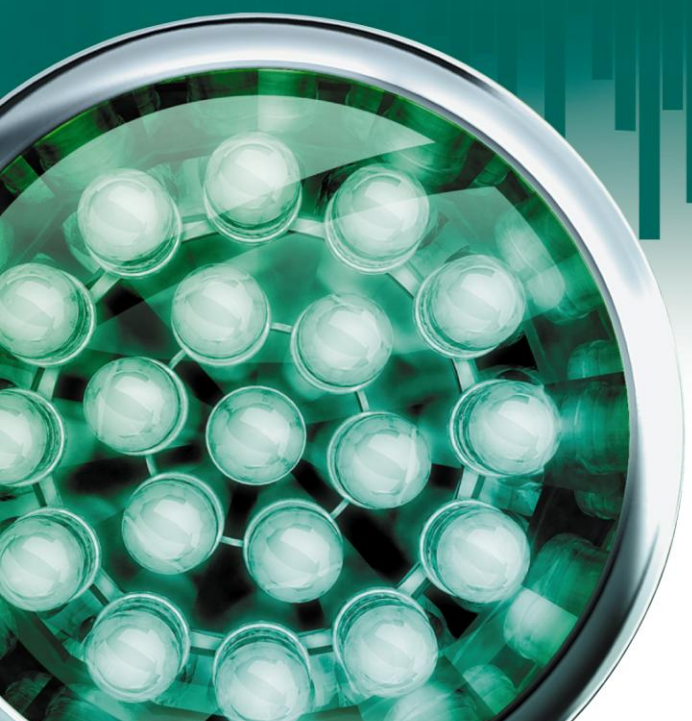
Kaspersky Endpoint Security 8 for Linux

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 fournira des réponses à la plupart de vos questions.

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

Date d'édition du document: le 13/05/11

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

TABLE DES MATIERES

INTRODUCTION 8
Informations générales sur Kaspersky Endpoint Security 8
Protection en temps réel et analyse à la demande 9
Particularités de l'analyse des liens symboliques et matériels 9
A propos des objets infectés, suspects et possédant le statut "Avertissement" 10
À propos de la mise en quarantaine et de la copie de sauvegarde des objets 10
Programmes détectés par Kaspersky Endpoint Security 11
Obtention d'informations sur Kaspersky Endpoint Security 13
Sources d'informations pour une recherche autonome 14
Contacter le service du Support Technique 16
Discussion sur les applications de Kaspersky Lab dans le forum 17
DÉMARRAGE ET ARRÊT DE KASPERSKY ENDPOINT SECURITY 18
ADMINISTRATION DES TÂCHES DE KASPERSKY ENDPOINT SECURITY 19
Création d'une tâche d'analyse à la demande ou de mise à jour 19
Suppression de la tâche d'analyse à la demande ou de mise à jour 20
Administration de la tâche en mode manuel 20
Administration automatique des tâches 21
Consultation de l'état de la tâche 21
Consultation des statistiques de la tâche 22
MISE À JOUR DE KASPERSKY ENDPOINT SECURITY 23
Sélection de la source des mises à jour 24
Mise à jour depuis un répertoire local ou de réseau 24
Utilisation d'un serveur proxy 26
Retour à la version antérieure des bases 27
PROTECTION EN TEMPS RÉEL DES FICHIERS 28
Paramètres de protection par défaut 28
Création de la zone de protection 30
Restriction de la zone de protection à l'aide de masques et d'expressions régulières 31
Exclusion des objets de la protection 31
Création d'une zone d'exclusion globale 32
Exclusion des objets de la zone de protection 32
Exclusion des objets en fonction des droits d'accès 33
Exclusion des objets en fonction du nom de la menace découverte 34
Sélection du mode d'interception 34
Sélection du mode de protection des objets 35
Utilisation de l'analyse heuristique 35
Utilisation du mode d'analyse en fonction des droits d'accès aux objets 36
Sélection de l'action à réaliser sur les objets détectés 37
Sélection des actions à exécuter en fonction du type de menace 38
Optimisation de l'analyse 39
Compatibilité entre Kaspersky Anti-Virus et d'autres applications de Kaspersky Lab 40
ANALYSE À LA DEMANDE 42
Paramètres de l'analyse par défaut 42
Analyse rapide des fichiers et des répertoires 43

Composition de la zone d'analyse 45
Restriction de la zone d'analyse à l'aide de masques et d'expressions régulières 46
Exclusion des objets de l'analyse 46
Création d'une zone d'exclusion globale 47
Exclusion des objets de la zone d'analyse 47
Exclusion des objets en fonction du nom de la menace découverte 48
Utilisation de l'analyse heuristique 49
Sélection de l'action à réaliser sur les objets détectés 49
Sélection des actions à exécuter en fonction du type de menace 51
Optimisation de l'analyse 52
Sélection de la priorité de la tâche 53
ISOLATION DES OBJETS SUSPECTS. COPIE DE SAUVEGARDE 54
Consultation des statistiques sur les objets mis en quarantaine 54
Analyse des objets mis en quarantaine 55
Mise des fichiers en quarantaine manuellement 56
Consultation de l'identificateur des objets 56
Restauration des objets 57
Suppression des objets 58
ADMINISTRATION DES LICENCES 59
Présentation du contrat de licence 59
A propos des licences de Kaspersky Endpoint Security 59
Présentation des fichiers de licence de Kaspersky Endpoint Security 60
Installation du fichier de licence 61
Consultation des informations relatives à la licence avant l'installation du fichier de licence 61
Suppression du fichier de licence 62
Consultation de la convention de licence 63
CRÉATION DES RAPPORTS 64
LES COMMANDES D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY DEPUIS LA LIGNE DE COMMANDE 65
Affichage des renseignements sur les commandes de Kaspersky Endpoint Security 68
Lancement de Kaspersky Endpoint Security 69
Arrêt de Kaspersky Endpoint Security 69
Redémarrage de Kaspersky Endpoint Security 69
Activation de l'affichage des événements 69
Analyse rapide des fichiers et des répertoires 70
Remise à l'état antérieur à la mise à jour des bases de Kaspersky Endpoint Security 70
Commandes de réception des statistiques et des rapports 71
Consultation des informations sur le programme 71
Consultation des rapports sur le fonctionnement de Kaspersky Endpoint Security 72
Consultation des rapports sur les menaces les plus fréquentes 73
Suppression des statistiques de fonctionnement de Kaspersky Endpoint Security 74
Commandes d'administration des paramètres de Kaspersky Endpoint Security et des tâches 75
Obtention des paramètres généraux de Kaspersky Endpoint Security 75
Modification des paramètres généraux de Kaspersky Endpoint Security 76
Consultation de la liste des tâches de Kaspersky Endpoint Security 77
Consultation de l'état de la tâche 78
Lancement d'une tâche 80

Arrêt d'une tâche....80
Suspension d'une tâche....80
Reprise d'une tâche....81
Obtention des paramètres d'une tâche....81
Modification des paramètres de la tâche....82
Création d'une tâche....83
Suppression d'une tâche....84
Obtention des paramètres de l'horaire d'une tâche....84
Modification des paramètres de l'horaire d'une tâche....85
Suppression de l'horaire de la tâche....86
Recherche d'événements selon la planification....86
Commandes d'administration des licences....88
Vérification de l'authenticité du fichier de licence avant l'installation....88
Consultation des informations relatives à la licence avant l'installation du fichier de licence....89
Consultation des informations relatives aux fichiers de licence installés....90
Consultation de l'état des licences installées....90
Installation d'un fichier de licence actif....91
Installation d'un fichier de licence de réserve....91
Suppression d'un fichier de licence actif....91
Suppression d'un fichier de licence de réserve....92
Commandes d'administration de la quarantaine et du répertoire de sauvegarde de réserve....92
Obtention des statistiques brèves de la quarantaine / du répertoire de sauvegarde....92
Obtention des informations sur les objets du répertoire de sauvegarde....93
Obtention des informations sur un objet du répertoire de sauvegarde....93
Restauration des objets depuis le répertoire de sauvegarde....94
Mise de la copie de l'objet en quarantaine manuellement....94
Suppression d'un objet depuis le répertoire de sauvegarde....95
Exportation des objets depuis le répertoire de sauvegarde dans le répertoire spécifié....95
Importation dans le répertoire de sauvegarde des objets qui ont été exportés avant....96
Purge du répertoire de sauvegarde....96
Instruction d'administration du journal des événements....97
Obtention du nombre d'événements de Kaspersky Endpoint Security par un filtre....97
Obtention des informations sur les événements de Kaspersky Endpoint Security....98
Consultation de l'intervalle de temps pendant lequel les événements du journal ont eu lieu....99
Rotation du journal des événements....99
Suppression des événements du journal des événements....99
Restriction de la sélection à l'aide des filtres....100
Expressions logiques....100
Paramètres de objets en quarantaine / dans le dossier de sauvegarde....101
Evénements de Kaspersky Endpoint Security et leurs paramètres....104
PARAMÈTRES DES FICHIERS DE CONFIGURATION DE KASPERSKY ENDPOINT SECURITY....112
Règles de mise au point des fichiers de configuration ini de Kaspersky Endpoint Security....112
Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande....114
Paramètres des tâches de mise à jour....129
Paramètres de l'horaire....134
Paramètres généraux de Kaspersky Endpoint Security.....137
Paramètres de la quarantaine et du dossier de sauvegarde....140
Les paramètres du journal des événements....141

ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY À L'AIDE DE KASPERSKY ADMINISTRATION KIT143
Consultation du statut de la protection de l'ordinateur 143
Boîte de dialogue "Paramètres de l'application" 144
Création et configuration des tâches 144
Création d'une tâche....145
Assistant pour la création d'une tâche locale....146
Etape 1. Saisie des informations générales sur la tâche 146
Etape 2. Choix de l'application et du type de tâche 146
Etape 3. Configuration des tâches....146
Etape 4. Configuration de la programmation....147
Etape 5. Fin de l'Assistant....147
Configuration des tâches....147
Composition de la zone d'analyse 147
Configuration des paramètres de sécurité 148
Création d'une zone d'exclusion 149
Sélection de la source des mises à jour....149
Sélection de type des mises à jour 150
Configuration de l'horaire de la tâche à l'aide de Kaspersky Administration Kit....151
Création de la règle du lancement de la tâche....151
Configuration de l'horaire de la tâche....152
Création et configuration des stratégies 154
Création d'une stratégie 154
Configuration d'une stratégie 155
Vérification manuelle de la connexion au Serveur d'administration. Utilitaire klnagchk....155
Connexion au Serveur d'administration en mode manuel. Utilitaire klmover 156
Paramètres des tâches....157
Mode d'interception....157
Mode de protection des objets....158
Analyse heuristique....158
Action à exécuter sur les objets infectés....159
Action à exécuter sur les objets suspects....159
Actions à exécuter sur des objets en fonction du type de menace 160
Exclusion des objets selon le nom....161
Exclusion des objets en fonction du nom de la menace 161
Analyse des objets composés....162
Durée maximum d'analyse d'un objet 162
Taille maximum de l'objet analysé 162
Source des mises à jour 162
Mode du serveur FTP 163
Délai d'attente pour la réponse du serveur FTP ou HTTP 163
Utilisation d'un serveur proxy lors de la connexion aux sources de mises à jour....163
Vérification de l'authenticité lors de l'accès au serveur proxy 164
Paramètres du serveur proxy....164
Répertoire de sauvegarde des mises à jour....164
Type de mises à jour....164
KASPERSKY LAB....165
INFORMATIONS SUR LE CODE TIERS....166
Code de programmation....166

BOOST 1.39.0 168
DEJAVU SANS 2.31 168
DROID SANS FALLBACK 169
EXPAT 1.95.8 171
LIBACL 2.2.45-1 172
ATTR 2.4.38-1 172
LIBFONTCONFIG 2.8 172
LIBFREETYPE 2.3.11 172
LIBICE 1.0.6 175
LIBPNG 1.2.44 175
LIBSM 1.1.1 175
LIBUTF 176
LIBX11 1.3.2 176
LIBXAU 1.0.5 187
LIBXCURSOR 1.1.10 187
LIBXDMCP 1.0.3 187
LIBXEXT 1.1.1 188
LIBXFIXES 4.0.4 190
LIBXI 1.3 191
LIBXINERAMA 1.1 192
LIBXML2 2.6.32 192
LIBXRANDR 1.3.0 192
LIBXRENDER 0.9.5 193
LIBXSLT 1.1.23 193
LZMALIB 4.43 194
NET-SNMP 5.5 194
QT 4.6.3 198
SQLITE 3.6.17 199
ZLIB 1.2.3 199
Code de programmation diffusé 199
REDIRFS 0.10 (MODIFIED) 199
Autre information 199

INTRODUCTION

Kaspersky Endpoint Security 8,0 for Linux (ci-après *Kaspersky Endpoint Security* ou *l'application*) protège les postes de travail fonctionnant sous le système d'exploitation Linux contre les programmes malveillants qui pénètrent par l'échange de fichiers.

Kaspersky Endpoint Security analyse les disques de l'ordinateur et 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 poste de travail à l'aide des protocoles SMB/CIFS et NFS.

DANS CETTE SECTION

Informations générales sur Kaspersky Endpoint Security 8

Obtention d'informations sur Kaspersky Endpoint Security 13

INFORMATIONS GÉNÉRALES SUR KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security 8 for Linux (ci-après *Kaspersky Endpoint Security* ou *l'application*) protège les postes de travail fonctionnant 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 poste de travail 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 Endpoint Security 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 Endpoint Security 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. Après chaque mise à jour des bases, Kaspersky Endpoint Security 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.

- Composer les statistiques et les rapports sur les résultats de l'utilisation.
- Actualiser, selon un horaire défini ou à la demande, les bases Kaspersky Endpoint Security depuis les serveurs 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 Endpoint Security:

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

PROTECTION EN TEMPS RÉEL ET ANALYSE À LA DEMANDE

Pour sécuriser les ordinateurs, 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 Endpoint Security lors du démarrage de l'ordinateur et elle est en service en continu. Kaspersky Endpoint Security analyse les fichiers à l'accès.

Kaspersky Endpoint Security vérifie qu'il n'y ait pas dans des fichiers de programmes malveillants de plusieurs types (cf. section "Programmes détectés par Kaspersky Endpoint Security" à la page 11). Lorsqu'un programme fait requête à un fichier de l'ordinateur (par exemple, l'enregistre et le lit), Kaspersky Endpoint Security 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 Endpoint Security détecte dans le fichier un programme malveillant, celui-ci 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.

PARTICULARITÉS DE L'ANALYSE DES LIENS SYMBOLIQUES ET MATÉRIELS

Lors de l'analyse des liens matériels et symboliques par Kaspersky Endpoint Security, 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 Endpoint Security 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 de l'ordinateur sera en danger!

Analyse des liens matériels

Quand Kaspersky Endpoint Security 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 INFECTÉS, SUSPECTS ET POSSÉDANT LE STATUT "AVERTISSEMENT"

Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security attribue à l'objet infecté le statut "Avertissement". La possibilité de faux-positif existe.

Kaspersky Endpoint Security 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 Endpoint Security isole des objets infectés et suspects détectés afin de protéger l'ordinateur contre une éventuelle action malveillante.

Placement des objets en quarantaine

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

Si le comportement d'un fichier vous permet de soupçonner qu'il renferme une menace alors que Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security les a réparés.

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 l'ordinateur. 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 Endpoint Security n'a pas pu préserver lors de la réparation, les rendant inaccessibles.

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

PROGRAMMES DÉTECTÉS PAR KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security est capable de détecter dans le système de fichiers de l'ordinateur beaucoup de programmes différents qui constituent une menace potentielle 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 Endpoint Security le rajoute à une catégorie déterminée possédant son propre niveau de sécurité (élevé, moyen ou bas).

Kaspersky Endpoint Security 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 Internet "-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 D'INFORMATIONS SUR KASPERSKY ENDPOINT SECURITY

Kaspersky Lab fournit différentes sources d'informations sur Kaspersky Endpoint Security. Sélectionnez la question qui vous convient le mieux en fonction de l'importance et de l'urgence.

Si vous avez déjà acheté Kaspersky Endpoint Security, vous pouvez vous adresser au Service du Support 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 UNE RECHERCHE AUTONOME

Vous pouvez utiliser les sources d'informations suivantes sur Kaspersky Endpoint Security:

- la page de Kaspersky Endpoint Security sur le site Internet de Kaspersky Lab;
- documentation;
- manuels d'aide.

La page sur le site Internet de Kaspersky Lab

http://www.kaspersky.com/fr/endpoint-security-linux

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

Documentation

Le **Manuel d'installation** décrit la fonction et l'utilisation de Kaspersky Endpoint Security, la configuration requise de l'ordinateur pour pouvoir installer Kaspersky Endpoint Security, 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 Endpoint Security à l'aide de l'utilitaire de la ligne de commande et Kaspersky Administration Kit.

Ces documentations au format PDF sont fournies avec Kaspersky Endpoint Security. Vous pouvez aussi télécharger les fichiers contenant les documents depuis la page de Kaspersky Endpoint Security sur le site de Kaspersky Lab.

Manuels d'aide

Vous pouvez consulter les fichiers "manuels d'aide" suivants afin d'obtenir des renseignements sur Kaspersky Endpoint Security:

- administration de Kaspersky Endpoint Security à l'aide de la ligne de commande:

/opt/kaspersky/kes4lwks/share/man/man1/kes4lwks-control.1.gz;

- configuration des paramètres généraux de Kaspersky Endpoint Security:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks.conf.5.gz;

- configuration de la tâche de protection en temps réel:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-oas.conf.5.gz;

- configuration des tâches d'analyse à la demande:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-ods.conf.5.gz;

- configuration des tâches de mise à jour:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-update.conf.5.gz;

- configuration des paramètres de stockage du dossier de quarantaine et des objets réservés avant leur réparation ou suppression:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-quarantine.conf.5.gz;

- configuration des paramètres du référentiel des événements:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-events.conf.5.gz;

- description de l'utilitaire qui modifie les paramètres de connexion avec le Serveur d'administration Kaspersky Administration Kit:

/opt/kaspersky/klnagent/share/man/man1/klmover.1.gz;

- description de l'utilitaire qui contrôle les paramètres de connexion avec le Serveur d'administration Kaspersky Administration Kit:

/opt/kaspersky/klnagent/share/man/man1/klnagchk.1.gz;

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

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

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application. En cas d'infection de votre ordinateur, ils vous aideront à éliminer dans la mesure du possible les programmes malveillants, ainsi qu'à surmonter leurs effets.

Avant de contacter le service du Support 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 du Support Technique

Vous pouvez poser vos questions aux experts du service du Support Technique en remplissant le formulaire en ligne dans le système de traitement des demandes des clients Helpdesk (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 du Support 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, indiquez *le code d'activation* de l'application ou *le nom du fichier de licence*.

L'ingénieur du service du Support Technique, vous enverra sa réponse dans votre Espace personnel (https://support.kaspersky.com/ru/PersonalCabinet), ainsi qu'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". Si vous ne trouvez pas le sujet qui vous concerne, sélectionnez "Question générale".
- **Nom et numéro de version de l'application**.
- **Texte de la demande**. Décrivez le plus exactement possible le problème que vous rencontrez.
- **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 du Support Technique.
- **Adresse de messagerie**. Il s'agit de l'adresse à laquelle les experts du Service du Support Technique enverront la réponse à votre question.

Assistance technique par téléphone

Si le problème est urgent, vous pouvez toujours téléphoner au Service du Support Technique dans votre ville. Si vous contactez le Support Technique français (http://partners.kaspersky.fr) ou international (http://support.kaspersky.com/fr/support/international) veuillez fournir les informations (http://support.kaspersky.com/fr/support/details) concernant votre ordinateur, ainsi que le logiciel antivirus y installé. Nos experts pourront ainsi vous venir en aide plus rapidement.

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.

DÉMARRAGE ET ARRÊT DE KASPERSKY ENDPOINT SECURITY

Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kes4lwks-supervisor est lancé sur l'ordinateur!

Par défaut, Kaspersky Endpoint Security est lancé automatiquement lors du démarrage du système d'exploitation (aux niveaux d'exécution par défaut adoptés pour chaque système d'exploitation). Kaspersky Endpoint Security lance toutes les tâches système ainsi que les tâches définies par l'utilisateur dont les paramètres de l'horaire (cf. section "Paramètres de l'horaire" à la page 134) contiennent la règle d'exécution PS.

Si vous arrêtez Kaspersky Endpoint Security, toutes les tâches en cours d'exécution seront arrêtées. Après le lancement réitéré de Kaspersky Endpoint Security, ces tâches ne reprendront pas automatiquement. Seules les tâches définies par l'utilisateur dont les paramètres de l'horaire (cf. section "Paramètres de l'horaire" à la page 134) contiennent la règle d'exécution PS seront à nouveau lancées.

- *Pour lancer Kaspersky Endpoint Security, exécutez la commande:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-app
  ```

- Pour arrêter *Kaspersky Endpoint Security*, saisissez l'instruction suivante:

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-app
  ```

- *Pour redémarrer Kaspersky Endpoint Security, exécutez la commande:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --restart-app
  ```

ADMINISTRATION DES TÂCHES DE KASPERSKY ENDPOINT SECURITY

Tâche – le composant de Kaspersky Endpoint Security qui implémente les fonctionnalités 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 Endpoint Security, etc.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-task-list
```

L'utilisateur peut gérer (cf. page 20) 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

Création d'une tâche d'analyse à la demande ou de mise à jour 19

Suppression de la tâche d'analyse à la demande ou de mise à jour 20

Administration de la tâche en mode manuel 20

Administration automatique des tâches 21

Consultation de l'état de la tâche 21

Consultation des statistiques de la tâche 22

CRÉATION D'UNE TÂCHE D'ANALYSE À LA DEMANDE OU DE MISE À JOUR

Une tâche de chaque type est créée lors de l'installation de Kaspersky Endpoint Security. Vous pouvez créer des tâches d'analyse à la demande et des tâches de mise à jour définies par l'utilisateur (cf. section "Création d'une tâche" à la page 83).

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--create-task <nom de la tâche> --use-task-type=ODS \
[--file=<nom du fichier de configuration>] [--file-format=<INI|XML>]
```

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 aura lieu avec les paramètres par défaut (cf. section "Paramètres de l'analyse par défaut" à la page 42).

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/kes4lwks/bin/kes4lwks-control \
--create-task <nom de la tâche> --use-task-type=Update \
--file=<chemin d'accès au fichier contenant les paramètres de la tâche>
```

SUPPRESSION DE LA TÂCHE D'ANALYSE À LA DEMANDE OU DE MISE À 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), **On-Demand Scan** (ID=9) et **Custom Scan** (ID=15)).

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

Pour supprimer une tâche, exécutez l'instruction suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --delete-task <ID de la tâche>
```

ADMINISTRATION DE LA TÂCHE 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/kes4lwks/bin/kes4lwks-control --start-task <ID de la tâche>
```

Pour arrêter une tâche, saisissez l'instruction suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task <ID de la tâche>
```

Pour suspendre une tâche, saisissez l'instruction suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --suspend-task <ID de la tâche>
```

Pour reprendre une tâche, saisissez l'instruction suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --resume-task <ID de la tâche>
```

ADMINISTRATION AUTOMATIQUE DES TÂCHES

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

L'horaire de la tâche est un ensemble de règles qui définissent l'heure de lancement et la durée d'exécution de la tâche.

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

- de protection en temps réel;
- d'analyse à la demande;
- de mise à jour des bases.

➧ *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/kes4lwks/bin/kes4lwks-control --get-schedule <ID de la tâche> \
   --file=<chemin d'accès complet au fichier>
   ```

2. Spécifiez les paramètres de la planification (cf. page 134).
3. Importez les paramètres de planification dans la tâche:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control --set-schedule <ID de la tâche> \
   --file=<chemin d'accès complet au fichier>
   ```

CONSULTATION DE L'ÉTAT DE LA TÂCHE

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

Les tâches de Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-control --get-task-state <ID de la tâche>
```

L'exemple suivant illustre l'affichage de la commande:

Exemple:

```
Name: On-demand scan

   Id: 9

   Class: ODS

   State: Stopped
```

CONSULTATION DES STATISTIQUES DE LA TÂCHE

Vous pouvez obtenir les statistiques du fonctionnement des tâches de Kaspersky Endpoint Security. Il est possible de consulter les statistiques pour les tâches suivantes:

- **Application** – statistiques générales de Kaspersky Endpoint Security;
- **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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \

--get-stat <type de la tâche> [--task-id <ID de la tâche>] --export-report=<chemin
d'accès complet>
```

MISE À JOUR DE KASPERSKY ENDPOINT SECURITY

Durant la validité de la licence, vous pouvez obtenir les mises à jour des bases de Kaspersky Endpoint Security.

Les bases sont des fichiers contenant des signatures qui permettent de détecter le code malveillant de menaces connues dans les objets analysés. 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 de l'ordinateur au minimum, téléchargez les mises à jour régulièrement.

Kaspersky Lab peut diffuser des paquets de mises à jour des modules logiciels de Kaspersky Endpoint Security. Les paquets de mises à jour sont répartis entre les paquets urgents (ou 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 Internet 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 Endpoint Security 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 Endpoint Security continuera d'utiliser les bases actualisées la dernière fois. Si les bases de Kaspersky Endpoint Security sont corrompues, vous pourrez revenir aux bases antérieures à la mise à jour.

Par défaut, si les bases de Kaspersky Endpoint Security ne sont pas mises à jour durant une semaine à partir de la dernière publication des mises à jour par Kaspersky Lab, Kaspersky Endpoint Security 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

Sélection de la source des mises à jour 24

Mise à jour depuis un répertoire local ou de réseau 24

Utilisation du serveur proxy 26

Retour à la version antérieure des bases 27

SÉLECTION DE LA SOURCE DES MISES À JOUR

La source des mises à jour (cf. page 162) est la source qui contient les mises à jour des bases de Kaspersky Endpoint Security. 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 Kaspersky Lab, saisissez l'instruction suivante:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.SourceType=KLServers
```

- *Pour sélectionner le serveur Kaspersky Administration Kit en tant que source des mises à jour, saisissez l'instruction suivante:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint Security depuis le répertoire local ou de réseau (cf. page 24).

MISE À JOUR DEPUIS UN RÉPERTOIRE LOCAL OU DE RÉSEAU

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 Endpoint Security 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.

2. Les mises à jour récupérées de la sorte sont placées dans un répertoire partagé.

3. Les autres ordinateurs sollicitent le répertoire partagé afin d'obtenir les mises à jour des bases de Kaspersky Endpoint Security.

- *Pour recevoir les mises à jour des bases de Kaspersky Endpoint Security 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 Endpoint Security.

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control --start-task <ID de la tâche de mise à jour>
```

Les bases de Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche de mise à jour> \
--file=<chemin d'accès complet au fichier>
```

UTILISATION D'UN SERVEUR PROXY

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

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 d'un serveur proxy lors de l'accès aux sources de mises à jour définies par l'utilisateur, saisissez l'instruction suivante:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche de mise à jour> \
CommonSettings.ProxyAuthType=Plain \
CommonSettings.ProxyAuthUser=user \
CommonSettings.ProxyAuthPassword=password
```

RETOUR À LA VERSION ANTÉRIEURE DES BASES

Avant d'appliquer les mises à jour des bases, Kaspersky Endpoint Security crée des copies de réserve des bases utilisées jusqu'à présent. Si la mise à jour échoue ou se solde par un échec, Kaspersky Endpoint Security 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 de Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-control --start-task 14
```

PROTECTION EN TEMPS RÉEL 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 Endpoint Security. 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

Paramètres de protection par défaut 28

Création de la zone de protection 30

Restriction de la zone de protection à l'aide de masques et d'expressions régulières 31

Exclusion des objets de la protection 31

Sélection du mode d'interception 34

Sélection du mode de protection des objets 35

Utilisation de l'analyse heuristique 35

Utilisation du mode d'analyse en fonction des droits d'accès aux objets 36

Sélection de l'action à réaliser sur les objets détectés 37

Sélection des actions à exécuter en fonction du type de menace 38

Optimisation de l'analyse 39

Compatibilité entre Kaspersky Anti-Virus et d'autres applications de Kaspersky Lab 40

PARAMÈTRES DE PROTECTION PAR DÉFAUT

Dans Kaspersky Endpoint Security pour la tâche de protection en temps réel, les paramètres suivants sont établis par défaut:

```
ProtectionType="Full"

TotalScanners=4

[ScanScope]

UseScanArea=yes

AreaMask="*"

UseAccessUser=no

AreaDesc="All objects"
```

```
[ScanScope:AreaPath]

Path="/"

[ScanScope:AccessUser]

[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=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Recommended"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

CRÉATION DE LA ZONE DE PROTECTION

Faites attention aux particularités de l'analyse des liens matériels et symboliques (cf. page 9).

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 de l'ordinateur.

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 31).

Kaspersky Endpoint Security analysera les objets dans les zones indiquées dans l'ordre d'énumération de celles-ci dans le fichier de configuration. 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 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/kes4lwks/bin/kes4lwks-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 36);
     - **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/kes4lwks/bin/kes4lwks-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 réel à l'aide de l'instruction suivante:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

RESTRICTION DE LA ZONE DE PROTECTION À L'AIDE DE MASQUES ET D'EXPRESSIONS RÉGULIÈRES

Kaspersky Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell permettent de spécifier le modèle du nom de fichier pour l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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

Création d'une zone d'exclusion globale 32

Exclusion des objets de la zone de protection 32

Exclusion des objets en fonction des droits d'accès 33

Exclusion des objets en fonction du nom de la menace découverte 34

CRÉATION 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

EXCLUSION DES OBJETS DE LA ZONE DE PROTECTION

Kaspersky Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

EXCLUSION DES OBJETS EN FONCTION DES DROITS D'ACCÈS

Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

EXCLUSION DES OBJETS EN FONCTION DU NOM DE LA MENACE DÉCOUVERTE

Si Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security.

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 ECMA-262.

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

SÉLECTION DU MODE D'INTERCEPTION

Kaspersky Endpoint Security 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 Endpoint Security.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=KernelOnly
```

- *Pour activer l'intercepteur des opérations Samba, saisissez l'instruction suivante:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=SambaOnly
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=Full
```

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

SÉLECTION DU MODE DE PROTECTION DES OBJETS

Par mode de protection (cf. page 158), il faut entendre la condition de l'activation de la tâche de protection en temps réel. Kaspersky Endpoint Security 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 Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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 réeldans le fichier à l'aide de l'instruction suivante:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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**, **Deep** ou **Recommended** 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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

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

Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-control \
   --get-settings 8 --file=<chemin d'accès au fichier>
   ```

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

   - attribuez la 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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

SÉLECTION DE L'ACTION À RÉALISER SUR LES OBJETS DÉTECTÉS

Suite à l'analyse, Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Endpoint Security place les objets en quarantaine.
- **Remove**. Kaspersky Endpoint Security supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

SÉLECTION DES ACTIONS À EXÉCUTER 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Endpoint Security place les objets en quarantaine.

- **Remove**. Kaspersky Endpoint Security supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<chemin d'accès au fichier>
   ```

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--get-settings 8 --file=<chemin d'accès au fichier>
```

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

   - attribuez la valeur **yes** au paramètre **UseSizeLimit** dans la section `[ScanScope]`;
   - 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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

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

Pour garantir la compatibilité de Kaspersky Endpoint Security 8 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 Endpoint Security 8 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

- *Pour configurer la compatibilité entre Kaspersky Endpoint Security 8 et Kaspersky Anti-Spam, veuillez procédez comme suit:*

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

- *Pour configurer la compatibilité entre Kaspersky Endpoint Security 8 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<chemin d'accès au fichier>
```

ANALYSE À 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 Endpoint Security peut exécuter plusieurs tâches d'analyse à la demande à la fois.

Kaspersky Endpoint Security 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, ainsi que 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 Endpoint Security permet également d'analyser rapidement les fichiers et les répertoires (cf. section "Analyse rapide des fichiers et des répertoires" à la page 43) depuis la ligne de commande.

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

DANS CETTE SECTION

Paramètres de l'analyse par défaut 42

Analyse rapide des fichiers et des répertoires 43

Composition de la zone d'analyse 45

Restriction de la zone d'analyse à l'aide de masques et d'expressions régulières 46

Exclusion des objets de l'analyse 46

Utilisation de l'analyse heuristique 49

Sélection de l'action à réaliser sur les objets détectés 49

Sélection des actions à exécuter en fonction du type de menace 51

Optimisation de l'analyse 52

Sélection de la priorité de la tâche 53

PARAMÈTRES DE L'ANALYSE PAR DÉFAUT

Dans Kaspersky Endpoint Security pour la tâche d'analyse à la demande, les paramètres suivants sont établis par défaut:

```
ScanPriority="System"

[ScanScope]

UseScanArea=yes

AreaMask="*"

AreaDesc="All objects"
```

```
[ScanScope:AreaPath]

Path="/"

[ScanScope:ScanSettings]

ScanArchived=yes

ScanSfxArchived=yes

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=no

TimeLimit=120

UseSizeLimit=no

SizeLimit=0

InfectedFirstAction="Recommended"

InfectedSecondAction="Skip"

SuspiciousFirstAction="Recommended"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Recommended"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

ANALYSE RAPIDE DES FICHIERS ET DES RÉPERTOIRES

Kaspersky Endpoint Security permet d'analyser rapidement les fichiers et les répertoires sans avoir à configurer une zone d'analyse (cf. section "Composition de la zone d'analyse" à la page 45). 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 Endpoint Security.

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

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --scan-file <chemin d'accès au fichier ou au répertoire>
  ```

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

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-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 par défaut à l'aide de l'instruction --scan-file:

```
ScanPriority="System"

[ScanScope]

UseScanArea=yes

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=yes

HeuristicLevel="Recommended"
```

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/kes4lwks/bin/kes4lwks-control --action <action> --scan-file <chemin d'accès au fichier ou au répertoire>
```

COMPOSITION DE LA ZONE D'ANALYSE

Faites attention aux particularités de l'analyse des liens matériels et symboliques (cf. page 9).

La tâche d'analyse à la demande analyse les objets du système de fichiers de l'ordinateur 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 46).

Kaspersky Endpoint Security analysera les objets dans les zones indiquées dans l'ordre d'énumération de celles-ci dans le fichier de configuration. 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 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: suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

RESTRICTION DE LA ZONE D'ANALYSE À L'AIDE DE MASQUES ET D'EXPRESSIONS RÉGULIÈRES

Kaspersky Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell permettent de spécifier le modèle du nom de fichier pour l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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

Création d'une zone d'exclusion globale 47

Exclusion des objets de la zone d'analyse 47

Exclusion des objets en fonction du nom de la menace découverte 48

CRÉATION 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

EXCLUSION DES OBJETS DE LA ZONE D'ANALYSE

Kaspersky Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

EXCLUSION DES OBJETS EN FONCTION DU NOM DE LA MENACE DÉCOUVERTE

Si Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security.

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 ECMA-262.

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

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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/kes4lwks/bin/kes4lwks-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**, **Deep** ou **Recommended** 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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

SÉLECTION DE L'ACTION À RÉALISER SUR LES OBJETS DÉTECTÉS

Suite à l'analyse, Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Endpoint Security place les objets en quarantaine.
- **Remove**. Kaspersky Endpoint Security supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
   ```

SÉLECTION DES ACTIONS À EXÉCUTER 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Quarantine**. Kaspersky Endpoint Security place les objets en quarantaine.
- **Remove**. Kaspersky Endpoint Security supprime l'objet après avoir créé une copie de sauvegarde.
- **Skip**. Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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:
   - attribuez la valeur **yes** au paramètre **UseTimeLimit** dans la section `[ScanScope]`;
   - 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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:
   - attribuez la valeur **yes** au paramètre **UseSizeLimit** dans la section `[ScanScope]`;
   - 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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche> --file=<chemin d'accès complet au fichier>
```

SÉLECTION DE LA PRIORITÉ DE LA TÂCHE

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 l'ordinateur 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 l'ordinateur 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/kes4lwks/bin/kes4lwks-control \
--set-settings <ID de la tâche> ScanPriority=<priorité>
```

ISOLATION DES OBJETS SUSPECTS. COPIE DE SAUVEGARDE

Kaspersky Endpoint Security 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.

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 Endpoint Security 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 Endpoint Security enregistre dans le référentiel des copies des objets avant de tenter de les réparer ou de les supprimer.

Si l'objet fait partie d'un objet conteneur, Kaspersky Endpoint Security enregistre l'objet conteneur entier dans le répertoire de sauvegarde de réserve. Par exemple, si Kaspersky Endpoint Security 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 101).

DANS CETTE SECTION

Consultation des statistiques sur les objets mis en quarantaine 54

Analyse des objets mis en quarantaine 55

Mise des fichiers en quarantaine manuellement 56

Consultation de l'identificateur des objets 56

Restauration des objets 57

Suppression des objets 58

CONSULTATION DES STATISTIQUES SUR LES OBJETS MIS EN QUARANTAINE

Vous pouvez recevoir des statistiques brèves ou détaillées sur les objets mis en quarantaine.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 succinctes, saisissez l'instruction suivante:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -S --get-stat Quarantine
```

Si les dates de début et de fin du rapport ne sont pas définies (cf. page 72), les statistiques seront proposées à partir de l'installation de Kaspersky Endpoint Security.

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 Endpoint Security.
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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security peut considérer certains d'entre eux comme étant sains (la valeur du champ **Type** (cf. page 101) pour ces objets devient **Clean**). Les autres objets peuvent être reconnus par Kaspersky Endpoint Security comme étant infectés.

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

*Pour lancer la tâche **Analyse des objets mis en quarantaine**, procédez comme suit:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 10
```

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

PARAMÈTRES DE LA TÂCHE "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 LA TÂCHE "ANALYSE DES OBJETS EN QUARANTAINE"	VALEUR
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***

PARAMETRES DE SECURITE	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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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/kes4lwks/bin/kes4lwks-control -Q --query "(OrigType!=s'Backup')"
```

L'exemple suivant illustre l'affichage de la commande:

Exemple:

```
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/kes4lwks/bin/kes4lwks-control -Q --query "(OrigType==s'Backup')"
```

L'exemple suivant illustre l'affichage de la commande:

Exemple:

```
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 de l'ordinateur.

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 Endpoint Security 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 101) pour ces objets devient **Clean**).

- Si vous considérez l'objet comme ne représente aucun danger pour l'ordinateur et que vous voulez l'utiliser. Pour que Kaspersky Endpoint Security 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 **Exclusion des objets selon le nom** (cf. page 161) ou **Exclusion des objets selon le nom de la menace** (cf. page 161) 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/kes4lwks/bin/kes4lwks-control --restore <ID de l'objet>
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 l'ordinateur, 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q \
--mass-remove --query "(OrigType!=s'Backup')"
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 96).

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.

PRÉSENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un accord conclu entre une personne physique ou morale détenant une copie légale de Kaspersky Endpoint Security et Kaspersky Lab ZAO. Ce contrat accompagne chaque application de Kaspersky Lab. Il reprend des informations détaillées sur les droits et les restrictions d'utilisation de Kaspersky Endpoint Security.

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 Endpoint Security;
- mise à jour des modules logiciels de Kaspersky Endpoint Security.

Pour en profiter, vous devez acheter et activer une licence (cf. rubrique "Présentation des licences de Kaspersky Endpoint Security" à la page 59).

A PROPOS DES LICENCES DE KASPERSKY ENDPOINT SECURITY

La licence représente le droit d'utiliser Kaspersky Endpoint Security et les services complémentaires associés offerts par 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 59). Le type de services dépend du type de licence.

Il existe différents types de licence:

- *Evaluation* - licence gratuite à durée de validité réduite (par exemple, 30 jours) qui permet de découvrir Kaspersky Endpoint Security.

  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 Endpoint Security deviennent inopérantes.

- *La licence commerciale* - est une licence payante avec une durée de validité limitée (par exemple, un an) octroyée à l'achat de Kaspersky Endpoint Security. 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 Endpoint Security 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 Endpoint Security sont accessibles, ainsi que les services complémentaires.

  À l'issue de la période de validité de la licence commerciale, Kaspersky Endpoint Security continue à remplir toutes ses fonctions, à l'exception de la mise à jour des bases antivirus. 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 Endpoint Security" à la page 60) associé à la licence.

PRÉSENTATION DES FICHIERS DE LICENCE DE KASPERSKY ENDPOINT SECURITY

Le fichier de licence est le moyen technique qui permet d'activer la licence associée (cf. rubrique "A propos des licences de Kaspersky Endpoint Security" à la page 59), et constitue de ce fait votre droit d'utiliser l'application et les services complémentaires (cf. page 59).

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 60): 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 Endpoint Security, le nouveau fichier remplace le fichier existant. Le fichier antérieur sera supprimé.

Si vous installez un fichier de licence en tant que fichier réserve, alors qu'il existe déjà un fichier de licence réserve pour Kaspersky Endpoint Security, 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--install-suppl-key <nom du fichier de licence>
```

CONSULTATION DES INFORMATIONS RELATIVES À 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 les informations relatives à la licence (cf. page 59), saisissez l'instruction suivante:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 60).
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 Endpoint Security.
License period	Durée de validité de la licence (cf. page 59).

Exemple d'instruction:

```
License info:

      Application name:                  Kaspersky Anti-Virus BO Suite International
Edition. 10-14 Workstation 6 months Beta License

      Key file creation date:            2010-09-03

      Key file expiration date:          2011-04-04

      License number:                    1222-0003F4-0A451011

      License type:                      Beta

      Usage restriction:                 10 Workstations

      License period:                    183
```

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/kes4lwks/bin/kes4lwks-control \
  --revoke-active-key
  ```

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

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control \
  --revoke-suppl-key
  ```

CONSULTATION DE LA CONVENTION DE LICENCE

Le contrat de licence est un accord conclu entre une personne physique ou morale détenant une copie légale de Kaspersky Endpoint Security et Kaspersky Lab ZAO. Ce contrat accompagne chaque application de Kaspersky Lab. Il reprend des informations détaillées sur les droits et les restrictions d'utilisation de Kaspersky Endpoint Security.

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/kes4lwks/share/doc/LICENSE`.

CRÉATION 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 73);
- rapports sur le fonctionnement des composants de Kaspersky Endpoint Security (cf. page 72).

La ligne de commande vous permet d'obtenir les rapports sur le fonctionnement de composants particuliers.

Vous pouvez exécuter les opérations suivantes:

- créer des rapports sur les périodes de temps spécifiées;
- enregistrer les rapports créés dans les formats suivants: HTML ou CSV.

LES COMMANDES D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY DEPUIS LA LIGNE DE COMMANDE

Lors de la saisie des commandes de Kaspersky Endpoint Security, 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 Endpoint Security est donnée dans le tableau suivant.

Tableau 5. Liste des commandes de Kaspersky Endpoint Security

COMMANDES	DESCRIPTION
--help (cf. page 68)	Affiche les renseignements sur les commandes de Kaspersky Endpoint Security.
Commandes d'administration de Kaspersky Endpoint Security	
--start-app (cf. page 69)	Lance Kaspersky Endpoint Security.
--restart-app (cf. page 69)	Redémarre Kaspersky Endpoint Security.
--stop-app (cf. page 69)	Arrête Kaspersky Endpoint Security.
--scan-file (cf. page 70)	Analyse fichiers ou répertoires.
-R (cf. page 70)	Remise à l'état antérieur vers la version précédente des bases.
Commandes de réception de la statistique de Kaspersky Endpoint Security	
-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 71)	Fait afficher les informations sur Kaspersky Endpoint Security.
-S --get-stat (cf. page 72)	Crée les rapports sur le fonctionnement de Kaspersky Endpoint Security et de ses composants.
-S --top-viruses (cf. page 73)	Crée les rapports sur les menaces les plus fréquentes sur l'ordinateur.
-S --clean-stat (cf. page 74)	Supprime les statistiques cumulées sur le fonctionnement de Kaspersky Endpoint Security.
Commandes de l'affichage des événements de Kaspersky Endpoint Security	
-W (cf. page 69)	Fait activer l'affichage des événements de Kaspersky Endpoint Security.
Commandes d'administration des paramètres de Kaspersky Endpoint Security et des tâches	

COMMANDES	DESCRIPTION
-T	Préfix; désigne que la commande appartient au groupe des commandes d'administration des paramètres de Kaspersky Endpoint Security / d'administration des tâches (facultatif).
-T --get-app-settings (cf. page 75)	Fait afficher les paramètres généraux de Kaspersky Endpoint Security.
-T --set-app-settings (cf. page 76)	Installe les paramètres généraux de Kaspersky Endpoint Security.
-T --get-task-list (cf. rubrique "Consultation de la liste des tâches de Kaspersky Endpoint Security" cf. page 77)	Reprend la liste des tâches en cours de Kaspersky Endpoint Security.
-T --get-task-state (cf. page 78)	Fait afficher l'état de la tâche spécifiée (par exemple, En cours, Arrêtée, Suspendue).
-T --start-task (cf. page 80)	Lance la tâche.
-T --stop-task (cf. page 80)	Arrête la tâche.
-T --suspend-task (cf. page 80)	Suspend la tâche.
-T --resume-task (cf. page 81)	Reprend la tâche.
-T --get-settings (cf. page 81)	Fait afficher les paramètres de la tâche.
-T --set-settings (cf. page 82)	Installe les paramètres de la tâche.
-T --create-task (cf. page 83)	Crée la tâche de type spécifié; importe dans la tâche les paramètres depuis le fichier de configuration spécifié.
-T --delete-task (cf. page 84)	Supprime la tâche.
-T --set-schedule (cf. page 84)	Détermine les paramètres de l'horaire de la tâche / les importe dans la tâche depuis le fichier de configuration.
-T --get-schedule (cf. page 85)	Fait afficher les paramètres de l'horaire de la tâche.
-T --del-schedule (cf. page 86)	Établit les paramètres de l'horaire d'une tâche qui sont définis par défaut.
-T --show-schedule (cf. page 86)	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 88)	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 (cf. rubrique "Consultation des informations relatives à la licence avant l'installation du fichier de licence" cf. page 89)	Affiche les informations sur la licence depuis le fichier de clé sans installer la licence.
-L --get-installed-keys (cf. page 90)	Fait afficher les informations sur les licences installées.
-L --query-status (cf. page 88)	Fait afficher l'état des licences installées.
-L --install-active-key (cf. page 91)	Installe la licence active.
-L --install-suppl-key (cf. page 91)	Installe la licence supplémentaire.
-L --revoke-active-key (cf. page 92)	Supprime la licence active.
-L --revoke-suppl-key (cf. page 92)	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 92)	Fait afficher la courte statistique du répertoire de sauvegarde.
-Q --query (cf. page 93)	Fait afficher les informations sur les objets dans le répertoire de sauvegarde.
-Q --get-one (cf. page 93)	Fait afficher les informations sur un seul objet du répertoire de sauvegarde.
-Q --restore (cf. page 94)	Restaure les objets depuis le répertoire de sauvegarde.
-Q --add-object (cf. page 94)	Met la copie de l'objet en quarantaine.
-Q --remove (cf. page 95)	Supprime l'objet du répertoire de sauvegarde.
-Q --export (cf. page 95)	Exporte les objets depuis le répertoire de sauvegarde dans le répertoire spécifié.
-Q --import (cf. page 96)	Importe les objets dans le répertoire de sauvegarde depuis le répertoire spécifié dans lequel ils ont été exportés avant.
-Q --mass-remove (cf. page 96)	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 97)	Affiche le nombre d'événement filtrés du journal des événements ou du fichier de rotation indiqué.
-E --query (cf. page 98)	Affiche le nombre d'événement filtrés du journal des événements ou du fichier de rotation indiqué.
-E --period (cf. page 99)	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 99)	Exécute la rotation du journal des événements.
-E --remove (cf. page 99)	Supprime les événements du journal des événements ou du fichier de rotation indiqué.

DANS CETTE SECTION

Affichage des renseignements sur les commandes de Kaspersky Endpoint Security 68

Lancement de Kaspersky Endpoint Security 69

Arrêt de Kaspersky Endpoint Security 69

Redémarrage de Kaspersky Endpoint Security 69

Activation de l'affichage des événements 69

Analyse rapide des fichiers et des répertoires 70

Remise à l'état antérieur à la mise à jour des bases de Kaspersky Endpoint Security 70

Commandes de réception des statistiques et des rapports 71

Commandes d'administration des paramètres de Kaspersky Endpoint Security et des tâches 75

Commandes d'administration des licences 88

Commandes d'administration de la quarantaine et du répertoire de sauvegarde 92

Instructions d'administration du journal des événements 97

Restriction de la sélection à l'aide des filtres 100

AFFICHAGE DES RENSEIGNEMENTS SUR LES COMMANDES DE KASPERSKY ENDPOINT SECURITY

L'instruction kes4lwks-control avec l'argument --help <ensemble des commandes de Kaspersky Endpoint Security> affiche les renseignements sur les commandes de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control --help [<ensemble des commandes de Kaspersky Endpoint Security>]
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ensemble des commandes de Kaspersky Endpoint Security>	Spécifiez l'ensemble des commandes de Kaspersky Endpoint Security 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 Endpoint Security; -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 Endpoint Security; -E [--event-log] – commandes d'administration des événements de Kaspersky Endpoint Security.

LANCEMENT DE KASPERSKY ENDPOINT SECURITY

Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kes4lwks-supervisor est lancé sur l'ordinateur!

La commande kes4lwks-control avec l'argument --start-app lance Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control --start-app
```

ARRÊT DE KASPERSKY ENDPOINT SECURITY

Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kes4lwks-supervisor est lancé sur l'ordinateur!

La commande kes4lwks-control avec l'argument --stop-app arrête Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control --stop-app
```

REDÉMARRAGE DE KASPERSKY ENDPOINT SECURITY

Avant d'exécuter les actions ou les instructions décrites ci-dessous, assurez-vous que le service kes4lwks-supervisor est lancé sur l'ordinateur!

La commande kes4lwks-control avec l'argument --restart-app lance Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control --restart-app
```

ACTIVATION DE L'AFFICHAGE DES ÉVÉNEMENTS

La commande -W fait activer le mode d'affichage des événements de Kaspersky Endpoint Security. Vous pouvez utiliser cette commande toute seule pour afficher tous les événements de Kaspersky Endpoint Security, ainsi que ensemble avec la commande --start-task (lancer la tâche (cf. rubrique "Lancement d'une tâche" à la page 80)) 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

```
kes4lwks-control -W [--file=<nom du fichier>]
```

Exemples:

- *Activer le mode d'affichage des événements de Kaspersky Endpoint Security:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control -W
  ```

Activer le mode de sauvegarde des événements de Kaspersky Endpoint Security dans le fichier; enregistrer les événements dans le fichier du registre 081808.xml du répertoire en cours:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
-W --file 081808.xml
```

CLE	SPECIFICATION ET VALEURS POSSIBLES
--file <nom du fichier>	Nom du fichier du registre dans lequel seront enregistrées les informations sur les événements de Kaspersky Endpoint Security. Le format du fichier du registre sauvegardé est XML.

ANALYSE RAPIDE DES FICHIERS ET DES RÉPERTOIRES

L'instruction kes4lwks-control avec l'argument --scan-file réalise une analyse rapide des fichiers et des répertoires.

Syntaxe de la commande

```
kes4lwks-control --action <action> --scan-file <chemin d'accès au fichier ou au
répertoire>[ <chemin d'accès au fichier ou au répertoire> ...]
```

ARGUMENT, CLES	SPECIFICATION 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 Endpoint Security.
--action <action>	Clé facultative. Valeurs possibles: • **Recommended** – exécuter l'action recommandée. • **Cure** – réparer. • **Quarantine** – mettre en quarantaine. • **Remove** – supprimer. • **Skip** – ignorer. Valeur par défaut: **Skip**.

REMISE À L'ÉTAT ANTÉRIEUR À LA MISE À JOUR DES BASES DE KASPERSKY ENDPOINT SECURITY

Avant d'appliquer les mises à jour des bases, Kaspersky Endpoint Security crée des copies de réserve des bases utilisées jusqu'à présent. Si la mise à jour échoue ou se solde par un échec, Kaspersky Endpoint Security 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 de Kaspersky Endpoint Security a été développée à cette fin.

Syntaxe d'exécution de la tâche

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -R
```

COMMANDES DE RÉCEPTION DES STATISTIQUES ET DES RAPPORTS

DANS CETTE SECTION

Consultation des informations sur le programme 71

Consultation des rapports sur le fonctionnement de Kaspersky Endpoint Security 72

Consultation des rapports sur les menaces les plus fréquentes 73

Suppression des statistiques de fonctionnement de Kaspersky Endpoint Security 74

CONSULTATION DES INFORMATIONS SUR LE PROGRAMME

La commande --app-info fait afficher les informations sur Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control [-S] --app-info [--export-report=<nom du fichier>] \
[--report-type=<format du fichier du rapport>]
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--export-report=<nom du fichier du rapport>	Clé facultative. Le nom du fichier à enregistrer les informations obtenues. 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 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 spécifié par la clé --export-report, est déterminé 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.

L'instruction affiche les informations suivantes:

CHAMP	DESCRIPTION
Name	Nom de Kaspersky Endpoint Security
Version	Version de Kaspersky Endpoint Security
Install date	Date et heure de la dernière installation de Kaspersky Endpoint Security
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 ENDPOINT SECURITY

La commande --get-stat fait afficher les statistiques sur le fonctionnement de Kaspersky Endpoint Security; permet de créer des rapports sur le fonctionnement de certains composants de Kaspersky Endpoint Security pour des périodes de temps spécifiées; permet d'enregistrer les rapports dans les fichiers.

Syntaxe de la commande

```
kes4lwks-control [-S] --get-stat <composant de Kaspersky Endpoint Security> \
[--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>] [--use-name]
```

Exemples:

- *Pour consulter la statistique du fonctionnement de Kaspersky Endpoint Security:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-stat Application
```

- *Pour afficher la statistique de la protection en temps réel pour janvier 2009:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-stat OAS --from=2009-01-01 --to=2009-01-31
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<composant de Kaspersky Endpoint Security>	Spécifiez le composant de Kaspersky Endpoint Security, 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; Lors de l'indication de la date et de l'heure, il faut placer toutes les expressions entre guillemets, et entre les valeurs de la date et de l'heure, il faut mettre l'espace. • 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 Endpoint Security.

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--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; Lors de l'indication de la date et de l'heure, il faut placer toutes les expressions entre guillemets, et entre les valeurs de la date et de l'heure, il faut mettre l'espace. • 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 analyse à la demande et mise à jour)>	Numéro d'identification de la tâche d'analyse à la demande dans Kaspersky Endpoint Security. Le rapport comprendra la statistique de la tâche d'analyse à la demande ou de mise à jour 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 spécifié par la clé --export-report, est déterminé 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.
--use-name -N	Nom de la tâche.

CONSULTATION DES RAPPORTS SUR LES MENACES LES PLUS FRÉQUENTES

La commande --top-viruses affiche les informations sur les programmes malveillants détectés dans la majorité des objets sur l'ordinateur durant la période de temps spécifiée; permet d'enregistrer le rapport dans le fichier.

Syntaxe de la commande

```
kes4lwks-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>]
```

Exemples:

- *Pour recevoir les informations sur cinq programmes malveillants les plus fréquents sur l'ordinateur pour janvier 2009, enregistrer le rapport dans le fichier /home/kavreports/2009_01_top_viruses.html:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--top-viruses 5 --from=2009-01-01 --to=2009-01-31 \
--export-report=/home/kavreports/2009_01_top_viruses.html
```

ARGUMENT, CLES	SPECIFICATION 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 l'ordinateur.
--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 Endpoint Security.
--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.
--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 spécifié par la clé --export-report, est déterminé 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.

SUPPRESSION DES STATISTIQUES DE FONCTIONNEMENT DE KASPERSKY ENDPOINT SECURITY

Commande --clean-stat supprime les statistiques cumulées de fonctionnement de Kaspersky Endpoint Security.

COMMANDES D'ADMINISTRATION DES PARAMÈTRES DE KASPERSKY ENDPOINT SECURITY ET DES TÂCHES

DANS CETTE SECTION

Obtention des paramètres généraux de Kaspersky Endpoint Security: ... 75

Modification des paramètres généraux de Kaspersky Endpoint Security: ... 76

Consultation de la liste des tâches de Kaspersky Endpoint Security ... 77

Consultation de l'état de la tâche ... 78

Lancement d'une tâche ... 80

Arrêt d'une tâche ... 80

Suspension d'une tâche ... 80

Reprise d'une tâche ... 81

Obtention des paramètres d'une tâche ... 81

Modification des paramètres de la tâche ... 82

Création d'une tâche ... 83

Suppression d'une tâche ... 84

Obtention des paramètres de l'horaire d'une tâche ... 84

Modification des paramètres de l'horaire d'une tâche ... 85

Suppression de l'horaire de la tâche ... 86

Recherche d'événements selon la planification ... 86

OBTENTION DES PARAMÈTRES GÉNÉRAUX DE KASPERSKY ENDPOINT SECURITY

L'instruction --get-app-settings fait afficher les paramètres généraux de Kaspersky Endpoint Security (cf. page 137). Cette instruction permet également d'obtenir les paramètres généraux de Kaspersky Endpoint Security définis à l'aide des arguments de l'instruction.

Vous pouvez utiliser cette commande pour modifier les paramètres généraux de Kaspersky Endpoint Security, installé sur l'ordinateur:

1. Enregistrez les paramètres généraux de Kaspersky Endpoint Security 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 Endpoint Security à l'aide de l'instruction --set-app-settings (cf. page 76). Kaspersky Endpoint Security utilisera les nouvelles valeurs des paramètres après que vous aurez arrêté et relancé le service Kaspersky Endpoint Security à l'aide des commandes --stop-app et --start-app.

Vous pouvez utiliser le fichier de configuration créé pour importer les paramètres dans Kaspersky Endpoint Security qui est installé sur un autre ordinateur.

Syntaxe de la commande

```
kes4lwks-control [-T] \
--get-app-settings [--file=<nom du fichier de configuration> \>] [--file-format=<INI|XML>]
kes4lwks-control [-T] --get-app-settings [<nom du paramètre>]
```

Exemples:

- *Exportez les paramètres généraux de Kaspersky Endpoint Security dans le fichier possédant le nom kav_config.xml. Enregistrer le fichier créé dans le répertoire en cours:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-app-settings -F kav_config.xml
```

- *Affiche la valeur du paramètre TraceLevel:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-app-settings TraceLevel
```

CLES	SPECIFICATION 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 Endpoint Security. 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 PARAMÈTRES GÉNÉRAUX DE KASPERSKY ENDPOINT SECURITY

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 Endpoint Security (cf. page 137).

Vous pouvez utiliser cette commande pour modifier les paramètres généraux de Kaspersky Endpoint Security:

1. Enregistrez les paramètres généraux de Kaspersky Endpoint Security dans le fichier de configuration à l'aide de l'instruction --get-app-settings (cf. page 75).

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 Endpoint Security à l'aide de la commande --set-app-settings. Kaspersky Endpoint Security utilisera les nouvelles valeurs des paramètres après que vous aurez arrêté et relancé le service Kaspersky Endpoint Security à l'aide des commandes --stop-app et --start-app ou à l'aide de la commande --restart-app.

Syntaxe de la commande

```
kes4lwks-control [-T] --set-app-settings \
--file=<nom du fichier de configuration> [--file-format=<INI|XML>]
kes4lwks-control [-T] \
--set-app-settings <nom du paramètre>=<valeur du paramètre> \
<nom du paramètre>=<valeur du paramètre>
```

Exemples:

- *Importez dans Kaspersky Endpoint Security les paramètres généraux depuis le fichier de configuration possédant le nom /home/test/kav_config.xml:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-app-settings -F /home/test/kav_config.xml
```

- *Déterminer le niveau de détails dans le registre du tracé "Evénements importants":*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-app-settings TraceLevel=Warning
```

CLES	SPECIFICATION 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 Endpoint Security, 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 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 TÂCHES DE KASPERSKY ENDPOINT SECURITY

La commande --get-task-list reprend la liste des tâches disponibles de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kes4lwks-control [-T] --get-task-list
```

Les informations suivantes sur les tâches de Kaspersky Endpoint Security 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 Endpoint Security.
Id	Le numéro d'identification de la tâche (nom alternatif que Kaspersky Endpoint Security attribue à la tâche lors de sa création).

Class	Type de tâche de Kaspersky Endpoint Security. 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); Rollback – la tâche de remise à la version précédente des bases (ID=14); • 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 – assure le "serveur des licences" (ID=5); EventStorage - assure le service du journal des événements (ID=11);
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'ÉTAT DE LA TÂCHE

La commande --get-task-state reprend l'état de la tâche spécifiée (par exemple, En cours d'exécution, Terminée, Suspendue).

Syntaxe de la commande

```
kes4lwks-control [-T] --get-task-state <ID de la tâche> [--use-name]
```

Exemple:

- *Obtenir l'état de la tâche avec ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-task-state 9
```

ARGUMENTS, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande kes4lwks-control --get-task-list.
--use-name -N	Nom de la tâche.

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; les noms des tâches de système est attribué par Kaspersky Endpoint Security.
Id	Le numéro d'identification de la tâche (nom alternatif que Kaspersky Endpoint Security attribue à la tâche lors de sa création).
Class	Type de tâche de Kaspersky Endpoint Security. 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); Rollback – la tâche de remise à la version précédente des bases (ID=14); • 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 – assure le "serveur des licences" (ID=5); EventStorage - assure le service du journal des événements (ID=11);
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 TÂCHE

La commande --start-task lance la tâche avec le numéro d'identification spécifié. Cette instruction peut être exécutée avec l'argument -W (cf. page 69) 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

```
kes4lwks-control --start-task <ID de la tâche> --[progress] [--use-name]
```

Exemple:

- *Lancer la tâche avec ID=6:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 6
  ```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande -T --get-task-list.
--progress	Affiche la progression de l'exécution de la tâche.
--use-name -N	Nom de la tâche.

ARRET D'UNE TACHE

La commande --stop-task lance la tâche avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kes4lwks-control [-T] --stop-task <ID de la tâche> [--use-name]
```

Exemple:

- *Arrêter la tâche avec ID=6:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task 6
  ```

ARGUMENT	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande kes4lwks-control -T--get-task-list.
--use-name -N	Nom de la tâche.

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

```
kes4lwks-control [-T] --suspend-task <ID de la tâche> [--use-name]
```

Exemple:

- *Suspendre la tâche avec ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --suspend-task 9
```

ARGUMENT	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande kes4lwks-control -T --get-task-list.
--use-name -N	Nom de la tâche.

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 80).

Syntaxe de la commande

```
kes4lwks-control [-T] --resume-task <ID de la tâche> [--use-name]
```

Exemple:

- *Reprendre la tâche avec ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --resume-task 9
```

ARGUMENT	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande -T --get-task-list.
--use-name -N	Nom de la tâche.

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. rubrique "Modification des paramètres de la tâche" à la page 82) depuis ce fichier de configuration dans la tâche du type approprié sur un autre ordinateur.

Syntaxe de la commande

```
kes4lwks-control [-T] --get-settings <ID de la tâche> \
[--file=<nom du fichier de configuration>] [--file-format=<INI|XML>] [--use-name]
kes4lwks-control [-T] --get-settings <ID de la tâche> \
<nom de la rubrique du fichier INI>.<nom du paramètre> [--use-name]
```

Exemples:

- *Exporter les paramètres de la tâche possédant ID=9 dans le fichier /home/test/configkavscanner.xml:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--get-settings 9 ScanScope.AreaPath.Path
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--get-settings <ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande -T --get-task-list.
--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 spécifié par la clé -F, est déterminé 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.
--use-name -N	Nom de la tâche.

MODIFICATION DES PARAMÈTRES DE LA TÂCHE

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 Endpoint Security 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

```
kes4lwks-control [-T] --set-settings <ID de la tâche> \
--file=<nom du fichier de configuration> [--file-format=<INI|XML>] [--use-name]
kes4lwks-control [-T] --set-settings <ID de la tâche> \
<nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre> \
[--use-name]
```

Exemple:

- *Importer dans la tâche ID=9 les paramètres depuis le fichier de configuration /home/test/config_fridayscan.xml:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --set-settings 9 \
```

```
--file=/home/test/config_fridayscan.xml
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--set-settings <ID de la tâche>	Spécifiez le numéro d'identification de la tâche (ID, nom alternatif que Kaspersky Endpoint Security attribue à la tâche). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande -T --get-task-list.
--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 spécifié n'est pas conforme à son format. Valeurs possibles de la clé: XML, INI.
--use-name -N	Nom de la tâche.

CREATION D'UNE TACHE

La commande --create-task crée la tâche de Kaspersky Endpoint Security 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

```
kes4lwks-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>]
```

Exemple:

- *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/kes4lwks/bin/kes4lwks-control \
--create-task Fridayscan --use-task-type=ODS \
--file=/home/test/config_kavscanner.xml
```

ARGUMENT, CLES	SPECIFICATION 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.

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--file=<nom du fichier de configuration> -F <nom du fichier de configuration>	Clé facultative. Spécifiez le chemin d'accès complet au fichier de configuration existant. Kaspersky Endpoint Security importe dans la tâche les paramètres spécifiés dans ce 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 spécifié n'est pas conforme à son format. Valeurs possibles de la clé: XML, INI.

SUPPRESSION D'UNE TACHE

La commande --delete-task supprime la tâche de Kaspersky Endpoint Security 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

```
kes4lwks-control [-T] --delete-task <ID de la tâche> [--use-name]
```

Exemple:

- *Supprimer la tâche avec ID=20:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --delete-task 20
```

ARGUMENT	SPECIFICATION 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 Endpoint Security attribue à la tâche lors de sa création). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande -T --get-task-list.
--use-name -N	Nom de la tâche.

OBTENTION DES PARAMÈTRES DE L'HORAIRE D'UNE TÂCHE

L'instruction --get-schedule fait afficher les paramètres de l'horaire de la tâche (cf. page 134). 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 Endpoint Security à l'aide de la commande --set-schedule (cf. rubrique "Modification des paramètres de l'horaire d'une tâche" à la page 85). Kaspersky Endpoint Security utilisera de nouvelles valeurs des paramètres de l'horaire immédiatement.

Syntaxe de la commande

```
kes4lwks-control [-T] --get-schedule <ID de la tâche>
[--file=<nom du fichier de configuration>] [--file-format=<INI|XML>] [--use-name]
```

```
kes4lwks-control [-T] --get-schedule <ID de la tâche> <nom du paramètre> [--use-name]
```

Exemples:

- *Enregistrer les paramètres de Kaspersky Endpoint Security dans le fichier appelé on_demand_schedule.xml. Enregistrer le fichier créé dans le répertoire en cours:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-schedule 9 -F on_demand_schedule.xml
```

- *Affiche la valeur du paramètre RuleType de la planification de la tâche de protection en temps réel:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-schedule 9 RuleType
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Le numéro d'identification de la tâche dans Kaspersky Endpoint Security.
--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.
--use-name -N	Nom de la tâche.

MODIFICATION DES PARAMÈTRES DE L'HORAIRE D'UNE TÂCHE

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 134).

Vous pouvez utiliser cette commande pour modifier les paramètres de Kaspersky Endpoint Security:

1. Enregistrez les paramètres de planification dans un fichier de configuration à l'aide de l'instruction -T --get-schedule (cf. rubrique "Obtention des paramètres de l'horaire d'une tâche" à la page 84).
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 Endpoint Security à l'aide de la commande -T --set-schedule. Kaspersky Endpoint Security utilisera de nouvelles valeurs des paramètres de l'horaire immédiatement.

Syntaxe de la commande

```
kes4lwks-control -T --set-schedule <ID de la tâche> --file=<nom du fichier de
configuration> \
[--file-format=<INI|XML>] [--use-name]
kes4lwks-control -T --set-schedule <ID de la tâche>
<nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre> \
[--use-name]
```

Exemple:

- *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/kes4lwks/bin/kes4lwks-control -T \
--set-schedule 9 -F /home/test/on_demand_schedule.xml
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Le numéro d'identification de la tâche dans Kaspersky Endpoint Security.
--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.
--use-name -N	Nom de la tâche.

SUPPRESSION DE L'HORAIRE DE LA TÂCHE

La commande -T --del-schedule établit les paramètres de l'horaire d'une tâche qui sont définis par défaut pendant la procédure de la configuration initiale de Kaspersky Endpoint Security (cf. Manuel d'installation de Kaspersky Endpoint Security 8 for Linux).

Syntaxe de la commande

```
kes4lwks-control -T --del-schedule <ID de la tâche> [--use-name]
```

Exemple:

- *Etablir pour la tâche avec ID=15 les paramètres de l'horaire, définis par défaut:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -T --del-schedule 15
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<ID de la tâche>	Le numéro d'identification de la tâche dans Kaspersky Endpoint Security.
--use-name -N	Nom de la tâche.

RECHERCHE D'EVENEMENTS SELON LA PLANIFICATION

La commande -T --show-schedule recherche les événements planifiés.

Syntaxe de la commande

```
kes4lwks-control -T --show-schedule <type de règle> --from=<date de début> \
--to=<date de fin> --task-id=<ID de la tâche> [--use-name]
```

Exemples de la commande

L'exemple suivant illustre la commande de recherche des événements dans l'intervalle de temps indiqué et son affichage.

Exemple:

- *Recherche d'événements dont le temps exacte du premier lancement est défini selon la planification et se trouve dans l'intervalle du 28/03/11 au 01/04/11:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--show-schedule Time --from=2011-03-28 --to=2011-04-01
```

Affichage de la commande:

```
Events number: 2

TaskId #9, Event: Start, Date: 2011-04-05 14:00:00, Start Rule: [Daily, 14:00:00;; 1]
TaskId #16, Event: Start, Date: 2011-04-06 00:00:00, Start Rule: [Once, 2011-04-06
00:00:00]
```

L'exemple suivant illustre la commande de recherche des événements et son affichage.

Exemple:

- *Recherche d'événements suivants de l'horaire pour la tâche indiquée:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--show-schedule Time --task-id="On-demand scan" --use-name
```

Affichage de la commande:

```
Events number: 1

TaskId #9, Event: Start, Date: 2011-04-25 16:30:00, Start Rule: [Monthly, 16:30:00; 25]
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<type de règle>	Type de règle de la planification. Valeurs possibles: • `Time` – des règles, contenant l'heure du lancement de la tâche. • `Startup` - des règles, contenant la condition PS (au lancement de Kaspersky Endpoint Security). • `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 --from=<date de debut>, la recherche sera exécutée depuis le moment du lancement de la commande.

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
--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 --to=<date de fin>, la recherche sera exécutée pendant la semaine depuis le lancement de la commande.
--task-id=<ID de la tâche>	Le numéro d'identification de la tâche à rechercher la planification.
--use-name -N	Nom de la tâche.

COMMANDES D'ADMINISTRATION DES LICENCES

DANS CETTE SECTION

Vérification de l'authenticité du fichier de licence avant l'installation 88

Consultation des informations relatives à la licence avant l'installation du fichier de licence 89

Consultation des informations relatives aux fichiers de licence installés 90

Consultation de l'état des licences installées 90

Installation d'un fichier de licence actif 91

Installation d'un fichier de licence de réserve 91

Suppression d'un fichier de licence actif 91

Suppression d'un fichier de licence de réserve 92

VÉRIFICATION DE L'AUTHENTICITÉ DU FICHIER DE LICENCE AVANT L'INSTALLATION

L'instruction kes4lwks-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 Endpoint Security. L'instruction affiche les informations relatives au fichier de licence sans l'installer.

Syntaxe de la commande

```
kes4lwks-control [-L] --validate-key <chemin d'accès au fichier de licence>
```

Exemple:

Vérifier l'authenticité du fichier de licence depuis le fichier de licence /home/test/00000001.key:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--validate-key /home/test/00000001.key
```

ARGUMENT	SPECIFICATION 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 Endpoint Security.
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 Endpoint Security. 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 À 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

```
kes4lwks-control [-L] --show-license-info <chemin d'accès au fichier de licence>
```

Exemple:

- *Afficher les informations sur la licence depuis le fichier /home/test/00000001.key:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--show-license-info /home/test/00000001.key
```

ARGUMENT	SPECIFICATION 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 Endpoint Security.
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 INSTALLÉS

L'instruction kes4lwks-control avec l'argument --get-installed-keys affiche les informations relatives aux fichiers de licence installé.

Syntaxe de la commande

```
kes4lwks-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 Endpoint Security. 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 Endpoint Security; 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 Endpoint Security 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 Endpoint Security.
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'ÉTAT DES LICENCES INSTALLÉES

L'instruction --query-status fait afficher l'état des licences installées.

Syntaxe de la commande

```
kes4lwks-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 Endpoint Security" (cf. page 59).

Syntaxe de la commande

```
kes4lwks-control [-L] --install-active-key <chemin d'accès au fichier de licence>
```

Exemple:

- *Installer la licence depuis le fichier /home/test/00000001.key en tant que licence active:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--install-active-key /home/test/00000001.key
```

ARGUMENT	SPECIFICATION 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 RÉSERVE

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 Endpoint Security" (cf. page 59).

Si le fichier de licence actif n'est pas installé, alors le fichier de licence de réserve deviendra le fichier principal.

Syntaxe de la commande

```
kes4lwks-control [-L] --install-suppl-key <chemin d'accès au fichier de licence>
```

Exemple:

- *Installer la licence supplémentaire depuis le fichier /home/test/00000002.key:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--install-suppl-key /home/test/00000002.key
```

ARGUMENT	SPECIFICATION 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

```
kes4lwks-control [-L] --revoke-active-key
```

SUPPRESSION D'UN FICHIER DE LICENCE DE RÉSERVE

L'instruction --revoke-suppl-key supprime le fichier de licence de réserve installé.

Syntaxe de la commande

```
kes4lwks-control [-L] --revoke-suppl-key
```

COMMANDES D'ADMINISTRATION DE LA QUARANTAINE ET DU RÉPERTOIRE DE SAUVEGARDE DE RÉSERVE

DANS CETTE SECTION

Obtention des statistiques brèves de la quarantaine / du répertoire de sauvegarde 92

Obtention des informations sur les objets du répertoire de sauvegarde 93

Obtention des informations sur un objet du répertoire de sauvegarde 93

Restauration des objets depuis le répertoire de sauvegarde 94

Mise en quarantaine manuelle de la copie de l'objet 94

Suppression d'un objet depuis le répertoire de sauvegarde 95

Exportation des objets depuis le répertoire de sauvegarde dans le répertoire spécifié 95

Importation dans le répertoire de sauvegarde des objets qui ont été exportés avant 96

Purge du répertoire de sauvegarde 96

OBTENTION DES STATISTIQUES BRÈVES DE LA QUARANTAINE / DU RÉPERTOIRE DE SAUVEGARDE

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

```
kes4lwks-control [-Q] --get-stat [--query "<expression logique>"]
```

Exemples:

- *Pour consulter la statistique brève de la quarantaine:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q \
--get-stat --query "(OrigType!=s'Backup')"
```

- *Pour consulter la statistique brève du répertoire de sauvegarde de réserve:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q \
--get-stat --query "(OrigType==s'Backup')"
```

OBTENTION DES INFORMATIONS SUR LES OBJETS DU RÉPERTOIRE 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

```
kes4lwks-control [-Q] --query "<expression logique>" \
[--limit=<nombre d'entrées maximum>]
[--offset=<écart du début de la sélection>][--detailed]
```

Exemples:

- *Pour consulter les informations sur les objets du répertoire de sauvegarde:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --query ""
  ```

- *Pour consulter les informations sur les objets mis en quarantaine, afficher 50 entrées à commencer par l'entrée 51:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q --query "(OrigType==s'Backup')"
  ```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre: expression logique (cf. page 100).
--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.
--detailed	Affiche des informations de service supplémentaires sur les objets dans le répertoire de sauvegarde.

OBTENTION DES INFORMATIONS SUR UN OBJET DU RÉPERTOIRE DE SAUVEGARDE

L'instruction --get-one affiche les informations sur un objet du référentiel avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kes4lwks-control [-Q] --get-one <numéro d'identification de l'objet> [--detailed]
```

Exemple:

- *Pour obtenir les informations sur l'objet avec ID=1:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-one 1
  ```

ARGUMENT, CLES	SPECIFICATION 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 93).
--detailed	Affiche des informations de service supplémentaires sur l'objet dans le répertoire de sauvegarde.

RESTAURATION DES OBJETS DEPUIS LE RÉPERTOIRE 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

```
kes4lwks-control [-Q] --restore <numéro d'identification de l'objet dans le référentiel>
\
[--file=<nom du fichier et chemin d'accès au fichier>]
```

Exemples:

- *Pour restaurer l'objet avec ID=1 dans l'emplacement d'origine:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control --restore 1 -F restored.exe
  ```

ARGUMENT, CLES	SPECIFICATION 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 93).
--file=<nom du fichier> -F <nom du fichier>	Nom de l'objet dans lequel Kaspersky Endpoint Security 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 Endpoint Security enregistrera le fichier dans le répertoire en cours. Si vous omettez cette clé, Kaspersky Endpoint Security 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

```
kes4lwks-control [-Q] --add-object <nom du fichier>
```

Exemple:

- *Pour mettre en quarantaine la copie du fichier /home/sample.exe:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control --add-object /home/sample.exe
  ```

ARGUMENT	SPECIFICATION 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 RÉPERTOIRE DE SAUVEGARDE

La commande --remove supprime depuis le répertoire de sauvegarde l'objet avec le numéro d'identification spécifié.

Syntaxe de la commande

```
kes4lwks-control [-Q] --remove <numéro d'identification de l'objet>
```

Exemple:

- *Pour supprimer l'objet avec ID=1:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --remove 1
```

ARGUMENT	SPECIFICATION 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 93).

EXPORTATION DES OBJETS DEPUIS LE RÉPERTOIRE DE SAUVEGARDE DANS LE RÉPERTOIRE SPÉCIFIÉ

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 l'ordinateur. L'emplacement du répertoire de sauvegarde sur l'ordinateur est spécifié dans le fichier de configuration de la quarantaine et du répertoire de sauvegarde (cf. page 140).

Vous pouvez utiliser des filtres pour n'exporter que des fichiers sélectionnés, par exemple, que des objets mis en quarantaine.

Syntaxe de la commande

```
kes4lwks-control [-Q] --export <répertoire de destination> \
"<expression logique>"
[--limit=<nombre d'entrées maximum>]
[--offset=<écart du début de la sélection>]
```

Exemples:

- *Pour exporter tous les objets depuis le répertoire de sauvegarde dans le répertoire /media/flash128/avpstorage:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q\
--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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q \
--export /media/flash128/avpstorage --query "(OrigType==s'Backup')"
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
<répertoire de destination>	Le répertoire dans lequel Kaspersky Endpoint Security 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 l'ordinateur via les protocoles SMB/CIFS et NFS.
--query="<expression logique>"	Met le filtre: expression logique (cf. page 100).
--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 RÉPERTOIRE DE SAUVEGARDE DES OBJETS QUI ONT ÉTÉ EXPORTÉS 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 l'ordinateur est spécifié dans le fichier de configuration de la quarantaine et du répertoire de sauvegarde (cf. page 140).

Syntaxe de la commande

```
kes4lwks-control [-Q] --import <répertoire avec des objets exportés>
```

Exemple:

- *Pour importer dans le répertoire de sauvegarde les objets depuis le répertoire /media/flash128/avpstorage:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q\
--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

```
kes4lwks-control [-Q] --mass-remove [--query="<expression logique>"] \
[--limit=<nom maximum d'enregistrements>] [--offset=<écart du début de la sélection>]
```

Exemples:

- *Pour supprimer tous les objets depuis le répertoire de sauvegarde:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --mass-remove
```

- *Pour ne supprimer que les objets mis en quarantaine: 50 entrées à commencer par l'entrée 51:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q \
--mass-remove --query "(OrigType==s'Backup')"
```

CLES	SPECIFICATION ET VALEURS POSSIBLES
--query="expression logique>"	Met le filtre: expression logique (cf. page 100).
--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 ÉVÉNEMENTS

DANS CETTE SECTION

Obtention du nombre d'événements de Kaspersky Endpoint Security par un filtre 97

Obtention des informations sur les événements de Kaspersky Endpoint Security 98

Consultation de l'intervalle de temps pendant lequel les événements du journal ont eu lieu 99

Rotation du journal des événements 99

Suppression des événements du journal des événements 99

OBTENTION DU NOMBRE D'ÉVÉNEMENTS DE KASPERSKY ENDPOINT SECURITY 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 98).

Syntaxe de la commande

```
kes4lwks-control [-E] --count "<expression logique>" [--db=<fichier de rotation>]
```

Exemples:

- *Pour obtenir le nombre d'événements de Kaspersky Endpoint Security consignés dans le journal des événements:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --count ""
```

- *Obtenir le nombre d'événements de Kaspersky Endpoint Security consignés dans le fichier de rotation EventStorage-2009-12-01-23-57-23.db:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --count "" \
--db=EventStorage-2009-12-01-23-57-23.db
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre: expression logique (cf. page 100).
--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 Endpoint Security affiche le nombre d'événements dans le journal pour l'instant.

OBTENTION DES INFORMATIONS SUR LES ÉVÉNEMENTS DE KASPERSKY ENDPOINT SECURITY

L'instruction --query permet d'obtenir des informations sur les événements de Kaspersky Endpoint Security 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

```
kes4lwks-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:

- *Pour consulter les informations sur 50 derniers événements de la quarantaine:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
-E --query "(TaskType == s'Quarantine')" --limit=50
```

ARGUMENT, CLES	SPECIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre: expression logique (cf. page 100).
--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 Endpoint Security 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 Endpoint Security. 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 du registre spécifié par la clé -F, est déterminé 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 ÉVÉNEMENTS 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

```
kes4lwks-control [-E] --period [--db=<fichier de rotation>]
```

Exemples:

- *Pour voir à quel intervalle de temps appartiennent les événements consignés dans le journal des événements:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control --period \
  --db=EventStorage-2009-12-01-23-57-23.db
  ```

ARGUMENTS ET CLES	SPECIFICATION ET VALEURS POSSIBLES
--db=<fichier de rotation>	Fichier de rotation (extension .db) dont les informations peuvent être consultées. Si vous n'utilisez pas cet argument, Kaspersky Endpoint Security affichera les informations tirées sur le journal des événements.

ROTATION DU JOURNAL DES ÉVÉNEMENTS

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.

Si la valeur du paramètre RotateMethod est Erase, Kaspersky Endpoint Security 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

```
kes4lwks-control [-E] --rotate
```

SUPPRESSION DES ÉVÉNEMENTS DU JOURNAL DES ÉVÉNEMENTS

L'instruction --remove supprime les enregistrements relatifs aux événements du journal des événements de Kaspersky Endpoint Security 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

```
kes4lwks-control [-E] --query ["<expression logique>"] \
[--db=<fichier de rotation>]
```

Exemple:

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/kes4lwks/bin/kes4lwks-control -E \
--remove "((EventType==s'ObjectProcessed') and (ObjectReason==s'ObjectClean'))"
```

ARGUMENTS ET CLES	SPECIFICATION ET VALEURS POSSIBLES
"<expression logique>"	Met le filtre: expression logique (cf. page 100).
--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 Endpoint Security supprime les enregistrements du journal des événements de Kaspersky Endpoint Security.

RESTRICTION DE LA SÉLECTION À L'AIDE DES FILTRES

DANS CETTE SECTION

Expressions logiques 100

Paramètres de objets en quarantaine / dans le dossier de sauvegarde 101

Evénements de Kaspersky Endpoint Security et leurs paramètres 104

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 Endpoint Security: -E --count "<expression logique>" (cf. page 97);
- obtention des informations sur les événements de Kaspersky Endpoint Security: -E --query "<expression logique>" (cf. page 98);
- obtention des informations sur les objets mis en quarantaine / du dossier de sauvegarde: -Q --query "<expression logique>" (cf. page 93);
- obtention de statistiques succinctes sur les objets mis en quarantaine / du dossier de sauvegarde: -Q --get-stat --query "<expression logique>" (cf. page 92);
- purge partielle du référentiel: -Q --mass-remove --query "<expression logique>" (cf. page 96);
- exportation sélective des objets depuis la quarantaine / le dossier de sauvegarde: -Q --export --query "<expression logique>" (cf. page 95).

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')"
```

ELEMENTS	SPECIFICATION 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 101). L'ordre peut avoir les valeurs suivantes: a ordre ascendant d ordre descendant
<type>	i numérique s linéaire

PARAMÈTRES 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 6. Paramètres de objets en quarantaine / dans le dossier de sauvegarde

CHAMP	TYPE	SPECIFICATION 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 Endpoint Security" à la page 11). L'ordre 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 qu'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	SPECIFICATION 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 Endpoint Security 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.

EVÉNEMENTS DE KASPERSKY ENDPOINT SECURITY ET LEURS PARAMÈTRES

Vous pouvez trier les événements de Kaspersky Endpoint Security en fonction de leurs paramètres. Le tableau suivant décrit les événements de Kaspersky Endpoint Security; les paramètres des événements sont donnés dans le tableau ci-dessous.

Tableau 7. Evénements

№	NOM DE L'EVENEMENT	DESCRIPTION	PARAMETRES
1	ApplicationStarted	Kaspersky Endpoint Security est lancé; cet événement survient une fois que toutes les tâches de service de Kaspersky Endpoint Security ont été lancées.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
2	ApplicationSettingsChanged	Les paramètres généraux de Kaspersky Endpoint Security 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, 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 Endpoint Security ont bien été installées après la mise à jour.	Date, EventId, EventType, RuntimeTaskID, AVBasesDate, TaskId, TaskName, TaskType
11	AVBasesAreOutOfDate	Les bases de Kaspersky Endpoint Security sont dépassées.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
12	AVBasesAreTotallyOutOfDate	Les bases de Kaspersky Endpoint Security sont fortement dépassées.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
13	AVBasesIntegrityCheckOK	La vérification de l'intégrité des bases de Kaspersky Endpoint Security a réussi.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
14	AVBasesIntegrityCheckFailed	L'intégrité des bases de Kaspersky Endpoint Security a été violée.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType

№	NOM DE L'EVENEMENT	DESCRIPTION	PARAMETRES
15	AVBasesApplied	Les bases de Kaspersky Endpoint Security sont appliquées.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
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, PersistentTaskId, 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,

№	NOM DE L'EVENEMENT	DESCRIPTION	PARAMETRES
			TaskId, TaskName, TaskType
29	ObjectNotProcessed	Objet non traité.	Date, EventId, EventType, AccessHost, AccessUser, 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,

№	NOM DE L'EVENEMENT	DESCRIPTION	PARAMETRES
			TaskType
39	ObjectRemovedFromBackup	L'objet est supprimé de la sauvegarde.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, 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 Endpoint Security 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 Endpoint Security a réussi.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType

№	NOM DE L'EVENEMENT	DESCRIPTION	PARAMETRES
54	AVBasesRollbackError	Erreur lors du retour à la version antérieure des bases de Kaspersky Endpoint Security.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
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 8. Paramètres des événements

PARAMETRE	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 Endpoint Security" à la page 11). L'ordre 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 qu'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 Endpoint Security 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

PARAMETRE	TYPE	DESCRIPTION
		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).
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 Endpoint Security (installé via le protocole SMB/CIFS).
Info	s	Informations supplémentaires sur l'erreur.
ModuleName	s	Nom du module de Kaspersky Endpoint Security 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 Endpoint Security 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:

PARAMETRE	TYPE	DESCRIPTION
		Cured – l'objet est réparé; Removed – l'objet est supprimé; Quarantined – l'objet est placé en quarantaine; Skipped – l'objet est ignoré; AllActionsFailed – toutes les actions sur l'objet se sont términées 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 Endpoint Security.
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 Endpoint Security. 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);

PARAMETRE	TYPE	DESCRIPTION
		ODS - tâche prédéfinie d'analyse à la demande (ID=9); QS – tâche de l'analyse des objets mis en quarantaine(ID=10); Rollback – la tâche de remise à la version précédente des bases (ID=14); • 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 – assure le "serveur des licences" (ID=5); EventStorage - assure le service du journal des événements (ID=11).
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.

Tableau 9.

PARAMÈTRES DES FICHIERS DE CONFIGURATION DE KASPERSKY ENDPOINT SECURITY

Vous pouvez créer des fichiers de configuration de Kaspersky Endpoint Security au format INI, ainsi qu'au format XML.

Cette section décrit la structure et les paramètres des fichiers de configuration de Kaspersky Endpoint Security au format INI.

DANS CETTE SECTION

Règles de mise au point des fichiers de configuration ini de Kaspersky Endpoint Security 112

Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande 114

Paramètres des tâches de mise à jour 129

Paramètres de l'horaire 134

Paramètres généraux de Kaspersky Endpoint Security. 137

Paramètres de la quarantaine et du dossier de sauvegarde 140

Les paramètres du journal des événements 141

RÈGLES DE MISE AU POINT DES FICHIERS DE CONFIGURATION INI DE KASPERSKY ENDPOINT SECURITY

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 Endpoint Security 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).

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.

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).

Exemple:

```
AreaDesc="Analyse des bases de messagerie"
```

Les autres valeurs peuvent être mises entre guillemets et sans guillemets.

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.

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. rubrique "Modification des paramètres de la tâche" à la page 82) 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" à la page 81), les commentaires ne sont pas affichés.

PARAMÈTRES DE LA TÂCHE DE PROTECTION EN TEMPS RÉEL ET DES TÂCHES D'ANALYSE À 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 81), 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 82).

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 Endpoint Security 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 Endpoint Security utilisera pour le secteur d'analyse spécifié dans la section [ScanScope:AreaPath]. Si vous ne spécifiez pas les paramètres de ces sections, Kaspersky Endpoint Security analysera le secteur déterminé selon les paramètres par défaut.

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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security (cf. page 112).

Tableau 10. Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande

PARAMETRE	SPECIFICATION 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**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
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 Endpoint Security 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 Endpoint Security. Si vous utilisez l'ordinateur protégé en tant que l'ordinateur SAMBA, vous pouvez spécifier la valeur SambaOnly. Dans ce cas, Kaspersky Endpoint Security n'analysera pas les objets auxquels la requête est faite non pas via le protocole SMB/CIFS. Les valeurs possibles comprennent: **Full.** Kaspersky Endpoint Security analyse les objets sur l'ordinateur lorsqu'on y fait requête via le protocole SMB/CIFS avec utilisation de l'intercepteur SAMBA. Kaspersky Endpoint Security intercepte toutes les autres opérations sur les fichiers disponibles sur l'ordinateur protégé (y compris, sur les fichiers des ordinateurs distants), en utilisant l'intercepteur du niveau du noyau. **SambaOnly.** Kaspersky Endpoint Security 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 Endpoint Security (cf. du Manuel d'installation de Kaspersky Endpoint Security 8 for Linux). **KernelOnly.** Kaspersky Endpoint Security analyse les objets sur l'ordinateur uniquement à l'aide de l'intercepteur de fichiers. Assurez-vous d'avoir installé l'intercepteur de noyau durant la configuration initiale de Kaspersky Endpoint Security (cf. du Manuel d'installation de Kaspersky Endpoint Security 8 for Linux). Valeur par défaut: se fixe pendant l'installation de Kaspersky Endpoint Security.
[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 Endpoint Security n'analysera que les fichiers ou les répertoires que vous spécifierez à l'aide des masques Shell ou des expressions régulières ECMA-262. Dans les expressions régulières, utilisez le préfix **re:**. Si vous ne spécifiez pas ce paramètre, Kaspersky Endpoint Security analysera tous les objets du secteur d'analyse. Vous pouvez spécifier plusieurs valeurs de ce paramètre.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES

	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: **no**.
`[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: **<type du système de fichiers>**. Les valeurs possibles comprennent: **Mounted**. Répertoires distants montés sur l'ordinateur. 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 de l'ordinateur accessibles via le protocole SMB/CIFS ou le protocole NFS. **AllRemotelyMounted**. Tous les répertoires distants montés sur l'ordinateur par l'intermédiaire des protocoles SMB/CIFS et NFS. **AllShared**. Toutes les ressources du système de fichiers de l'ordinateur 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 9).

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	Exemples: `Path=/` – *analyser tous les répertoires locaux de l'ordinateur; 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 de l'ordinateur 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 de l'ordinateur 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 Endpoint Security analyse les objets 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 Endpoint Security analyse 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. 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 Endpoint Security analyse 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 Endpoint Security analyse 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.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
[ScanScope:ScanSettings] Paramètres de sécurité que Kaspersky Endpoint Security utilise lors de l'analyse du secteur spécifié par le paramètre [ScanScope:AreaPath].	
ScanByAccessType	Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security analyse les archives (y compris les archives autoextractibles SFX). Faites attention à ce que Kaspersky Endpoint Security 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**.
ScanSfxArchived	Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
ScanPacked	Kaspersky Endpoint Security analyse les fichiers exécutables archivés par les programmes d'archivage de code binaire tels qu'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 Endpoint Security bloque l'accès à l'objet pour l'application qui y a fait requête. Les valeurs possibles comprennent: **Cure** (réparer). Kaspersky Endpoint Security 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 Endpoint Security garde l'objet intact. **Remove** (supprimer). Kaspersky Endpoint Security supprime l'objet infecté après avoir créé une copie de sauvegarde. **Recommended** (exécuter l'action recommandée). Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security transfère l'objet dans le répertoire de sauvegarde de la quarantaine. **Skip** (sauter). L'objet reste intact. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security, 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'exécuter l'action que vous avez choisie sur l'objet, Kaspersky Endpoint Security bloque l'accès à l'objet pour l'application qui y a fait requête. Les valeurs possibles comprennent: **Cure** (réparer). Kaspersky Endpoint Security essaie de réparer l'objet ayant

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	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 Endpoint Security garde l'objet intact. **Quarantine** (mettre en quarantaine). Kaspersky Endpoint Security transfère l'objet dans le répertoire de sauvegarde de la quarantaine. **Remove** (supprimer). Kaspersky Endpoint Security supprime l'objet après avoir créé une copie de sauvegarde. **Recommended** (exécuter l'action recommandée). Kaspersky Endpoint Security 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 Endpoint Security 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. **Skip** (sauter). L'objet reste intact. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security, 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). **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 le volume de l'objet analysé est supérieur à la valeur spécifiée, Kaspersky Endpoint Security saute cet 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 Endpoint Security 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 Endpoint Security

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	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 ECMA-262. 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.

`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**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES

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 Endpoint Security 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 Endpoint Security sur ce que l'objet est infecté ou suspect.
	
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet, dans le registre de Kaspersky Endpoint Security.
	
	De même, vous pouvez trouver la signature complète de la menace détectée dans le logiciel, sur le site Internet de l'Encyclopédie des virus Viruslist.ru (cf. section Encyclopédie des virus - http://www.viruslist.com/fr). 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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. Valeur par défaut: **yes**.
ReportCleanObjects	Fait activer / désactiver la consignation dans le journal des informations relatives aux objets analysés que Kaspersky Endpoint Security a considéré comme étant sains. Vous pouvez activer ce paramètre, par exemple, pour confirmer qu'un objet quelconque a été analysé par Kaspersky Endpoint Security. 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

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	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**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
`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 Endpoint Security. 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: **yes**.
`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; **Deep** - analyse la plus poussée, charge maximale du système; **Recommended** – valeur recommandée. Valeur par défaut: **Recommended**.
`[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 Endpoint Security à exécuter sur les objets qui contiennent les menaces des types spécifiés.	

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES

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 Endpoint Security effectuera ces actions s'il détecte dans cet objet la menace de type spécifié.
	Kaspersky Endpoint Security 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 Endpoint Security, 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 – logiciels 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 Endpoint Security" (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] 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"

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	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 Endpoint Security n'exclura que les objets que vous aurez spécifiés à l'aide des masques Shell ou des expressions régulières ECMA-262. 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 l'ordinateur. 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 de l'ordinateur accessibles via le protocole SMB/CIFS ou le protocole NFS. **AllRemotelyMounted**. Tous les répertoires distants montés sur l'ordinateur par l'intermédiaire des protocoles SMB/CIFS et NFS. **AllShared**. Toutes les ressources du système de fichiers de l'ordinateur 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 exclure>**. Chemin d'accès complet au répertoire à exclure.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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.

PARAMÈTRES DES TÂCHES DE MISE À 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 en cours, vous devez exporter les paramètres de la tâche dans un fichier (cf. page 81), 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 82).

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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security (cf. page 112).

Tableau 11. Paramètres des tâches de mise à jour

PARAMETRE	SPECIFICATION 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 Endpoint Security. **RetranslateProductComponents** (Copier toutes les mises à jour disponibles pour Kaspersky Endpoint Security). Kaspersky Endpoint Security 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 Endpoint Security 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 l'ordinateur protégé en tant que intermédiaire pour répartir les mises à jour. Vous pouvez consulter les noms des mises à jour sur le site du Service du Support Technique de Kaspersky Lab. L'installation automatique des mises à jour critiques des modules de Kaspersky Endpoint Security n'est pas prévue. Valeur par défaut: **AllBases**.
`[CommonSettings]` Source de la mise à jour et paramètres de connexion à celle-là.	

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
SourceType	Sélectionnez la source depuis laquelle Kaspersky Endpoint Security recevra les mises à jour: **KLServers**. Kaspersky Endpoint Security 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 Endpoint Security téléchargera les mises à jour sur l'ordinateur 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 Endpoint Security 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 l'ordinateur protégé, y compris sur les ordinateurs distants montés via les protocoles SMB/CIFS ou NFS. Valeur par défaut: **KLServers**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
UseKLServersWhenUnavailable	Vous pouvez configurer la requête de Kaspersky Endpoint Security 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**.
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.
ProxyBypassLocalAddresses	Utilisation du serveur proxy pour la connexion aux serveurs locaux des mises à jour. Par défaut, le serveur proxy n'est pas utilisé pour la connexion aux serveurs locaux des mises à jour. Désactivez ce paramètre pour se connecter aux serveurs locaux des mises à jour via le serveur proxy indiqué dans le paramètre ProxyServer. **yes** – ne pas utiliser le serveur proxy pour la connexion aux serveurs locaux des mises à jour; **no** – utiliser le serveur proxy pour la connexion aux serveurs locaux des mises à jour. Valeur par défaut: **yes**.
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**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
ProxyAuthUser	Si vous avez activé la vérification de l'authenticité, spécifiez le nom d'utilisateur avec les droits duquel Kaspersky Endpoint Security 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 d'utilisateur avec les droits duquel Kaspersky Endpoint Security 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 Endpoint Security 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**.
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 Endpoint Security 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 Endpoint Security fera requête à chaque source spécifiée suivante si la source précédente n'est pas disponible. Vous pouvez configurer la requête de Kaspersky Endpoint Security 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 l'ordinateur 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:

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	• Kaspersky Endpoint Security charge les mises à jour, si le paramètre UpdateType possède la valeur RetranslateProductComponents ou RetranslateComponentsList; • Kaspersky Endpoint Security 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 Endpoint Security 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 recevoir.
	Vous pouvez consulter les noms des mises à jour 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.

PARAMÈTRES DE L'HORAIRE

Cette section décrit les paramètres du fichier de configuration que vous pouvez utiliser pour configurer l'horaire du lancement des tâches.

En spécifiant les paramètres, respectez les règles de mise au point des fichiers de configuration ini de Kaspersky Endpoint Security (cf. page 112).

Structure du fichier de configuration ini de l'horaire

```
RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR
[StartTime=<date heure>; <jour du mois|jour de la semaine>; <période de lancement>]
[RandomInterval=<minutes>]
[ExecuteTimeLimit=<minutes>]
[RunMissedStartRules=yes|no]
```

Tableau 12. Paramètres de l'horaire

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
`RuleType`	Mode de lancement programmé de la tâche. Les valeurs possibles comprennent: • `Once` – une fois; • `Monthly` – chaque mois; • `Weekly` – chaque semaine; • `Daily` – Tous les N jours; • `Hourly` – Toutes les N heures; • `Minutely` – Toutes les N minutes; • `Manual` – mode manuel; • `BR` – après la mise à jour des bases. La tâche sera lancée chaque fois après la mise à jour réussie des bases de Kaspersky Endpoint Security (cette option n'est pas utilisée dans les tâches de mise à jour). • `PS` – au démarrage de l'application. La tâche sera lancée chaque fois lors du lancement de Kaspersky Endpoint Security. Pour la tâche de protection en temps réel, uniquement les valeurs `Manual` et `PS` sont disponibles.
`StartTime`	L'heure de lancement. Si vous indiquez l'heure du lancement, la date système et/ou l'heure système actuels sont remplacés par défaut. Le format de ce paramètre dépend du paramètre `RuleType`, cf. tableau ci-après.
`RandomInterval`	Répartir le lancement aléatoire de la tâche sur l'intervalle (en minutes) pour aligner la charge sur le serveur lors du lancement simultané de plusieurs tâches selon la programmation. Format – [0;999].
`ExecuteTimeLimit`	Limiter l'exécution de la tâche par l'intervalle (en minutes). Format – [0;999].
`RunMissedStartRules`	Lancer les tâches non exécutées. Les valeurs possibles comprennent: • `yes` – lancer les tâches ignorées lors du démarrage suivant de l'application; • `no` – lancer les tâches uniquement selon l'horaire.

Tableau 13. Paramètres Mode d'exécution et Heure d'exécution

LA VALEUR DU PARAMÈTRE RULETYPE	FORMAT DE LA VALEUR DU PARAMÈTRE STARTTIME
Once	<date heure>
Monthly	<heure>; <jour du mois>
Weekly	<heure>; <jour de la semaine>
Daily	<heure>;;<période du lancement>
Hourly	<date heure>;;<période du lancement>
Minutely	<heure>;;<période du lancement>
Manual	N'est pas utilisé
BR	N'est pas utilisé
PS	N'est pas utilisé

Le paramètre <heure exacte> a le format suivant.

```
[<année>/][<mois>/][<jour du mois>] [hh]:[mm]:[ss]; [<jour du mois>|<jour de la semaine>]; [<période du lancement>]
```

Tableau 14. Valeurs des champs du paramètre Heure du lancement

CHAMP	LA VALEUR DU PARAMÈTRE STARTTIME
<an>	[année actuelle -1;année actuelle +10]
<mois>	JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC
<jour du mois>	[1;31]
hh	heures [00;23]
mm	minutes [00;59]
ss	secondes [00;59]
<jour de la semaine>	MON | TUE | WED | THU | FRI | SAT | SUN
<période du lancement>	[0-999], où 0 – la période du lancement n'est pas définie

Exemples

L'exemple suivant illustre le lancement de la tâche en mode "Une fois".

Exemple:

Lancer la tâche le30 mars 2011 à 10:00:

```
RuleType="Once"
StartTime="2011/Mar/30 10:00:00"
```

L'exemple suivant illustre le lancement de la tâche en mode "Chaque mois".

Exemple:

Lancer la tâche chaque 15ième jour du mois à 12:00:

```
RuleType=Monthly
StartTime=12:00:00; 15
```

L'exemple suivant illustre le lancement de la tâche en mode "Chaque semaine".

Exemple:

Lancer la tâche tous les lundis à 00:00:

```
RuleType=Weekly
StartTime=00:00:00; Mon
```

L'exemple suivant illustre le lancement de la tâche en mode "Tous les N jours".

Exemple:

Lancer la tâche tous les deux jours à 12:30:

```
RuleType=Daily
StartTime=12:30:00;; 2
```

L'exemple suivant illustre le lancement de la tâche en mode "Toutes les N heures".

Exemple:

Lancer la tâche toutes les 3 heures depuis l'heure indiquée:

```
RuleType=Hourly
StartTime=2011/Apr/01 00:00:00;; 3
```

L'exemple suivant illustre le lancement de la tâche en mode "Toutes les N minutes".

Exemple:

Lancer la tâche toutes les 10 minutes depuis l'heure indiquée:

```
RuleType=Minutely
StartTime=14:30:00;; 10
```

L'exemple suivant illustre le lancement de la tâche après la mise à jour des bases.

Exemple:

Lancer la tâche après la mise à jour des bases:

```
RuleType=BR
```

L'exemple suivant illustre le lancement de la tâche au démarrage de l'application.

Exemple:

Lancer la tâche au démarrage de Kaspersky Endpoint Security:

```
RuleType=PS
```

PARAMÈTRES GÉNÉRAUX DE KASPERSKY ENDPOINT SECURITY.

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 Endpoint Security (cf. page 112).

Après la modification des paramètres généraux de Kaspersky Endpoint Security il faut redémarrer le service Kaspersky Lab Framework à l'aide de la commande `/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restart-app`.

Tableau 15. Paramètres généraux de Kaspersky Endpoint Security.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
StartWithUser	Compte avec les droits duquel sont exécutés les processus de Kaspersky Endpoint Security. Vous ne pouvez pas modifier ce paramètre. Valeur par défaut: **root**.
StartWithGroup	Compte avec les droits duquel sont exécutés les processus de Kaspersky Endpoint Security. Vous ne pouvez pas modifier ce paramètre. Valeur par défaut: **default**.
UpdateFolder	Chemin d'accès au répertoire sur l'ordinateur protégé; contient les répertoires des mises à jour définis par les paramètres AVBasesFolderName et AVBasesBackupFolderName. Valeur par défaut: **/var/opt/kaspersky/kes4lwks/update**.
AVBasesFolderName	Nom du répertoire dans lequel Kaspersky Endpoint Security enregistre les mises à jour des bases. Valeur par défaut: **avbases**.
AVBasesBackupFolderName	Chemin d'accès complet au répertoire que Kaspersky Endpoint Security 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 Endpoint Security. 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 l'ordinateur. 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 l'ordinateur. 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 Endpoint Security 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 Endpoint Security. Valeur par défaut: **/var/run/kes4lwks**.
TraceEnable	Tenue du journal de trace. Kaspersky Endpoint Security 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;

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	no – ne pas maintenir à jour le registre du tracé. Valeur par défaut: **yes**.
TraceFolder	Répertoire dans lequel Kaspersky Endpoint Security 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 Endpoint Security. Valeur par défaut: **/var/log/kaspersky/kes4lwks**.
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 Endpoint Security tracera les sous-systèmes de Kaspersky Endpoint Security 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**.

PARAMÈTRES 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.

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 Endpoint Security (cf. page 112).

Tableau 16. Paramètres de la quarantaine et du dossier de sauvegarde

PARAMETRE	SPECIFICATION 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 de l'ordinateur. Il est déconseillé de spécifier les répertoires placés sur les ordinateurs distants, par exemple, montés via les protocoles SMB/CIFS et NFS. Kaspersky Endpoint Security commencera à mettre les objets dans le répertoire spécifié par le paramètre, après que vous aurez importé les paramètres depuis le fichier dans Kaspersky Endpoint Security à l'aide de la commande -T --set-settings, arrêté et relancé Kaspersky Endpoint Security. Si le répertoire spécifié n'existe pas ou n'est pas disponible, Kaspersky Endpoint Security utilisera le répertoire de sauvegarde installé par défaut. Valeur par défaut: **/var/opt/kaspersky/kes4lwks/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 Endpoint Security ne met plus les objets en quarantaine et ne réserve plus les objets avant leur réparation ou suppression. Dans le registre de Kaspersky Endpoint Security 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 – $1,8*10^{19}$. Valeur par défaut: **1073741824**.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
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 Endpoint Security continue de mettre les objets en quarantaine et de réserver les objets avant leur réparation ou suppression. Dans le registre de Kaspersky Endpoint Security est enregistré l'événement QuarantineSoftSizeLimitExceeded signalant que la taille recommandée du répertoire de sauvegarde 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 – $1,8*10^{19}$. Valeur par défaut: **858993459**.

LES PARAMÈTRES DU JOURNAL DES ÉVÉNEMENTS

Cette rubrique décrit les paramètres du fichier de configuration du journal des événements de Kaspersky Endpoint Security.

En cas de modification des paramètres dans le fichier, respectez les règles de modification des fichiers de configuration ini de Kaspersky Endpoint Security (cf. page 112).

Tableau 17. Les paramètres du journal des événements

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
EventStorageFolder	Répertoire du journal des événements. Kaspersky Endpoint Security 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 98). Vous ne pouvez pas modifier ce paramètre. Valeur par défaut: **/var/opt/kaspersky/kes4lwks/db/event_storage**.
RotateMethod	Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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.

PARAMETRE	SPECIFICATION ET VALEURS POSSIBLES
	À chaque rotation, Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security réalise la rotation des événements tous les jours à minuit. **Weekly** (chaque semaine). Kaspersky Endpoint Security réalise la rotation des événements tous les lundi à minuit. **Monthly** (chaque mois). Kaspersky Endpoint Security 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**.
`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 Endpoint Security 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 Endpoint Security. Valeur par défaut: **10485760**.

ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY À 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 ordinateurs sur lesquels est installé Kaspersky Endpoint Security, via la Console d'administration de 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 de l'ordinateur 143

Boîte de dialogue "Paramètres de l'application" 144

Création et configuration des tâches 144

Création d'une tâche 145

Assistant pour la création d'une tâche locale 146

Configuration des tâches 147

Configuration de l'horaire de la tâche à l'aide de Kaspersky Administration Kit 151

Création et configuration des stratégies 154

Vérification manuelle de la connexion au Serveur d'administration. Utilitaire klnagchk 155

Connexion au Serveur d'administration en mode manuel. Utilitaire klmover 156

Paramètres des tâches 157

CONSULTATION DU STATUT DE LA PROTECTION DE L'ORDINATEUR

Dans la Console d'administration, vous pouvez consulter le statut de la protection de l'ordinateur choisi, le statut général du point de vue de la sécurité antivirus et son accessibilité.

Pour consulter le statut de la protection de l'ordinateur:

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés** et sélectionnez le groupe dont l'ordinateur à protéger fait partie.

2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur lordinateur 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 l'ordinateur protégé:

Tableau 18. Informations sur l'état de la protection de l'ordinateur dans la boîte de dialogue

CHAMP	DESCRIPTION
Statut de l'ordinateur	Statut de l'ordinateur protégé du point de vue de la sécurité antivirus. Pour de plus amples informations, consultez lesite du service du Support Technique de Kaspersky Lab, code de l'article: 987.
Etat de la PTR	Affiche l'état de la protection en temps réel, par exemple, *En cours d'exécution*, *Arrêtée*, *Suspendue*.
Dernière analyse à la demande	Date et heure de la dernière tâche d'analyse à la demande exécutée.
Nombre de virus détectés	Nombre total de programmes malveillants (signatures de menaces) détectés sur l'ordinateur à protégé (compteur de menaces détectées) dès l'installation de Kaspersky Endpoint Security ou dès la mise à zéro du compteur. Pour mettre à zéro le compteur, cliquez sur le bouton **Mettre à zéro**.

BOÎTE DE DIALOGUE "PARAMÈTRES DE L'APPLICATION"

Dans la boîte de dialogue **Paramètres de l'application**, vous pouvez effectuer l'administration de Kaspersky Endpoint Security à distance et sa configuration sur l'ordinateur 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 l'ordinateur 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 l'ordinateur à protéger et sélectionnez la commande **Propriétés**.
4. Dans la boîte de dialogue **Propriétés**: <**Nom de l'ordinateur**> dans l'onglet **Applications**, sélectionnez **Kaspersky Endpoint Security 8 for Linux** dans la liste des applications installées et cliquez sur le bouton **Propriétés**.

CRÉATION ET CONFIGURATION DES TÂCHES

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 l'ordinateur 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.*

CRÉATION D'UNE TÂCHE

Lorsque vous gérez Kaspersky Endpoint Security via Kaspersky Administration Kit, vous avez la possibilité de créer les types de tâche suivants:

- 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 146) 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 gérés**, 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 nouvelle 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 une sélection d'ordinateurs** (**Tâches Kaspersky Administration Kit**).

3. Cliquez sur le lien **Créer une nouvelle 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 CRÉATION D'UNE TÂCHE 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 GÉNÉRALES SUR LA TÂCHE

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 TÂCHE

Cette étape vous permet d'indiquer l'application, pour laquelle la tâche se crée: Kaspersky Anti-Virus 8 for Linux ou l'Agent d'administration. Outre cela, il est nécessaire de sélectionner le type de tâche.

Pour Kaspersky Endpoint Security 8 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 TÂCHES

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 147) et définir les paramètres d'analyse (cf. page 148);
- définir les zones d'exclusion (cf. page 149).

Pour la tâche de mise à jour des bases et des modules de l'application il faut:

- indiquer une source (cf. page 149), 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 150).

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 Endpoint Security.

ETAPE 4. CONFIGURATION DE LA PROGRAMMATION

Configurez les paramètres de l'horaire de la tâche (cf. rubrique "Configuration de l'horaire de la tâche" à la page 152). 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 TÂCHES

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, déployez le nœud **Ordinateurs administrés** et sélectionnez le groupe auquel appartient l'ordinateur à protéger.
2. Dans le panneau des résultats, ouvrez le menu contextuel à la ligne contenant les informations sur lordinateur 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 de l'ordinateur analysé par Kaspersky Endpoint Security. 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, exécutez les actions suivantes:

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 (**SMB/CIFS** 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 permettent de spécifier le modèle du nom de fichier pour l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier pour l'analyse par Kaspersky Endpoint Security. 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 Endpoint Security 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 **En haut** et **En bas**.

CONFIGURATION DES PARAMÈTRES DE SÉCURITÉ

Par défaut, Kaspersky Endpoint Security 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 162), qui seront analysés par Kaspersky Endpoint Security.

4. Sous l'onglet **Paramètres** dans le groupe **Optimisation d'analyse** définissez la durée maximale de l'analyse de l'objet (cf. page 162) et la taille maximale de l'objet analysé (cf. page 162).

5. Dans l'onglet **Actions** sélectionnez actions à effectuer sur des objets infectés (cf. page 159), et actions à effectuer sur des objets suspects (cf. page 159).

6. Sous l'onglet **Zone d'exclusion** définissez les objets exclus de l'analyse selon le nom (cf. page 161), et les objets exclus de l'analyse selon le nom de la menace détectée (cf. page 161).

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.

CRÉATION D'UNE ZONE D'EXCLUSION

Kaspersky Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Endpoint Security. 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 (**SMB/CIFS** 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.

SÉLECTION DE LA SOURCE DES MISES À JOUR

La source des mises à jour est la source qui contient les mises à jour des bases de Kaspersky Endpoint Security. 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 162).
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 163)
   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 163)
   c. utilisation du serveur proxy (cf. page 163)
   d. paramètres du serveur proxy (cf. page 164)
   e. vérification de l'authenticité lors de l'accès au serveur proxy (cf. page 164)
   f. emplacement de l'ordinateur protégé
4. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

SÉLECTION DE TYPE DES MISES À JOUR

La tâche des mises à jour de Kaspersky Endpoint Security exécute une des actions suivantes:

1. Le téléchargement et l'installation des bases.
2. La copie des mises à jour des modules de Kaspersky Endpoint Security. 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 164) 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 164) dans le champ **Répertoire cible**.
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 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 TÂCHE À L'AIDE DE KASPERSKY ADMINISTRATION KIT

Vous pouvez configurer l'horaire de la tâche lors de sa création dans l'Assistant de création d'une tâche, 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.

DANS CETTE SECTION

Création de la règle du lancement de la tâche 151

Configuration de l'horaire de la tâche 152

CRÉATION DE LA RÈGLE DU LANCEMENT DE LA TÂCHE

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 Endpoint Security.

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 l'ordinateur 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 lordinateur 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. Configurez de l'horaire de la tâche (cf. rubrique "Configuration de l'horaire de la tâche" à la page 152).
7. Cliquez sur le bouton **OK**, pour enregistrer les modifications.

CONFIGURATION DE L'HORAIRE DE LA TÂCHE

Dans la liste déroulante **Planification**, sélectionnez le mode nécessaire de la mise en marche de la tâche:

- **Toutes les N heures**.
- **Toutes les N minutes**.
- **Tous les N jours**.
- **Chaque semaine**.
- **Chaque mois**.
- **Une fois**.
- **Mode manuel**: démarre la tâche manuellement à partir de la fenêtre principale de Kaspersky Endpoint Security, à l'aide de la commande **Démarrer** du menu contextuel ou du point analogique dans le menu **Action**.
- **Après la mise à jour de l'application**: démarre la tâche après chaque mise à jour des bases de l'application.
- **Au lancement de l'application**.
- **Lors du téléchargement des mises à jour dans le référentiel**: démarre la tâche automatiquement après la réception de mises à jour par le Serveur d'administration.
- **Lors de la détection d'une attaque de virus**.
- **A la fin d'une autre tâche**.

C'est ici que figurent les modes de lancement des tâches de Kaspersky Administration Kit. Pour les tâches créées pour d'autres applications, la programmation peut varier. Les informations détaillées sur les tâches de Kaspersky Administration Kit sont données dans le document *Kaspersky Administration Kit. Manuel d'administrateur.*

Après avoir sélectionné le mode de lancement d'une tâche, il faut indiquer la fréquence de son lancement dans le groupe des champs correspondants au mode sélectionné. Selon le mode sélectionné, les valeurs suivantes sont indiquées:

- Pour le mode de lancement d'une tâche **Toutes les N heures**, dans le champ **Tous les** il faut indiquer la fréquence en heures, et dans le champ **A partir de** – la date et l'heure du premier lancement d'une tâche.

  Par exemple, si dans le champ **Toutes les** la valeur **2** est établie et dans la champ **A partir de** la valeur du **3 avril 2011. 15:00:00** est établie, la tâche démarrera toutes les deux heures à partir de 15 heures, le 3 avril 2011.

  La fréquence est définie par défaut à **6** et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- Pour le mode de lancement de la tâche **Toutes les N minutes** dans le champ **Toutes les** la fréquence est définie en minutes, et dans le champ **A partie de** – l'heure du premier lancement.

  Par exemple, si dans le champ **Toutes les** la valeur **30** est établie, et dans le champ **A partie de** – **15:00:00**, la tâche démarrera toutes les 30 minutes à partir de 15h00 du jour actuel.

La fréquence est définie par défaut à **30** et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- Pour le mode de lancement de la tâche **Tous les N jours** dans le champ **Tous les** la fréquence du lancement de la tâche est définie en jours, et dans le champ **Heure du lancement** – l'heure à laquelle la tâche doit être lancée dans les jours indiqués.

  Par exemple, si le champ Chaque affiche la valeur 2 et le champ Heure d'exécution indique 15h00, la tâche commencera une fois tous les deux jours à 3 heures de l'après midi.**Tous les** affiche la valeur **2** et le champ **Heure du lancement** indique **15h00**, la tâche commencera une fois tous les deux jours à 15h00.

  La fréquence est définie par défaut à **1** et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- Pour le mode de lancement de la tâche **Chaque semaine**, dans le champ **Tous les**, il faut indiquer le jour de la semaine à lancer une tâche, et dans le champ **Heure du lancement** – l'heure du lancement d'une tâche le jour indiqué de la semaine.

  Par exemple, si la valeur du champ **Chaque** est **lundi** et la valeur du champ **Heure du lancement** est **15h00**, la tâche commencera chaque lundi à 15h00.

  Par défaut, la valeur du champ **Jour du lancement** est **dimanche** et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- Pour le mode de lancement de la tâche **Chaque mois**, dans le champ **Chaque**, il faut indiquer le jour du mois à lancer une tâche, et dans le champ **Heure du lancement** – l'heure du lancement d'une tâche le jour indiqué du mois.

  Par exemple, si la valeur du champ **Chaque** contient **20** et la valeur du champ **Heure du lancement** est **15h00**, la tâche commencera le 20 de chaque mois à 15h00.

  La valeur par défaut du champ **Chaque** contient **1** et dans le champ **Heure du lancement** – l'heure système actuelle est utilisée.

- Pour le mode de lancement de la tâche **Une fois**, le champ **Date d'exécution** indique le jour à lancer la tâche, et le champ **Heure du lancement** indique l'heure du lancement de la tâche le jour indiqué.

  Les valeurs de ces champs sont définies automatiquement et correspondent à la date et à l'heure courante du système, mais vous pouvez les modifier.

- Pour le mode de lancement **Lors de la détection d'une attaque de virus**, il est nécessaire d'indiquer les types des applications pour lesquelles il faut tenir compte de l'événement *Attaque de virus* lors du lancement de la tâche. Pour ce faire, il faut cocher les cases à côté des types sélectionnés des applications.

- Si la tâche sera lancée après la fin d'une autre tâche, dans le champ **Nom de la tâche** à l'aide du bouton **Sélectionner**, il faut indiquer quelle tâche doit se terminer d'autre part. Dans le champ **Résultat de la tâche**, il faut indiquer la manière dont la tâche sélectionnée doit se terminer.

Configurez les paramètres avancés d'exécution de la tâche (ils varient en fonction du mode d'exécution):

- La procédure que la tâche doit démarrer si le poste client n'est pas disponible (éteint, déconnecté du réseau, etc.) ou si l'application n'est pas lancée à l'heure programmée.

  Si la case **Lancer les tâches non exécutées** est cochée, lors du lancement suivant de l'application sur cet ordinateur, une tentative de lancement de la tâche sera faite. Si l'option **Mode manuel** et **Une fois** a été sélectionnée, la tâche sera exécutée dès l'apparition de l'ordinateur sur le réseau.

  Si cette case n'est pas cochée, l'exécution de la tâche sur les postes clients aura lieu uniquement selon la programmation et pour les options **Manuel** et **Une fois**, uniquement pour les postes clients visibles dans le réseau. Par défaut, cette case n'est pas cochée.

- Définir la marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients. Cette possibilité est offerte pour résoudre le problème d'appels simultané par de nombreux postes clients au Serveur d'administration lors du lancement de la tâche.

Cochez la case **Répartir le lancement aléatoire de la tâche sur l'intervalle (min)** et indiquez l'intervalle de temps pendant lequel les postes clients appelleront le Serveur d'administration après le démarrage de la tâche, au lieu de le faire simultanément. Par défaut, cette case n'est pas cochée.

CRÉATION ET CONFIGURATION DES STRATÉGIES

Vous pouvez créer des stratégies Kaspersky Administration Kit communes pour gérer la protection de plusieurs ordinateurs sur lesquels est installé Kaspersky Endpoint Security.

La stratégie utilise les valeurs des paramètres qui y sont spécifiées pour tous les ordinateurs 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 Endpoint Security 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 Endpoint Security 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 tâches de protection en temps réel de Kaspersky Endpoint Security.

DANS CETTE SECTION

Création d'une stratégie 154

Configuration d'une stratégie 155

CREATION D'UNE STRATEGIE

Pour créer une stratégie pour un groupe des serveurs sur lesquels est installé Kaspersky Endpoint Security, procédez comme suit:

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Ordinateurs administrés**; déployez le groupe d'administration pour les ordinateurs duquel vous souhaitez créer une stratégie.

2. Dans le menu contextuel du nœud incorporé **Stratégies**, sélectionnez la commande **Nouveau** → **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 Endpoint Security 8 for Linux** 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 157).

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 STRATÉGIE

Dans la boîte de dialogue **Propriétés** de la stratégie en cours, vous pouvez spécifier les paramètres de la protection en temps réel de Kaspersky Endpoint Security.

*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**.

VÉRIFICATION 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 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 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 de l'ordinateur.

- `-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.

PARAMETRES DES TACHES

DANS CETTE SECTION

Mode d'interception 157

Mode de protection des objets 158

Analyse heuristique 158

Action à exécuter sur les objets infectés 159

Action à exécuter sur les objets suspects 159

Actions à exécuter sur des objets en fonction du type de menace 160

Exclusion des objets selon le nom 161

Exclusion des objets en fonction du nom de la menace 161

Analyse des objets composés 162

Durée maximum d'analyse d'un objet 162

Taille maximum de l'objet analysé 162

Source des mises à jour 162

Mode du serveur FTP 163

Délai d'attente pour la réponse du serveur FTP ou HTTP 163

Utilisation d'un serveur proxy lors de la connexion aux sources de mises à jour 163

Vérification de l'authenticité lors de l'accès au serveur proxy 164

Paramètres du serveur proxy 164

Répertoire de sauvegarde des mises à jour 164

Type de mises à jour 164

MODE D'INTERCEPTION

Le paramètre de sécurité **Mode d'interception** n'est utilisé que dans les tâches de protection en temps réel.

Kaspersky Endpoint Security 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 Endpoint Security.

Si vous utilisez l'ordinateur protégé uniquement en tant que serveur SAMBA vous pouvez spécifier la valeur **Uniquement SAMBA**. Dans ce cas, Kaspersky Endpoint Security 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 Endpoint Security analyse les objets sur l'ordinateur lorsqu'on y fait requête via le protocole SMB/CIFS avec utilisation de l'intercepteur SAMBA. Kaspersky Endpoint Security intercepte toutes les autres opérations sur les fichiers disponibles sur l'ordinateur protégé (y compris, sur les fichiers des ordinateurs distants), en utilisant l'intercepteur du niveau du noyau.

- **Uniquement SAMBA**. Kaspersky Endpoint Security 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 Endpoint Security (cf. du Manuel d'installation de Kaspersky Endpoint Security 8 for Linux).

- **Uniquement le système de fichiers**. Kaspersky Endpoint Security analyse les objets sur l'ordinateur sans utilisation de l'intercepteur SAMBA.

  Assurez-vous d'avoir installé l'intercepteur de noyau durant la configuration initiale de Kaspersky Endpoint Security (cf. du Manuel d'installation de Kaspersky Endpoint Security 8 for Linux).

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. Il détermine à quel type d'accès aux objets Kaspersky Endpoint Security les analysera.

Sélectionnez un des modes de protection en fonction de vos besoins pour la sécurité de l'ordinateur, en fonction des formats des fichiers sauvegardés sur l'ordinateur et des informations qu'ils contiennent:

- **Mode intelligent**. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 l'ordinateur:

- **Superficiel**;
- **Moyenne**;
- **Profond**;
- **Recommandé**.

Valeur par défaut: **Recommandé**.

ACTION À EXÉCUTER SUR LES OBJETS INFECTÉS

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 Endpoint Security 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 Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Supprimer**. Kaspersky Endpoint Security supprime l'objet.
- **Exécuter l'action recommandée**. Kaspersky Endpoint Security choisit automatiquement et effectue actions 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 Endpoint Security 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. Vous pouvez indiquer cette action uniquement en tant que première action à exécuter sur des objets infectés.
- **Ignorer**. L'objet reste intact: Kaspersky Endpoint Security 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.

Avant de modifier l'objet (traiter ou supprimer), Kaspersky Endpoint Security 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 Endpoint Security sont affichées dans le registre.

Sélectionnez dans la liste deux actions que Kaspersky Endpoint Security essaiera d'effectuer sur l'objet. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security, avant d'exécuter une action, verrouille l'accès à l'objet pour l'application qui l'a sollicité.

ACTION À EXÉCUTER 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 Endpoint Security reconnaît l'objet analysé 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.
- **Réparer**. Kaspersky Endpoint Security essaie de réparer l'objet; si la réparation ne s'avère pas possible, l'objet reste intact.
- **Supprimer**. Kaspersky Endpoint Security supprime l'objet suspect de l'ordinateur.

  Avant de supprimer l'objet, Kaspersky Endpoint Security met sa copie dans le répertoire de sauvegarde de réserve. Kaspersky Endpoint Security 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 Endpoint Security sont consignées dans le journal.

- **Exécuter l'action recommandée**. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security essaiera d'effectuer sur l'objet. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security, avant d'exécuter une action, verrouille l'accès à l'objet pour l'application qui l'a sollicité.

ACTIONS À EXÉCUTER 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 Endpoint Security sur des objets qui contiennent des menaces de types différents.

Si vous déterminez les valeurs de ce paramètre, Kaspersky Endpoint Security les utilisera au lieu des valeurs des paramètres Actions à exécuter sur des objets infectés (cf. page 159) et Actions à exécuter sur des objets suspects (cf. page 159).

Pour chaque type de menace, sélectionnez dans la liste deux actions que Kaspersky Endpoint Security essaiera d'effectuer sur l'objet s'il y détecte une menace du type spécifié. Kaspersky Endpoint Security effectuera la deuxième action sur l'objet s'il n'arrive pas à effectuer la première action.

Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 ECMA-262.

Les masques Shell vous permettent de spécifier le modèle du nom du fichier exclu de l'analyse par Kaspersky Endpoint Security.

Les expressions régulières vous permettent d'indiquer le modèle du chemin d'accès au fichier exclus de l'analyse par Kaspersky Endpoint Security. 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security.

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 ECMA-262.

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 Endpoint Security 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 ECMA-262. Ajoutez le préfixe **re:** aux expressions régulières ECMA-262.

Par exemple, pour ne pas exécuter les actions sur les fichiers dans lesquels Kaspersky Endpoint Security détectera n'importe quelle menace pour Linux de la catégorie not-a-virus, saisissez: **re:not-a-virus:.*\.Linux\..***.

ANALYSE DES OBJETS COMPOSÉS

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 Endpoint Security 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 Endpoint Security analysera.

Sélectionnez une ou plusieurs valeurs:

- **Analyse des archives**. Kaspersky Endpoint Security analyse les archives (y compris les archives autoextractibles SFX). Faites attention à ce que Kaspersky Endpoint Security détecte des menaces dans les archives sans les réparer.
- **Analyser des archives autoextractibles**. Kaspersky Endpoint Security analyse des archives autoextractibles (archives qui comprennent un module de désarchivage).
- **Analyser les bases de messagerie**. Kaspersky Endpoint Security analyse les objets des bases de messagerie Microsoft Office Outlook et Microsoft Outlook Express.
- **Analyser les objets compactés**. Kaspersky Endpoint Security analyse les fichiers exécutables archivés par les programmes d'archivage de code binaire tels qu'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 Endpoint Security analyse les fichiers des messages informatiques au format texte (plain text).

DURÉE 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 Endpoint Security 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 ANALYSÉ

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 Endpoint Security 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 À JOUR

Vous pouvez sélectionner la source depuis laquelle Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security téléchargera les mises à jour sur l'ordinateur protégé depuis le serveur d'administration Kaspersky Administration Kit installé dans le réseau local.

- **Autres répertoires dans le réseau local ou mondial**. Kaspersky Endpoint Security 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 de l'ordinateur, 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 définies par l'utilisateur. Kaspersky Endpoint Security fera requête à chaque source spécifiée suivante si la source précédente n'est pas disponible.

Vous pouvez modifier l'ordre selon lequel Kaspersky Endpoint Security 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 Endpoint Security aux serveurs des mises à jour de Kaspersky Lab dans le cas où toutes les sources d'utilisateurs ne sont pas disponibles.

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 Endpoint Security 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.

DÉLAI D'ATTENTE POUR LA RÉPONSE 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 Endpoint Security 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 D'UN SERVEUR PROXY LORS DE LA CONNEXION AUX SOURCES DE MISES À 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 Endpoint Security 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 Endpoint Security n'utilise pas le serveur proxy. On suppose que ces sources se trouvent dans le réseau local.

VÉRIFICATION DE L'AUTHENTICITÉ LORS DE L'ACCÈS 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.

PARAMÈTRES 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.

RÉPERTOIRE DE SAUVEGARDE DES MISES À 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 de l'ordinateur.

Valeur par défaut: non spécifié.

TYPE DE MISES À 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 sur le site du Service du Support Technique de Kaspersky Lab.

  L'installation automatique des mises à jour critiques des modules de Kaspersky Endpoint Security n'est pas prévue.

Valeur par défaut: **Uniquement les bases**.

KASPERSKY LAB

Kaspersky Lab a été fondée en 1997. C'est aujourd'hui le concepteur le plus connu de Russie en technologies de sécurité de l'information. La société produit un large éventail de logiciels de sécurité de données: des systèmes de protection contre les virus, les courriers électroniques non sollicités ou indésirables (spam) et contre les tentatives d'intrusion.

Kaspersky Lab est une société internationale. Son siège principal se trouve en Russie, et la société possède des filiales 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 société, le centre européen de recherches anti-virus, a été récemment installé en France. Le réseau des partenaires de Kaspersky Lab compte plus de 500 entreprises dans le 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 une analyse continue de l'activité de virus, 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 antivirus 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 antivirus 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 Internet 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) http://support.kaspersky.com/fr/virlab/helpdesk.html (pour les questions aux experts antivirus)

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt qui se trouve dans le dossier d'installation de l'application.