertoire en cours, dans le fichier avec le nom restored.exe :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --restore 1 -F restored.exe
  ```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<numéro d'identification de l'objet>	Pour avoir le numéro d'identification de l'objet, vous pouvez utiliser la commande -Q --query (cf. page 115).
--file=<nom du fichier> -F <nom du fichier>	Nom de l'objet dans lequel Kaspersky Anti-Virus enregistre l'objet lors de la restauration, contient le chemin d'accès à l'objet. Si vous ne spécifiez pas le chemin d'accès au fichier, Kaspersky Anti-Virus enregistrera le fichier dans le répertoire en cours. Si vous omettez cette clé, Kaspersky Anti-Virus enregistrera l'objet dans l'emplacement d'origine, dans le fichier avec le nom d'origine.

MISE DE LA COPIE DE L'OBJET EN QUARANTAINE MANUELLEMENT

La commande --add-object met la copie de l'objet en quarantaine.

Syntaxe de la commande

```
kav4fs-control [-Q] --add-object <nom du fichier>
```

Exemple de la commande

- *Pour mettre en quarantaine la copie du fichier /home/sample.exe :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --add-object /home/sample.exe
  ```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<nom du fichier>	Le nom du fichier dont la copie vous voulez mettre en quarantaine, comprend le chemin au fichier.

SUPPRESSION D'UN OBJET DEPUIS LE REPERTOIRE DE SAUVEGARDE

La commande --remove supprime depuis le répertoire de sauvegarde l'objet avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kav4fs-control [-Q] --remove <numéro d'identification de l'objet>
```

Exemple de la commande

- *Pour supprimer l'objet avec ID=1 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --remove 1
```

ARGUMENT	SPÉCIFICATION ET VALEURS POSSIBLES
<numéro d'identification de l'objet>	Pour avoir le numéro d'identification de l'objet, vous pouvez utiliser la commande -Q --query (cf. page 115).

EXPORTATION DES OBJETS DEPUIS LE REPERTOIRE DE SAUVEGARDE DANS LE REPERTOIRE SPECIFIE

La commande --export exporte les objets qui se trouvent dans le répertoire de sauvegarde dans le répertoire spécifié. Il peut s'avérer nécessaire d'exporter les objets depuis le répertoire de sauvegarde pour libérer de l'espace sur le serveur. L'emplacement du répertoire de sauvegarde sur le serveur est spécifié dans le fichier de configuration de la quarantaine et du répertoire de sauvegarde (cf. page 163).

Vous pouvez utiliser des filtres pour n'exporter que des fichiers sélectionnés, par exemple, que des objets mis en quarantaine.

Syntaxe de la commande

```
kav4fs-control [-Q] --export <répertoire de destination> \
"<expression logique>"
[--limit=<nombre d'entrées maximum>]
[--offset=<écart du début de la sélection>]
```

Exemple de la commande

- *Pour exporter tous les objets depuis le répertoire de sauvegarde dans le répertoire /media/flash128/avpstorage :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--export /media/flash128/avpstorage
```

- *Pour exporter dans le répertoire /media/flash128/avpstorage des objets mis en quarantaine, 50 entrées à commencer par l'entrée 51 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--export /media/flash128/avpstorage --query "(OrigType!=s'Backup')" \
--limit=50 --offset=50
```

- *Pour exporter dans le répertoire /media/flash128/avpstorage tous les objets réservés :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--export /media/flash128/avpstorage \
--query "(OrigType==s'Backup')"
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
<répertoire de destination>	Le répertoire dans lequel Kaspersky Anti-Virus sauvegardera les objets depuis le répertoire de sauvegarde. Si le répertoire n'existe pas, il sera créé. Vous pouvez spécifier les répertoires sur des ressources distantes installées sur le serveur via les protocoles SMB/CIFS et NFS.
--query="<expression logique>"	Met le filtre : expression logique (cf. page 122).
--limit=<nombre d'entrées maximum>	Met le filtre : nombre d'entrées maximum de la sélection à afficher.
--offset=<écart du début de la sélection>	Met le filtre : nombre d'entrées à s'écarter du début de la sélection.

IMPORTATION DANS LE REPERTOIRE DE SAUVEGARDE DES OBJETS QUI ONT ETE EXPORTES AVANT

La commande --import importe dans le répertoire de sauvegarde les objets qui en ont été exportés avant.

L'emplacement du répertoire de sauvegarde sur le serveur est spécifié dans le fichier de configuration de la quarantaine et du répertoire de sauvegarde (cf. page 163).

Syntaxe de la commande

```
kav4fs-control [-Q] --import <répertoire avec des objets exportés>
```

Exemple de la commande

- *Pour importer dans le répertoire de sauvegarde les objets depuis le répertoire /media/flash128/avpstorage :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--import /media/flash128/avpstorage
```

PURGE DU REPERTOIRE DE SAUVEGARDE

La commande --mass-remove effectue la purge complète ou partielle du répertoire de sauvegarde.

Avant d'exécuter la commande, arrêtez la tâche de protection en temps réel et de la tâche d'analyse à la demande.

Syntaxe de la commande

```
kav4fs-control [-Q] --mass-remove \
[--query="<expression logique>"] \
[--limit=<nombre d'entrées maximum>]
[--offset=<écart du début de la sélection>]
```

Exemple de la commande

- *Pour supprimer tous les objets depuis le répertoire de sauvegarde :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --mass-remove
```

- *Pour ne supprimer que les objets mis en quarantaine : 50 entrées à commencer par l'entrée 51 :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
```

```
-Q --mass-remove --query "(OrigType!=s'Backup')" \
--limit=50 --offset=50
```

- *Pour supprimer les objets depuis le répertoire de sauvegarde de réserve :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \
--mass-remove --query "(OrigType==s'Backup')"
```

CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--query="<expression logique>"	Met le filtre : expression logique (cf. page 122).
--limit=<nombre d'entrées maximum>	Met le filtre : nombre d'entrées maximum de la sélection à afficher.
--offset=<écart du début de la sélection>	Met le filtre : nombre d'entrées à s'écarter du début de la sélection.

INSTRUCTION D'ADMINISTRATION DU JOURNAL DES EVENEMENTS

DANS CETTE SECTION

OBTENTION DU NOMBRE D'EVENEMENTS DE KASPERSKY ANTI-VIRUS PAR UN FILTRE

L'instruction --count affiche le nombre d'événements consignés dans le journal ou dans le fichier de rotations indiqués, en fonction du filtre. Cette instruction permet d'évaluer le volume d'informations qui sera affiché par l'instruction -E --query (cf. page 120).

Syntaxe de la commande

```
kav4fs-control [-E] --count "<expression logique>" [--db=<fichier de rotation>]
```

Exemple de la commande

- *Pour obtenir le nombre d'événements de Kaspersky Anti-Virus consignés dans le journal des événements :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --count ""
```

- *Pour obtenir le nombre d'événements consignés dans le fichier de rotation EventStorage-2009-12-01-23-57-23.db :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --count "" \
--db=EventStorage-2009-12-01-23-57-23.db
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre : expression logique (cf. page 122).
--db=<fichier de rotation>	Fichier de rotation dont vous pouvez consulter le contenu (possède l'extension db). Si vous n'indiquez pas cet argument, Kaspersky Anti-Virus affiche le nombre d'événements dans le journal pour l'instant.

OBTENTION DES INFORMATIONS SUR LES EVENEMENTS DE KASPERSKY ANTI-VIRUS

L'instruction --query permet d'obtenir des informations sur les événements de Kaspersky Anti-Virus depuis le journal de l'application ou depuis le fichier de rotation ; permet d'enregistrer les informations obtenues dans un fichier.

Syntaxe de la commande

```
kav4fs-control -E --query "<expression logique>" \
[--db=<nom du fichier de rotation>][--limit=<nom maximum d'enregistrements>] \
[--offset=<écart par rapport à la sélection de départ>][--file=<nom du fichier de journal>]\
[--file-format=<format du fichier du registre>]
```

Exemple de la commande

- *Pour consulter les informations sur 50 derniers événements de la quarantaine :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
-E --query "(TaskType == s'Quarantine')" --limit=50
```

ARGUMENT, CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre : expression logique (cf. page 122).
--db=<nom du fichier de rotation>	Fichier de rotation dont vous pouvez consulter les informations relatives aux événements (possède l'extension db). Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus affichera les informations tirées du journal des événements.
--limit=<nombre d'entrées maximum>	Met le filtre : nombre d'entrées maximum de la sélection à afficher.
--offset=<écart du début de la sélection>	Met le filtre : nombre d'entrées à s'écarter du début de la sélection.
--file=<nom du fichier du registre> -F <nom du fichier du registre>	Clé facultative. Nom du fichier dans lequel seront enregistrés les événements de Kaspersky Anti-Virus. Si vous spécifiez le nom du fichier du registre sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire spécifié, il sera réenregistré. Si le répertoire spécifié n'est pas présent sur le disque, le fichier du registre ne sera pas créé. Vous pouvez sauvegarder le fichier du registre au format XML ou INI. Vous pouvez attribuer au fichier du journal l'extension XML ou INI, ou, si vous spécifiez en supplément le format du fichier à l'aide de la clé --file-format, vous pouvez attribuer au fichier n'importe quelle extension.
--file-format=<format du fichier du registre>	Clé facultative. Par défaut, le format du fichier de journal indiqué par l'argument -F, est défini par son extension. Spécifiez cette clé si l'extension du fichier du registre que vous avez spécifiée, est différente de son format. Valeurs possibles de la clé : XML, INI.

CONSULTATION DE L'INTERVALLE DE TEMPS PENDANT LEQUEL LES EVENEMENTS DU JOURNAL ONT EU LIEU

Cette instruction permet de voir à quel intervalle de temps appartiennent les événements consignés dans le journal des événements ou dans le fichier de rotation indiqué.

Syntaxe de la commande

```
kav4fs-control [-E] --period
```

Exemples de la commande

- *Pour voir à quel intervalle de temps appartiennent les événements consignés dans le journal des événements :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control --period
  ```

- *Pour voir à quel intervalle de temps appartiennent les événements consignés dans le fichier de rotation EventStorage-2009-12-01-23-57-23.db :*

  ```
  /opt/kaspersky/kav4fs/bin/kav4fs-control \
  --period --db=EventStorage-2009-12-01-23-57-23.db
  ```

ARGUMENTS ET CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
--db=<fichier de rotation>	Fichier de rotation (extension .db) dont les informations peuvent être consultées. Si vous ne désignez pas cet argument, Kaspersky Anti-Virus affiche les informations relatives au journal des événements.

ROTATION DU JOURNAL DES EVENEMENTS

L'instruction --rotate exécute la rotation forcée des événements dans le journal conformément aux paramètres RotateMethod et RotateMoveFolder, définis dans le fichier de configuration du journal des événements (cf. page 164).

Si la valeur du paramètre RotateMethod est Erase, Anti-Virus supprime les informations relatives aux événements dans le journal.

Si la valeur du paramètre RotateMethod est Move, les informations relatives aux événements sont transférées du journal vers le répertoire RotateMoveFolder, et conservée dans le fichier de rotation.

Syntaxe de la commande

```
kav4fs-control [-E] --rotate
```

SUPPRESSION DES EVENEMENTS DU JOURNAL DES EVENEMENTS

L'instruction --remove supprime les enregistrements relatifs aux événements du journal des événements de Kaspersky Anti-Virus ou du fichier de rotation indiqué.

Vous pouvez supprimer tous les enregistrements ou uniquement certains d'entre eux en utilisant des filtres.

Syntaxe de la commande

```
kav4fs-control [-E] --query ["<expression logique>"] \
[--db=<fichier de rotation>]
```

Exemple de la commande

- *Pour supprimer uniquement les enregistrements relatifs aux événements liés à l'attribution de l'état "sain" dans le journal des événements (le paramètre ReportCleanObjects était activé) :*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
-E --remove "((EventType==s'ObjectProcessed') and \
(ObjectReason==s'ObjectClean'))"
```

ARGUMENTS ET CLÉS	SPÉCIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre : expression logique (cf. page 122).
--db=<fichier de rotation>	Fichier de rotation contenant les enregistrements que vous souhaitez modifié (possède l'extension .db). Si vous ne définissez pas cet argument, Kaspersky Anti-Virus supprime les enregistrements du journal des événements de Kaspersky Anti-Virus.

RESTRICTION DE LA SELECTION A L'AIDE DES FILTRES

DANS CETTE SECTION

EXPRESSIONS LOGIQUES

Vous pouvez utiliser les expressions logiques en tant que argument / clé --query des commandes suivantes pour appliquer des restrictions de la sélection des informations :

- obtention des informations sur le nombre d'événements de Kaspersky Anti-Virus : -E --count "<expression logique>" (cf. page 119) ;
- obtention des informations sur les événements de Kaspersky Anti-Virus : -E --query "<expression logique>" (cf. page 120) ;
- obtention des informations sur les objets mis en quarantaine / du dossier de sauvegarde : -Q --query "<expression logique>" (cf. page 115) ;
- obtention de statistiques succinctes sur les objets mis en quarantaine / du dossier de sauvegarde : -Q --get-stat --query "<expression logique>" (cf. page 114) ;
- purge partielle du référentiel : -Q --mass-remove --query "<expression logique>" (cf. page 118) ;
- exportation sélective des objets depuis la quarantaine / le dossier de sauvegarde : -Q --export --query "<expression logique>" (cf. page 117).

Vous pouvez spécifier plusieurs filtres en les regroupant par " ET " logique ou " OU " logique. Mettez chacun des filtres entre parenthèses ; mettez l'expression logique entre guillemets.

Vous pouvez trier les informations sur les événements (les objets) par chaque champ dans l'ordre ascendant ou descendant.

Syntaxe

```
"(<champ> <opérateur de comparaison> <type>'<valeur>'){<champ> <ordre>}"
```

```
"((<champ> <opérateur de comparaison> <type>'<valeur>') <opérateur logique> (<champ> <opérateur de comparaison> <type>'<valeur>')){<champ> <ordre>}"
```

Exemple

- *Obtenir des informations sur les objets en quarantaine possédant le niveau de danger Elevé :*

```
-Q --query "(DangerLevel == s'High')"
```

Le tableau suivant présente la spécification et les valeurs possibles des éléments des expressions logiques.

ELÉMENTS	SPÉCIFICATION ET VALEURS POSSIBLES
<opérateur de comparaison>	> plus < moins like correspond au modèle spécifié == égal != non égal >= plus ou égal <= moins ou égal
<opérateur logique>	and " ET " logique or " OU " logique
{<champ> <ordre>}	Ordre d'affichage des événements. N'est pas utilisé avec l'instruction -E --query. Vous pouvez trier les événements par chaque champ dans l'ordre ascendant ou descendant. Pour les instructions -Q --query, -Q --get-stat et -Q --mass-remove, vous pouvez désigner en tant que champ les paramètres des objets dans le référentiel (cf. page 123). L'ordre peut avoir les valeurs suivantes : a ordre ascendant d ordre descendant
<type>	i numérique s linéaire

PARAMETRES DE OBJETS EN QUARANTAINE / DANS LE DOSSIER DE SAUVEGARDE

Vous pouvez trier les objets de la quarantaine / du dossier de sauvegarde en fonction des champs décrits dans le tableau suivant.

Tableau 16. Paramètres de objets en quarantaine / dans le dossier de sauvegarde

CHAMP	TYPE	SPÉCIFICATION ET VALEURS POSSIBLES
Filename	s	Nom du fichier et chemin d'accès complet au fichier. Vous pouvez utiliser des masques à l'aide de l'opérateur de comparaison like.
OrigType Type	s	OrigType – état de l'objet ; est attribué à l'objet lors de sa mise dans le répertoire de sauvegarde. Type – état de l'objet mis en quarantaine après qu'il a été analysé avec utilisation des bases actualisées. Les valeurs possibles comprennent : Clean – non infecté ; Backup – l'objet est la copie réservée ; Infected – infecté ; UserAdded – ajouté par l'utilisateur ; Error – une erreur s'est produite durant l'analyse de l'objet ; PasswordProtected – protégé par un mot de passe ; Corrupted – endommagé ; Curable – peut être réparé.
OrigVerdict Verdict	s	OrigVerdict – type de menace détectée avant la mise de l'objet dans le répertoire de sauvegarde. Verdict – type de menace détectée dans l'objet mis en quarantaine après qu'il a été analysé avec utilisation des bases actualisées. Les valeurs possibles comprennent : Virware – virus classiques et vers de réseau ; Trojware – chevaux de Troie ; Malware – autres programmes malveillants ; Adware – programmes publicitaires ; Pornware – programmes à contenu pornographique ; Riskware – applications potentiellement dangereuses.
OrigDangerLevel DangerLevel	s	OrigDangerLevel – niveau de danger de menace détectée dans l'objet avant la mise de l'objet dans le répertoire de sauvegarde. DangerLevel – niveau de danger de menace détectée dans l'objet mis en quarantaine après qu'il a été analysé avec utilisation des bases actualisées. Le niveau de danger dans l'objet est fonction du type de la menace dans l'objet (cf. section " Programmes détectées par Kaspersky Anti-Virus " cf. page 11). Il peut avoir les valeurs suivantes : High – Elevé. L'objet peut contenir la menace telle que vers de réseau, virus classiques, chevaux de Troie. Medium – Moyen. L'objet peut contenir la menace telle que autres programmes malveillants, programmes publicitaires ou programmes à contenu pornographique. Low – Bas. L'objet peut contenir la menace telle que programmes potentiellement dangereux. Info – D'information. Objet placé en quarantaine par l'utilisateur.

CHAMP	TYPE	SPÉCIFICATION ET VALEURS POSSIBLES
OrigDetectCertainty DetectCertainty	s	OrigDetectCertainty – état de l'objet découvert lors de sa mise dans le répertoire de sauvegarde. DetectCertainty – état que Kaspersky Anti-Virus a attribué à l'objet mis en quarantaine suite à l'analyse avec utilisation des bases actualisées. Les valeurs possibles comprennent : Sure – l'objet est reconnu comme étant infecté ; Suspicion – l'objet est considéré comme suspect (identifié via l'analyseur heuristique) ; Warning – l'objet possède l'état :" Avertissement " (le code de l'objet correspond partiellement au code d'une menace connue ; la possibilité d'un faux positif existe).
OrigThreatName ThreatName	s	OrigThreatName – nom de la menace détectée dans l'objet, selon la classification de Kaspersky Lab (lors de la mise de l'objet dans le répertoire de sauvegarde). ThreatName – nom de la menace détectée dans l'objet mis en quarantaine après qu'il a été analysé avec utilisation des bases actualisées. Vous pouvez utiliser des masques à l'aide de l'opérateur de comparaison like.
Compound	i	Indique qu'il s'agit d'un fichier composé. Les valeurs possibles comprennent : yes – l'objet est conteneur ; no – l'objet n'est pas conteneur.
UID	i	Identificateur de l'utilisateur (UID) qui a créé l'objet.
GID	i	Identificateur du groupe (GID) dont l'utilisateur qui a créé l'objet fait partie.
Mode	i	Privilège d'accès à l'objet.
AddTime	s	Date et heure de mise de l'objet dans le répertoire de sauvegarde au format YYYY-MM-DD HH:MM:SS. Si vous spécifiez la date sans avoir spécifié l'heure, l'heure sera mise à 00:00:00. Si vous spécifiez l'heure sans avoir spécifié la date, la date courante sera attribuée. Si vous spécifiez la date et l'heure comme suit : (AddTime== s"), la date et l'heure courantes seront attribuées.
Size	i	Taille originale de l'objet en octets.

EVENEMENTS DE KASPERSKY ANTI-VIRUS ET LEURS PARAMETRES

Vous pouvez trier les événements de Kaspersky Anti-Virus en fonction de leurs paramètres. Le tableau suivant décrit les événements de Kaspersky Anti-Virus ; les paramètres des événements sont donnés dans le tableau ci-dessous.

Tableau 17. Evénements

№	NOM DE L'ÉVÉNEMENT	DESCRIPTION	PARAMÈTRES
1	ApplicationStarted	Kaspersky Anti-Virus est lancé ; cet événement survient une fois que toutes les tâches de service de Kaspersky Anti-Virus ont été lancées.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
2	ApplicationSettingsChanged	Les paramètres généraux de Kaspersky Anti-Virus ont été modifiés.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
3	LicenseInstalled	Licence est installée.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
4	LicenseNotInstalled	Erreur de l'installation de la licence.	Date, EventId, EventType, RuntimeTaskId, KeySerial, TaskName, TaskType
5	LicenseRevoked	Licence a été supprimée.	Date, EventId, EventType, RuntimeTaskId, KeySerial, TaskName, TaskType
6	LicenseNotRevoked	Erreur de la suppression de la licence.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
7	LicenseExpired	Licence a expiré.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
8	LicenseExpiresSoon	Délai de validité de la licence va bientôt expirer.	Date, EventId, EventType, RuntimeTaskId, DaysLeft, TaskName, TaskType
9	LicenseError	Erreur interne du système de licence.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
10	AVBasesAttached	Les bases de Kaspersky Anti-Virus ont bien été installées après la mise à jour.	Date, EventId, EventType, RuntimeTaskId, AVBasesDate, TaskId, TaskName, TaskType
11	AVBasesAreOutOfDate	Les bases de Kaspersky Anti-Virus sont dépassées.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
12	AVBasesAreTotallyOutOfDate	Les bases de Kaspersky Anti-Virus sont fortement dépassées.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
13	AVBasesIntegrityCheckOK	La vérification de l'intégrité des bases de Kaspersky Anti-Virus a réussi.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
14	AVBasesIntegrityCheckFailed	L'intégrité des bases de Kaspersky Anti-Virus a été violée.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
15	AVBAsesApplied	Les bases de Kaspersky Anti-Virus sont appliquées.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType

№	NOM DE L'ÉVÉNEMENT	DESCRIPTION	PARAMÈTRES
16	UpdateSourceSelected	Source de la mise à jour est sélectionnée.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
17	UpdateSourceNotSelected	Erreur de la connexion à la source de la mise à jour.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
18	NothingToUpdate	Rien à mettre à jour ; cet événement survient si la version des mises à jour des bases installées sur l'ordinateur est conforme à la version des mises à jour des bases qui se trouvent dans la source des mises à jour ou plus récente.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
19	UpdateError	Une erreur s'est produite lors de la mise à jour.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
20	ModuleDownloaded	Le module de programme est téléchargé.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
21	ModuleNotDownloaded	Erreur de téléchargement du module de programme.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
22	ModuleRetranslated	Le module de programme a été copié pour la répartition.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
23	ModuleNotRetranslated	Erreur de copie du module de programme.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
24	TaskStateChanged	L'état de la tâche a changé.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskState, TaskType
25	TaskSettingsChanged	Les paramètres de la tâche ont changé.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
26	PackedObjectDetected	L'objet archivé a été détecté.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, PackerName, FileName, FileOwner, FileOwnerId, ObjectName, ObjectSource, RuntimeTaskId, TaskId, TaskName, TaskType
27	ThreatDetected	Une menace a été détectée.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, DetectCertainty, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, TaskId, TaskName, TaskType, ThreatName, VerdictType
28	ObjectProcessed	L'objet est traité.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, ProcessResult, RuntimeTaskId, TaskId, TaskName, TaskType
29	ObjectNotProcessed	Objet non traité.	Date, EventId, EventType, AccessHost, AccessUser,

№	NOM DE L'ÉVÉNEMENT	DESCRIPTION	PARAMÈTRES
			AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, SkipReason, TaskId, TaskName, TaskType
30	ObjectProcessingError	Erreur de traitement de l'objet.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, ObjectProcessError, RuntimeTaskId, TaskId, TaskName, TaskType
31	ObjectDisinfected	Objet réparé.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, TaskId, TaskName, TaskType
32	ObjectNotDisinfected	Objet non réparé.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectNotDisinfectedReason, RuntimeTaskId, TaskId, TaskName, TaskType
33	ObjectDeleted	Objet supprimé.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskId, TaskId, TaskName, TaskType
34	ObjectBlocked	Dans la tâche de protection en temps réel, l'accès à l'objet est bloqué pour l'application qui y fait requête.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskId, TaskId, TaskName, TaskType
35	ObjectActionsCompleted	L'exécution de l'action sur l'objet infecté est terminée.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectReason, ObjectSource, ObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
36	ObjectSavedToQuarantine	Objet est placé en quarantaine.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
37	ObjectSavedToBackup	L'objet est placé dans le dossier de sauvegarde.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
38	ObjectRemovedFromQuarantine	L'objet est supprimé de la quarantaine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
39	ObjectRemovedFromBackup	L'objet est supprimé de la sauvegarde.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType,

№	NOM DE L'ÉVÉNEMENT	DESCRIPTION	PARAMÈTRES
			RuntimeTaskId, TaskId, TaskName, TaskType
40	ObjectRestoredFromQuarantine	L'objet est restauré depuis la quarantaine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
41	ObjectRestoredFromBackup	L'objet est restauré depuis la sauvegarde.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
42	QuarantineSizeLimitReached	La taille maximale de la quarantaine est atteinte.	Date, EventId, EventType, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
43	QuarantineSoftSizeLimitExceeded	La taille maximale de la quarantaine définie par le paramètre **QuarantineSoftSizeLimit** est atteinte.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
44	QuarantineObjectCorrupted	L'objet en quarantaine est corrompu.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
45	QuarantineObjectCurable	L'objet en quarantaine peut être réparé.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
46	QuarantineObjectFalseDetect	Suite à l'analyse des objets en quarantaine, Kaspersky Anti-Virus a considéré l'objet infecté ou suspect comme étant sain.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
47	QuarantineObjectPasswordProtected	L'objet en quarantaine est protégé par un mot de passe.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
48	QuarantineObjectProcessingError	Erreur lors du traitement de l'objet en quarantaine.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
49	QuarantineThreatDetected	L'objet en quarantaine est infecté.	Date, EventId, EventType, DetectCertainty, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
50	ObjectAddToQuarantineFailed	Erreur lors de la mise de l'objet en quarantaine.	Date, EventId, EventType, Description, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
51	ObjectAddToBackupFailed	Erreur lors de l'ajout d'un objet dans le référentiel.	Date, EventId, EventType, Description, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
52	RetranslationError	Erreur lors de la copie des mises à jour.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
53	AVBasesRollbackCompleted	Le retour à la version antérieure des bases de Kaspersky Anti-Virus a réussi.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
54	AVBasesRollbackError	Erreur lors du retour à la version antérieure des bases de Kaspersky Anti-virus.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType

№	NOM DE L'ÉVÉNEMENT	DESCRIPTION	PARAMÈTRES
55	OASTaskError	Erreur de la tâche de protection en temps réel.	Date, Error, EventId, EventType, Info, RuntimeTaskId, TaskId, TaskName, TaskType
56	ODSTaskError	Erreur de la tâche d'analyse à la demande.	Date, Error, EventId, EventType, Info, RuntimeTaskId, TaskId, TaskName, TaskType
57	EventsErased	Les événements sont supprimés.	Date, BeginDate, EndDate, EventId, EventType, Reason, RuntimeTaskId, TaskId, TaskName, TaskType
58	EventsMoved	Les événements sont déplacés.	Date, BeginDate, EndDate, EventId, EventType, Path, Reason, RuntimeTaskId, TaskId, TaskName, TaskType

Tableau 18. Paramètres des événements

PARAMÈTRE	TYPE	DESCRIPTION
AccessHost	s	Nom de l'ordinateur distant si l'accès au fichier est effectué via le protocole SMB/CIFS.
AccessUser	s	Nom de l'utilisateur qui a initié l'accès au fichier.
AccessUserId	i	Identifiant de l'utilisateur qui a initié l'accès au fichier.
AVBasesDate	s	Date de publication des dernières mises à jour installées des bases.
BeginDate	s	Date à partir de laquelle les événements ont été supprimés ou déplacés.
DangerLevel	s	DangerLevel – niveau de danger de la menace détectée dans l'objet, est attribué avant la mise de l'objet dans le répertoire de sauvegarde. OrigDangerLevel – niveau de danger de la menace détectée dans l'objet mis en quarantaine après son analyse avec utilisation des bases actualisées. Le niveau de danger dans l'objet est fonction du type de la menace dans l'objet (cf. section " Programmes détectées par Kaspersky Anti-Virus " cf. page 11). Il peut avoir les valeurs suivantes : High – Elevé. L'objet peut contenir la menace telle que vers de réseau, virus classiques, chevaux de Troie. Medium – Moyen. L'objet peut contenir la menace telle que autres programmes malveillants, programmes publicitaires ou programmes à contenu pornographique. Low – Bas. L'objet peut contenir la menace telle que programmes potentiellement dangereux. Info – D'information. Objet placé en quarantaine par l'utilisateur.
Date	s	Date et heure d'apparition de l'événement.
DetectCertainty (OrigDetectCertainty)	s	OrigDetectCertainty – état de l'objet découvert lors de sa mise dans le répertoire de sauvegarde. DetectCertainty – état que Kaspersky Anti-Virus a attribué à l'objet mis en quarantaine suite à l'analyse avec utilisation des bases actualisées. Etat de l'objet découvert : Sure – l'objet est reconnu comme étant infecté ; Suspicion – l'objet est considéré comme suspect (identifié via l'analyseur heuristique) ; Warning – l'objet possède l'état :" Avertissement " (le code de l'objet correspond partiellement au code d'une menace connue ; la possibilité d'un

PARAMÈTRE	TYPE	DESCRIPTION
		faux positif existe).
EndDate	s	Date jusqu'à laquelle les événements ont été supprimés ou déplacés.
Error	s	Type de l'erreur. Les valeurs possibles comprennent : IncorrectUser – l'utilisateur indiqué dans les paramètres de la tâche est inexistant, son nom est saisi dans le champ Info ; IncorrectGroup – le groupe indiqué dans les paramètres de la tâche est inexistant, le nom du groupe est saisi dans le champ Info ; IncorrectPath – le chemin d'analyse dans les paramètres de la tâche est incorrect, le chemin est saisi dans le champ Info ; InterceptorNotFound – la tâche ne peut pas télécharger le module de l'intercepteur au lancement.
FileName	s	Nom complet du fichier.
FileOwner	s	Nom de l'utilisateur propriétaire du fichier.
FileOwnerId	i	Identifiant de l'utilisateur propriétaire du fichier.
Host	s	Nom de réseau de l'ordinateur distant qui a fait requête à l'objet au moment de l'interception par Kaspersky Anti-Virus (installé via le protocole SMB/CIFS).
Info	s	Informations supplémentaires sur l'erreur.
ModuleName	s	Nom du module de Kaspersky Anti-Virus avec lequel est lié l'événement.
ObjectName	s	Nom de l'objet avec lequel est lié l'événement.
ObjectNotDisinfectedReason	s	Raisons de l'échec de la réparation de l'objet : Unknown – raison inconnue ; InternalError – erreur de la tâche ; ObjectNotCurable – l'objet de ce type ne peut pas être réparé ; ObjectNotFound – objet non trouvé ; ObjectReadOnly – Kaspersky Anti-Virus a le droit d'accès en lecture de l'objet uniquement.
ObjectProcessError	s	Type de l'erreur lors du traitement de l'objet : Unknown InternalError ObjectNotCurable ObjectNoRights ObjectIOError OutOfSpace ObjectNotFound ObjectReadOnly SystemError
ObjectReason	s	Résultat des actions exécutées sur l'objet. Les valeurs possibles comprennent : Cured – l'objet est réparé ; Removed – l'objet est supprimé ;

PARAMÈTRE	TYPE	DESCRIPTION
		Quarantined – l'objet est placé en quarantaine ; Skipped – l'objet est ignoré ; AllActionsFailed – toutes les actions sur l'objet se sont términé par une erreur.
ObjectSource	s	Source du fichier infecté : LocalFile – système de fichiers local ; RemoteNfsFile – ressource distante accessible via le protocole NFS ; RemoteSambaFile – ressource distante accessible via le protocole SMB/CIFS ;
ObjectType	s	Type de l'objet (l'objet, est-il conteneur) : Object – l'objet n'est pas conteneur ; Archive – l'objet est conteneur.
Path	s	Chemin d'accès au fichier où les événements ont été déplacés.
QuarantineId	i	Identificateur de l'objet dans le répertoire de sauvegarde ; est attribué par Kaspersky Anti-Virus.
Reason	s	Cause de déplacement ou de suppression des événements : Date – déplacement ou de suppression en fonction de la date ; Manual – déplacement ou de suppression suite à une commande de l'utilisateur ; Size – déplacement ou de suppression en fonction de la taille de la base.
RuntimeTaskId	i	Identificateur unique de la séance de lancement de la tâche. Actualisé à chaque lancement de la tâche.
TaskName	s	Nom de la tâche durant laquelle l'événement s'est produit.
TaskState	s	Etat de la tâche : Stopped – arrêtée ; Stopping – en cours d'arrêt ; Started – en cours d'exécution ; Starting – en cours de lancement ; Suspended – suspendue ; Suspending – en cours de suspension ; Resumed – reprise ; Resuming – en cours de reprise ; Failed – terminée par une erreur.
TaskType	s	Type de tâche de Kaspersky Anti-Virus. Il peut avoir les valeurs suivantes : • tâches que l'utilisateur peut administrer : Update : tâche prédéfinie de mise à jour (ID=6) ; OAS – tâche de protection en temps réel (ID=8) ; ODS : tâche prédéfinie d'analyse à la demande (ID=9) ; QS – tâche de l'analyse des objets mis en quarantaine (ID=10) ;

PARAMÈTRE	TYPE	DESCRIPTION
		• tâches qui assurent des fonctions de service : EventManager : assure l'échange des messages à l'intérieur de l'application (ID=1) ; AVS : assure le service d'analyse antivirus (ID=2) ; Quarantine : administre la quarantaine et le dossier de sauvegarde (ID=3) ; Statistics : récolte les statistiques (ID=4); License : réalise le " serveur de licence " (ID=5) ; Notifier : administre l'envoi de notifications et l'exécution des actions en fonction des événements (ID=7) ; EventStorage : assure le service du journal des événements (ID=11) ; Snmp plugin : assure le transfert des informations relatives au programme via le protocole SNMP (ID=12).
ThreatName	s	Nom de la menace détectée dans l'objet avec lequel est lié l'événement.
Type (OrigType)	s	OrigType – état de l'objet ; est attribué à l'objet lors de sa mise dans le répertoire de sauvegarde. Type – état de l'objet mis en quarantaine après qu'il a été analysé avec utilisation des bases actualisées. Les valeurs possibles comprennent : Clean – non infecté ; Backup – l'objet est la copie réservée ; Infected – infecté ; UserAdded – ajouté par l'utilisateur ; Error – une erreur s'est produite durant l'analyse de l'objet ; PasswordProtected – protégé par un mot de passe ; Corrupted – endommagé ; Curable – peut être réparé.

PARAMETRES DES FICHIERS DE CONFIGURATION DE KASPERSKY ANTI-VIRUS

Vous pouvez créer des fichiers de configuration de Kaspersky Anti-Virus au format INI, ainsi qu'au format XML.

Cette section décrit la structure et les paramètres des fichiers de configuration de Kaspersky Anti-Virus au format INI.

DANS CETTE SECTION

REGLES DE MISE AU POINT DES FICHIERS DE CONFIGURATION INI DE KASPERSKY ANTI-VIRUS

Lors de la mise au point du fichier de configuration, veuillez respecter les règles suivantes :

- Si le paramètre fait partie d'une section, ne le placez que dans cette section. Respectez l'ordre et la structure des sections. Au sein d'une section, vous pouvez placer les paramètres dans tout ordre.
- Si vous omettez un des paramètres, Kaspersky Anti-Virus utilisera la valeur de ce paramètre par défaut, s'il y en a.
- Mettez les noms des sections entre crochets [ ].
- Saisissez les valeurs au format **nom du paramètre=valeur** (les espaces entre le nom du paramètre et sa valeur ne sont pas traités).

  Par exemple :

```
[ScanScope]

AreaDesc="Analyse de sdc"

AreaMask=re:\.exe
```

- Certains paramètres acceptent une seule valeur et d'autres, plusieurs. S'il s'avère nécessaire de spécifier plusieurs valeurs, répétez le paramètre le nombre de fois égal au nombre de valeurs que vous voulez spécifier, par exemple :

```
AreaMask=re:home/.*/Documents/

AreaMask=re:.*\.doc
```

- Lors de la saisie des noms des paramètres, il n'est pas nécessaire de respecter le registre.
- Respectez le registre lors de la saisie des valeurs des paramètres des types suivants :
  - noms (masques, expression régulières) des objets analysés et des objets d'exclusion ;
  - signatures (masques, expressions régulières) des menaces ;
  - nom des utilisateurs ;
  - nom des groupes d'utilisateurs.

  Lors de la saisie des autres valeurs des paramètres, il n'est pas nécessaire de respecter le registre.
- Vous pouvez spécifier les valeurs des paramètres de type booléen comme suit : **yes** – **no**, **true** – **false** ou **1** – **0**.
- Les chaînes de valeur contenant un " espace " doivent être saisies entre guillemets (par exemple, les noms de fichiers ou les répertoires et les chemins d'accès à ceux ci :

```
AreaDesc="Analyse des bases de messagerie"
```

  Les autres valeurs peuvent être mises entre guillemets et sans guillemets, par exemple :

```
AreaMask="re:home/.*/Documents/"

AreaMask=re:home/.*/Documents/
```

- Un guillemet solitaire en début ou en fin de ligne est une erreur.
- Si la valeur est entre guillemets, tout caractère au sein de cette valeur, y compris les guillemets, les " espaces " et les " tabulations " font partie de cette valeur. Par exemple :

```
AreaDesc="Scanning "useless" documents"
```

- Les espaces et les tabulations sont ignorés dans les cas suivants :
  - avant le guillemet d'ouverture et après le guillemet de fermeture de la valeur ;
  - au début et à la fin de la chaîne de valeur non comprise entre guillemets.
- Vous pouvez utiliser des commentaires textuels. Un commentaire est une ligne qui commence par le caractère **;** ou #. Lors de l'importation des paramètres de la tâche (cf. la rubrique " Modification des paramètres de la tâche " cf. page 104) depuis le fichier de configuration, les commentaires sont ignorés. Lors de la consultation des paramètres de la tâche (cf. rubrique " Récupération des paramètres de la tâche " cf. page 103), les commentaires ne sont pas affichés.

PARAMETRES DE LA TACHE DE PROTECTION EN TEMPS REEL ET DES TACHES D'ANALYSE A LA DEMANDE

Cette section décrit les paramètres que vous pouvez utiliser pour l'importation dans les tâches de protection en temps réel et les tâches d'analyse à la demande.

Vous pouvez utiliser le fichier de configuration avec les paramètres spécifiés pour modifier les paramètres de la tâche de protection en temps réel en cours (d'analyse à la demande) ou pour créer une nouvelle tâche.

Pour modifier les paramètres de la tâche en cours, vous devez exporter les paramètres de la tâche dans un fichier (cf. page 103), ensuite ouvrir ce fichier dans n'importe quel programme de traitement de texte, modifier les paramètres selon vos besoins et ensuite importer les paramètres spécifiés dans le fichier dans la tâche (cf. page 104).

Structure du fichier de configuration ini de la tâche de protection en temps réel (d'analyse à la demande)

Le fichier de configuration de la tâche de protection en temps réel (d'analyse à la demande) comprend un ensemble des sections. Les sections du fichier décrivent un ou plusieurs secteurs d'analyse et les paramètres de sécurité qui sont utilisés par Kaspersky Anti-Virus lors de l'analyse de chacun des secteurs spécifiés.

La section [ScanScope] comprend le nom du secteur d'analyse ; applique des limites au secteur d'analyse.

La section [ScanScope:AreaPath] décrit le chemin d'accès au répertoire à analyser. Son format est différent de celui des autres sections du fichier de configuration INI. Vous devez spécifier au moins un seul secteur d'analyse pour lancer la tâche.

La section [ScanScope:ScanSettings] et la section fille [ScanScope:ScanSettings:AdvancedActions] décrivent les paramètres de sécurité que Kaspersky Anti-Virus utilisera pour le secteur d'analyse spécifié dans la section [ScanScope:AreaPath]. Si vous ne spécifiez pas les paramètres de ces sections, Kaspersky Anti-Virus analysera le secteur déterminé selon les paramètres de sécurité correspondant au niveau de sécurité prédéterminé **Recommandé**.

Si vous voulez spécifier plusieurs secteurs d'analyse, énumérez les paramètres des sections [ScanScope], [ScanScope:AreaPath], [ScanScope:AccessUser] (uniquement dans les tâches de protection en temps réel) et [ScanScope:ScanSettings] pour un seul secteur, et ensuite répétez-les pour chaque secteur suivant :

[ScanScope]

zone 1

...

[ScanScope:AreaPath]

chemin d'accès au répertoire analysé spécifié dans le secteur 1

...

[ScanScope:AccessUser]

(uniquement dans les tâches de protection en temps réel) liste d'utilisateurs pour le secteur 1

...

[ScanScope:ScanSettings]

paramètres de sécurité de la zone 1

...

[ScanScope]

zone 2

...

[ScanScope:AreaPath]

chemin d'accès au répertoire analysé spécifié dans le secteur 2

...

[ScanScope:AccessUser]

(uniquement dans les tâches de protection en temps réel) liste d'utilisateurs pour le secteur 2

...

[ScanScope:ScanSettings]

paramètres de sécurité de la zone 2

...

Kaspersky Anti-Virus analyse les secteurs dans l'ordre spécifié dans le fichier de configuration.

N'oubliez pas que si un fichier fait partie de plusieurs zones d'analyse spécifiées, Kaspersky Anti-Virus ne l'analysera qu'une seule fois selon les paramètres de sécurité spécifiés dans le premier secteur d'analyse énuméré dont ce fichier fait partie.

Il peut s'avérer nécessaire de spécifier les paramètres de sécurité du répertoire incorporé différents des paramètres de sécurité du répertoire parental. Par exemple, il est nécessaire d'analyser dans le répertoire /home/ les objets suivant l'expression régulière re:.*\.doc ; de supprimer des objets infectés, et d'analyser les objets du répertoire incorporé /home/dir1/ suivant l'expression régulière re:.*\.doc ; de réparer des objets infectés.

Placez les secteurs d'analyse dans le fichier de configuration comme suit :

[ScanScope]

Sous-répertoire

AreaMask="re:.*\.doc"

[ScanScope:AreaPath]

/home/dir1/

[ScanScope:ScanSettings]

InfectedFirstAction=Cure

...

[ScanScope]

Répertoire parent

AreaMask="re:.*\.doc"

[ScanScope:AreaPath]

/home/

[ScanScope:ScanSettings]

InfectedFirstAction=Remove

...

Kaspersky Anti-Virus essayera de réparer les fichiers infectés re:.*\.doc dans le répertoire /home/dir1/, et supprimera les autres fichiers infectés re:.*\.doc dans le répertoire /home/.

Spécification des paramètres du fichier de configuration, leurs valeurs possibles et valeurs par défaut sont données dans le tableau ci-dessous.

En spécifiant les paramètres dans le fichier, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Tableau 19. Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
ScanPriority	Priorité de la tâche. Ce paramètre est utilisé uniquement dans les tâches d'analyse à la demande, il n'est pas utilisé dans les tâches de protection en temps réel. Vous pouvez désigner une des priorités prédéfinies de la tâche selon les priorités des processus Linux. Les valeurs possibles comprennent : **System** (système). La priorité du processus dans lequel la tâche est exécutée est définie par le système d'exploitation. **High** (élevée). La priorité du processus dans lequel la tâche est exécutée est augmentée. **Medium** (moyenne). La priorité du processus dans lequel la tâche est exécutée n'est pas modifiée. **Low** (faible). La priorité du processus dans lequel la tâche est exécutée est réduite. La réduction de la priorité du processus augmente la durée d'exécution de la tâche, mais a également un effet positif sur la vitesse d'exécution des processus des autres applications actives. L'élévation de la priorité du processus accélère l'exécution de la tâche mais, en même temps, elle peut ralentir la vitesse d'exécution des processus des autres applications actives. Valeur par défaut **System**.
ProtectionType	Mode d'interception. Utilisation de l'intercepteur SAMBA pour analyser les objets lorsqu'on y fait requête via le protocole SMB/CIFS. Utilisation de l'intercepteur du niveau du noyau pour l'analyse des objets lorsqu'on y fait requête via d'autres modes (via les protocoles NFS, FTP et autre). Ce paramètre n'est utilisé que dans la tâche de protection en temps réel, il n'est pas utilisé dans les tâches d'analyse à la demande. Kaspersky Anti-Virus comprend deux composants qui interceptent les requêtes aux fichiers et leur analyse : intercepteur SAMBA (il sert à analyser les objets sur les ordinateurs distants lorsqu'on y fait requête via le protocole SMB/CIFS) et intercepteur du niveau du noyau. Il analyse les objets lorsqu'on y fait requête via d'autres modes. L'intercepteur SAMBA permet de recevoir en tant que informations supplémentaires sur l'objet, IP de l'ordinateur distant depuis lequel l'application a fait requête à l'objet au moment de son interception par Kaspersky Anti-Virus. Si vous utilisez l'ordinateur protégé en tant que serveur SAMBA, vous pouvez spécifier la valeur SambaOnly. Dans ce cas, Kaspersky Anti-Virus n'analysera pas les objets auxquels la requête est faite non pas via le protocole SMB/CIFS. Les valeurs possibles comprennent : **Full.** Kaspersky Anti-Virus analyse les objets sur le serveur lorsqu'on y fait requête via le protocole SMB/CIFS avec utilisation de l'intercepteur SAMBA. Kaspersky Anti-Virus intercepte toutes les autres opérations sur les fichiers disponibles sur le serveur protégé (y compris, sur les fichiers des ordinateurs distants), en utilisant l'intercepteur du niveau du noyau. **SambaOnly.** Kaspersky Anti-Virus analyse les objets uniquement lorsqu'on y fait requête via le protocole SMB/CIFS, en utilisant l'intercepteur SAMBA. Assurez-vous d'avoir installé le module SAMBA VFS durant la configuration initiale de Kaspersky Anti-Virus (cf. la rubrique " Étape 7. Intégration au serveur Samba " du Guide d'installation de Kaspersky Anti-Virus 8.0 for Linux File Server). **KernelOnly.** Kaspersky Anti-Virus analyse les objets sur le serveur uniquement à

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	l'aide de l'intercepteur de fichiers. Assurez-vous d'avoir installé l'intercepteur de noyau durant la configuration initiale de Kaspersky Anti-Virus (cf. la rubrique " Étape 6. Compilation du module du noyau " du Guide d'installation de Kaspersky Anti-Virus 8.0 for Linux File Server). Valeur par défaut : se fixe pendant l'installation de Kaspersky Anti-Virus.
`[ScanScope]` Secteur d'analyse.	
`AreaDesc`	Description de la zone d'analyse ; contient les informations supplémentaires sur la zone d'analyse. La chaîne de ce paramètre peut contenir un maximum de **4096** caractères. Exemple : `AreaDesc="Analyse des bases de messagerie"` Valeur par défaut : All local objects.

`AreaMask`	A l'aide de ce paramètre, vous pouvez limiter la zone d'analyse spécifiée dans la section [ScanScope:AreaPath]. La chaîne de ce paramètre peut contenir un maximum de **4096** caractères.
	
	Dans le secteur d'analyse, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires que vous spécifierez à l'aide des masques Shell ou des expressions régulières étendues POSIX. Dans les expressions régulières, utilisez le préfix **re:**.
	
	Si vous ne spécifiez pas ce paramètre, Kaspersky Anti-Virus analysera tous les objets du secteur d'analyse.
	
	Vous pouvez spécifier plusieurs valeurs de ce paramètre.
	
	Exemple :
	
	`AreaMask=re:.*/Documents/`
	
	`AreaMask=re:.*\.doc`
	
	`AreaMask=re:\.exe`
	
	Valeur par défaut : *.

`UseAccessUser`	Ce paramètre fait activer / désactiver l'application des paramètres de la section [ScanScope:AccessUser] (analyse lors de l'accès avec les droits des utilisateurs déterminés). Ce paramètre n'est utilisé que dans les tâches de protection en temps réel. Il n'est pas utilisé dans les tâches d'analyse à la demande. Les valeurs possibles comprennent : **yes** – n'analyser les objets que dans le cas où les applications avec les droits des utilisateurs spécifiés par les paramètres dans la section [ScanScope:AccessUser] font requête à ceux-là ; **no** – analyser les objets lorsqu'on y fait requête avec n'importe quels droits. Valeur par défaut : non spécifié.
`[ScanScope:AreaPath]` Zone d'analyse, chemin d'accès au répertoire à analyser. Vous devez spécifier au moins un seul secteur d'analyse pour lancer la tâche de protection en temps réel.	
`Path`	La valeur du paramètre est composée de trois éléments : **<type du système de fichiers>:<protocole d'accès>:<chemin d'accès au répertoire à analyser>**, où :

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	<type du système de fichiers>. Les valeurs possibles comprennent : **Mounted**. Répertoires distants montés sur le serveur. A l'aide de l'élément <protocole d'accès>, spécifiez le protocole qui assurera l'accès à distance aux répertoires. **Shared**. Ressources du système de fichiers du serveur accessibles via le protocole SMB/CIFS ou le protocole NFS. **AllRemotelyMounted**. Tous les répertoires distants montés sur le serveur par l'intermédiaire des protocoles SMB/CIFS et NFS. **AllShared**. Toutes les ressources du système de fichiers du serveur accessibles via les protocoles SMB/CIFS et NFS. **<protocole d'accès>**. Protocole qui assure l'accès à distance aux ressources spécifiées. Ce paramètre est utilisé uniquement dans le cas où le <type du système de fichiers> a la valeur Mounted ou Shared. Les valeurs possibles comprennent : **SMB**. Protocole d'accès à distance aux ressources SMB/CIFS. **NFS**. Protocole d'accès à distance aux ressources NFS. **<chemin d'accès au répertoire à analyser>**. Chemin d'accès complet au répertoire à analyser. Lisez les particularités de l'analyse des liens symboliques et matériels dans la rubrique Particularités de l'analyse des liens symboliques et matériels (cf. page 10). Exemples: `Path=/` – *analyser tous les répertoires locaux du serveur ; analyser les répertoires montés via les protocoles SMB/CIFS et NFS.* `Path=/home/ivanov` – *analyser le répertoire /home/ivanov* `Path=Mounted:SMB` – *analyser tous les répertoires distants montés à l'aide de SMB/CIFS.* `Path=Mounted:NFS` – *analyser tous les répertoires distants montés à l'aide de NFS.* `Path=Mounted:SMB:/remote-resources/ivanov-windows` – *analyser le répertoire /remote-resources/ivanov-windows, monté à l'aide de SMB/CIFS.* `Path=Mounted:NFS:/remote-resources/ivanov-linux` – *analyser le répertoire /remote-resources/ivanov-windows, monté à l'aide de NFS.* `Path=Shared:SMB` – *analyser tous les répertoires du système de fichiers du serveur accessibles via SMB/CIFS.* `Path=Shared:SMB:my_samba_share` – *analyser la ressource avec le nom my_samba_share, accessible via SMB/CIFS.* `Path=Shared:NFS` – *analyser tous les répertoires du serveur accessibles via NFS.* `Path=Shared:NFS:/nfs_shares/my_share` – *analyser la ressource avec le nom /nfs_shares/my_share, accessible via NFS.* Valeur par défaut : /.
`[ScanScope:AccessUser]` Analyse lors de l'accès avec les droits des utilisateurs déterminés. Kaspersky Anti-Virus n'analyse les objets qu'au cas où les applications avec les droits des utilisateurs et des groupes spécifiés par les paramètres de cette section font requête à ceux-là. Si les paramètres de cette section ne sont pas spécifiés, Kaspersky Anti-Virus analyse les objets lorsqu'on y fait requête avec n'importe quels droits.	

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
Les paramètres de cette section ne sont utilisés que dans les tâches de protection en temps réel. Ils ne sont pas utilisés dans les tâches d'analyse à la demande. Si les paramètres de cette section indiquent un utilisateur ou un groupe qui n'existe pas, la tâche de protection en temps réel analysera les objets lors des tentatives d'accès sous les privilèges de n'importe quel utilisateur ou groupe.	

`UserName`	Kaspersky Anti-Virus n'analyse les objets qu'au cas où les applications avec les droits des utilisateurs déterminés y font requête. Vous pouvez spécifier plusieurs valeurs de ce paramètre, par exemple :
	
	`UserName=usr1`
	
	`UserName=usr2`
	
	Valeur par défaut : non spécifié.

`UserGroup`	Nom du groupe. Kaspersky Anti-Virus n'analyse les objets qu'au cas où les applications avec les droits des groupes déterminés y font requête. Vous pouvez spécifier plusieurs valeurs de ce paramètre, par exemple :
	
	`UserGroup=group1`
	
	`UserGroup=group2`
	
	Valeur par défaut : non spécifié.

`[ScanScope:ScanSettings]` Paramètres de sécurité que Kaspersky Anti-Virus utilise lors de l'analyse du secteur spécifié par le paramètre [ScanScope:AreaPath].	
`ScanByAccessType`	Kaspersky Anti-Virus analyse les objets au moment du prochain accès à ceux-là (n'est utilisé que dans la tâche de protection en temps réel ; n'est pas utilisé dans les tâches d'analyse à la demande) : **SmartCheck** (mode intellectuel). Kaspersky Anti-Virus analyse l'objet lors de la tentative d'ouverture et encore une fois lors sa fermeture si il a été modifié. Si le processus lors de son fonctionnement adresse plusieurs requêtes à l'objet durant une certaine période de temps et le modifie, Kaspersky Anti-Virus n'analysera l'objet qu'à la dernière tentative de fermeture de ce fichier par ce processus. **Open** (lors d'une tentative d'ouverture). Kaspersky Anti-Virus analyse l'objet lors de son ouverture en lecture, ainsi qu'en exécution ou modification. **OpenAndModify** (lors d'une tentative d'ouverture et de modification). Kaspersky Anti-Virus analyse l'objet lors de la tentative d'ouverture et encore une fois lors sa fermeture si il a été modifié. Valeur par défaut : **SmartCheck**.
`ScanArchived`	Kaspersky Anti-Virus analyse les archives (y compris les archives autoextractibles SFX). Faites attention à ce que Kaspersky Anti-Virus détecte des menaces dans les archives sans les réparer. **yes** – analyser les archives ; **no** – ne pas analyser les archives. Valeurs par défaut : tâche de protection en temps réel – **no** ; tâche d'analyse à la demande – **yes**.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
ScanSfxArchived	Kaspersky Anti-Virus analyse les archives auto-extractibles (archives qui comprennent le module de désarchivage exécutable) (self-extracting archive). **yes** – analyser les archives SFX ; **no** – ne pas analyser les archives SFX. Valeurs par défaut : tâche de protection en temps réel – **no** ; tâche d'analyse à la demande – **yes**.
ScanMailBases	Kaspersky Anti-Virus analyse les bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat et autres. **yes** – analyser les fichiers des bases de messagerie ; **no** – ne pas analyser les fichiers des bases de messagerie. Valeur par défaut : **no**.
ScanPlainMail	Kaspersky Anti-Virus analyse les fichiers des messages informatiques au format texte (plain text). **yes** – analyser les fichiers de messagerie au format texte ; **no** – ne pas analyser les fichiers de messagerie au format texte. Valeur par défaut : **no**.
ScanPacked	Kaspersky Anti-Virus analyse les fichiers exécutables archivés par les programmes d'archivage de code binaire tels que UPX ou ASPack. Les objets composés de ce type ont plus de probabilité de contenir une menace. **yes** – analyser les fichiers archivés ; **no** – ne pas analyser les fichiers archivés. Valeur par défaut : **yes**.
InfectedFirstAction	Première action à exécuter sur des objets infectés. Dans les tâches de protection en temps réel, avant d'exécuter l'action que vous avez choisie sur l'objet infecté, Kaspersky Anti-Virus bloque l'accès à l'objet pour l'application qui y a fait requête. Les valeurs possibles comprennent : **Cure** (réparer). Kaspersky Anti-Virus essaie de réparer l'objet ayant sauvegardé la copie de l'objet dans le répertoire de sauvegarde. Si la réparation ne s'avère pas possible, par exemple, le type de l'objet ou le type de la menace dans l'objet ne suppose pas la réparation, Kaspersky Anti-Virus garde l'objet intact. **Remove** (supprimer). Kaspersky Anti-Virus supprime l'objet infecté après avoir créé une copie de sauvegarde. **Recommended** (exécuter l'action recommandée). Kaspersky Anti-Virus choisit automatiquement et effectue l'action sur l'objet à la base des données sur le danger de la menace détectée dans l'objet et sur la possibilité de sa réparation, Kaspersky Anti-Virus supprime immédiatement les chevaux de Troie puisqu'ils ne s'introduisent pas dans les autres objets et ne les infectent pas et, donc, ne supposent pas la réparation. **Quarantine** (mettre en quarantaine). Kaspersky Anti-Virus transfère l'objet dans le répertoire de sauvegarde de la quarantaine dans lequel l'objet est conservé sous forme codée.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	Skip (sauter). L'objet reste intact. Kaspersky Anti-Virus n'essaie pas le supprimer ou réparer ; il enregistre les informations sur l'objet dans le registre. Valeur par défaut : **Recommended**.
`InfectedSecondAction`	Deuxième action à exécuter sur des objets infectés. Les valeurs sont identiques à celles du paramètre InfectedFirstAction. Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action. Si vous sélectionnez Skip (sauter) ou Remove (supprimer) en tant que première action, il n'est pas nécessaire de spécifier la deuxième action. Pour les autres valeurs, il est recommandé de spécifier les deux actions. Si vous ne spécifiez pas la deuxième action, Kaspersky Anti-Virus, en tant que deuxième action, appliquera l'action Skip (sauter). Valeur par défaut : **Skip**.
`SuspiciousFirstAction`	Première action à exécuter sur des objets suspects. Dans les tâches de protection en temps réel, avant d'effectuer l'action sur l'objet que vous avez choisie, Kaspersky Anti-Virus bloque l'accès à l'objet pour l'application qui y a fait requête. Les valeurs possibles comprennent : **Cure** (réparer). Kaspersky Anti-Virus essaie de réparer l'objet ayant sauvegardé la copie de l'objet dans le répertoire de sauvegarde. Si la réparation ne s'avère pas possible, par exemple, le type de l'objet ou le type de la menace dans l'objet ne suppose pas la réparation, Kaspersky Anti-Virus garde l'objet intact. **Quarantine** (mettre en quarantaine). Kaspersky Anti-Virus transfère l'objet dans le répertoire de sauvegarde de la quarantaine dans lequel l'objet est conservé sous forme codée. **Remove** (supprimer). Kaspersky Anti-Virus supprime l'objet après avoir créé une copie de sauvegarde. **Recommended** (exécuter l'action recommandée). Kaspersky Anti-Virus choisit automatiquement et effectue l'action sur l'objet à la base des données sur le danger de la menace détectée dans l'objet et sur la possibilité de sa réparation ; par exemple, Kaspersky Anti-Virus supprime immédiatement les chevaux de Troie puisqu'ils ne s'introduisent pas dans les autres fichiers et ne les infectent pas et, donc, ne supposent pas la réparation. **Skip** (sauter). L'objet reste intact. Kaspersky Anti-Virus n'essaie pas le supprimer ou réparer ; il enregistre les informations sur l'objet dans le registre. Valeur par défaut : **Recommended**.
`SuspiciousSecondAction`	Les valeurs sont identiques à celles du paramètre SuspiciousFirstAction. Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action. Si vous sélectionnez Skip (sauter) ou Remove (supprimer) en tant que première action, il n'est pas nécessaire de spécifier la deuxième action. Pour les autres valeurs, il est recommandé de spécifier les deux actions. Si vous ne spécifiez pas la deuxième action, Kaspersky Anti-Virus, en tant que deuxième action, appliquera l'action Skip (sauter). Valeur par défaut : **Skip**.
`UseSizeLimit`	Fait activer / désactiver l'utilisation du paramètre SizeLimit (taille maximum de l'objet analysé).

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	yes – utiliser le paramètre SizeLimit ; **no** – ne pas utiliser le paramètre SizeLimit. Valeur par défaut : **no**.
SizeLimit	Taille maximum de l'objet analysé (octet). Si la taille de l'objet analysé est supérieure à la valeur spécifiée, Kaspersky Anti-Virus saute l'objet. Ce paramètre est utilisé ensemble avec le paramètre UseSizeLimit. Spécifiez la taille maximum de l'objet en octets. Valeurs possibles : 0 – 2147483647 (2 Gigaoctet environ). **0** – Kaspersky Anti-Virus analyse les objets de toutes tailles. Valeur par défaut : **0**.
UseTimeLimit	Fait activer / désactiver l'utilisation du paramètre TimeLimit (durée maximum de l'analyse de l'objet). **yes** – utiliser le paramètre TimeLimit ; **no** – ne pas utiliser le paramètre TimeLimit. Valeurs par défaut : tâche de protection en temps réel – **yes** ; tâche d'analyse à la demande – **no**.
TimeLimit	Durée maximum de l'analyse de l'objet (secondes). Kaspersky Anti-Virus interrompt l'analyse d'un objet s'il est dure plus longtemps que la valeur définie dans ce paramètre. Ce paramètre est utilisé ensemble avec le paramètre UseTimeLimit. Spécifiez la durée maximum de l'analyse de l'objet en secondes. **0** – la durée de l'analyse des objets n'est pas limitée. Valeurs par défaut : tâche de protection en temps réel – **60** ; tâche d'analyse à la demande – **120**.
UseExcludeMasks	Fait activer / désactiver l'exclusion des objets spécifiés par le paramètre ExcludeMasks. **yes** – exclure les objets spécifiés par le paramètre ExcludeMasks. **no** – ne pas exclure les objets spécifiés par le paramètre ExcludeMasks. Valeur par défaut : **no**.

ExcludeMasks	Exclusion des objets selon leur nom, masque ou expressions régulières. A l'aide de ce paramètre, vous pouvez exclure du secteur d'analyse spécifié un fichier particulier selon le nom, ou plusieurs fichiers en utilisant les masques Shell et expressions régulières étendues POSIX. Dans les expressions régulières, utilisez le préfix **re:**.
	Exemple :
	`ExcludeMasks=re:.*\.tar\.gz`
	`ExcludeMasks=re:.*\.avi`
	`ExcludeMasks=re:/.*\.avi$`
	`ExcludeMasks=*.doc`
	Valeur par défaut : non spécifié.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
UseExcludeThreats	Fait activer / désactiver l'exclusion des objets qui contiennent les menaces spécifiées par le paramètre ExcludeThreats. **yes** – exclure les objets qui contiennent les menaces spécifiées par le paramètre ExcludeThreats. **no** – ne pas exclure les objets qui contiennent les menaces spécifiées par le paramètre ExcludeThreats. Valeur par défaut : **no**.

ExcludeThreats	Exclusion des objets selon les signatures des menaces détectées dans les objets. Avant de spécifier les valeurs de ce paramètre, assurez-vous que le paramètre UseExcludeThreats est activé.
	
	Par exemple, vous utilisez un des utilitaires pour recevoir les informations sur le réseau. La majorité des applications antivirus rapportent le code de ces utilitaires aux menaces de type **Programmes potentiellement malveillants**. Pour que Kaspersky Anti-Virus ne le bloque pas, rajoutez la signature complète de la menace dans cet utilitaire dans la liste des menaces à exclure.
	
	Pour exclure de l'analyse un objet, spécifiez la signature complète de la menace détectée dans cet objet, – ligne-conclusion de Kaspersky Anti-Virus sur ce que l'objet est infecté ou suspect.
	
	Vous pouvez trouver la signature complète de la menace détectée dans l'objet, dans le registre de Kaspersky Anti-Virus.
	
	De même, vous pouvez trouver la signature complète de la menace détectée dans le logiciel, sur le site web de l'Encyclopédie des virus Viruslist.ru (cf. section Encyclopédie des virus - http://www.viruslist.com). Pour trouver la signature d'une menace, saisissez le nom du logiciel dans le champ **Recherche**.
	
	La valeur du paramètre est sensible à la casse.
	
	Exemple :
	
	Ne pas exécuter l'action sur les fichiers dans lesquels Kaspersky Anti-Virus détectera les menaces avec les signatures NetTool.Linux.SynScan.a et Monitor.Linux.Keylogger.a :
	
	`ExcludeThreats=not-a-virus:NetTool.Linux.SynScan.a`
	
	`ExcludeThreats=not-a-virus:Monitor.Linux.Keylogger.a`
	
	Dans les noms des menaces, vous pouvez utiliser des masques Shell ou des expressions régulières étendues POSIX. Ajoutez le préfixe re: aux expressions régulières POSIX.
	
	Ne pas exécuter les actions sur les fichiers dans lesquels Kaspersky Anti-Virus découvre n'importe quelle menace pour Linux de la catégorie not-a-virus:
	
	`ExcludeThreats=re:not-a-virus:.*\.Linux\..*`
	
	Valeur par défaut : non spécifié.

UseAdvancedActions	Fait activer / désactiver l'utilisation des actions sur l'objet en fonction du type de la menace détectée dans l'objet. Si vous activez ce paramètre, Kaspersky Anti-Virus appliquera les actions que vous aurez spécifiées dans la section [ScanScope:ScanSettings:AdvancedActions] au lieu des actions spécifiées par les paramètres InfectedFirstAction, InfectedSecondAction, SuspiciousFirstAction et SuspiciousSecondAction. Valeurs possibles : **yes** – appliquer les actions sur les objets en fonction du type de la menace ; **no** – ne pas appliquer les actions sur les objets en fonction du type de la menace.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	Valeur par défaut : **no**.
ReportCleanObjects	Fait activer / désactiver la consignation dans le journal des informations relatives aux objets analysés que Kaspersky Anti-Virus a considéré comme étant sains. Vous pouvez activer ce paramètre, par exemple, pour confirmer qu'un objet quelconque a été analysé par Kaspersky Anti-Virus. Il est déconseillé d'activer ce paramètre pour une longue durée car la consignation d'un grand volume d'informations dans le journal peut réduire les performances du système d'exploitation. Valeurs possibles : **yes** : consigner dans le journal les informations relatives aux objets sains ; **no** : ne pas consigner dans le journal les informations relatives aux objets sains. Valeur par défaut : **no**.
ReportPackedObjects	Fait activer / désactiver la consignation dans le journal des informations relatives aux objets analysés qui font partie d'objets complexes. Vous pouvez activer ce paramètre, par exemple, pour confirmer qu'un objet quelconque appartenant à une archive a été analysé par Kaspersky Anti-Virus. Il est déconseillé d'activer ce paramètre pour une longue durée car la consignation d'un grand volume d'informations dans le journal peut réduire les performances du système d'exploitation. Valeurs possibles : **yes** : consigner dans le journal les informations relatives à l'analyse des objets des archives ; **no** : ne pas consigner dans le journal les informations relatives à l'analyse des objets des archives. Valeur par défaut : **no**.
UseAnalyzer	Active/désactive l'analyseur heuristique. L'analyseur heuristique analyse les séquences typiques d'opérations qui permettent de tirer une conclusion sur la nature du fichier avec un certain degré de certitude. L'avantage de cette méthode tient au fait que les nouvelles menaces peuvent être identifiées avant que leur activité ne soit remarquée par les spécialistes des virus. Valeurs possibles : **yes** : active l'analyseur heuristique ; **no** : désactive l'analyseur heuristique. Valeur par défaut : **no**.
HeuristicLevel	Niveau de détails de l'analyse à l'aide de l'analyseur heuristique. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure. Valeurs possibles : **Light** : analyse la moins détaillée, charge minime sur le système. **Medium** : profondeur moyenne de l'analyse, charge équilibrée sur le système ;

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	Deep : analyse la plus poussée, charge maximale du système. Valeur par défaut : **Medium**.
`[ScanScope:ScanSettings:AdvancedActions]` Actions en fonction du type de menace. A l'aide des paramètres de cette section, vous pouvez spécifier les actions spécifiques de Kaspersky Anti-Virus à exécuter sur les objets qui contiennent les menaces des types spécifiés.	

`Verdict`
`FirstAction`
`SecondAction`
	Avant de spécifier les valeurs des paramètres de cette rubrique, assurez-vous que la valeur du paramètre UseAdvancedActions est yes.
	Pour le type des menaces spécifiées par le paramètre Verdict, spécifiez deux actions (FirstAction et SecondAction). Kaspersky Anti-Virus effectuera ces actions s'il détecte dans cet objet la menace de type spécifié.
	Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action.
	Si vous sélectionnez Skip (sauter) ou Remove (supprimer) en tant que première action, il n'est pas nécessaire de spécifier la deuxième action. Pour les autres valeurs, il est recommandé de spécifier les deux actions.
	Si vous ne spécifiez pas la deuxième action, Kaspersky Anti-Virus, en tant que deuxième action, appliquera l'action Skip (sauter).
	Cf. valeurs des paramètres FirstAction et SecondAction dans la spécification de ces sections.
	Les valeurs possibles du paramètre Verdict (type de la menace) comprennent :
	Virware – virus et vers ;
	Trojware – chevaux de Troie ;
	Malware – autres programmes malveillants ;
	Pornware – programmes à contenu pornographique ;
	Adware – programmes publicitaires ;
	Riskware – applications potentiellement dangereuses.
	Les valeurs du paramètre Verdict sont sensibles à la casse.
	Pour de plus amples informations, consultez la rubrique " Programmes détectés par Kaspersky Anti-Virus " (cf. page 11).
	Exemple :
	`UseAdvancedActions=yes`
	`[ScanScope:ScanSettings:AdvancedActions]`
	`Verdict=Adware`
	`FirstAction=Cure`
	`SecondAction=Skip`
	`[ScanScope:ScanSettings:AdvancedActions]`
	`Verdict=Pornware`
	`FirstAction=Cure`
	`SecondAction=Skip`
	Valeur par défaut : non spécifié.

`[ExcludedFromScanScope]`	

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
Secteur d'exclusion.	
`AreaDesc`	Nom de la zone d'exclusion, comprend les informations supplémentaires sur la zone d'exclusion. Exemple : AreaDesc="L'exclusion des SAMBA répartés" Valeur par défaut : non spécifié.
`AreaMask`	A l'aide de ce paramètre, vous pouvez limiter le secteur d'exclusion spécifié dans la section [ExcludedFromScanScope:AreaPath]. Kaspersky Anti-Virus n'exclura que les objets que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX. Dans les expressions régulières, utilisez le préfix **re:**. `AreaMask=re:.*\.tar\.gz` Valeur par défaut : non spécifié.
`UseAccessUser`	Ce paramètre fait activer / désactiver l'utilisation des paramètres de la section [ExcludedFromScanScope:AccessUser] (exclusion lors de l'accès avec les droits des utilisateurs déterminés). Ce paramètre n'est utilisé que dans les tâches de protection en temps réel. Il n'est pas utilisé dans les tâches d'analyse à la demande. Les valeurs possibles comprennent : **yes** – exclure les objets uniquement dans le cas où les applications avec les droits des utilisateurs spécifiés par les paramètres dans la section [ExcludedFromScanScope:AccessUser] y font requête ; **no** – exclure les objets lors de la requête à ceux-ci avec n'importe quels droits. Valeur par défaut : non spécifié.
`[ExcludedFromScanScope:AreaPath]` Secteur d'exclusion. Chemin d'accès au répertoire à exclure.	
`Path`	La valeur du paramètre est composée de trois éléments : **<type du système de fichiers>:<protocole d'accès>:<chemin au répertoire à exclure>**, où : **<type du système de fichiers>**. Les valeurs possibles comprennent : **Mounted**. Répertoires distants montés sur le serveur. A l'aide de l'élément <protocole d'accès>, spécifiez le protocole qui assurera l'accès à distance aux répertoires. **Shared**. Ressources du système de fichiers du serveur accessibles via le protocole SMB/CIFS ou le protocole NFS. **AllRemotelyMounted**. Tous les répertoires distants montés sur le serveur par l'intermédiaire des protocoles SMB/CIFS et NFS. **AllShared**. Toutes les ressources du système de fichiers du serveur accessibles via les protocoles SMB/CIFS et NFS. **<protocole d'accès>**. Protocole qui assure l'accès à distance aux ressources spécifiées. Ce paramètre est utilisé uniquement dans le cas où le <type du système de fichiers> a la valeur Mounted ou Shared. Les valeurs possibles comprennent : **SMB**. Protocole d'accès à distance aux ressources SMB/CIFS.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	NFS. Protocole d'accès à distance aux ressources NFS. **<chemin d'accès au répertoire à exclure>**. Chemin d'accès complet au répertoire à exclure. Exemples: `Path=Mounted:NFS` – *exclure tous les répertoires distants montés à l'aide de NFS*. Valeur par défaut : non spécifié.
`[ExcludedFromScanScope:AccessUser]` Exclusion de l'analyse lors de l'accès avec les droits des utilisateurs déterminés. Kaspersky Anti-Virus exclut les objets de l'analyse uniquement dans le cas où les applications avec les droits des utilisateurs et des groupes spécifiés par les paramètres de cette section y font requête. Si les paramètres de cette section ne sont pas spécifiés, Kaspersky Anti-Virus exclut les objets si la requête à ceux-ci est faite avec n'importe quels droits. Les paramètres de cette section ne sont utilisés que dans les tâches de protection en temps réel. Ils ne sont pas utilisés dans les tâches d'analyse à la demande.	

`UserName`	Kaspersky Anti-Virus exclut les objets uniquement dans le cas où les applications avec les droits des utilisateurs déterminés y font requête. Vous pouvez spécifier plusieurs valeurs de ce paramètre, par exemple :
	`UserName=usr1`
	`UserName=usr2`
	Valeur par défaut : non spécifié.

`UserGroup`	Nom du groupe. Kaspersky Anti-Virus exclut les objets uniquement dans le cas où les applications avec les droits des groupes déterminés y font requête. Vous pouvez spécifier plusieurs valeurs de ce paramètre, par exemple :
	`UserGroup=group1`
	`UserGroup=group2`
	Valeur par défaut : non spécifié.

PARAMETRES DES TACHES DE MISE A JOUR

Cette section décrit les paramètres du fichier de configuration des tâches de mise à jour. Vous pouvez l'utiliser pour créer de nouvelles tâches de mise à jour et modifier les paramètres des tâches en cours.

Pour modifier les paramètres de la tâche, vous devez exporter les paramètres de la tâche dans un fichier (cf. page 103), ensuite ouvrir ce fichier dans n'importe quel programme de traitement de texte, modifier les paramètres selon vos besoins et ensuite importer les paramètres spécifiés dans le fichier dans la tâche (cf. page 104).

Structure du fichier de configuration ini des tâches de mise à jour

Le fichier de configuration des tâches de mise à jour comprend l'ensemble des paramètres et des sections. Les sections du fichier décrivent la fonction qui est exécutée par la tâche de mise à jour, la source des mises à jour et les paramètres de connexion à celle-là.

A l'aide du paramètre UpdateType, sélectionnez la fonction qui sera exécutée par la tâche de mise à jour. Ce paramètre est obligatoire.

Dans la section [UpdateComponentsSettings], spécifiez s'il faut télécharger les mises à jour spécifiées par le paramètre UpdateType, ou s'il ne faut que recevoir les informations sur ces mises à jour. Ce paramètre est obligatoire.

La section [CommonSettings] décrit le type de la source des mises à jour et les paramètres de connexion à celle-là. A l'aide des paramètres de cette section, spécifiez si Kaspersky Anti-Virus doit faire requête au serveur proxy lors de la connexion aux différentes sources des mises à jour, et spécifiez les paramètres du serveur proxy.

La section [CommonSettings:CustomSources] est obligatoire si vous avez sélectionné en tant que source des mises à jour les sources d'utilisateur. Spécifiez dans cette section l'adresse de la source des mises à jour d'utilisateur. Si vous voulez spécifier plusieurs sources des mises à jour d'utilisateur, spécifiez chacune des sources dans la section à part [CommonSettings:CustomSources]. Kaspersky Anti-Virus fera requête aux sources des mises à jour d'utilisateur en utilisant les paramètres de connexion spécifiés dans la section [CommonSettings].

La section [RetranslateUpdatesSettings] est obligatoire si vous avez choisi à l'aide du paramètre UpdateType la copie des mises à jour sans les utiliser. Dans cette section, spécifiez le répertoire dans lequel Kaspersky Anti-Virus sauvegardera les mises à jour spécifiées. Si vous avez choisi la copie uniquement des mises à jour spécifiées, spécifiez de même les noms des bases et des modules dont les mises à jour vous voulez recevoir dans la tâche.

La spécification des paramètres du fichier de configuration, les valeurs possibles des paramètres et les valeurs par défaut sont données dans le tableau suivant.

En spécifiant les paramètres dans le fichier, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Tableau 20. Paramètres des tâches de mise à jour

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
UpdateType	Spécifiez la fonction qui sera exécutée par la tâche de mise à jour : **AllBases**. Mettre à jour les bases de Kaspersky Anti-Virus. **RetranslateProductComponents** (Copier toutes les mises à jour disponibles pour Kaspersky Anti-Virus). Kaspersky Anti-Virus enregistrera les mises à jour reçues dans le répertoire spécifié par le paramètre RetranslationFolder sans les utiliser. **RetranslateComponentsList** (Copier uniquement les mises à jour spécifiées). Kaspersky Anti-Virus ne téléchargera que les mises à jour dont les noms sont spécifiés par les paramètres de la section [RetranslateUpdatesSettings]. Il enregistrera les mises à jour reçues dans le répertoire spécifié par le paramètre RetranslationFolder sans les utiliser. A l'aide du paramètre **RetranslateComponentsList**, vous pouvez recevoir les mises à jour des modules des autres applications de Kaspersky Lab si vous voulez utiliser le serveur protégé en tant que intermédiaire pour répartir les mises à jour. Vous pouvez consulter les noms des mises à jour dans le document http://support.kaspersky.ru/downloads/updater/update_components_21112008.pdf , publié sur le site du Service du Support Technique de Kaspersky Lab. L'installation automatique des mises à jour critiques des modules de Kaspersky Anti-Virus n'est pas prévue. Valeur par défaut : **AllBases**.
[CommonSettings] Source de la mise à jour et paramètres de connexion à celle-là.	
SourceType	Sélectionnez la source depuis laquelle Kaspersky Anti-Virus recevra les mises à jour: **KLServers**. Kaspersky Anti-Virus recevra les mises à jour depuis un des serveurs de mise à jour de Kaspersky Lab. Les mises à jour seront téléchargées via le protocole HTTP ou le protocole FTP. **AKServer**. Kaspersky Anti-Virus téléchargera les mises à jour sur le serveur protégé depuis le serveur d'administration Kaspersky Administration Kit installé dans le réseau local. Vous pouvez sélectionner cette source de mise à jour si vous utilisez l'application Kaspersky Administration Kit pour l'administration centralisée de la protection antivirus des ordinateurs au sein de votre entreprise. **Custom**. Kaspersky Anti-Virus téléchargera les mises à jour depuis la source d'utilisateur spécifiée par les paramètres de la section [CommonSettings:CustomSources]. Vous pouvez spécifier les répertoires des serveurs FTP ou HTTP, les répertoires sur tout dispositif monté sur le serveur protégé, y compris sur les ordinateurs distants montés via les protocoles SMB/CIFS ou NFS. Valeur par défaut : **KLServers**.
UseKLServersWhenUnavailable	Vous pouvez configurer la requête de Kaspersky Anti-Virus aux serveurs des mises à jour de Kaspersky Lab dans le cas où toutes les sources d'utilisateurs ne sont pas disponibles. **yes** – faire requête aux serveurs des mises à jour de Kaspersky Lab si aucune source d'utilisateur n'est disponible ; **no** – ne pas faire requête aux serveurs des mises à jour de Kaspersky Lab si aucune source d'utilisateur n'est disponible. Valeur par défaut : **yes**.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
UseProxyForKLServers	Utilisation du serveur proxy pour la connexion aux serveurs des mises à jour de Kaspersky Lab. **yes** – utiliser le serveur proxy pour la connexion aux serveurs des mises à jour de Kaspersky Lab ; **no** – ne pas utiliser le serveur proxy pour la connexion aux serveurs de mises à jour de Kaspersky Lab. Valeur par défaut : **no**.
UseProxyForCustomSources	Utilisation du serveur proxy pour la connexion aux sources des mises à jour d'utilisateur. Activer ce paramètre si pour la connexion à un des serveurs d'utilisateur FTP ou HTTP, il faut avoir l'accès au serveur proxy. **yes** – utiliser le serveur proxy pour la connexion aux sources des mises à jour d'utilisateur ; **no** – ne pas utiliser le serveur proxy pour la connexion aux sources des mises à jour d'utilisateur. Valeur par défaut : **no**.
ProxyPort	Paramètres du serveur proxy : port. Valeur par défaut : **3128**.
ProxyServer	Paramètres du serveur proxy : nom de réseau ou adresse IP. Valeur par défaut : non spécifié.
ProxyAuthType	Validation lors de l'accès au serveur proxy qui est utilisé lors de la connexion aux serveurs sources des mises à jour FTP ou HTTP. **NotRequired** (aucune vérification de l'authenticité). Sélectionnez si la vérification de l'authenticité n'est pas nécessaire pour l'accès au serveur proxy. **Plain** (vérification de l'authenticité par le nom et le mot de passe, Basic authentication). Spécifiez le nom et le mot de passe de l'utilisateur à l'aide des paramètres ProxyAuthUser et ProxyAuthPassword. Valeur par défaut : **NotRequired**.
ProxyAuthUser	Si vous avez activé la vérification de l'authenticité, spécifiez le nom d'utilisateur avec les droits duquel Kaspersky Anti-Virus fera requête au serveur proxy. Valeur par défaut : non spécifié.
ProxyAuthPassword	Si vous avez activé la vérification de l'authenticité, spécifiez le mot de passe de l'utilisateur avec les droits duquel Kaspersky Anti-Virus fera requête au serveur proxy. Valeur par défaut : non spécifié.
UseFtpPassiveMode	Pour la connexion aux serveurs des mises à jour via le protocole FTP, Kaspersky Anti-Virus utilise par défaut le mode passif du serveur FTP : il est supposé que dans le réseau local de l'entreprise, le pare-feu est utilisé. Valeurs possibles : **yes** – utiliser le mode passif du serveur FTP ; **no** – utiliser le mode actif du serveur FTP. Valeur par défaut : **yes**.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
ConnectionTimeout	Ce paramètre détermine le délai d'attente de la réponse de la source des mises à jour (serveur FTP ou HTTP). Si durant la période de temps spécifiée la réponse de la part de la source des mises à jour n'est pas reçue, Kaspersky Anti-Virus fait requête à une autre source des mises à jour spécifiée, par exemple, à un autre serveur des mises à jour de Kaspersky Lab, si vous avez configuré la mise à jour depuis les serveurs des mises à jour de Kaspersky Lab. Spécifiez le temps d'attente en secondes. En guise de valeur, le paramètre accepte uniquement des nombres entiers compris entre **0** et **120**. Valeur par défaut : **10**.
[CommonSettings:CustomSources] Si vous avez spécifié SourceType=Custom, spécifiez la source des mises à jour d'utilisateur à l'aide des paramètres de cette section. Vous pouvez spécifier plusieurs sources de la mise à jour d'utilisateur. Spécifiez chacune des sources dans la section à part. Kaspersky Anti-Virus fera requête à chaque source spécifiée suivante si la source précédente n'est pas disponible. Vous pouvez configurer la requête de Kaspersky Anti-Virus aux serveurs des mises à jour de Kaspersky Lab dans le cas où toutes les sources ne seraient pas disponibles, à l'aide du paramètre UseKLServersWhenUnavailable.	
Url	Spécifiez la source des mises à jour d'utilisateur : répertoire dans le réseau local ou global. Exemple : Url=http://primer.ru/bases/ – adresse du serveur HTTP ou FTP sur lequel se trouve le répertoire contenant les mises à jour. Url=/home/bases/ : répertoire sur le serveur protégé. Valeur par défaut : non spécifié.
Enabled	A l'aide de ce paramètre, vous pouvez activer ou désactiver l'utilisation de la source spécifiée par le paramètre Url de la section en cours. **yes** – utiliser la source de la mise à jour ; **no** – ne pas utiliser la source de la mise à jour. Valeur par défaut : non spécifié.
[UpdateComponentsSettings] Chargement des mises à jour.	
Action	Ce paramètre est obligatoire ; il possède la valeur **DownloadAndApply** : • Kaspersky Anti-Virus charge les mises à jour, si le paramètre **UpdateType** possède la valeur **RetranslateProductComponents ou RetranslateComponentsList** ; • Kaspersky Anti-Virus charge et installe les mises à jour, si le paramètre **UpdateType** possède la valeur **AllBases**. Valeur par défaut : **DownloadAndApply**.
[RetranslateUpdatesSettings] Copie des mises à jour depuis les sources des mises à jour sans les utiliser. Spécifiez les paramètres de cette section si vous avez sélectionné le téléchargement des mises à jour sans leur application : si vous avez attribué la valeur RetranslateComponentsList au paramètre UpdateType.	
RetranslationFolder	Spécifiez le répertoire dans lequel Kaspersky Anti-Virus enregistrera les mises à jour reçues. Valeur par défaut : non spécifié.
RetranslationComponents	Si vous avez spécifié le paramètre UpdateType dans la valeur RetranslateComponentsList, spécifiez les noms des mises à jour que vous voulez

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES

	recevoir.
	Vous pouvez consulter les noms des mises à jour dans le document http://support.kaspersky.ru/downloads/updater/update_components_21112008.pdf , publié sur le site du Service du Support Technique de Kaspersky Lab.
	Exemple :
	Pour copier les mises à jour pour Kaspersky Anti-Virus 6,0 pour Windows Servers Enterprise Edition de la version 6.0.2.551 :
	`RetranslationComponents=UPDATER`
	`RetranslationComponents=AVS`
	`RetranslationComponents=BLST`
	`RetranslationComponents=KAV6WSEE`
	`RetranslationComponents=RT`
	`RetranslationComponents=AK6`
	`RetranslationComponents=INDEX60`
	Valeur par défaut : non spécifié.

PARAMETRES DE L'HORAIRE

Cette section décrit les paramètres du fichier de configuration que vous pouvez utiliser pour configurer l'horaire des tâches.

En spécifiant les paramètres, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Structure du fichier de configuration ini de l'horaire

```
Enable=yes | no

StartRules=<règle_de_lancement>;<règle_de_lancement_2>...<règle_de_lancement_n>

[StopRules=<règle_d'arrêt>;<règle_d'arrêt_2>...<règle_d'arrêt_n>]

[SuspendRules=<règle_de_suspension>;<règle_de_suspension_2>;...
<règle_de_suspension_n>]
```

Tableau 21. Paramètres de l'horaire

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
`Enable`	Fait activer / désactiver le lancement de la tâche conformément à l'horaire. Les valeurs possibles comprennent : **yes** – activer le lancement de la tâche conformément à l'horaire ; **no** – désactiver le lancement de la tâche programmé.
`StartRules`	Liste des règles de lancement (cf. page 156) de la tâche. Séparez les valeurs par le caractère **;** (point-virgule).
`StopRules`	Liste des règles d'arrêt (cf. page 157) de la tâche. Séparez les valeurs par le caractère **;** (point-virgule).
`SuspendRules`	Liste des règles de suspension (cf. page 158) de la tâche. Séparez les valeurs par le caractère **;** (point-virgule).

DANS CETTE SECTION

RÈGLES DE LANCEMENT

Vous pouvez décrire une ou plusieurs règles de lancement.

Syntaxe

```
<règle_de_lancement>=PS
<règle_de_lancement>=BR
<règle_de_lancement>=<heure exacte>
```

Exemples

- *Lancer la tâche le 10 de chaque mois et le dernier jour de chaque mois à 20h45 :*

```
Enable=yes
StartRules=10::; -01:20:45
```

- *Lancer la tâche le lundi de décembre 2009 à 00h00 :*

```
Enable=yes
StartRules=2009/Dec/Mon::
```

- *Lancer la tâche tous les jours à 13h00 :*

```
Enable=yes
StartRules=:13:00
```

- *Lancer la tâche toutes les 30 minutes :*

```
Enable=yes
```

```
StartRules=::30
```

Tableau 22. Paramètres de la règle de lancement

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
<règle_de_lancement>	Condition du lancement d'une tâche. Vous pouvez spécifier plusieurs conditions du lancement d'une tâche. Par exemple, pour configurer le lancement de la tâche d'analyse à la demande deux fois par mois, vous devez créer deux règles de lancement.
BR	Après la mise à jour des bases. La tâche sera lancée chaque fois après la mise à jour réussie des bases de Kaspersky Anti-Virus (cette option n'est pas utilisée dans les tâches de mise à jour).
PS	Lors du lancement de l'application. La tâche sera lancée chaque fois lors du lancement de Kaspersky Anti-Virus.
<heure exacte>	Indiquez la date et l'heure de lancement de la tâche (cf. page 159).

REGLES D'ARRET

Vous pouvez décrire une ou plusieurs règles d'arrêt.

Syntaxe

```
<règle_d'arrêt>=StopAfter <durée en minutes> CanRunAfter <durée en minute>
<règle_d'arrêt>=StopAt <heure exacte> CanRunAfter <durée en minute>
<règle_d'arrêt>=StopAt <heure exacte> CanRunAt <heure exacte>
```

Exemples

- *Arrêter la tâche 10 minutes après le lancement, ne pas autoriser le relancement durant 10 minutes après l'arrêt :*

```
Enable=yes
StopRules=StopAfter 10 CanRunAfter 10
```

- *Arrêter la tâche à 00h00 le mercredi, ne pas autoriser le relancement avant 18h45 le mercredi :*

```
Enable=yes
StopRules=StopAt Wed:: CanRunAt :18:45
```

Tableau 23. Paramètres de la règle d'arrêt

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
<règle_d'arrêt>	A l'aide de la règle d'arrêt, vous pouvez configurer la durée maximum de l'exécution de la tâche. La règle d'arrêt permet également de préciser l'intervalle de temps au cours duquel la tâche ne peut pas être exécutée selon la planification. A l'issue de la période de temps spécifiée, elle ne sera pas reprise. Si la période de temps spécifiée comprend l'heure du prochain lancement de la tâche programmé, cette tâche n'est pas considérée comme manquée.
StopAfter	Durée maximum d'exécution de la tâche, minutes. Si la durée d'exécution de la tâche est supérieure à la valeur du paramètre, la tâche sera arrêtée par Kaspersky Anti-Virus. La tâche ainsi arrêtée ne sera considérée comme étant manquée. Ce paramètre n'est pas utilisé dans les tâches de mise à jour. Spécifiez le nombre de minutes. Séparez la valeur par un espace.
StopAt	Heure d'arrêt de la tâche. Indiquez l'heure au format <heure exacte> (cf. page 159). Séparez la valeur par un espace.
CanRunAfter	Durée en minutes depuis l'arrêt de la tâche, défini par le paramètre StopAfter. Durant cette période, la tâche ne peut pas être relancée. Si ce paramètre n'est pas défini dans la règle de suspension, la tâche reprendra directement après la suspension (la valeur du paramètre est égale à zéro par défaut). Séparez la valeur par un espace.
CanRunAt	Heure à laquelle la tâche peut être à nouveau lancée selon la planification, au format <heure exacte> (cf. page 159). Séparez la valeur par un espace.

REGLES DE SUSPENSION

Vous pouvez décrire une ou plusieurs règles de suspension.

Syntaxe

```
<règle_de_suspension>=PauseAfter <durée en minutes> [ResumeAfter <durée en minutes>]
<règle_de_suspension>=PauseAt <heure exacte> [ResumeAfter <durée en minutes>]
<règle_de_suspension>=PauseAt <heure exacte> [ResumeAt <heure exacte>]
```

Exemples

- *Lancer la tâche à 00h00 ; suspendre la tâche de 10h00 à 18h00 :*

```
Enable=yes
StartRules=:00:00
SuspendRules=PauseAt :10:00 ResumeAt :18:00
```

Tableau 24. Paramètres de la règle de suspension

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
<règle_de_suspension>	A l'aide de la règle de suspension, vous pouvez spécifier la période de temps durant laquelle la tâche sera suspendue. À l'issue de la période de temps spécifiée, Kaspersky Anti-Virus reprendra la tâche. Il peut s'avérer nécessaire de suspendre la tâche pour une certaine période de temps, par exemple, de 10 à 18 heures. Si la période de temps spécifiée comprend l'heure du prochain lancement de la tâche programmé, cette tâche n'est pas considérée comme manquée. Les règles de suspension ne sont pas utilisées dans les tâches de mise à jour.
PauseAfter	Durée maximum d'exécution de la tâche, minutes. Si la durée d'exécution de la tâche est supérieure à la valeur du paramètre, la tâche sera arrêtée par Kaspersky Anti-Virus. La tâche ainsi arrêtée ne sera considérée comme étant manquée. Séparez la valeur par un espace.
PauseAt	Heure de suspension de la tâche. Indiquez l'heure au format du paramètre <heure exacte> (cf. page 159). Séparez la valeur par un espace.
ResumeAfter	Durée de la suspension de la tâche, minutes. Kaspersky Anti-Virus reprendra la tâche à l'issue de l'intervalle que vous aurez défini depuis la suspension. Si ce paramètre n'est pas défini dans la règle de suspension, la tâche reprisera directement après la suspension (la valeur du paramètre est égale à zéro par défaut). Séparez la valeur par un espace.
ResumeAt	Heure de reprise de la tâche. Indiquez l'heure au format du paramètre <heure exacte> (cf. page 159). Séparez la valeur par un espace.

INDICATION DE L'HEURE EXACTE

Le paramètre <heure exacte> a le format suivant.

```
[<année>/][<mois>/][<jour du mois>|<jour de la semaine>]:[hh]:[mm]
```

Les champs du paramètre <heure exacte> sont décrits dans le tableau suivant :

CHAMP	VALEUR
<an>	[1900;2100]
<mois>	JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC
<jour du mois>	[-1;31], où 1 est le dernier jour du mois, 0 : le jour du mois n'est pas défini.
<jour de la semaine>	MON | TUE | WED | THU | FRI | SAT | SUN | Weekend | Working days
hh	heures [00;23]
mm	Si vous avez spécifié la valeur HH – au format [00,59]. Si vous n'avez pas spécifié la valeur HH – au format [0,24*60]. Vous pouvez spécifier les valeurs suivantes : :23h30 – à 23h30. Non spécifié (ou ::) – la tâche sera lancée / arrêtée / suspendue / reprise à 00h00. ::90 – toutes les 1,5 heures.

PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS

La spécification des paramètres du fichier de configuration, les valeurs possibles des paramètres et les valeurs par défaut sont données dans le tableau suivant.

En spécifiant les paramètres dans le fichier, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Après la modification des paramètres généraux de Kaspersky Anti-Virus, il faut redémarrer le service Kaspersky Lab Framework à l'aide de la commande `/opt/kaspersky/kav4fs/bin/kav4fs-control --restart-app`.

Tableau 25. Paramètres généraux de Kaspersky Anti-Virus

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
StartWithUser	Compte avec les droits duquel sont exécutés les processus de Kaspersky Anti-Virus. Vous ne pouvez pas modifier ce paramètre. Valeur par défaut : **root**.
StartWithGroup	Compte avec les droits duquel sont exécutés les processus de Kaspersky Anti-Virus. Vous ne pouvez pas modifier ce paramètre. Valeur par défaut : **default**.
UpdateFolder	Chemin d'accès au répertoire sur le serveur protégé ; contient les répertoires des mises à jour définis par les paramètres AVBasesFolderName et AVBasesBackupFolderName. Valeur par défaut : **/var/opt/kaspersky/kav4fs/update**.
AVBasesFolderName	Nom du répertoire dans lequel Kaspersky Anti-Virus enregistre les mises à jour des bases. Valeur par défaut : **avbases**.
AVBasesBackupFolderName	Chemin d'accès complet au répertoire que Kaspersky Anti-Virus utilise en tant que répertoire de service lors de la mise à jour des bases. Si vous spécifiez un autre répertoire, assurez-vous qu'il est disponible en lecture et modification pour le compte avec les droits duquel fonctionne Kaspersky Anti-Virus. Valeur par défaut : **avbases-backup**.
SambaConfigPath	Répertoire dans lequel est sauvegardé le fichier de configuration SAMBA. Par défaut, est spécifié le chemin d'accès standard au répertoire du fichier de configuration SAMBA sur le serveur. Vous devez spécifier ce paramètre si le fichier de configuration Samba est conservé dans l'emplacement autre que celui standard. Valeur par défaut : **/etc/samba/smb.conf**.
NfsExportPath	Répertoire dans lequel est sauvegardé le fichier de configuration NFS. Par défaut, est spécifié le chemin d'accès standard au répertoire du fichier de configuration NFS sur le serveur. Vous devez spécifier ce paramètre si le fichier de configuration NFS est sauvegardé dans l'emplacement autre que celui standard. Valeur par défaut : **/etc/exports**.
TempFolder	Chemin d'accès complet au répertoire dans lequel Kaspersky Anti-Virus enregistre des fichiers créés temporaires. Si vous spécifiez un autre répertoire, assurez-vous qu'il est disponible en lecture et modification pour le compte avec les droits duquel fonctionne Kaspersky Anti-Virus. Valeur par défaut : **/var/run/kav4fs**.
TraceEnable	Tenue du journal de trace. Kaspersky Anti-Virus enregistre dans le registre du tracé tous les événements. Les fichiers du registre du tracé sont conservés dans le répertoire spécifié par le paramètre TraceFolder. Les valeurs possibles comprennent : **yes** – maintenir à jour le registre du tracé ;

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
	no – ne pas maintenir à jour le registre du tracé. Valeur par défaut : **yes**.
TraceFolder	Répertoire dans lequel Kaspersky Anti-Virus enregistre les fichiers du registre du tracé. Si vous spécifiez un autre répertoire, assurez-vous qu'il est disponible en lecture et modification pour le compte avec les droits duquel fonctionne Kaspersky Anti-Virus. Valeur par défaut : **/var/log/kaspersky/kav4fs**.
TraceLevel	Niveau de détails du registre du tracé Les valeurs possibles comprennent : **Fatal**. Evénements critiques. **Error**. Erreurs. **Warning**. Evénements importants. **Info**. Evénements d'information. **Debug**. Informations de mise au point. Le niveau le plus détaillé est **Informations de débogage**, avec lequel tous les événements sont enregistrés dans le registre ; le niveau le moins détaillé est **Evénements critiques**, avec lequel seuls les événements critiques sont enregistrés dans le registre. Faites attention à ce que le registre du tracé peut consommer beaucoup d'espace disque. Si, après avoir activé la création du registre du tracé, vous ne modifiez pas les paramètres du registre, Kaspersky Anti-Virus tracera les sous-systèmes de Kaspersky Anti-Virus avec le niveau de détails **Informations de débogage**. Valeur par défaut : **Error**.
MaxFileNameLength	Longueur maximum du chemin d'accès complet au fichier à analyser, en octets. Si la longueur du chemin d'accès complet au fichier à analyser dépasse la valeur de ce paramètre, la tâche d'analyse à la demande ignore ce fichier et si la valeur du paramètre**BlockFilesGreaterMAxFileName** est **yes**, la tâche de protection en temps réel bloque l'accès au fichier. Valeurs possibles : **4096 – 33554432**. Valeur par défaut : **16384**.
BlockFilesGreaterMaxFileName	Blocage de l'accès au fichier dont le chemin d'accès est plus long que la valeur du paramètre **MaxFileNameLength**. Les tâches d'analyse à la demande ignorent ces fichiers, quelle que soit la valeur du paramètre **BlockFilesGreaterMaxFileName**. Les valeurs possibles comprennent : **yes** : la tâche de protection en temps réel bloque l'accès au fichier. **no** : l'accès n'est pas bloqué. Valeur par défaut : **yes**.

PARAMETRES DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Cette section décrit les paramètres du fichier de configuration que vous pouvez utiliser pour configurer les paramètres de la quarantaine et du répertoire de sauvegarde.

La spécification du fichier de configuration, leurs valeurs possibles et les valeurs par défaut sont données dans le tableau suivant.

En spécifiant les paramètres dans le fichier, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Tableau 26. Paramètres de la quarantaine et du dossier de sauvegarde

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
QuarantineFolder	Répertoire de sauvegarde des objets mis en quarantaine et des objets réservés. Vous pouvez spécifier le répertoire de sauvegarde autre que celui spécifié par défaut. Pour le répertoire de sauvegarde, vous pouvez utiliser les répertoires sur tous dispositifs du serveur. Il est déconseillé de spécifier les répertoires placés sur les ordinateurs distants, par exemple, montés via les protocoles SMB/CIFS et NFS. Kaspersky Anti-Virus commencera à mettre les objets dans le répertoire spécifié par le paramètre, après que vous aurez importé les paramètres depuis le fichier dans Kaspersky Anti-Virus à l'aide de la commande -T --set-settings, arrêté et relancé Kaspersky Anti-Virus. Si le répertoire spécifié n'existe pas ou n'est pas disponible, Kaspersky Anti-Virus utilisera le répertoire de sauvegarde installé par défaut. Valeur par défaut : **/var/opt/kaspersky/kav4fs/quarantine/**.
QuarantineSizeLimit	Taille maximum du répertoire de sauvegarde. La valeur de ce paramètre détermine le volume maximum des données dans le répertoire de sauvegarde. Faites attention à ce que une fois la taille maximum du répertoire de sauvegarde atteinte, Kaspersky Anti-Virus ne met plus les objets en quarantaine et ne réserve plus les objets avant leur réparation ou suppression. Dans le registre de Kaspersky Anti-Virus est enregistré l'événement QuarantineSizeLimitReached signalant que la taille maximum du répertoire de sauvegarde est atteinte. Si la valeur de ce paramètre est égale à zéro, la taille maximale du référentiel n'est pas définie. Spécifiez la valeur en octets. Valeurs possibles : 0 à $1,8*10^{19}$ Valeur par défaut : **1073741824**.
QuarantineSoftSizeLimit	Taille du répertoire de sauvegarde recommandée. La valeur de ce paramètre détermine le volume total recommandé des données dans le répertoire de sauvegarde. Ce paramètre est purement informatif. Il ne limite pas la taille du répertoire de sauvegarde, mais il permet à l'administrateur d'analyser l'état du répertoire de sauvegarde. Une fois la taille du répertoire de sauvegarde recommandée atteinte, Kaspersky Anti-Virus continue de mettre les objets en quarantaine et de réserver les objets avant leur réparation ou suppression. Dans le registre de Kaspersky Anti-Virus, est enregistré l'événement QuarantineSoftSizeLimitExceeded signalant que la taille du répertoire de sauvegarde recommandée est atteinte. Si la valeur de ce paramètre est égale à zéro, la taille recommandée du référentiel n'est pas définie. Spécifiez la valeur en octets. Valeurs possibles : 0 à $1,8*10^{19}$ Valeur par défaut : **858993459**.

LES PARAMETRES DU JOURNAL DES EVENEMENTS

Cette rubrique décrit les paramètres du fichier de configuration du journal des événements de Kaspersky Anti-Virus.

En cas de modification des paramètres dans le fichier, respectez les règles de modification des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Tableau 27. Les paramètres du journal des événements

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
EventStorageFolder	Répertoire du journal des événements. Kaspersky Anti-Virus y consigne les informations relatives aux événements et les informations de service du journal des événements. Vous pouvez consulter les informations relatives aux événements consignés dans ces fichiers à l'aide de l'instruction -E --query (cf. page 120). Vous ne pouvez pas modifier ce paramètre. Valeur par défaut : **/var/opt/kaspersky/kav4fs/db/event_storage**.
RotateMethod	Kaspersky Anti-Virus exécute la rotation des événements : suppression (transfert) partielle des informations relatives aux événements hors du répertoire EventStorageFolder. La méthode de rotation RotateMethod accepte les valeurs suivantes : **Erase** (supprimer). Kaspersky Anti-Virus supprime les informations relatives aux événements du journal à l'échéance de la période RotatePeriod ou lorsque le volume d'informations dépasse la valeur maximum définie par le paramètre EventStorageMaxSize. **Move** (déplacer). À l'issue de la période RotatePeriod ou lorsque le volume d'informations relatives aux événements dépasse la valeur maximum définie par le paramètre EventStorageMaxSize, Kaspersky Anti-Virus transfère les informations du journal vers le répertoire RotateMoveFolder et conserve les données dans le fichier de rotation. Le nom du fichier de rotation contient l'heure d'enregistrement de l'événement le plus ancien consigné dans le journal ; le format est EventStorage-AAA-MM-JJ-hh-mm-ss.db. À chaque rotation, Kaspersky Anti-virus conserve les informations relatives aux événements dans un fichier distinct. Les fichiers créés peuvent être de taille différente si la rotation s'opère selon le paramètre RotatePeriod ou le paramètre EventStorageMaxSize ou si elle est exécutée manuellement par l'utilisateur. La taille d'un fichier ne dépasse pas la moitié de la taille définie par le paramètre EventStorageMaxSize (à 100 Ko près). Vous pouvez supprimer les fichiers de rotation ou créer des copies de sauvegarde de ceux-ci sur un périphérique externe. Valeur par défaut : **Erase**.
RotateMoveFolder	Répertoire vers lequel Kaspersky Anti-Virus transfère les informations relatives aux événements quand le mode de rotation Move a été choisi. Ce répertoire doit se trouver sur une partition du disque dur et dans un point de montage (mount point) avec le répertoire EventStorageFolder. Il doit exister et être accessible en écriture. Si ces conditions ne sont pas remplies, Kaspersky Anti-Virus ne transfère pas les informations relatives aux événements mais les supprime du répertoire EventStorageFolder. Valeur par défaut : non spécifié.
RotatePeriod	Période de rotation ; accepte les valeurs suivantes : **Daily** (chaque jour). Kaspersky Anti-Virus réalise la rotation des événements tous les jours à minuit. **Weekly** (chaque semaine). Kaspersky Anti-Virus réalise la rotation des événements tous les lundi à minuit. **Monthly** (chaque mois). Kaspersky Anti-Virus réalise la rotation des événements le premier de chaque mois à minuit. **Never**. La période de rotation des événements n'a pas été définie. Valeur par défaut : **Never**.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
EventStorageMaxSize	Taille maximale du répertoire du journal des événements. Lorsque le volume d'informations du répertoire EventStorageFolder dépasse la taille définie par ce paramètre, Kaspersky Anti-Virus assure la rotation des événements. Ce paramètre peut-être appliqué en même temps que le paramètre RotatePeriod afin de limiter davantage la taille du répertoire du journal des événements. Spécifiez la valeur en octets. **0** : la taille maximale du répertoire du journal des événements n'a pas été définie. Il est déconseillé d'attribuer une valeur nulle ou élevée à ce paramètre car un volume d'informations élevé dans le répertoire EventStorageFolder peut ralentir Kaspersky Anti-Virus. Valeur par défaut : **1073741824**.

PARAMETRES DE NOTIFICATION ET ACTIONS A REALISER EN FONCTION DES EVENEMENTS

Cette rubrique décrit les paramètres du fichier de configuration des notifications et des actions en fonction des événements.

En cas de modification des paramètres dans le fichier, respectez les règles de modification des fichiers de configuration ini de Kaspersky Anti-Virus (cf. page 134).

Tableau 28. Paramètres de notification et actions à réaliser en fonction des événements

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
EnableSmtp	Fait activer / désactiver l'envoi de notifications par courrier électronique. **yes** : l'envoi de notifications par courrier électronique est activé. **no** : l'envoi de notifications par courrier électronique est désactivé. Valeur par défaut : **no**.
EnableActions	Fait activer / désactiver l'exécution d'actions en fonction des événements. **yes** : l'exécution d'action en fonction des événements est activée. **no** : l'exécution d'action en fonction des événements est désactivée. Valeur par défaut : **no**.
[CommonSmtpSettings] Paramètres généraux des notifications	
Sender	Courrier électronique de l'expéditeur. Valeur par défaut : non spécifié.
DefaultRecipients	Adresse du destinataire issue d'une liste " globale ". Les destinataires de cette liste peuvent recevoir n'importe quelle notification sur les événements décrits dans le fichier. Il est possible d'indiquer plusieurs destinataires : répétez le paramètre autant de fois qu'il y a d'adresses. Exemple : DefaultRecipients=admin1@example.com DefaultRecipients=admin2@example.com Vous pouvez activer ou désactiver l'utilisation de cette liste de manière individuelle pour chaque notification à l'aide du paramètre UseRecipientList. Valeur par défaut : non spécifié.
Mailer	Client de messagerie utilisé pour envoyer les notifications. Il peut avoir les valeurs suivantes : **Internal**. Client de messagerie intégré de Kaspersky Anti-Virus. Kaspersky Anti-Virus possède son propre client de messagerie pour l'envoi de notifications via le protocole SNMP. Vous pouvez choisir cette option si l'envoi de messages électroniques ne requiert pas la vérification de l'authenticité. Définissez les paramètres du client de messagerie dans la rubrique [CommonSmtpSettings:InternalMailerSettings]. **Sendmail**. Client de messagerie Sendmail. Choisissez cette option si Sendmail est installé et configuré sur le serveur à protéger. Définissez ensuite le paramètre SendmailPath. Valeur par défaut : **Internal**.
SendmailPath	Chemin d'accès au fichier exécutable Sendmail, inclut les paramètres Sendmail : -t : argument obligatoire (prendre la liste des destinataires dans le message) ; -i : clé facultative (ne pas tracer un point unique) (.) dan la ligne en tant que symbole de fin du message). Valeur par défaut : **/usr/sbin/sendmail -t -i**.
[CommonSmtpSettings:InternalMailerSettings] Paramètres du client de messagerie intégré de Kaspersky Anti-Virus.	

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
SmtpServer	Adresse du serveur SMTP Valeur par défaut : non spécifié.
SmtpPort	Port du serveur SMTP Valeur par défaut : **25**.
SmtpQueueFolder	Répertoire pour l'enregistrement de la file des messages sortant. Valeur par défaut : **/var/opt/kaspersky/kav4fs/db/notifier**.
ConnectionTimeout	Délai d'attente, en secondes, de la réponse du serveur. Valeur par défaut : **10**.
[SmtpNotification] Paramètres de notification selon l'événement, texte du message. Créez une rubrique [SmtpNotification] pour chaque événement pour lequel vous souhaitez configurer une notification.	
Recipients	Liste " locale " des destinataires : les destinataires de la liste reçoivent uniquement le message décrit dans la rubrique [SmtpNotification]. Il est possible d'indiquer plusieurs destinataires : répétez le paramètre autant de fois qu'il y a d'adresses. Exemple : Recipients=admin3@example.com Recipients=admin4@example.com Vous pouvez activer ou désactiver l'utilisation de cette liste de manière individuelle pour chaque notification à l'aide du paramètre UseRecipientList. Valeur par défaut : non spécifié.
UseRecipientList	Règle d'utilisation des listes de destinataires. Définit les destinataires de quelle liste recevront le message : **Local**. Le message est envoyé aux destinataires de la liste locale ; **Global**. Le message est envoyé aux destinataires de la liste globale ; **Both**. Les messages sont envoyés aux destinataires des deux listes. Valeur par défaut : **Global**.
Subject	Le champ " Objet " du message. Si vous ne définissez pas ce paramètre, le champ " Objet " contiendra le nom de l'événement. Valeur par défaut : non spécifié.
Body	Corps du message. Vous pouvez ajouter des macros au corps du message (cf. rubrique " Utilisation de macros " cf. page 73). Valeur par défaut : non spécifié.
EventName	Nom de l'événement qui déclenchera l'envoi d'une notification. Valeur par défaut : non spécifié.
Enable	Fait activer / désactiver l'envoi de notification : **yes** : l'envoi de notifications est activé. **no** : l'envoi de notifications es désactivé. Valeur par défaut : **no**.

PARAMÈTRE	SPÉCIFICATION ET VALEURS POSSIBLES
`[Actions]` Paramètres des actions en fonction de l'événement. Créez une rubrique `[Actions]` pour chaque événement pour lequel vous souhaitez configurer une action.	
`Command`	Script Shell contenant les instructions ; exécuté lorsque l'événement survient. Par exemple, vous pouvez configure l'envoi de SMS et de notification via le système de messagerie instantanée (tel que jabber) et intégrer Kaspersky Anti-Virus à divers systèmes de surveillance. Vous pouvez modifier les paramètres du pare-feu ou couper le serveur Samba en cas d'épidémie de virus (plusieurs événements du style " Une menace a été découverte "). Vous pouvez ajouter des macros au script (cf. rubrique " Utilisation de macros " cf. page 73). Valeur par défaut : non spécifié.
`EventName`	Nom de l'événement qui déclencher l'exécution de l'action. Valeur par défaut : non spécifié.
`Enable`	Fait activer / désactiver l'exécution de l'action décrite dans la rubrique [Actions]: **yes** : l'exécution de l'action est activée. **no** : l'exécution de l'action est désactivée. Valeur par défaut : **no**.

ADMINISTRATION DE KASPERSKY ANTI-VIRUS A L'AIDE DE KASPERSKY ADMINISTRATION KIT

Si Kaspersky Administration Kit pour l'administration centralisée des applications antivirus est utilisé au sein de votre entreprise, vous pouvez administrer la protection des serveurs sur lesquels est installé Kaspersky Anti-Virus, via la Console d'administration Kaspersky Administration Kit.

Vous pouvez consulter l'état de la protection des ordinateurs, configurer les paramètres généraux de la protection des serveurs, créer des stratégies, créer des tâches d'analyse à la demande, de mise à jour et d'installation des fichiers de licence.

DANS CETTE SECTION

CONSULTATION DU STATUT DE LA PROTECTION DU SERVEUR

Dans la Console d'administration, vous pouvez consulter le statut de la protection du serveur choisi, le statut général du point de vue de la sécurité antivirus et son accessibilité.

Pour consulter le statut de la protection du serveur :

1. Dans l'arborescence de la console, déployez le noeud **Ordinateurs administrés** et sélectionnez le groupe auquel appartient le serveur à protéger.

2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.

3. Dans la boîte de dialogue **Propriétés: <Nom de l'ordinateur>**, ouvrez l'onglet **Protection**.

Dans l'onglet **Protection**, sont affichées les informations suivantes sur le serveur protégé :

*Tableau 29. Informations sur l'état de la protection du serveur dans la boîte de dialogue **Propriétés : <Nom de l'ordinateur>***

CHAMP	DESCRIPTION
Statut de l'ordinateur	Statut du serveur protégé du point de vue de la sécurité antivirus. Pour de plus amples informations, consultez le site du Service du Support Technique de Kaspersky Lab, code de l'article : 987.
Etat de PTR	Affiche l'état de la protection en temps réel, par exemple, *En cours d'exécution*, *Arrêtée*, *Suspendue*.
Dernière analyse complète	Date et heure de la dernière tâche d'analyse à la demande exécutée.
Virus trouvés	Nombre total de programmes malveillants (signatures de menaces) détectés sur le serveur à protégé (compteur de menaces détectées) dès l'installation de Kaspersky Anti-Virus ou dès la mise à zéro du compteur. Pour mettre à zéro le compteur, cliquez sur le bouton **Remettre à zéro**.

BOITE DE DIALOGUE " PARAMETRES DE L'APPLICATION "

Dans la boîte de dialogue **Paramètres de l'application**, vous pouvez effectuer l'administration de Kaspersky Anti-Virus à distance et sa configuration sur le serveur à protéger choisi.

Pour ouvrir la boîte de dialogue Paramètres de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés**.
2. Déployez le groupe dont le serveur à protéger fait partie, et sélectionnez le nœud **Postes clients**.
3. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.
4. Dans la boîte de dialogue **Propriétés** : <**Nom de l'ordinateur**> dans l'onglet **Applications**, sélectionnez **Kaspersky Anti-Virus 8.0 for Linux File Server** dans la liste des applications installées et cliquez sur le bouton **Propriétés**.

CREATION ET CONFIGURATION DES TACHES

Vous pouvez créer des tâches locales, des tâches pour plusieurs ordinateurs sélectionnés et des tâches de groupe de types suivants :

- mise à jour ;
- recul de mise à jour des bases ;
- analyse à la demande ;
- installation du fichier de licence.

Vous créez des tâches locales pour le serveur à protéger sélectionné dans la boîte de dialogue **Tâches**, des tâches de groupe dans le nœud **Tâches de groupe**, du groupe sélectionné, des tâches pour les ordinateurs sélectionnés dans le nœud **Tâches pour les sélections d'ordinateurs**.

Les informations générales sur les tâches de Kaspersky Administration Kit sont données dans le document *Kaspersky Administration Kit. Manuel d'administrateur.*

CREATION D'UNE TACHE

Lorsque vous gérez Kaspersky Anti-Virus via Kaspersky Administration Kit, vous avez la possibilité de créer les types de tâche suivantes:

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe, définies pour les ordinateurs appartenant à un groupe d'administration donné;
- des tâches pour une sélection d'ordinateurs, définies pour certains ordinateurs d'un groupe d'administration donné;
- les tâches de Kaspersky Administration Kit – les tâches spécifiques du Serveur de mises à jour : les tâches de réception des mises à jour, les tâches de copie de sauvegarde et les tâches d'envoie des rapports.

> Les tâches pour une sélection d'ordinateurs ne sont exécutées que sur les ordinateurs faisant partie de la sélection. La tâche d'installation à distance définie pour les ordinateurs d'un groupe ne sera pas appliquée aux nouveaux ordinateurs clients qui seraient ajoutés à ce groupe. Il faudra donc créer une nouvelle tâche ou modifier comme il se doit les paramètres de la tâche existante.

Les tâches peuvent être associées aux actions suivantes :

- configurez les paramètres de la tâche ;
- surveillance de l'exécution de la tâche;
- la copie et le transfert de la tâche d'un groupe dans un autre, ainsi que la suppression à l'aide des commandes standards du menu contextuel **Copier** / **Coller**, **Couper** / **Coller** et **Supprimer**, des points analogues dans le menu **Action**.
- importation et exportation de tâches.

Pour de plus amples informations concernant le fonctionnement des tâches, référez-vous au Manuel de référence de Kaspersky Administration Kit.

Pour créer une tâche locale, procédez comme suit:

1. Ouvrez la fenêtre des propriétés du poste client, dans l'onglet **Tâches**.
2. Cliquez sur le bouton **Ajouter**.
3. Finalement, l'Assistant de création d'une nouvelle tâche (cf. page 173) se lance, suivez ses consignes.

Pour créer une tâche de groupe, procédez comme suit :

1. Ouvrez la console d'administration de Kaspersky Administration Kit.
2. Dans **Ordinateurs administrés**, ouvrez le dossier portant le nom du groupe souhaité.
3. Dans le groupe sélectionné, ouvrez le sous-dossier **Tâches de groupe**, dans lequel toutes les tâches créées pour le groupe seront présentées.
4. Cliquez sur le lien **Créer une tâche** dans le panneau des tâches pour lancer l'assistant de création d'une nouvelle tâche. Pour de plus amples informations sur la création des tâches de groupe, référez-vous au Manuel de référence de Kaspersky Administration Kit.

Pour créer une tâche destinée à une sélection d'ordinateurs (tâche Kaspersky Administration Kit), procédez comme suit:

1. Ouvrez la Console d'administration de Kaspersky Administration Kit.

2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** (**Tâches Kaspersky Administration Kit**).

3. Cliquez sur le lien **Créer une tâche** dans le panneau des tâches pour lancer l'assistant de création d'une nouvelle tâche. Pour de plus amples informations sur la création de tâches Kaspersky Administration Kit et de tâches destinées à une sélection d'ordinateurs, référez-vous au Manuel de référence de Kaspersky Administration Kit.

ASSISTANT POUR LA CREATION D'UNE TACHE LOCALE

L'Assistant pour la création d'une tâche locale peut être lancé depuis le menu contextuel ou la fenêtre des propriétés du poste client.

L'Assistant est une suite des fenêtres (étapes), où la commutation entre elles s'effectue à l'aide des boutons **Précédent** et **Suivant**, et la fin de l'Assistant - à l'aide du bouton **Terminer**. Pour arrêter le programme à n'importe quelle étape, cliquez sur **Annuler**.

ETAPE 1. SAISIE DES INFORMATIONS GENERALES SUR LA TACHE

La première fenêtre de l'Assistant nécessite l'encodage du nom de la tâche (champ **Nom**).

ETAPE 2. CHOIX DE L'APPLICATION ET DU TYPE DE TACHE

Cette étape vous permet d'indiquer l'application, pour laquelle la tâche se crée : Kaspersky Anti-Virus 8.0 for Linux File Server ou l'Agent d'administration. Outre cela, il est nécessaire de sélectionner le type de tâche.

Pour Kaspersky Anti-Virus 8.0 il est possible de créer des tâches suivantes :

- La recherche de virus : une tâche d'analyse sur la présence d'éventuels virus dans lez zones indiquées par l'utilisateur.
- La mise à jour : une tâche de réception et d'application du paquet des mises à jour pour l'application.
- Annulation de la mise à jour : une tâche d'annulation de la dernière mise à jour effectuée de l'application.
- Installation du fichier de licence : une tâche d'installation du fichier de licence d'une nouvelle licence nécessaire pour le fonctionnement de l'application.

ETAPE 3. CONFIGURATION DES TACHES

Selon le type de tâche sélectionné lors de l'étape précédente, le contenu de la fenêtre des paramètres varie.

Pour la tâche d'analyse à la demande il faut :

- composer la zone d'analyse (à la page 174) et définir les paramètres d'analyse (cf. page 175) ;
- définir les zones d'exclusion (cf. page 176).

Pour la tâche de mise à jour des bases et des modules de l'application il faut :

- indiquer une source (cf. page 176), de laquelle les mises à jour seront téléchargées, et définir les paramètres de connexion avec la source de mises à jour ;
- sélectionner le type de mises à jour (cf. page 177).

La tâche d'annulation de mises à jour n'a pas de configurations spécifiques.

Il faut indiquer le chemin d'accès au fichier de licence pour une tâche d'installation du fichier de licence.

Pour ce faire, exécutez les opérations suivantes :

1. Cliquez sur le bouton **Parcourir** dans la fenêtre de l'Assistant de création d'une tâche.
2. Choisissez le fichier avec extension .key reçu lors de l'achat de Kaspersky Anti-Virus.

ETAPE 4. CONFIGURATION DE LA PROGRAMMATION

Configurez les paramètres de l'horaire de la tâche (cf. section " Configuration de l'horaire de la tâche à l'aide de Kaspersky Administration Kit " cf. page 178). Vous pouvez configurer l'horaire pour tous les types sauf les tâches d'installation de la licence.

ETAPE 5. FIN DE L'ASSISTANT

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

CONFIGURATION DES TACHES

Une fois la tâche créée, vous pouvez :

- modifier les paramètres de la tâche ;
- modifier l'horaire de la tâche, activer / désactiver l'exécution d'une tâche selon l'horaire.

Pour configurer les paramètres d'une tâche, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés** et sélectionnez le groupe dont le serveur à protéger fait partie.
2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de l'ordinateur**, dans l'onglet **Tâches**, ouvrez le menu contextuel à la tâche que vous voulez configurer, et sélectionnez la commande **Propriétés**.
4. Dans la fenêtre ouverte **Propriétés de la tâche** configurez les paramètres de la tâche.
5. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

COMPOSITION DE LA ZONE D'ANALYSE

Zone d'analyse : les objets du système de fichiers du serveur analysé par Kaspersky Anti-Virus. Pour que les tâches de protection en temps réel et les tâches d'analyse à la demande puissent fonctionner normalement, il faut au moins une zone d'analyse.

Pour créer une zone d'analyse, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Paramètres** dans le groupe **Zone d'analyse** cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre ouverte **<Nouvelle zone d'analyse>**, procédez comme suit :

a. Dans le champ **Nom de la zone**, attribuez un nom au secteur à créer. Ce nom sera affiché dans la liste des secteurs à analyser dans la fenêtre **Zones d'analyse**.

b. Dans la liste à gauche ouverte choisissez le type de la ressource.

Si vous avez sélectionné le type de la ressource **Partagée** ou **Distante**, dans la liste à droite ouverte, sélectionnez le protocole de l'accès à distance qui est utilisé pour accéder à la ressource (**Samba** ou **NFS**).

c. Dans le champ de saisie du chemin d'accès, saisissez le chemin d'accès au répertoire à analyser.

Si vous avez sélectionné le type de la ressource **Partagée** ou **Distante**; en tant que chemin d'accès, vous pouvez spécifier le chemin d'accès au répertoire ou le nom de la ressource, par exemple, **MySamba**. Si vous avez sélectionné **Toutes partagées** ou **Toutes distantes**, laissez le champ de saisie vide.

d. Dans le groupe **Masques** cliquez sur le bouton **Ajouter**, et dans la fenêtre ouverte **Masque de l'objet** définissez les modèles des noms ou des chemins d'accès des objets analysés.

> Les masques Shell vous permettent de spécifier le modèle du nom du fichier pour l'analyse par Kaspersky Anti-Virus.
>
> Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire qui définit la zone d'analyse ou de protection.
>
> Ajoutez le préfixe **re:** aux expressions régulières.

e. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

4. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés de la tâche**, pour enregistrer les modifications.

Kaspersky Anti-Virus analysera des objets dans les secteurs spécifiés dans l'ordre d'énumération de ces secteurs dans la liste. Si vous souhaitez définir des paramètres de protection différents pour le répertoire parent et les sous-répertoires, placez le sous-répertoire avant le répertoire parent dans la liste.

Pour déplacer les lignes dans lesquelles sont spécifiés les chemins d'accès, au début ou à la fin de la liste, utilisez les boutons **Monter** et **Descendre**.

CONFIGURATION DES PARAMETRES DE SECURITE

Par défaut, Kaspersky Anti-Virus applique des paramètres de sécurité à toutes les zones d'analyse. Ces paramètres sont recommandés par les spécialistes de Kaspersky Lab. Vous pouvez configurer les paramètres de sécurité selon vos exigences.

➧ *Pour configurer les paramètres de sécurité de la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés de la tâche**.

2. Sous l'onglet **Paramètres** sélectionnez la zone d'analyse dans le groupe **Zones d'analyse** et cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre ouverte sous l'onglet **Paramètres** dans le groupe **Analyser les objets composés** cochez la case en regard des types des objets composés (cf. page 189), qui seront analysés par Kaspersky Anti-Virus.

4. Sous l'onglet **Paramètres** dans le groupe **Optimisation d'analyse** définissez la durée maximale de l'analyse de l'objet (cf. page 189) et la taille maximale de l'objet analysé (cf. page 190).

5. Dans l'onglet **Actions** sélectionnez actions à effectuer sur des objets infectés (cf. page 186), et actions à effectuer sur des objets suspects (cf. page 187).

6. Sous l'onglet **Zone d'exclusion** définissez les objets exclus de l'analyse selon le nom (cf. page 188), et les objets exclus de l'analyse selon le nom de la menace détectée (cf. page 188).

La zone d'exclusion, définie dans les paramètres de sécurité de la zone d'analyse sélectionnée, se propage uniquement sur cette zone.

7. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CREATION D'UNE ZONE D'EXCLUSION

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone d'analyse.

Vous pouvez indiquer les modèles des noms ou des chemins d'accès exclus de la zone d'analyse. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone d'analyse que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire contenant l'objet à exclure.

Pour créer une zone d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Zones d'exclusion** cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre ouverte **<Nouvelle zone d'exclusion>**, procédez comme suit :
   a. Dans le champ **Nom de la zone**, attribuez un nom au secteur à créer. Ce nom sera affiché dans la liste des zones à exclure dans la fenêtre **Zones d'exclusion**.
   b. Dans la liste à gauche ouverte choisissez le type de la ressource.

      Si vous avez sélectionné le type de la ressource **Partagée** ou **Distante**, dans la liste à droite ouverte, sélectionnez le protocole de l'accès à distance qui est utilisé pour accéder à la ressource (**Samba** ou **NFS**).
   c. Dans le champ de saisie du chemin d'accès, saisissez le chemin d'accès au répertoire à analyser.

      Si vous avez sélectionné le type de la ressource **Partagée** ou **Distante**; en tant que chemin d'accès, vous pouvez spécifier le chemin d'accès au répertoire ou le nom de la ressource, par exemple, **MySamba**. Si vous avez sélectionné **Toutes partagées** ou **Toutes distantes**, laissez le champ de saisie vide.
   d. Dans le groupe **Masques** cliquez sur le bouton **Ajouter**, et dans la fenêtre ouverte **Masque de l'objet** définissez les modèles des noms ou des chemins d'accès des objets à exclure de l'analyse.
   e. Cliquez sur le bouton **OK**, pour enregistrer les modifications.
4. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés de la tâche**, pour enregistrer les modifications.

SELECTION DE LA SOURCE DES MISES A JOUR

La source des mises à jour (cf. page 190) est la source qui contient les mises à jour des bases de Kaspersky Anti-Virus. Les serveurs HTTP ou FTP, les répertoires locaux ou de réseau peuvent être utilisés en tant que source de mise à jour.

Les serveurs de mises à jour de Kaspersky Lab sont une source principale de mises à jour. Il s'agit de sites Internet spéciaux qui hébergent les mises à jour des bases et des modules de programme pour tous les logiciels de Kaspersky Lab.

Pour sélectionner la source de la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Sources des mises à jour** sélectionnez une source des mises à jour (cf. page 190).
3. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

Pour ajouter une source d'utilisateur des mises à jour, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Sources des mises à jour** sélectionnez l'option **Autres répertoires dans le réseau local ou mondial** et cliquez sur le bouton **Personnaliser**.
3. Dans la fenêtre ouverte **Sources des mises à jour**, cliquez sur le bouton **Ajouter** et saisissez le chemin d'accès au répertoire dans lequel sont sauvegardés les mises à jour ou l'adresse du serveur FTP ou HTTP.
4. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

Pour configurer les paramètres de connexion avec les sources des mises à jour, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Sources des mises à jour** cliquez sur le bouton **Paramètres de connexion**.
3. Dans la fenêtre ouverte spécifiez les paramètres suivants :
   a. mode du serveur FTP (cf. page 190)
   b. temps d'attente de la réponse de la part de la source des mises à jour lors de la connexion avec le serveur FTP (cf. page 190)
   c. utilisation du serveur proxy (cf. page 191)
   d. paramètres du serveur proxy (cf. page 191)
   e. vérification de l'authenticité lors de l'accès au serveur proxy (cf. page 191)
   f. emplacement de l'ordinateur protégé
4. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

SELECTION DE TYPE DES MISES A JOUR

La tâche des mises à jour de Kaspersky Anti-Virus exécute une des actions suivantes :

1. Le téléchargement et l'installation des bases.
2. La copie des mises à jour des modules de Kaspersky Anti-Virus. Avec cela, les modules sont uniquement téléchargés dans le répertoire indiqué, et l'installation des modules ne s'exécute pas.
3. Copie des mises à jour selon la liste indiquée. Avec cela, uniquement les modules définis par la liste sont téléchargés. L'installation des modules ne s'exécute pas.

Pour sélectionner un type des mises à jour, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés de la tâche**.
2. Sous l'onglet **Type des mises à jour** choisissez le type des mises à jour (cf. page 191) de la liste déroulante.

3. Si vous avez sélectionné **Copie de toutes les mises à jour accessibles de l'application**, spécifiez le répertoire pour enregistrer les mises à jour (cf. page 191) dans le champ **Sauvegarder les mises à jour dans un directoire**.

4. Si vous avez sélectionné **Copie des mises à jour selon la liste indiquée**, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Copier les mises à jour suivantes**.

   b. Dans la fenêtre ouverte indiquez le nom de la mise à jour.

   > Vous pouvez consulter les noms des mises à jour dans le document http://support.kaspersky.ru/downloads/updater/update_components_21112008.pdf, publié sur le site du Service du Support Technique de Kaspersky Lab.

   c. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

   d. Répétez les étapes a-c autant qu'il faut.

5. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CONFIGURATION DE L'HORAIRE DE LA TACHE A L'AIDE DE KASPERSKY ADMINISTRATION KIT

Vous pouvez configurer l'horaire de la tâche lors de sa création, ainsi que plus tard, dans la boîte de dialogue **Propriétés de la tâche**. Cette section décrit la procédure de configuration de l'horaire dans la boîte de dialogue **Propriétés de la tâche**. Dans l'assistant de création des tâches, la configuration de l'horaire se fait de la manière analogue.

CREATION DE LA REGLE DU LANCEMENT DE LA TACHE

Vous pouvez créer *les règles du lancement de la tâche* : un seul lancement de la tâche à la date et à l'heure déterminées ; lancement de la tâche à la fréquence spécifiée (par exemple, toutes les semaines ou tous les mois) ; lancement de la tâche après chaque mise à jour des bases ou lors du lancement de Kaspersky Anti-Virus.

Pour créer la règle du lancement de la tâche, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés**.

2. Déployez le groupe dont le serveur à protéger fait partie, et sélectionnez le nœud **Postes clients**.

3. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.

4. Dans la boîte de dialogue **Propriétés de l'ordinateur**, ouvrez l'onglet **Tâches**. Ouvrez le menu contextuel à la tâche que vous voulez configurer, et sélectionnez la commande **Propriétés**.

5. Dans la boîte de dialogue **Propriétés de la tâche**, ouvrez l'onglet **Programmation**.

6. Activez l'horaire de la tâche, en cochant la case **Exécuter de manière planifiée** en bas de la fenêtre.

7. Cliquez sur le bouton **Ajouter** et dans la fenêtre ouverte **Création d'une règle de lancement de la tâche** procédez comme suit :

   a. Sélectionnez le type de la règle dans la liste homonyme déroulante :

      - **Au moment prédéfini**, pour configurer le lancement de la tâche à la date spécifiée ou à la fréquence spécifiée, par exemple, toutes les semaines.

- **À la mise à jour de la base antivirus**, pour lancer la tâche après chaque mise à jour des bases.
- **Au lancement de l'Anti-Virus**, pour lancer la tâche après chaque lancement de Kaspersky Anti-Virus.

b. Si vous avez sélectionné le mode **Au moment prédéfini**, effectuez une des actions suivantes :

- Sélectionnez le mode **À l'heure indiquée** et indiquez la date et l'heure précises du lancement de la tâche.
- Sélectionnez le mode **Périodiquement** et spécifiez la fréquence du lancement de la tâche : à intervalle de la quantité de minutes spécifiée, tous les jours, toutes les semaines, tous les mois ou tous les ans.

c. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

8. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CREATION DE LA REGLE DE SUSPENSION D'UNE TACHE

A l'aide de la règle de l'arrêt de la tâche, vous pouvez spécifier quand la tâche doit être arrêtée. En supplément, vous pouvez spécifier la période de temps durant laquelle la tâche ne peut pas être relancée selon l'horaire, par exemple, *arrêter la tâche à 08h00 le lundi et ne pas la relancer avant 18h00 le vendredi.*

➧ *Pour créer la règle d'arrêt de la tâche, procédez comme suit :*

1. Dans l'arborescence de la console, déployez le noeud **Ordinateurs administrés** et sélectionnez le groupe auquel appartient le serveur à protéger.
2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de l'ordinateur**, ouvrez l'onglet **Tâches**. Ouvrez le menu contextuel à la tâche que vous voulez configurer, et sélectionnez la commande **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de la tâche**, ouvrez l'onglet **Programmation**.
5. Activez l'horaire de la tâche, en cochant la case **Exécuter de manière planifiée** en bas de la fenêtre.
6. Cliquez sur le bouton **Ajouter** et dans la fenêtre ouverte **Créer une nouvelle règle de lancement d'une tâche** procédez comme suit :

a. Sélectionnez le type de la règle dans la liste homonyme déroulante :

- **Durée d'exécution ; temps avant le lancement**. Kaspersky Anti-Virus arrêtera la tâche à l'issue de la période de temps spécifiée depuis son lancement. En supplément, vous pouvez déterminer l'intervalle de temps depuis l'arrêt de la tâche durant lequel la tâche ne peut pas être relancée.
- **Heure d'arrêt ; temps avant le lancement**. Kaspersky Anti-Virus arrêtera la tâche à l'heure spécifiée. En supplément, vous pouvez déterminer l'intervalle de temps depuis l'arrêt de la tâche durant lequel la tâche ne peut pas être relancée.
- **Heure d'arrêt ; temps du prochain lancement**. Kaspersky Anti-Virus arrête l'exécution de la tâche à l'heure spécifiée ; vous pouvez déterminer le moment de temps quand la tâche doit être relancée.

b. Si vous avez sélectionné le mode **Durée de l'exécution; intervalle entre les lancements**, procédez comme suit :

- Dans le champ **Exécuter pas plus de, min**, spécifiez le temps maximal d'exécution de la tâche, en minutes.
- Dans le champ **Ne pas relancer pendant, min**, spécifiez l'intervalle de temps durant lequel la tâche ne peut pas être lancée.

c. Si vous avez sélectionné le mode **Heure d'arrêt ; temps avant le lancement**, procédez comme suit :

- Dans le champ **Heure d'arrêt d'une tâche** indiquez la date et l'heure quand la tâche doit être arrêtée.
- Dans la champ **Durée de la règle, sec** indiquez l'intervalle de temps pendant lequel la tâche ne peut pas être lancée.

d. Si vous avez sélectionné le mode **Heure de l'arrêt; heure du prochain lancement**, procédez comme suit :

- Dans le champ **Arrêter** indiquez la date et l'heure quand la tâche doit être arrêtée.
- Dans le champ **Rétablir**, spécifiez la date et l'heure où Kaspersky Anti-Virus pourra relancer la tâche suivant l'horaire.

e. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

7. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CREATION DE LA REGLE DE SUSPENSION DE LA TACHE

Si vous lancer la tâche après avoir appliqué la règle d'arrêt (cf. page 179), l'exécution de la tâche commence dès le début. Les règles de suspension permettent de reprendre l'exécution de la tâche dès le moment où elle a été suspendue.

Pour créer la règle de suspension de la tâche, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés** et sélectionnez le groupe dont le serveur à protéger fait partie.
2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur le serveur à protéger et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de l'ordinateur**, ouvrez l'onglet **Tâches**. Ouvrez le menu contextuel à la tâche que vous voulez configurer, et sélectionnez la commande **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de la tâche**, ouvrez l'onglet **Programmation**.
5. Activez l'horaire de la tâche, en cochant la case **Exécuter de manière planifiée** en bas de la fenêtre.
6. Cliquez sur le bouton **Ajouter** et dans la fenêtre ouverte **Création d'une règle de suspension de la tâche** procédez comme suit :

   a. Sélectionnez le type de la règle dans la liste homonyme déroulante :

   - **Durée d'exécution ; temps avant le lancement**. Kaspersky Anti-Virus va suspendre la tâche à l'issue de la période de temps spécifiée depuis son lancement. En supplément, vous pouvez déterminer l'intervalle de temps depuis la suspension de la tâche durant lequel la tâche ne peut pas être relancée.
   - **Heure de suspension ; temps avant le lancement**. Kaspersky Anti-Virus va suspendre la tâche à l'heure spécifiée. En supplément, vous pouvez déterminer l'intervalle de temps depuis la suspension de la tâche durant lequel la tâche ne peut pas être relancée.
   - **Heure de suspension ; temps du prochain lancement**. Kaspersky Anti-Virus suspend la tâche à l'heure spécifiée ; vous pouvez spécifier la période de temps, vous pouvez spécifier le moment de temps quand la tâche peut être relancée.

   b. Si vous avez sélectionné le mode **Durée d'exécution ; temps avant le lancement**, procédez comme suit :

   - Dans le champ **Exécuter pas plus de, min**, spécifiez le temps maximal d'exécution de la tâche, en minutes.

- Dans le champ **Ne pas relancer pendant, min**, spécifiez l'intervalle de temps durant lequel la tâche ne peut pas être lancée.

c. Si vous avez sélectionné le mode **Heure de suspension ; temps avant le lancement**, procédez comme suit :

- Dans le champ **Heure de suspension d'une tâche** indiquez la date et l'heure quand la tâche doit être suspendue.

- Dans la champ **Durée de la règle, sec** indiquez l'intervalle de temps pendant lequel la tâche ne peut pas être lancée.

d. Si vous avez sélectionné le mode **Heure de suspension ; temps du prochain lancement**, procédez comme suit :

- Dans le champ **Heure de suspension d'une tâche** indiquez la date et l'heure quand la tâche doit être suspendue.

- Dans le champ **Heure d'autorisation du lancement d'une tâche**, spécifiez la date et l'heure où Kaspersky Anti-Virus pourra relancer la tâche suivant l'horaire.

e. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

7. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CREATION ET CONFIGURATION DES STRATEGIES

Vous pouvez créer des stratégies Kaspersky Administration Kit communes pour gérer la protection de plusieurs serveurs sur lesquels est installé Kaspersky Anti-Virus.

La stratégie utilise les valeurs des paramètres qui y sont spécifiées pour tous les serveurs à protéger d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un seul groupe d'administration et les utiliser tour à tour. Dans la Console d'administration, la stratégie valable dans un groupe au moment en cours, possède le statut de **active**.

Kaspersky Anti-Virus pour la période de validité de la stratégie, utilise les valeurs des paramètres à côté desquels, dans les propriétés de la stratégie, vous avez mis 🔒, au lieu des valeurs de ces paramètres valables avant l'application de la stratégie. Kaspersky Anti-Virus n'utilise pas les valeurs des paramètres à côté desquels, dans les propriétés de la stratégie, vous avez mis 🔓. Lorsque l'action de la stratégie termine, les paramètres dont les valeurs ont été modifiées par la stratégie, gardent les valeurs qui étaient valables lors de son application.

A l'aide des stratégies, vous pouvez configurer les paramètres généraux de Kaspersky Anti-Virus et les paramètres de mise à jour.

DANS CETTE SECTION

CRÉATION D'UNE STRATÉGIE

➧ *Pour créer une stratégie pour un groupe des serveurs sur lesquels est installé Kaspersky Anti-Virus, procédez comme suit :*

1. Dans l'arborescence de la console, déployez le noeud **Ordinateurs administrés** ; déployez le groupe d'administration pour les serveurs duquel vous souhaitez créer une stratégie.

2. Dans le menu contextuel du nœud incorporé **Stratégies**, sélectionnez la commande **Créer** → **Stratégie**.

   La fenêtre de l'assistant de création des stratégies s'ouvre.

3. Dans la fenêtre **Nom de la stratégie**, dans la section de saisie, saisissez le nom de la stratégie à créer (il ne doit pas contenir les caractères **" * < : > ? \ / |**).

4. Dans la fenêtre **Application** sélectionnez **Kaspersky Anti-Virus 8.0 for Linux File Server** dans la liste déroulante.

5. Dans la fenêtre **Création d'une stratégie**, sélectionnez un des statuts suivants de la stratégie :

   - **Stratégie active**, si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, cette stratégie deviendra inactive, et la stratégie que vous créez sera activée.

   - **Stratégie inactive**, si vous ne voulez pas utiliser immédiatement la stratégie créée. Vous pourrez activer la stratégie plus tard.

   Dans les fenêtres de l'assistant de création des stratégies suivantes, déterminez, en fonction de vos besoins, les paramètres des tâches de protection en temps réel et les paramètres de mise à jour.

6. Dans la fenêtre **Zones de protection** ajoutez une ou plusieurs zones de protection et sélectionnez le mode d'interception (cf. page 185).

7. S'il faut, dans la fenêtre **Zones d'exclusion d'une tâche de protection en temps réel** ajoutez une ou plusieurs zones à ne pas protéger.

8. Cliquez sur le bouton **Terminer** dans la fenêtre **Fin du fonctionnement de l'assistant de création des stratégies**.

CONFIGURATION D'UNE STRATEGIE

Dans la boîte de dialogue **Propriétés** de la stratégie en cours, vous pouvez spécifier les paramètres généraux de Kaspersky Anti-Virus et les paramètres de la mise à jour.

➧ *Pour déterminer les paramètres de la stratégie dans la boîte de dialogue **Propriétés de la stratégie** ::*

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés**, déployez le groupe d'administration dont les paramètres de la stratégie vous voulez spécifier, ensuite déployez le nœud incorporé **Stratégies**.

2. Dans le panneau des résultats, ouvrez le menu contextuel dans la stratégie dont les paramètres vous voulez spécifier, et sélectionnez la commande **Propriétés**.

3. Dans la boîte de dialogue **Propriétés** : **<Nom de la stratégie>**, déterminez les paramètres appropriés de la stratégie et cliquez sur le bouton **OK**.

VERIFICATION MANUELLE DE LA CONNEXION AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLNAGCHK

La distribution de l'Agent d'administration contient l'utilitaire *klnagchk* conçu pour l'analyse de la connexion avec le serveur d'administration.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve dans le répertoire /opt/kaspersky/klnagent/bin et et son exécution, en fonction des clés utilisées, effectue les actions suivantes :

- il renvoie à l'écran ou enregistre dans un fichier les valeurs des paramètres de connexion de l'Agent d'administration installé sur le poste client, utilisés afin de se connecter au Serveur d'administration ;

- il enregistre dans le fichier journal les statistiques de l'Agent d'administration (à partir du dernier démarrage du composant) et les résultats de son activité, ou les afficher à l'écran ;
- il tente de connecter l'Agent d'administration au Serveur d'administration ;
- si la connexion n'a pas pu être établie, il envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état du poste.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nomFichier>] 1 [-sp] [-savecert <chemin du fichier certificat>]
[-restart]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur, ainsi que les résultats de l'exécution ; par défaut les informations sont conservées dans le fichier stdout.tx ; si le paramètre n'est pas utilisé, les résultats et les messages d'erreur sont affichés à l'écran.
- `-sp` : affiche le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy ; ce paramètre est utilisé si la connexion au Serveur d'administration est effectuée via un serveur proxy.
- `-savecert <nom du fichier>` : enregistre le certificat utilisé pour accéder au Serveur d'administration dans le fichier spécifié.
- `-restart` : redémarre l'Agent d'administration après exécution de l'utilitaire.

CONNEXION AU SERVEUR D'ADMINISTRATION EN MODE MANUEL UTILITAIRE KLMOVER

La distribution de l'Agent d'administration contient l'utilitaire *klmover*, conçu pour l'administration de la connexion au Serveur d'administration.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve dans le répertoire /opt/kaspersky/klnagent/bin et et son exécution, en fonction des clés utilisées, effectue les actions suivantes :

- connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués ;
- enregistre les résultats de l'opération dans le fichier journal des événements, ou les afficher à l'écran.

Syntaxe de l'utilitaire :

```
klmover [-logfile <nom du fichier>] 1 [-address <adresse serveur>] [-pn <numéro du
port>] [-ps < numéro du port SSL>] [-nossl] [-cert <chemin du fichier certificat>] [-
silent] [-dupfix]
```

Description des paramètres :

- `-logfile <nom du fichier>` : consigne les résultats de l'exécution de l'utilitaire dans le fichier indiqué ; si l'argument n'est pas utilisé, les résultats et les messages d'erreur sont affichés dans stdout.
- `-address <adresse serveur>` : adresse du Serveur d'administration pour la connexion ; l'adresse peut être une adresse IP, un nom NetBIOS ou DNS du serveur.
- `-pn <numéro du port>` : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration, par défaut le port 14000 est utilisé.
- `-ps <numéro du port SSL>` : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Par défaut, il s'agit du port 13000.

- `-nossl` : utilise une connexion non sécurisée au Serveur d'administration ; si aucun modificateur n'est utilisé, la connexion à l'Agent d'administration est établie à l'aide du protocole sécurisé SSL.
- `-cert <chemin complet du fichier certificat>` : utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au nouveau Serveur d'administration. Si aucun modificateur n'est utilisé, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.
- `-silent` : exécute l'utilitaire en mode non interactif ; ce paramètre est utile, par exemple, pour exécuter l'outil à partir du scénario d'ouverture de session de l'utilisateur.
- `-dupfix` : paramètre utilisé en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

PARAMÈTRES DES TÂCHES

DANS CETTE SECTION

MODE D'INTERCEPTION

Le paramètre de sécurité **Moyen d'interception** n'est utilisé que dans les tâches de protection en temps réel.

Kaspersky Anti-Virus comprend deux composants qui interceptent les requêtes aux fichiers et leur analyse : intercepteur SAMBA (il sert à analyser les objets sur les ordinateurs distants lorsqu'on y fait requête via le protocole SMB/CIFS) et intercepteur du niveau du noyau. Il analyse les objets lorsqu'on y fait requête via d'autres modes.

L'intercepteur SAMBA permet de recevoir en tant que informations supplémentaires sur l'objet, IP de l'ordinateur distant depuis lequel l'application a fait requête à l'objet au moment de son interception par Kaspersky Anti-Virus.

Si vous utilisez l'ordinateur protégé uniquement en tant que serveur SAMBA vous pouvez spécifier la valeur **Uniquement SAMBA**. Dans ce cas, Kaspersky Anti-Virus n'analysera pas les objets auxquels la requête est faite non pas via le protocole SMB/CIFS.

Les valeurs possibles comprennent :

- **Toutes les opérations**. Kaspersky Anti-Virus analyse les objets sur le serveur lorsqu'on y fait requête via le protocole SMB/CIFS avec utilisation de l'intercepteur SAMBA. Kaspersky Anti-Virus intercepte toutes les autres opérations sur les fichiers disponibles sur le serveur protégé (y compris, sur les fichiers des ordinateurs distants), en utilisant l'intercepteur du niveau du noyau.

- **Uniquement SAMBA**. Kaspersky Anti-Virus analyse les objets uniquement lorsqu'on y fait requête via le protocole SMB/CIFS, en utilisant l'intercepteur SAMBA.

  Assurez-vous d'avoir installé le module SAMBA VFS durant la configuration initiale de Kaspersky Anti-Virus (cf. la rubrique " Étape 7. Intégration au serveur Samba " du Guide d'installation de Kaspersky Anti-Virus 8.0 for Linux File Server).

- **Uniquement le système de fichiers**. Kaspersky Anti-Virus analyse les objets sur le serveur sans utilisation de l'intercepteur SAMBA.

  Assurez-vous d'avoir installé l'intercepteur de noyau durant la configuration initiale de Kaspersky Anti-Virus (cf. la rubrique " Étape 6. Compilation du module du noyau " du Guide d'installation de Kaspersky Anti-Virus 8.0 for Linux File Server).

MODE DE PROTECTION DES OBJETS

Le paramètre de sécurité **Mode de protection des objets** n'est utilisé que dans les tâches de protection en temps réel.

Ce paramètre n'est utilisé que dans les tâches de protection en temps réel. Il détermine à quel type d'accès aux objets Kaspersky Anti-Virus les analysera.

Sélectionnez un des modes de protection en fonction de vos besoins pour la sécurité du serveur, en fonction des formats des fichiers sauvegardés sur le serveur et des informations qu'ils contiennent :

- **Mode intelligent**. Kaspersky Anti-Virus analyse l'objet lors de la tentative d'ouverture et encore une fois lors sa fermeture si il a été modifié. Si le processus lors de son fonctionnement adresse plusieurs requêtes à l'objet durant une certaine période de temps et le modifie, Kaspersky Anti-Virus n'analysera l'objet qu'à la dernière tentative de fermeture de ce fichier par ce processus.

- **A l'accès et à la modification**. Kaspersky Anti-Virus analyse l'objet lors de la tentative d'ouverture et encore une fois lors sa fermeture si il a été modifié.

- **A l'accès**. Kaspersky Anti-Virus analyse l'objet lors de son ouverture en lecture, ainsi qu'en exécution ou modification.

Valeur par défaut : **Mode intelligent**.

ANALYSE HEURISTIQUE

Le paramètre de sécurité **Analyse heuristique** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Anti-Virus compare l'objet trouvé aux entrées des bases, ce qui permet d'affirmer sans faute si l'objet analysé est malveillant ou non et d'identifier la catégorie d'applications dangereuses à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. *L'analyse heuristique* permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Par conséquent, les nouvelles menaces peuvent être détectées avant qu'elles ne soient connues des analystes de virus.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

Cochez la case **Analyse heuristique** pour activer l'analyse heuristique.

Sélectionnez une des valeurs suivantes pour la profondeur de l'analyse en fonction de vos besoins en matière de sécurité et de la vitesse de l'échange de fichiers sur le serveur :

- **Superficiel** ;
- **Moyenne** ;
- **Profond**.

Valeur par défaut : **Moyenne**.

ACTION A EXECUTER SUR LES OBJETS INFECTES

Le paramètre de sécurité **Actions à exécuter sur les objets infectés** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Lorsque Kaspersky Anti-Virus reconnaît l'objet analysé comme étant infecté il effectue sur cet objet l'action que vous avez spécifiée.

Sélectionnez une des valeurs suivantes :

- **Réparer**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Supprimer**. Kaspersky Anti-Virus supprime l'objet.
- **Exécuter l'action recommandée**. Kaspersky Anti-Virus choisit automatiquement et effectue les actions sur les objets à la base des données sur le danger de la menace détectée dans l'objet et de la possibilité de sa réparation ; par exemple, Kaspersky Anti-Virus supprime immédiatement les chevaux de Troie puisqu'ils ne s'introduisent pas dans les autres fichiers et ne les infectent pas et, donc, ne supposent pas la réparation. Vous pouvez indiquer cette action uniquement en tant que première action à exécuter sur des objets infectés.
- **Ignorer**. L'objet reste intact : Kaspersky Anti-Virus n'essaie pas de le réparer ou supprimer. Les informations sur l'objet détecté seront consignées dans le journal.
- **Placer en quarantaine**. L'objet est placé en quarantaine et il est sauvegardé sous forme codée.

Avant de modifier l'objet (traiter ou supprimer), Kaspersky Anti-Virus enregistre sa copie dans le dossier de sauvegarde. S'il n'arrive pas à réserver un objet, il n'essaie pas de le réparer ou de le supprimer ; l'objet reste intact. Les informations

sur les raisons de l'échec de la réparation ou de la suppression de l'objet par Kaspersky Anti-Virus sont affichées dans le registre.

Sélectionnez dans la liste deux actions que Kaspersky Anti-Virus essaiera d'effectuer sur l'objet. Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action.

N'oubliez pas que dans la tâche de protection en temps réel, Anti-Virus, avant d'exécuter une action, verrouille l'accès à l'objet pour l'application qui l'a sollicité.

ACTION A EXECUTER SUR LES OBJETS SUSPECTS

Le paramètre de sécurité **Action à exécuter sur les objets suspects** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Lorsque Kaspersky Anti-Virus reconnaît l'objet comme étant suspect il effectue sur cet objet l'action que vous avez spécifiée.

Sélectionnez une des valeurs suivantes :

- **Placer en quarantaine**. L'objet est placé en quarantaine et il est sauvegardé sous forme codée.
- **Réparer**. Kaspersky Anti-Virus essaie de réparer l'objet ; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Supprimer**. Kaspersky Anti-Virus supprime l'objet suspect du serveur.

  Avant de supprimer l'objet, Kaspersky Anti-Virus met sa copie dans le répertoire de sauvegarde de réserve dans lequel l'objet est conservé sous forme codée. Kaspersky Anti-Virus ne supprime pas l'objet s'il n'arrive pas à mettre préalablement sa copie dans le dossier de sauvegarde. L'objet reste intact. Les informations sur les raisons de l'échec de la suppression de l'objet par Kaspersky Anti-Virus sont consignées dans le journal.
- **Exécuter l'action recommandée**. Kaspersky Anti-Virus choisit et effectue des actions sur les objets à la base des données sur le niveau de danger de la menace détectée dans l'objet.
- **Ignorer**. L'objet reste intact : Kaspersky Anti-Virus n'essaie pas de le réparer ou supprimer ; il consigne les informations sur l'objet suspect détecté dans le journal.

Sélectionnez dans la liste deux actions que Kaspersky Anti-Virus essaiera d'effectuer sur l'objet. Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action.

N'oubliez pas que dans la tâche de protection en temps réel, Anti-Virus, avant d'exécuter une action, verrouille l'accès à l'objet pour l'application qui l'a sollicité.

ACTIONS A EXECUTER SUR DES OBJETS EN FONCTION DU TYPE DE MENACE

Le paramètre de sécurité **Action à exécuter sur des objets en fonction du type de la menace** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Certaines menaces sont plus dangereuses pour l'ordinateur que d'autres. Par exemple, les chevaux de Troie peuvent provoquer des dégâts bien plus importants que ceux d'un logiciel publicitaire. À l'aide de ce paramètre, vous pouvez configurer différentes actions de Kaspersky Anti-Virus sur des objets qui contiennent des menaces de types différents.

Si vous déterminez les valeurs de ce paramètre, Kaspersky Anti-Virus les utilisera au lieu des valeurs des paramètres Actions à exécuter sur des objets infectés (cf. page 186) et Actions à exécuter sur des objets suspects (cf. page 187).

Pour chaque type de menace, sélectionnez dans la liste deux actions que Kaspersky Anti-Virus essaiera d'effectuer sur l'objet s'il y détecte une menace du type spécifié. Kaspersky Anti-Virus effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action.

Kaspersky Anti-Virus appliquera les actions spécifiées aux objets infectés, ainsi qu'aux objets suspects si cela s'avère possible.

Si vous sélectionnez **Ignorer** en tant que première action, la deuxième action ne sera pas possible.

Si Kaspersky Anti-Virus n'arrive pas à mettre l'objet dans le dossier de sauvegarde ou en quarantaine, il n'exécutera pas l'action suivante sur l'objet (par exemple, sa réparation ou sa suppression). L'objet est considéré comme ignoré. Vous pouvez consulter la raison de l'omission de l'objet dans le journal.

Dans la liste des types de menaces, les types **Vers de réseau** et **Virus classiques** sont regroupés sous un seul nom de **Virus**.

EXCLUSION DES OBJETS SELON LE NOM

Le paramètre de sécurité **Exclusion des objets selon le nom** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Kaspersky Anti-Virus analyse par défaut tous les objets repris dans la zone de protection.

Vous pouvez indiquer les modèles des noms ou des chemins d'accès exclus de la zone de protection. Dans ce cas, Kaspersky Anti-Virus n'analysera que les fichiers ou les répertoires de la zone de protection que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières étendues POSIX.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Anti-Virus.

Les expressions régulières étendues vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Anti-Virus. L'expression régulière ne doit pas contenir le nom du répertoire contenant l'objet à exclure.

Les informations sur les raisons de l'exclusion de l'objet de l'analyse sont consignées dans le journal.

EXCLUSION DES OBJETS EN FONCTION DU NOM DE LA MENACE

Le paramètre de sécurité **Exclusion des objets selon le nom de menace** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Si Kaspersky Anti-Virus considère que l'objet analysé est infecté ou qu'il est suspect, l'action définie sera exécutée. Si vous estimez que cet objet ne présente aucun danger pour l'ordinateur protégé, vous pouvez l'exclure de l'analyse en fonction du nom de la menace découverte. Dans ce cas, Kaspersky Anti-Virus considère ces objets comme étant sains et ne les traite pas.

Le nom complet de la menace peut contenir les informations suivantes :

<classe de la menace>:<type de la menace>.<nom abrégé du système d'exploitation>.<nom de la menace>.<code de la modification de la menace>. Par exemple : **not-a-virus:NetTool.Linux.SynScan.a**.

Vous pouvez trouver le nom complet de la menace détectée dans l'objet, dans le registre de Kaspersky Anti-Virus.

Vous pouvez également trouver le nom complet de la menace détectée dans le logiciel sur le site de l'Encyclopédie des virus (cf. rubrique l'Encyclopédie des virus – http://www.viruslist.com/fr). Pour trouver le type de menace, saisissez le nom du logiciel dans le champ **Recherche**.

Lors de la définition des modèles de nom de menaces, vous pouvez utiliser les masques Shell ou les expressions régulières étendues POSIX.

Pour exclure une menace de l'analyse, indiquez le nom complet d'une menace détectée dans cet objet, ou le modèle du nom d'une menace.

Par exemple, vous utilisez l'utilitaire pour la réception des informations sur le réseau ; Kaspersky Anti-Virus le bloque en rapportant son code aux menaces de type **Programmes potentiellement malveillants**. Vous pouvez ajouter le nom complet de la menace, détectée dans le programme, dans la liste des menaces à exclure, par exemple, **not-a-virus:NetTool.Linux.SynScan.a**.

Vous pouvez spécifier les noms des menaces à l'aide des masques Shell et des expressions régulières étendues POSIX. Ajoutez le préfixe **re:** aux expressions régulières POSIX.

Par exemple, pour ne pas exécuter les actions sur les fichiers dans lesquels Kaspersky Anti-Virus détectera n'importe quelle menace pour Linux de la catégorie not-a-virus, saisissez : **re:not-a-virus:.*\.Linux\..***.

ANALYSE DES OBJETS COMPOSES

Le paramètre de sécurité **Analyse des objets composés** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

L'analyse des objets composés dure un certain temps. Par défaut, Kaspersky Anti-Virus analyse uniquement les objets composés des types qui sont le plus sujets à l'infection et sont les plus dangereux pour l'ordinateur s'ils sont infectés. Les objets composés des autres types ne sont pas analysés.

Ce paramètre vous permet, suivant vos exigences relatives à la sécurité, de sélectionner les types des objets conteneurs que Kaspersky Anti-Virus analysera.

Sélectionnez une ou plusieurs valeurs :

- **Analyse des archives**. Kaspersky Anti-Virus analyse les archives (y compris les archives autoextractibles SFX). Faites attention à ce que Kaspersky Anti-Virus détecte des menaces dans les archives sans les réparer.
- **Analyser des archives autoextractibles**. Kaspersky Anti-Virus analyse des archives autoextractibles (archives qui comprennent un module de désarchivage).
- **Analyser les bases de messagerie**. Kaspersky Anti-Virus analyse les objets des bases de messagerie Microsoft Office Outlook et Microsoft Outlook Express.
- **Analyser les objets compactés**. Kaspersky Anti-Virus analyse les fichiers exécutables archivés par les programmes d'archivage de code binaire tels que UPX ou ASPack. Les objets composés de ce type ont plus de probabilité de contenir une menace.
- **Analyser les fichiers au format de messagerie**. Kaspersky Anti-Virus analyse les fichiers des messages informatiques au format texte (plain text).

DUREE MAXIMUM D'ANALYSE D'UN OBJET

Le paramètre de sécurité **Interrompre l'analyse, si elle dure plus de** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Kaspersky Anti-Virus arrête d'analyser l'objet si la durée de cette analyse est supérieure à la durée indiquée, en secondes. Les informations sur les raisons de l'exclusion de l'objet de l'analyse sont consignées dans le journal.

TAILLE MAXIMUM DE L'OBJET ANALYSE

Le paramètre de sécurité **Ne pas analyser les objets dont la taille dépasse** est utilisé dans les tâches de protection en temps réel et dans les tâches d'analyse à la demande.

Si le volume de l'objet analysé est supérieur à la valeur spécifiée, Kaspersky Anti-Virus saute cet objet. Les informations relatives à l'omission de l'objet sont consignées dans le journal.

Valeurs possibles : 0-2147483647 (2 Go environ).

SOURCE DES MISES A JOUR

Vous pouvez sélectionner la source depuis laquelle Kaspersky Anti-Virus va recevoir des mises à jour en fonction du schéma de mise à jour utilisé au sein de votre entreprise.

En tant que source des mises à jour il est possible d'indiquer une des valeurs suivantes :

- **Serveurs de mise à jour de Kaspersky Lab**. Kaspersky Anti-Virus téléchargera les mises à jour depuis un des serveurs de mise à jour de Kaspersky Lab. Les mises à jour sont téléchargées via le protocole HTTP ou le protocole FTP.

- **Serveur d'administration Kaspersky Administration Kit**. Vous pouvez sélectionner cette source de mise à jour si l'administration centralisée de la protection antivirus des ordinateurs de votre réseau s'opère via Kaspersky Administration Kit. Kaspersky Anti-Virus téléchargera les mises à jour sur le serveur protégé depuis le serveur d'administration Kaspersky Administration Kit installé dans le réseau local.

- **Autres répertoires dans le réseau local ou mondial**. Kaspersky Anti-Virus téléchargera des mises à jour depuis la source que vous spécifiez. Vous pouvez désigner les répertoires des serveurs FTP ou HTTP, les répertoires sur tout périphérique monté du serveur, y compris les répertoires des ordinateurs distants montés via les protocoles SMB/CIFS ou NFS.

Vous pouvez spécifier une ou plusieurs sources de mises à jour définie par l'utilisateur. Kaspersky Anti-Virus fera requête à chaque source spécifiée suivante si la source précédente n'est pas disponible.

Vous pouvez modifier l'ordre selon lequel Kaspersky Anti-Virus va solliciter les sources définies par l'utilisateur ou configurer l'envoi de requêtes à certaines sources de la liste uniquement.

Vous pouvez configurer la requête de Kaspersky Anti-Virus aux serveurs de mises à jour de Kaspersky Lab au cas où toutes les sources définies par l'utilisateur seraient inaccessibles.

La valeur du paramètre par défaut : les Serveurs de mises à jour de Kaspersky Lab.

MODE DU SERVEUR FTP

Pour la connexion aux serveurs des mises à jour via le protocole FTP, Kaspersky Anti-Virus utilise par défaut le mode passif du serveur FTP : il est supposé que dans le réseau local de l'entreprise, le pare-feu est utilisé.

La valeur par défaut : utiliser le FTP en mode passif.

DELAI D'ATTENTE POUR LA REPONSE DU SERVEUR FTP OU HTTP

Ce paramètre détermine le délai d'attente de la réponse de la source des mises à jour (serveur FTP ou HTTP). Si la source des mises à jour ne répond pas au cours de la période spécifiée, Kaspersky Anti-Virus fait appel à une autre source de mises à jour. Par exemple, il contactera à l'autre serveur de mises à jour de Kaspersky Lab si vous avez configuré la mise à jour depuis les serveurs de mises à jour de Kaspersky Lab.

Indiquez le délai d'attente de la réponse en secondes. Seuls des nombres entiers sont admis.

Valeur par défaut : **10 sec**.

UTILISATION DU SERVEUR PROXY LORS DE LA CONNEXION AUX SOURCES DE MISES A JOUR

Ce paramètre active ou désactive l'utilisation du serveur proxy lors de la connexion aux différentes sources de mises à jour.

Si vous avez choisi les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour, cochez **Utiliser le serveur proxy pour les serveurs de mises à jour de Kaspersky Lab**, si l'accès à Internet s'opère via le serveur proxy.

Si l'accès au serveur proxy est requis pour la connexion à un serveur FTP ou HTTP défini par l'utilisateur, cochez **Utiliser le serveur proxy pour les sources de mises à jour d'utilisateurs**.

Valeurs par défaut :

- Lors de la connexion aux serveurs des mises à jour de Kaspersky Lab, Kaspersky Anti-Virus fait requête au serveur proxy.
- Lors de la connexion aux sources des mises à jour d'utilisateur (serveurs HTTP ou FTP, ainsi que ordinateurs spécifiés par l'utilisateur), Kaspersky Anti-Virus n'utilise pas le serveur proxy. On suppose que ces sources se trouvent dans le réseau local.

VERIFICATION DE L'AUTHENTICITE LORS DE L'ACCES AU SERVEUR PROXY

Ce paramètre comprend la vérification de l'authenticité lors de l'accès au serveur proxy qui est utilisé pour la connexion aux serveurs FTP ou HTTP - sources de mises à jour.

Activez le mode **Utiliser l'authentification**. et spécifiez le **Nom** et le **Mot de passe** de l'utilisateur.

La valeur par défaut : la vérification de l'authenticité lors de l'accès au serveur proxy n'est pas effectuée.

PARAMETRES DU SERVEUR PROXY

Si vous avez activé l'utilisation du serveur proxy lors de la connexion aux sources de mises à jour, spécifiez les paramètres du serveur proxy.

Spécifiez l'adresse IP ou le nom DNS du serveur (par exemple, proxy.mycompany.com) et son port.

Valeur par défaut : non spécifié.

REPERTOIRE DE SAUVEGARDE DES MISES A JOUR

Ce paramètre est utilisé lorsque le type des mises à jour **Copie de toutes les mises à jour accessibles de l'application** ou **Copie des mises à jour selon la liste indiquée** est sélectionné. À l'aide de ce paramètre, spécifiez le répertoire dans lequel seront enregistrés les fichiers des mises à jour.

Vous pouvez spécifier le répertoire sur tout disque monté du serveur.

Valeur par défaut : non spécifié.

TYPE DE MISES A JOUR

À l'aide de ce paramètre, vous pouvez sélectionner une fonction qui sera exécutée par la tâche de mise à jour.

Sélectionnez une des valeurs suivantes :

- **Uniquement les bases**. Kaspersky Anti-Virus téléchargera et installera des mises à jour des bases.
- **Copie de toutes les mises à jour accessibles de l'application**. Sélectionnez, pour télécharger et enregistrer dans le répertoire spécifié toutes les mises à jour disponibles pour Kaspersky Anti-Virus sans les utiliser.
- **Copie des mises à jour selon la liste indiquée**. Choisissez cette option si vous souhaitez télécharger uniquement les mises à jour indiquées. Kaspersky Anti-Virus enregistrera les mises à jour reçues dans le répertoire spécifié sans les utiliser.

  Vous pouvez recevoir les mises à jour des modules des autres applications de Kaspersky Lab si vous voulez utiliser l'ordinateur protégé en tant qu'intermédiaire pour répartir les mises à jour. Vous pouvez consulter les noms des mises à jour dans le document http://support.kaspersky.ru/downloads/updater/update_components_21112008.pdf, publié sur le site du Service du Support Technique de Kaspersky Lab.

  L'installation automatique des mises à jour critiques des modules de Kaspersky Anti-Virus n'est pas prévue.

Valeur par défaut : **Uniquement les bases**.

KASPERSKY LAB

Kaspersky Lab a été fondée en 1997. Aujourd'hui, elle est le concepteur le plus connu en Russie en technologies de sécurité de l'information. Elle produit un large éventail de logiciels de sécurité des données : systèmes de protection contre des virus, les courriers électroniques non sollicités ou indésirables (spam) et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve en Russie, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). 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 1000 spécialistes, 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes en chef en matière de virus siègent en tant que membres de l'organisation pour la recherche antivirus en informatique Computer Anti-virus Researcher's Organization (CARO).

La valeur principale de la société c'est une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Kaspersky Anti-Virus, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : postes de travail, serveurs de fichiers, systèmes de messagerie, pare-feu et passerelles Internet, ordinateurs de poche. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

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. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirale pour entreprise. Les bases antivirus de Kaspersky Lab sont mises à jour en temps réel toutes les heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez une réponse complète à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.fr
L'Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive) https://my.kaspersky.com/fr/support (pour les questions aux experts antivirus)

INFORMATIONS SUR LE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

DANS CETTE SECTION

CODE DE PROGRAMME

Informations sur le code tiers d'application développé par des éditeurs tiers a été utilisé pour créer l'application.

DANS CETTE SECTION

APACHE 1.3.41

Apache License

Version 2,0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purpose of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or addition to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or

Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices

stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works

that You distribute, all copyright, patent, trademark, and

attribution notices from the Source form of the Work,

excluding those notices that do not pertain to any part of

the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its

distribution, then any Derivative Works that You distribute must

include a readable copy of the attribution notices contained

within such NOTICE file, excluding those notices that do not

pertain to any part of the Derivative Works, in at least one

of the following places: within a NOTICE text file distributed

as part of the Derivative Works; within the Source form or

documentation, if provided along with the Derivative Works; or,

within a display generated by the Derivative Works, if and

wherever such third-party notices normally appear. The contents

of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution

notices within Derivative Works that You distribute, alongside

or as an addendum to the NOTICE text from the Work, provided

that such additional attribution notices cannot be construed

as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly

negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or

malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APACHE HTTP SERVER SUBCOMPONENTS:

The Apache HTTP Server includes a number of subcomponents with

separate copyright notices and license terms. Your use of the source

code for the these subcomponents is subject to the terms and

conditions of the following licenses.

For the MD5 Message-Digest library component:

Copyright (C) 1995, Board of Trustees of the University of Illinois

****

(C) Copyright 1993,1994 by Carnegie Mellon University

All Rights Reserved.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Carnegie Mellon University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Carnegie Mellon University makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER INAN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

****

Copyright (c) 1991 Bell Communications Research, Inc. (Bellcore)

Permission to use, copy, modify, and distribute this material for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Bellcore not be used in advertising or publicity pertaining to this material without the specific, prior written permission of an authorized representative of Bellcore.

BELLCORE MAKES NO REPRESENTATIONS ABOUT THE ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE. IT IS PROVIDED "AS IS",

WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES.

****

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that i is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

"THE BEER-WARE LICENSE" (Revision 42):

<phk@login.dknet.dk> wrote this file. As long as you retain this notice you

can do whatever you want with this stuff. If we meet some day, and you think

this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

---

For the expat-lite library component:

Copyright (c) 1998, 1999 James Clark. Expat is subject to the Mozilla Public License Version 1,1. Alternatively you may use expat under the GNU General Public License instead.

For the regex library component:

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this

   software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by

   explicit claim or by omission. Since few users ever read sources,

   credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be

   misrepresented as being the original software. Since few users

   ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

For the expat xml parser library component:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

For the mod_mime_magic component:

Copyright (c) 1996-1997 Cisco Systems, Inc.

This software was submitted by Cisco Systems to the Apache Group in July 1997. Future revisions and derivatives of this source code must acknowledge Cisco Systems as the original contributor of this module. All other licensing and usage conditions are those of the Apache Group.

Some of this code is derived from the free version of the file command originally posted to comp.sources.unix. Copyright info for that program is included below as required.

Copyright (c) Ian F. Darwin, 1987. Written by Ian F. Darwin.

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

For the mod_imap component: "macmartinized" polygon code copyright 1992 by Eric Haines, erich@eye.com

For the zb test and ab support components:

This program is Copyright (C) Zeus Technology Limited 1996.

This program may be used and copied freely providing this copyright notice is not removed.

This software is provided "as is" and any express or implied waranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Zeus Technology Ltd. be liable for any direct, indirect, incidental, special, exemplary, or consequential damaged (including, but not limited to, procurement of substitute good or services; loss of use, data, or profits; or business interruption) however caused and on theory of liability. Whether in contract, strict liability or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

NOTICE

Apache HTTP Server

Copyright 2006 The Apache Software Foundation.

This product includes software developed at

The Apache Software Foundation (http://www.apache.org/).

Portions of this software were developed at the National Center

for Supercomputing Applications (NCSA) at the University of

Illinois at Urbana-Champaign.

This software contains code derived from the RSA Data Security

Inc. MD5 Message-Digest Algorithm, including various

modifications by Spyglass Inc., Carnegie Mellon University, and

Bell Communications Research, Inc (Bellcore).

This work includes the Expat xml parsing library Copyright (c)

1998, 1999 James Clark, distributed under and subject to the

Mozilla Public License Version 1,1.

This work includes the regex library Copyright 1992, 1993, 1994

Henry Spencer, all rights reserved.

EXPAT 1.95.8

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GSOAP

---

gSOAP license

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

gSOAP Public License

1.1.1 Version 1.3a

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1,0.1, 2,1.(c),(d), 2,2.(c),(d), 8,2.(b), 10, and 11. Section 3,8 was added. The modified sections are 2,1.(b), 2,2.(b), 3,2 (simplified), 3,5 (deleted the last sentence), and 3,6 (simplified).

1.2 1 DEFINITIONS.

1.0.1.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1,8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A.

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B.

Any new file that contains any part of the Original Code, or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6,1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

1.3 2 SOURCE CODE LICENSE.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a)

under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell ("offer to sell and import") the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a)

under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell ("offer to sell and import") the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

1.4 3 DISTRIBUTION OBLIGATIONS.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2,2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3,5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3,4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

1.5 4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3,4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

1.6 5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

1.7 6 VERSIONS OF THE LICENSE.

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

1.8 7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

1.9 8 TERMINATION.

8.1.

This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3.

If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2,1 or 2,2 shall be taken into account in determining the amount or value of any payment or license.

8.4.

In the event of termination under Sections 8,1 or 8,2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

1.10 9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

1.11 10 U.S. GOVERNMENT END USERS.

1.12 11 MISCELLANEOUS.

1.13 12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

JQUERY 1.3.2

Copyright (c) 2009 John Resig, http://jquery.com/.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION1 OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBHARU 2.1.0

Copyright (C) 1999-2006 Takeshi Kanno

Copyright (C) 2007-2008 Antony Dovgal

LIBXML2-2.6.32

LIBXSLT-1.1.23

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

LIBPCRE 7.4

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ZLIB 1.2.3

Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes, Rene Rivera

LIBACL 2.2.45-1

Copyright (C) 2002, Andreas Gruenbacher <agruen@suse.de>, SuSE Linux AG

ATTR 2.4.38-1

Copyright (C) 2000-2002, 2004, Silicon Graphics, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

LIBPNG 1.2.44

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUTF

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

LZMALIB 4.43

NET-SNMP 5.5

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SQLITE 3.6.17

DEJAVU SANS 2.31

Copyright (C) 2003, Bitstream, Inc

Copyright (C) 2006, Tavmjong Bah

Fonts are © Bitstream (see below). DejaVu changes are in public domain. Explanation of copyright is on Gnome page on Bitstream Vera fonts. Glyphs imported from Arev fonts are © Tavmjung Bah (see below)

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Original text

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong@free.fr.

PROTOTYPE-1.6.0.3

CODE DE PROGRAMMATION DIFFUSE

L'application contient du code de programmation indépendant de développeurs tiers sous forme binaire.

DANS CETTE SECTION

REDIRFS 0.10 (MODIFIED)

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 3 of the License

AUTRE INFORMATION

Informations sur le code tiers

La bibliothèque du programme "Agava-C", développée par OOO "R-Alpha", est utilisée pour vérifier une signature numérique.

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel.

=======

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

=======

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are

used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it

has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not

convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

=======

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6,)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright

notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the

Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either

version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

=======