KASPERSKY lab

Kaspersky Endpoint Security 10 for Linux

Manuel d'administrateur

Version du logiciel : 10

Chers utilisateurs,

Nous vous remercions de votre confiance. Nous espérons que le présent manuel vous sera utile dans votre travail et qu'il fournira des réponses à la plupart de vos questions.

Date d'édition du document : 22/02/2017

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

Table des matières

A propos de ce document

Le manuel de l'administrateur de Kaspersky Endpoint Security 10 for Linux (ci-après "Kaspersky Endpoint Security") s'adresse aux spécialistes de l'installation et de l'administration de Kaspersky Endpoint Security, et aux spécialistes de l'assistance technique des organisations utilisant Kaspersky Endpoint Security.

Les informations reprises dans ce manuel peuvent être utiles dans l'exécution des tâches suivantes :

- préparatifs de l'installation, installation et activation de Kaspersky Endpoint Security ;
- configuration et utilisation de Kaspersky Endpoint Security.

Ce manuel renseigne également les sources d'informations sur l'application et les méthodes d'obtention de l'assistance technique.

Dans cette section

Dans ce document

Ce manuel contient les sections suivantes.

Sources d'informations sur l'application (cf. page 14)

Cette section présente les différentes sources d'informations sur l'application.

Kaspersky Endpoint Security (cf. page 17)

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des composants de l'application. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés de l'application.

Installation et suppression de l'application (cf. page 23)

Cette section décrit l'installation de Kaspersky Endpoint Security sur l'ordinateur, la configuration initiale de l'application ainsi que la suppression de l'application de l'ordinateur.

Licence de l'application (cf. page 40)

Cette section présente les notions principales relatives à la mise sous licence de l'application.

Lancement et arrêt de l'application (cf. page 48)

Cette section contient des informations indiquant comment lancer, relancer et terminer le fonctionnement de l'application à partir de la ligne de commande.

Gestion des tâches Kaspersky Endpoint Security (cf. page 50)

Cette section contient des informations sur les types de tâches de Kaspersky Endpoint Security et des instructions relatives à la gestion de ces tâches.

Mise à jour des bases de données et des modules de l'application (cf. page 56)

Cette section contient des informations sur la mise à jour des bases antivirus et des modules de l'application (également appelées ci-après "mises à jour") et des instructions indiquant comment configurer les paramètres de mise à jour.

Protection en temps réel et analyse à la demande (cf. page 63)

Cette section fournit des informations sur les tâches de protection en temps réel et d'analyse à la demande. Elle explique également comment configurer les paramètres de ces tâches.

Utilisation de la Sauvegarde (cf. page 84)

Cette section contient des instructions indiquant comment configurer les paramètres de la Sauvegarde et des informations sur les actions exécutables sur les objets dans la sauvegarde.

Participation au Kaspersky Security Network (cf. page 89)

Cette section contient des informations relatives à la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de Kaspersky Security Network.

Administration de l'application via Kaspersky Security Center (cf. page 94)

Cette section contient les informations relatives à l'administration de l'application Kaspersky Endpoint Security via Kaspersky Security Center.

Contacter le Service du Support Technique (à la page 117)

Cette section contient des informations sur les modes et les conditions d'obtention de l'assistance technique.

Appendices (cf. page 120)

Cette section présente les paramètres des fichiers de configuration, les commandes pour l'administration de Kaspersky Endpoint Security via la ligne de commande, ainsi que les codes de retour de la ligne de commande.

AO Kaspersky Lab (à la page 180)

Cette section contient des informations sur AO Kaspersky Lab.

Information sur le code tiers (cf. page 182)

Cette section fournit des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page 183)

Cette section contient des informations sur les marques déposées mentionnées dans le document.

Glossaire (cf. page 184)

Cette section contient une liste des termes qui apparaissent dans le document et leur définition.

Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

Conventions

Le présent document respecte des conventions (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple du texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Ils contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple : …	Les exemples sont présentés en blocs sur un fond bleu sous le titre "Exemple".

Exemple du texte	Description de la convention
La *mise à jour*, c'est... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
► *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir à l'aide du clavier.
<Nom de l'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

Sources d'informations sur l'application

Cette section présente les différentes sources d'informations sur l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

Dans cette section

Sources pour les recherches indépendantes d'informations

Vous pouvez utiliser les sources suivantes pour rechercher des informations sur Kaspersky Endpoint Security :

- la page de Kaspersky Endpoint Security sur le site Web de Kaspersky Lab ;
- la page de Kaspersky Endpoint Security sur le site du Support technique (base de solutions) ;
- documentation.

Si vous ne trouvez pas la solution à votre problème, contactez le Support technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 117).

Une connexion Internet est requise pour utiliser les sources d'informations sur les sites Web.

Page de Kaspersky Endpoint Security sur le site Web de Kaspersky Lab

La page Kaspersky Endpoint Security (http://www.kaspersky.ru/business-security/endpoint-linux) propose des informations générales sur l'application, ses possibilités et les particularités de son fonctionnement.

La page de Kaspersky Endpoint Security contient un lien vers la boutique en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page de Kaspersky Endpoint Security dans la base de connaissances

La base de connaissances est une section du site Web du Support technique.

La page de Kaspersky Endpoint Security dans la base de connaissances (http://support.kaspersky.fr/kes10linux) propose des articles qui contiennent des informations utiles, des recommandations et des réponses aux questions souvent posées sur l'acquisition, l'installation et l'utilisation de l'application.

Les articles de la base de connaissances peuvent répondre à des questions qui portent non seulement sur Kaspersky Endpoint Security, mais également sur d'autres applications de Kaspersky Lab. Les articles de la base de connaissances peuvent également comporter des actualités sur le Service de Support technique.

Documentation

La documentation de l'application inclut les fichiers du Manuel de l'administrateur.

Le manuel de l'administrateur fournit des informations sur l'exécution des tâches suivantes :

- préparatifs de l'installation, installation et activation de Kaspersky Endpoint Security ;
- configuration et utilisation de Kaspersky Endpoint Security ;
- gestion à distance de Kaspersky Endpoint Security via Kaspersky Security Center.

Discussions sur les applications de Kaspersky Lab sur le forum

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications sur notre forum (http://forum.kaspersky.fr).

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

Kaspersky Endpoint Security

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Endpoint Security ainsi que les configurations matérielle et logicielle requises pour Kaspersky Endpoint Security.

Dans cette section

Présentation de Kaspersky Endpoint Security

Kaspersky Endpoint Security protège les ordinateurs qui tournent sous les systèmes d'exploitation Linux® contre les applications malveillantes. Les menaces peuvent pénétrer le système via les canaux de transmission de données du réseau ou depuis des disques amovibles.

L'application permet :

- D'analyser les objets du système de fichiers sur les disques locaux de l'ordinateur, ainsi que sur les ressources montées et partagées accessibles via les protocoles SMB et NFS.

  L'application analyse les objets du système de fichiers aussi bien en temps réel à l'aide de la tâche de protection en temps réel qu'à la demande de l'utilisateur à l'aide de la tâche d'analyse à la demande.

- D'analyser les secteurs d'amorçage à l'aide de la tâche d'analyse des secteurs d'amorçage.

- D'analyser la mémoire des processus à l'aide de la tâche d'analyse de la mémoire des processus.
- De détecter les objets infectés.

  Kaspersky Endpoint Security considère qu'un objet est infecté s'il contient le code d'un virus connu.
- De neutraliser les menaces détectées dans les fichiers.

  En fonction du type de menace, l'application choisit automatiquement l'action à exécuter pour neutraliser la menace.
- D'enregistrer des copies de sauvegarde des fichiers avant la désinfection et de restaurer les fichiers à partir des copies de sauvegarde.
- D'administrer les tâches et de configurer leurs paramètres.

  Vous pouvez administrer la tâche de protection en temps réel, ainsi que les tâches d'analyse à la demande, d'analyse des secteurs d'amorçage, d'analyse de la mémoire des processus, de mise à jour, sans oublier les tâches d'annulation des mises à jour et de copie de celles-ci.
- D'ajouter des clés, activer l'application à l'aide de codes d'activation, utiliser l'application sous abonnement.
- De signaler à l'administrateur les événements qui ont eu lieu pendant le fonctionnement de Kaspersky Endpoint Security.
- De mettre à jour les bases de Kaspersky Endpoint Security depuis les serveurs de mise à jour de Kaspersky Lab, via le Serveur d'administration ou depuis une source de mise à jour programmée ou à la demande définie par l'utilisateur.

  L'application utilise les bases antivirus pour détecter et désinfecter les fichiers infectés. Kaspersky Endpoint Security recherche la présence éventuelle de menaces dans chaque fichier : le code du fichier est comparé au code caractéristique d'une menace ou d'une autre.
- D'administrer Kaspersky Endpoint Security à l'aide des moyens suivants :
  - à l'aide des commandes d'administration de l'application depuis la ligne de commande ;
  - via Kaspersky Security Center.

Nouveautés

Kaspersky Endpoint Security offre les nouvelles possibilités suivantes :

- Ajout de la prise en charge de Kaspersky Security Network.
- Ajout de la prise en charge de Kaspersky Private Security Network lors de l'utilisation de Kaspersky Security Center.
- Possibilité d'utiliser Kaspersky Endpoint Security sous un abonnement.
- Prise en charge du service d'activation 2.0.
- Possibilité d'analyser la mémoire des processus.
- Possibilité d'analyser les secteurs d'amorçage.
- Ajout de nouvelles commandes pour simplifier l'administration de Kaspersky Endpoint Security.
- Prise en charge de la technologie fanotify.
- Possibilité offerte aux utilisateurs dépourvus de privilèges d'analyser les fichiers.

Distribution

Le kit de distribution de Kaspersky Endpoint Security contient les fichiers suivants :

- kesl-10.0.0-<numéro de version>.i386.rpm, kesl_10.0.0-<numéro de version>_i386.deb

  Ils contiennent les fichiers principaux de Kaspersky Endpoint Security. Ces paquets peuvent être installés sur des systèmes d'exploitation de 32 bits conformément au type de gestionnaire de paquet.

- kesl-10.0.0-<numéro de version>.x86_64.rpm, kesl_10.0.0-<numéro de version>_amd64.deb

  Ils contiennent les fichiers principaux de Kaspersky Endpoint Security. Ces paquets peuvent être installés sur des systèmes d'exploitation de 64 bits conformément au type de gestionnaire de paquet.

- kesl.zip

  Contient les fichiers utilisés dans la procédure d'installation à distance de Kaspersky Endpoint Security à l'aide de Kaspersky Security Center.

- klnagent-<numéro de version>.i386.rpm, klnagent_<numéro de version>_i386.deb

  Ils contiennent l'Agent d'administration (l'utilitaire de communication entre Kaspersky Endpoint Security et Kaspersky Security Center.

- klnagent-rpm.tar.gz, klnagent-deb.tar.gz

  Ils contiennent les fichiers klnagent.kpd et akinstall.sh utilisés dans la procédure d'installation à distance de l'Agent d'administration à l'aide de Kaspersky Security Center.

- Le fichier ksn_license.<ID de la langue> qui vous permet de prendre connaissance des conditions de participation à Kaspersky Security Network.

- Le fichier license.<ID de la langue> qui permet de prendre connaissance du Contrat de licence utilisateur final. Le Contrat de licence utilisateur final indique les conditions dans le cadre desquelles vous pouvez utiliser l'application.

Configurations logicielle et matérielle

Afin de garantir le fonctionnement de Kaspersky Endpoint Security, l'ordinateur doit posséder la configuration minimum suivante.

Configuration minimale requise :

- processeur Core™ 2 Duo 1,86 GHz ou supérieur ;
- 1 Go de mémoire vive pour les systèmes d'exploitation de 32 bits ;
- 2 Go de mémoire vive pour les systèmes d'exploitation de 64 bits ;
- un secteur de pagination d'au moins 1 Go ;
- 1 Go d'espace libre sur le disque dur.

Configuration logicielle :

- Systèmes d'exploitation 32 bits pris en charge :
  - Red Hat® Enterprise Linux® 6.7 ;

- Red Hat Enterprise Linux 6.8 ;
- CentOS-6.7 ;
- CentOS-6.8 ;
- Ubuntu Server 14.04 LTS ;
- Ubuntu Server 16.04 LTS ;
- Ubuntu Server 16.10 LTS ;
- Debian GNU/Linux 7.10 ;
- Debian GNU/Linux 7.11 ;
- Debian GNU/Linux 8.6 ;
- Debian GNU/Linux 8.7.

- Systèmes d'exploitation 64 bits pris en charge :
  - Red Hat Enterprise Linux 6.7 ;
  - Red Hat Enterprise Linux 6.8 ;
  - Red Hat Enterprise Linux 7.2 ;
  - Red Hat Enterprise Linux 7.3 ;
  - CentOS-6.7 ;
  - CentOS-6.8 ;
  - CentOS-7.2 ;
  - CentOS-7.3 ;
  - Ubuntu Server 14.04 LTS ;
  - Ubuntu Server 16.04 LTS ;
  - Ubuntu Server 16.10 LTS ;
  - Debian GNU/Linux 7.10 ;
  - Debian GNU/Linux 7.11 ;
  - Debian GNU/Linux 8.6 ;
  - Debian GNU/Linux 8.7 ;
  - openSUSE 42.2 ;

- Novell OES11 SP3 ;
- Novell OES2015 SP1 ;
- Oracle Linux 7.3.

- Interpréteur de langage Perl version 5.10 ou suivante.
- Utilitaire which.
- Paquets d'installation pour la compilation des applications (gcc, binutils, glibc, glibc-devel, make, ld).
- Code source du noyau du système d'exploitation ; pour la compilation des modules de Kaspersky Endpoint Security sur les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify.
- Kaspersky Endpoint Security 10 for Linux est compatible avec Kaspersky Security Center 10 SP1 et Kaspersky Security Center 10 SP2.
- Pour garantir le bon fonctionnement du plug-in d'administration de Kaspersky Endpoint Security, Microsoft® Visual C ++ 2015 Redistributable Update 3 RC doit être installé.
- Avant d'installer l'Agent d'administration, il faut installer les modules suivants :
  - Le module libc6-i386 doit être installé sur les versions 64 bits de Debian et Ubuntu.
  - Le module glibc.i686 doit être installé sur Red Hat Enterprise Linux 7 et suivant, CentOS 7 et suivant, ainsi que sur Oracle Linux 7 et suivant.
  - Le module glibc-32bit doit être installé sur openSUSE 42.2.

Installation et suppression de l'application

Cette section explique, étape par étape, comment installer et désinstaller Kaspersky Endpoint Security.

Dans cette section

Procédure d'installation de l'application

Cette section explique comment installer le paquet d'installation (ci-après, le "paquet") de Kaspersky Endpoint Security et de l'Agent d'administration.

Présentation de l'installation de Kaspersky Endpoint Security

Kaspersky Endpoint Security est diffusé sous forme de paquets aux formats DEB et RPM.

Pour pouvoir utiliser Kaspersky Endpoint Security, il faut réaliser les opérations suivantes :

1. installer le paquet de Kaspersky Endpoint Security ;
2. lancer le script de mise à jour des paramètres ;

3. installer le paquet de l'Agent d'administration et le plug-in d'administration de Kaspersky Endpoint Security, en cas d'intention d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Security Center.

Installation du paquet de Kaspersky Endpoint Security

Kaspersky Endpoint Security est diffusé sous forme de paquets aux formats DEB et RPM.

► *Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :*

```
# rpm -i kesl-10.0.0-<numéro de version>.i386.rpm
```

► *Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :*

```
# rpm -i kesl-10.0.0-<numéro de version>.x86_64.rpm
```

► *Pour installer Kaspersky Endpoint Security depuis un paquet au format DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :*

```
# dpkg -i kesl-10.0.0-<numéro de version>_i386.deb
```

► *Pour installer Kaspersky Endpoint Security depuis un paquet au format DEB sur un système d'exploitation 64 bits, exécutez la commande suivante :*

```
# dpkg -i kesl_10.0.0-<numéro de version>_amd64.deb
```

Mise à jour des paramètres de Kaspersky Endpoint Security

Après l'installation de Kaspersky Endpoint Security, il faut lancer le script de configuration post-installation de Kaspersky Endpoint Security. Le script de configuration de Kaspersky Endpoint Security après l'installation figure dans le paquet de Kaspersky Endpoint Security.

► *Pour lancer manuellement le script de configuration post-installation de Kaspersky Endpoint Security, exécutez la commande suivante :*

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Le script de configuration post-installation sollicite, étape par étape, les valeurs des paramètres de Kaspersky Endpoint Security (cf. section "Présentation de la configuration initiale de Kaspersky Endpoint Security" à la page 26).

La mise à jour de la version précédente de l'application jusqu'à Kaspersky Endpoint Security 10 for Linux n'est pas prise en charge. Il faut supprimer la version antérieure de l'application et installer Kaspersky Endpoint Security.

Installation de l'Agent d'administration

L'installation de l'Agent d'administration est requise si vous envisagez d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Security Center.

Il faut posséder les autorisations root pour lancer l'installation de l'Agent d'administration.

- *Pour installer l'Agent d'administration depuis un paquet au format RPM sur un système d'exploitation 32 ou 64 bits, exécutez la commande suivante :*

  ```
  # rpm -i klnagent-<numéro de version>.i386.rpm
  ```

- *Pour installer l'Agent d'administration depuis un paquet au format DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :*

  ```
  # dpkg -i klnagent_<numéro de version>_i386.deb
  ```

- *Pour installer l'Agent d'administration depuis un paquet au format DEB sur un système d'exploitation 64 bits, exécutez la commande suivante :*

  ```
  # dpkg -i --force-architecture klnagent_<numéro de version>_i386.deb
  ```

Une fois que le paquet a été installé, lancez le script de configuration post-installation de Kaspersky Endpoint Security en exécutant la commande suivante :

```
/opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

Installation de Kaspersky Endpoint Security à l'aide de Kaspersky Security Center

Vous pouvez installer Kaspersky Endpoint Security sur l'ordinateur à l'aide de Kaspersky Security Center.

Pour en savoir plus sur ce type d'installation de l'application, lisez le *Manuel de l'administrateur de Kaspersky Security Center*.

Préparation de l'application au travail

Cette section présente la configuration initiale de Kaspersky Endpoint Security.

Présentation de la configuration initiale de Kaspersky Endpoint Security

A la fin de l'installation de Kaspersky Endpoint Security sur l'ordinateur, il faut procéder à la configuration initiale de Kaspersky Endpoint Security.

Si vous ne réalisez pas la procédure de configuration initiale de Kaspersky Endpoint Security, la protection antivirus de l'ordinateur ne fonctionne pas.

La procédure de configuration initiale se présente sous la forme d'une succession d'étapes.
Cette procédure se déroule sous la forme d'un script de configuration post-installation. Le script de configuration post-installation de Kaspersky Endpoint Security doit être lancé sous les autorisations root après la fin de l'installation du paquet de Kaspersky Endpoint Security.

Assistant de configuration initiale de Kaspersky Endpoint Security

► *Pour lancer manuellement le script de configuration initiale de Kaspersky Endpoint Security, exécutez la commande suivante :*

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Dans cette section

Etape 1. Sélection de la locale

Cette étape correspond à la définition de la locale utilisée par Kaspersky Endpoint Security.

Vous pouvez désigner la locale au format défini dans RFC 3066.

► *Pour obtenir la liste complète des valeurs de locales, exécutez la commande suivante :*

```
# locale -a
```

L'application propose d'utiliser par défaut la locale définie pour root.

Etape 2. Consultation du Contrat de licence utilisateur final

Cette étape correspond à l'acceptation ou au rejet des conditions du Contrat de licence utilisateur final.

Vous pouvez consulter le texte à l'aide de l'utilitaire `less`. Pour naviguer dans texte, utilisez les touches de direction du curseur ou la touche **B** (pour revenir à l'écran antérieur) et **F** (pour passer à

l'écran suivant). Pour obtenir l'aide, appuyez sur la touche **H**. Pour quitter la consultation, appuyez sur la touche **Q**.

Après avoir quitté le mode de consultation, saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions du Contrat de licence utilisateur final ;
- `no` (ou `n`), si vous refusez les conditions du Contrat de licence utilisateur final.

Si vous refusez les conditions du Contrat de licence utilisateur final, l'application interrompt le processus de configuration de Kaspersky Endpoint Security.

Etape 3. Participation au Kaspersky Security Network

Cette étape correspond à l'acceptation ou au rejet des conditions de la Déclaration de Kaspersky Security Network. Le fichier contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire `/opt/kaspersky/kesl/doc/ksn_license.<ID de la langue>`.

Définissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions de la Déclaration de Kaspersky Security Network ;
- `no` (ou `n`), si vous refusez les conditions de la Déclaration de Kaspersky Security Network.

Le refus de participer au Kaspersky Security Network n'interrompt pas l'installation de Kaspersky Endpoint Security. Vous pouvez décider de participer ou non au Kaspersky Security Network à n'importe quel moment (cf. section "Activation et désactivation de l'utilisation de Kaspersky Security Network" à la page 91).

Etape 4. Définition du type d'intercepteur des opérations sur les fichiers

Cette étape correspond à la définition du type d'intercepteur des opérations de fichier pour le système d'exploitation utilisé. Pour les systèmes d'exploitation qui ne prennent pas en charge la

technologie fanotify, la compilation du module du noyau est lancée. Le module du noyau est requis pour le fonctionnement de la tâche de protection en temps réel.

> Pour pouvoir compiler le module de noyau, le fichier System.map-<version du noyau> doit se trouver dans le répertoire /boot.

Si le script détecte les codes sources du noyau du système d'exploitation dans le répertoire par défaut, l'application utilise le chemin d'accès à ce répertoire. Dans le cas contraire, il convient d'indiquer le chemin d'accès au code source du noyau.

Si les paquets requis ne sont pas détectés lors de la compilation du noyau, Kaspersky Endpoint Security tente de les télécharger lui-même. En cas d'échec du téléchargement des paquets, un message d'erreur s'affiche.

Il est possible de compiler le module du noyau plus tard, après la configuration initiale de Kaspersky Endpoint Security.

Etape 5. Configuration des paramètres du serveur proxy

Cette étape correspond à la définition des paramètres du serveur proxy, si vous accédez à Internet via un serveur proxy. Le téléchargement des bases antivirus de Kaspersky Endpoint Security depuis les serveurs de mise à jour requiert une connexion Internet (cf. section "Etape 6. Chargement des bases antivirus de Kaspersky Endpoint Security" à la page 30).

► *Pour configurer le serveur proxy, exécutez une des actions suivantes :*

- Si la connexion à Internet s'opère via un serveur proxy, indiquez l'adresse de ce dernier dans un des formats suivants :
  - `adresse_IP_du_serveur_proxy:port` si l'authentification n'est pas requise lors de la connexion au serveur proxy ;
  - `nom_de_l'utilisateur:mot_de_passe@adresse_IP_du_serveur_proxy:port` si l'authentification est requise pour la connexion au serveur proxy.
- Si la connexion à Internet s'opère sans serveur proxy, introduisez la réponse `no`.

L'application propose par défaut la réponse `no`.

Vous pouvez configurer le serveur proxy sans utiliser le script de configuration initiale (cf. section "Utilisation du serveur proxy lors de l'accès aux sources de mises à jour" à la page 61).

Etape 6. Chargement des bases antivirus de Kaspersky Endpoint Security

Cette étape correspond au téléchargement des bases antivirus de Kaspersky Endpoint Security sur l'ordinateur. Les bases antivirus contiennent les descriptions des signatures des menaces et les méthodes de lutte contre celles-ci. Kaspersky Endpoint Security utilise ces enregistrements pour détecter et neutraliser les menaces. Les experts antivirus de Kaspersky Lab ajoutent régulièrement des enregistrements sur les nouvelles menaces.

Pour télécharger les bases antivirus de Kaspersky Endpoint Security sur l'ordinateur, vous devez saisir la réponse `yes`.

Saisissez `no` si vous souhaitez refuser le téléchargement immédiat des bases antivirus.

La réponse proposée par défaut est `yes`.

L'application garantit la protection antivirus de l'ordinateur uniquement après le téléchargement des bases antivirus de Kaspersky Endpoint Security.

Vous pouvez lancer la tâche de la mise à jour des bases antivirus de Kaspersky Endpoint Security sans utiliser le script de configuration initiale (cf. section "Mise à jour des bases de données et des modules de l'application" à la page 56).

Etape 7. Activation de la mise à jour automatique des bases antivirus

Cette étape correspond à l'activation de la mise à jour automatique des bases antivirus.

Saisissez la réponse `yes` pour activer la mise à jour automatique des bases antivirus. Kaspersky Endpoint Security recherche la présence éventuelle de mises à jour pour les bases

antivirus toutes les 60 minutes par défaut. Si des mises à jour des bases antivirus sont disponibles, Kaspersky Endpoint Security les télécharge.

Saisissez la réponse `no` si vous ne souhaitez pas que Kaspersky Endpoint Security mette à jour automatiquement les bases antivirus.

Vous pouvez activer la mise à jour automatique des bases antivirus sans l'aide du script de configuration initiale grâce à l'administration de la planification de la tâche de mise à jour (cf. section "Modification des paramètres de l'horaire d'une tâche" à la page 162).

Etape 8. Activation de l'application

Cette étape correspond à l'activation de l'application à l'aide du code d'activation ou du fichier clé.

Pour activer l'application à l'aide du code d'activation, il faut saisir le code d'activation.

Pour activer l'application à l'aide du fichier clé, il faut indiquer le chemin d'accès complet au fichier clé.

Si le code d'activation ou le fichier clé ne sont pas indiqués, l'application est activée à l'aide de la clé d'évaluation pour un mois.

Vous pouvez installer le fichier clé sans utiliser le script de configuration initiale (cf. section "Commande de gestion des clés" à la page 174).

Mode automatique de configuration initiale de Kaspersky Endpoint Security

Vous pouvez réaliser la configuration initiale de Kaspersky Endpoint Security en mode automatique. L'application applique les valeurs des paramètres indiquées dans le fichier de configuration de la configuration initiale.

Lancement de la configuration initiale de Kaspersky Endpoint Security en mode automatique

► *Pour lancer la configuration initiale de Kaspersky Endpoint Security en mode automatique, exécutez la commande suivante :*

```
/opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<chemin
d'accès complet au fichier de configuration de la configuration
initiale>
```

Paramètres du fichier de configuration de la configuration initiale de Kaspersky Endpoint Security

Le fichier de configuration de la configuration initiale de Kaspersky Endpoint Security contient les paramètres repris dans le tableau ci-dessous.

Tableau 2. Paramètres du fichier de configuration de la configuration initiale de Kaspersky Endpoint Security

Paramètre	Description	Valeurs possibles
EULA_AGREED	Paramètre obligatoire. Acceptation des dispositions du Contrat de licence utilisateur final	`yes` : il est indispensable d'accepter les dispositions du Contrat de licence utilisateur final pour pouvoir poursuivre la procédure d'installation de l'application.
USE_KSN	Acceptation de la Déclaration de Kaspersky Security Network	`yes` : accepter la Déclaration de Kaspersky Security Network `no` : ne pas accepter la Déclaration de Kaspersky Security Network
SERVICE_LOCALE	Locale utilisée par Kaspersky Endpoint Security	La locale est indiquée au format défini dans RFC 3066
INSTALL_LICENSE	Code d'activation ou fichier clé	
UPDATER_SOURCE	Source des mises à jour	• `SCServer` : utiliser le Serveur d'administration Kaspersky Security Center en guise de source des mises à jour ; • `KLServers` : utiliser les serveurs de Kaspersky Lab en guise de source des mises à jour ; • adresse de la source des mises à jour.

Paramètre	Description	Valeurs possibles
PROXY_SERVER	Adresse du serveur proxy à utiliser pour la connexion à Internet	• adresse du serveur proxy ; • `no` : ne pas utiliser de serveur proxy.
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de données pendant la procédure de configuration	• `yes` : lancer la tâche de mise à jour ; • `no` : ne pas lancer la tâche de mise à jour.
KERNEL_SRCS_INSTALL	Lancement automatique de la compilation du module du noyau	• `yes` : compiler le module du noyau ; • `no` : ne pas compiler le module du noyau.

Si vous voulez modifier les paramètres dans le fichier de configuration de la configuration initiale de Kaspersky Endpoint Security, saisissez les valeurs des paramètres au format `nom du paramètre=valeur_du_paramètre` (l'application ne traite pas les espaces entre le nom du paramètre et sa valeur).

Configuration des paramètres de l'Agent d'administration

Si vous envisagez d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, il faut configurer les paramètres de l'Agent d'administration.

► *Pour configurer les paramètres de l'Agent d'administration, procédez comme suit :*

1. Exécutez la commande :

   ```
   # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
   ```

2. Indiquez le nom DNS ou l'adresse IP du Serveur d'administration.

3. Indiquez le numéro de port du Serveur d'administration.

Par défaut, le port 14000 est utilisé.

4. Si vous voulez utiliser une connexion SSL, indiquez le numéro du port SSL du Serveur d'administration.

   Par défaut, le port 13000 est utilisé.

5. Exécutez une des actions suivantes :

   - Saisissez `yes` si vous voulez utiliser une connexion SSL.
   - Saisissez `no` si vous ne voulez pas utiliser de connexion SSL.

   La connexion SSL est activée par défaut.

Pour obtenir de plus amples informations sur la configuration de l'Agent d'administration, consultez le *Manuel de l'administrateur de Kaspersky Security Center*.

Configuration des règles d'autorisation dans le système SELinux

► *Pour créer le module SELinux avec les règles indispensables au fonctionnement de Kaspersky Endpoint Security, procédez comme suit :*

1. Placez SELinux en mode d'autorisation :

   - Si SELinux a été activé, exécutez la commande suivante :

     ```
     # setenforce Permissive
     ```

   - Si SELinux était désactivé, ouvrez le fichier de configuration `/etc/selinux/config`, attribuez la valeur suivante au paramètre `SELINUX=permissive` et redémarrez le système d'exploitation.

2. Lancez les tâches suivantes :

   - tâche de protection en temps réel :

     ```
     /opt/kaspersky/kesl/bin/kesl-control --start-t 1
     ```

- tâche d'analyse de la mémoire des processus :

  ```
  /opt/kaspersky/kesl/bin/kesl-control --start-t 4 -W
  ```

- tâche d'analyse des secteurs d'amorçage :

  ```
  /opt/kaspersky/kesl/bin/kesl-control --start-t 5 -W
  ```

3. Créez le module des règles sur la base des enregistrements de blocage :

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   ```

   > Assurez-vous que la liste créée contient uniquement les règles qui se rapportent à Kaspersky Endpoint Security.

4. Chargez le module de règles obtenu :

   ```
   # semodule -i kesl.pp
   ```

5. Placez SELinux en mode d'imposition :

   ```
   # setenforce Enforcing
   ```

> En cas d'apparition de nouveaux messages audit liés à Kaspersky Endpoint Security, il faut mettre à jour le fichier du module des règles (cf. section "Mise à jour du fichier du module des règles" à la page 38).

Pour obtenir de plus amples informations, consultez la documentation du système d'exploitation utilisé.

Configuration des règles d'autorisation dans le système AppArmor

► *Pour mettre à jour les profils AppArmor nécessaires au fonctionnement de Kaspersky Endpoint Security, procédez comme suit :*

1. Utilisez une des méthodes suivantes pour confirmer que le module AppArmor est chargé :

   - `systemctl status apparmor`

- `/etc/init.d/apparmor status`

2. Créez un profil Kaspersky Endpoint Security :

   a. Dans la première console, exécutez les commandes :

   ```
   cd /etc/apparmor.d
   aa-genprof /opt/kaspersky/kesl/libexec/kesl
   ```

   b. Dans la deuxième console, lancez les tâches suivantes :

   - tâche de protection en temps réel :

     ```
     /opt/kaspersky/kesl/bin/kesl-control --start-t 1
     ```

   - tâche d'analyse de la mémoire des processus :

     ```
     /opt/kaspersky/kesl/bin/kesl-control --start-t 4 -W
     ```

   - tâche d'analyse des secteurs d'amorçage :

     ```
     opt/kaspersky/kesl/bin/kesl-control --start-t 5 -W
     ```

   - tâche de la mise à jour :

     ```
     /opt/kaspersky/kesl/bin/kesl-control --start-t 6 -W
     ```

   c. Dans la première console, cliquez sur **S**. Une fois l'analyse des événements terminée, cliquez sur **F**.

3. Transférez le profil Kaspersky Endpoint Security créé dans le mode d'affichage des messages :

   ```
   aa-complain opt.kaspersky.kesl.libexec.kesl
   ```

4. Après quelques jours de fonctionnement de l'application, actualisez le profil à l'aide de la commande :

   ```
   aa-logprof
   ```

   Octroyez les autorisations `Allow` ou `Glob` à tous les fichiers que Kaspersky Endpoint Security a utilisé pendant cette période.

5. Transférez le profil Kaspersky Endpoint Security dans le mode de blocage :

   ```
   aa-enforce opt.kaspersky.kesl.libexec.kesl
   ```

En cas d'apparition de nouveaux messages audit liés à Kaspersky Endpoint Security, il faut mettre à jour le fichier du module des règles (cf. section "Mise à jour du fichier du module des règles" à la page 38).

Pour obtenir de plus amples informations, consultez la documentation du système d'exploitation utilisé.

Mise à jour du fichier du module des règles

Installez le paquet policycoreutils-python avant d'utiliser l'utilitaire audit2allow.

► *Pour mettre à jour le fichier du module des règles, exécutez les commandes suivantes :*

```
# audit2allow -l -M kesl –i /var/log/audit/audit.log

# semodule -u kesl.pp
```

Suppression de l'application

Cette section explique comment supprimer Kaspersky Endpoint Security localement ou via Kaspersky Security Center.

Suppression locale de Kaspersky Endpoint Security

Pendant la suppression de l'application, toutes les tâches de Kaspersky Endpoint Security sont arrêtées.

► *Pour supprimer une copie de Kaspersky Endpoint Security installée à l'aide d'un paquet au format RPM, exécutez la commande suivante :*

```
# rpm -e kesl
```

- *Pour supprimer une copie de Kaspersky Endpoint Security installée à l'aide d'un paquet au format DEB, exécutez la commande suivante :*

  ```
  # dpkg -r kesl
  ```

- *Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format RPM, exécutez la commande suivante :*

  ```
  # rpm -e klnagent
  ```

- *Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format DEB, exécutez la commande suivante :*

  ```
  # dpkg -r klnagent
  ```

L'application exécute automatiquement la procédure de suppression. À la fin de celle-ci, l'application affiche un message sur les résultats de la suppression.

Suppression de Kaspersky Endpoint Security via Kaspersky Security Center

Vous pouvez supprimer Kaspersky Endpoint Security via Kaspersky Security Center. Pour ce faire, il faut créer, puis lancer une tâche de suppression de Kaspersky Endpoint Security.

Pour en savoir plus sur la création et le lancement de la tâche de suppression de Kaspersky Endpoint Security, consultez le *Manuel de l'administrateur de Kaspersky Security Center.*

Licence de l'application

Cette section présente les notions principales relatives à la mise sous licence de l'application.

Dans cette section

A propos du contrat de licence

Le *Contrat de licence Utilisateur final* est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions d'utilisation de l'application que vous avez achetée.

Lisez attentivement le contrat de licence avant de commencer à utiliser l'application.

Vous pouvez prendre connaissance des conditions du Contrat de licence de l'une des manières suivantes :

- Pendant l'installation de Kaspersky Endpoint Security.
- En lisant le document license.txt. Ce document est fourni dans la distribution de l'application.

Vous acceptez les conditions du contrat de licence, en confirmant votre accord avec le texte du contrat de licence lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application et ne pas l'utiliser.

A propos de la licence

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence.

La licence vous accorde le droit d'obtenir les types de service suivants :

- utilisation de l'application conformément aux conditions du Contrat de licence ;
- Support Technique.

Le volume de services offerts et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Il existe différents types de licence :

- *Evaluation* : une licence gratuite qui permet de découvrir les fonctionnalités de l'application.

  La durée de validité de la licence d'évaluation est courte. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, il faut acheter une licence commerciale.

  Vous pouvez activer l'application à l'aide d'une licence d'évaluation une seule fois uniquement.

- *Commerciale* – licence payante délivrée lors de l'achat de l'application.

  A l'expiration de la durée de validité de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases de données de Kaspersky Endpoint Security n'est pas disponible). Pour pouvoir profiter de toutes les fonctionnalités de Kaspersky Endpoint Security, il faut renouveler la licence commerciale.

Il est conseillé de renouveler la durée de validité de la licence avant la date d'expiration de la licence active afin de garantir la protection antivirus maximale contre les menaces informatiques.

A propos du certificat de licence

Le *Certificat de licence* est un document qui vous est transmis avec le fichier clé ou le code d'activation.

Le Certificat de licence comporte les informations suivantes à propos de la licence :

- numéro de la commande ;
- informations relatives à l'utilisateur qui reçoit la licence ;
- informations relatives à l'application qui peut être activée à l'aide de la licence octroyée ;
- restrictions associées au niveau du nombre (par exemple, le nombre de périphériques sur lesquels la licence permet l'utilisation de l'application) ;
- début de validité de la licence ;
- date d'expiration de la licence ou de l'abonnement ou durée de validité de la licence ;
- type de licence.

A propos du code d'activation

Le *code d'activation* est une suite unique de 20 caractères alphanumériques (alphabet latin). Vous le saisissez pour ajouter le code d'activation de Kaspersky Endpoint Security. Le code d'activation est envoyé à l'adresse email que vous avez indiquée après l'achat de Kaspersky Endpoint Security ou après la commande de la version d'essai de Kaspersky Endpoint Security.

Pour activer l'application avec un code d'activation, il est nécessaire de disposer d'un accès à Internet en vue de se connecter aux serveurs d'activation Kaspersky Lab.

Si le code d'activation a été perdu après l'activation de l'application, vous pouvez le restaurer.
Le code d'activation peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount,

par exemple. Pour la restauration du code d'activation, vous devez vous adresser au Support technique de Kaspersky Lab (cf. "Mode d'obtention de l'assistance technique" p. 117).

A propos de la clé

La *clé* est une séquence de bits qui permet d'activer, puis d'utiliser l'application conformément aux conditions du Contrat de licence. La clé est créée par les experts de Kaspersky Lab.

Vous pouvez ajouter la clé à l'application d'une des manières suivantes : utiliser le *fichier clé* ou saisir le *code d'activation*. La clé apparaît dans l'interface de l'application sous la forme d'une séquence de caractères alpha-numériques unique une fois que vous l'avez ajoutée à l'application.

La clé peut être bloquée par Kaspersky Lab en cas de violation des conditions du Contrat de licence. Si cela se produit, il faudra ajouter une autre clé pour pouvoir utiliser l'application.

La clé peut être active ou complémentaire.

Clé active est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé active peut être ajoutée pour la licence d'évaluation ou la licence commerciale. L'application ne peut comporter plus d'une clé active.

Une *Clé complémentaire* est une clé qui confirme le droit d'utilisation de l'application, non utilisée au moment présent. La clé additionnelle devient automatiquement active lorsque la durée de validité de la licence associée à la clé active expire. La clé complémentaire ne peut être ajoutée qu'en cas de présence d'une clé active.

La clé de la licence d'évaluation peut uniquement être ajoutée en tant que clé active. Elle ne sera pas acceptée en tant que clé additionnelle.

A propos du fichier clé

Le *Fichier clé* est un fichier avec une extension key qui vous est fourni par Kaspersky Lab. Le fichier clé est destiné à l'ajout de la clé activant l'application.

Le fichier clé est envoyé à l'adresse email que vous avez indiquée après l'achat de Kaspersky Endpoint Security ou après la commande de la version d'essai de Kaspersky Endpoint Security.

Pour activer l'application à l'aide du fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation Kaspersky Lab.

Si le fichier clé a été accidentellement supprimé, vous pouvez le restaurer. Le fichier clé peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple.

Afin de restaurer le fichier clé, vous devez effectuer l'une des opérations suivantes :

- Contacter le Support Technique (http://support.kaspersky.fr).
- Obtenir le fichier clé sur le site Web de Kaspersky Lab (https://activation.kaspersky.com/fr/) à partir du code d'activation que vous possédez.

A propos de l'abonnement

L'*abonnement à Kaspersky Endpoint Security* constitue une commande pour l'utilisation de l'application selon des paramètres sélectionnés (date d'expiration de l'abonnement, nombre d'appareils protégés). Il est possible d'enregistrer un abonnement à Kaspersky Endpoint Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur Internet). L'abonnement peut être renouvelé manuellement ou automatiquement. Il peut également être résilié. L'administration de l'abonnement est accessible sur le site Internet du fournisseur de services.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour prolonger le fonctionnement de Kaspersky Endpoint Security après la date d'expiration d'un abonnement limité, il est nécessaire de renouveler ce dernier. L'abonnement illimité se renouvelle automatiquement si le montant dû au fournisseur de services est versé dans les délais.

Si l'abonnement est limité, une période de grâce de renouvellement vous est proposée après sa date d'expiration. Pendant cette période, l'application continue à fonctionner. C'est le fournisseur du service qui détermine l'existence et la durée de cette période de grâce.

Pour utiliser Kaspersky Endpoint Security sur abonnement, il est nécessaire de saisir le code d'activation fourni par le prestataire de services. Quand le code d'activation a été appliqué, la clé active est installée. Celle-ci définit la licence d'utilisation de l'application selon un abonnement. Il est possible d'installer une clé additionnelle uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé ou d'un abonnement.

Les fonctionnalités de l'application disponibles sur abonnement peuvent correspondre aux fonctions de l'application sous une des licences commerciales suivantes : standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Ces types de licence sont conçus pour protéger les serveurs de fichiers, les postes de travail, les appareils mobiles et permettent l'utilisation de modules de contrôle sur les postes de travail et les appareils mobiles.

Le choix des possibilités de gestion de l'abonnement varie selon les prestataires de services. Le prestataire de services peut ne pas proposer de période de grâce où l'application continue à fonctionner après la date d'expiration de l'abonnement.

Les codes d'activation achetés par abonnement ne peuvent pas être utilisés pour l'activation de versions antérieures de Kaspersky Endpoint Security.

A propos des données

En acceptant les conditions du Contrat de licence utilisateur final, vous acceptez de transmettre automatiquement les informations suivantes :

- les informations liées à l'activation de l'application à l'aide d'un code ;
- les statistiques d'utilisation de la tâche de protection en temps réel et des tâches d'analyse à la demande ;
- l'identifiant de l'application ;
- la version de l'application ;
- l'identifiant de l'ordinateur où l'application est installée ;
- le nom et la version du système d'exploitation utilisé (y compris les noms et les versions des mises à jour installées).

En acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez également de transmettre automatiquement les informations suivantes :

- les informations relatives à la date et la durée d'installation de l'application sur l'ordinateur ;

- l'identifiant du partenaire chez qui la licence a été achetée ;
- le type de l'installation de l'application sur l'ordinateur (installation initiale) ;
- les données relatives au système d'exploitation installé sur l'ordinateur (y compris le nom, le type et le nombre de bits) ;
- les informations relatives aux applications lancées sur l'ordinateur ;
- le hash (MD5) du fichier exécutable et la quantité de lancements du fichier depuis la dernière fois que les informations ont été présentées ;
- le chemin d'accès complet au fichier exécutable sur l'ordinateur ;
- l'identifiant de la présence dans le fichier d'une signature numérique valide ;
- l'identifiant indiquant un des chemins standard de l'emplacement du fichier lancé dans le système ;
- le hash (MD5) et la catégorie à laquelle appartient l'objet analysé (selon la version du titulaire du droit) ;
- l'identifiant de la source de la catégorie ;
- les informations relatives à l'éditeur de l'objet et l'identifiant de réception des informations sur l'éditeur ;
- la version de l'objet analysé ;
- les informations sur la version des bases de catégories des fichiers utilisées par l'application et l'identifiant de l'enregistrement de la base utilisée lors de l'analyse ;
- l'identifiant du composant de l'application qui a demandé la catégorie de l'objet.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi et aux politiques de Kaspersky Lab.

Kaspersky Lab utilise les informations obtenues uniquement de manière impersonnelle et sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas de données personnelles ou d'autres données confidentielles. Les informations obtenues sont supprimées au fur et à mesure de

leur accumulation (une fois par an). Les statistiques générales sont conservées pour une durée indéterminée.

Pour en savoir plus sur l'obtention, le traitement, la conservation et la suppression des informations relatives à l'utilisation de l'application après l'acceptation du Contrat de licence utilisateur final, veuillez lire le contenu de ce dernier ou vous rendre sur le site Internet de Kaspersky Lab (http://www.kaspersky.ru/privacy). Le fichier license.txt qui contient le texte du Contrat de licence utilisateur final est intégré au kit de distribution de l'application.

Lancement et arrêt de l'application

Par défaut, Kaspersky Endpoint Security est lancé automatiquement au démarrage du système d'exploitation (pour les niveaux d'exécution par défaut applicables à chacun des systèmes d'exploitation). Kaspersky Endpoint Security lance toutes les tâches de service, ainsi que les tâches personnalisées pour lesquelles le mode de lancement PS est défini dans les paramètres de la planification.

Si vous arrêtez Kaspersky Endpoint Security, toutes les tâches en cours d'exécution sont interrompues. Sachez que les tâches personnalisées ne sont pas rétablies automatiquement après que Kaspersky Endpoint Security a été relancé. Seules les tâches personnalisées, dans les paramètres du calendrier desquelles le mode de lancement PS est spécifié seront lancées de nouveau.

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

  ```
  /etc/init.d/kesl-supervisor start
  ```

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

  ```
  /etc/init.d/kesl-supervisor stop
  ```

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

  ```
  /etc/init.d/kesl-supervisor restart
  ```

- *Pour afficher l'état de Kaspersky Endpoint Security, exécutez la commande suivante :*

  ```
  /etc/init.d/kesl-supervisor status
  ```

- *Pour lancer Kaspersky Endpoint Security dans le système systemd, exécutez la commande suivante :*

  ```
  systemctl start kesl-supervisor
  ```

- *Pour arrêter Kaspersky Endpoint Security dans le système systemd,* exécutez la commande suivante :

```
systemctl stop kesl-supervisor
```

- *Pour relancer Kaspersky Endpoint Security dans le système systemd, exécutez la commande suivante :*

```
systemctl restart kesl-supervisor
```

- *Pour afficher l'état de Kaspersky Endpoint Security dans le système systemd, exécutez la commande suivante :*

```
systemctl status kesl-supervisor
```

Administration des tâches de Kaspersky Endpoint Security

Cette section contient des informations sur les types de tâches de Kaspersky Endpoint Security et des instructions relatives à la gestion de ces tâches.

Dans cette section

A propos des tâches de Kaspersky Endpoint Security

Vous pouvez administrer le fonctionnement de l'application Kaspersky Endpoint Security à l'aide de tâches aussi bien localement sur les ordinateurs (via la ligne de commande ou les fichiers de configuration) que de manière centralisée via Kaspersky Security Center (cf. section "Administration de l'application via Kaspersky Security Center" à la page 94).

Au niveau de l'utilisation de Kaspersky Endpoint Security, il existe deux types de tâches :

- *Tâche prédéfinie*, à savoir une tâche créée lors de l'installation de l'application. Vous ne pouvez pas créer ou supprimer des tâches prédéfinies, mais vous pouvez en modifier les paramètres.

- *Tâche personnalisée*, à savoir une tâche que vous pouvez créer ou supprimer vous-même.

Vous pouvez administrer les tâches suivantes :

- **File_Monitoring** : tâche de protection en temps réel (ID=1, type – OAS) ;

- **Scan_My_Computer** : tâche d'analyse à la demande (ID=2, type – ODS) ;

- **Scan_File** : tâche d'analyse personnalisée (ID=3, type – ODS). Les paramètres de cette tâche correspondent par défaut aux paramètres de la tâche Scan_My_Computer ;

- **Boot_Scan** : tâche d'analyse des secteurs d'amorçage (ID=4, type – BootScan) ;

- **Memory_Scan** : tâche d'analyse de la mémoire système (ID=5, type – MemoryScan) ;

- **Update** : tâche de mise à jour (ID=6, type – Update) ;

- **Rollback** : tâche de retour à l'état antérieur à la mise à jour (ID=7, type – Rollback) ; Cette tâche n'a pas de paramètres. Vous pouvez seulement administrer cette tâche ;

- **Retranslate** : tâche de copie des mises à jour (ID=8, type – Retranslate) ;

- **License** : tâche de réalisation du serveur de licences (ID=9, type – License) ;
- **Backup** : tâche d'administration de la Sauvegarde (ID=10, le type – Backup).

Vous pouvez réaliser les opérations suivantes sur les tâches :

- lancer et arrêter des tâches ;
- créer et supprimer des tâches (uniquement pour les tâches personnalisées) ;
- modifier les paramètres des tâches.

ID est le numéro d'identification de la tâche attribué par Kaspersky Endpoint Security lors de la création de la tâche.

Consultation de la liste des tâches de Kaspersky Endpoint Security

► *Pour consulter la liste des tâches de Kaspersky Endpoint Security, exécutez la commande suivante :*

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

Création d'une tâche

Vous pouvez créer des tâches.

► *Pour créer une tâche, exécutez la commande suivante :*

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche>
--type <type de la tâche>
```

Lancement et arrêt de la tâche

Vous pouvez lancer et arrêter uniquement les tâches des types OAS, ODS, BootScan, MemoryScan, Rollback, Retranslate et Update.

Vous ne pouvez pas lancer et arrêter les tâches de type Backup et License.

► *Pour lancer une tâche, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --start-task
<ID_de_la_tâche>|<nom_de_la_tâche>
```

► *Pour arrêter une tâche, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --stop-task <ID de la tâche>|<nom
de la tâche>
```

Suppression d'une tâche

Vous pouvez supprimer les tâches que vous avez créées (tâches personnalisées).

► *Pour supprimer une tâche, exécutez la commande suivante :*

```
/opt/kaspersky/kesl/bin/kesl-control --delete-task <ID de la
tâche>|<nom de la tâche>
```

Suspension et reprise d'une tâche

Vous pouvez suspendre et reprendre l'exécution des tâches de type ODS, BootScan, MemoryScan, Rollback, Retranslate et Update.

► *Pour suspendre une tâche, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --suspend-task <ID de la tâche>|<nom de la tâche>
```

Une fois la commande exécutée, la tâche est suspendue.

► *Pour reprendre, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --resume-task <ID de la tâche>|<nom de la tâche>
```

Une fois la commande exécutée, la tâche reprend.

Paramètres de planification d'une tâche

► *Pour planifier une tâche, procédez comme suit :*

1. Enregistrez les paramètres de planification d'une tâche dans le fichier de configuration à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kesl/bin/kesl-control

   --get-schedule <ID de la tâche>|<nom de la tâche> --file <chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier de configuration afin de le modifier.

3. Précisez les paramètres de planification.

4. Enregistrez les modifications dans le fichier de configuration.

5. Importez les paramètres de planification dans la tâche à jour à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kesl/bin/kesl-control --set-schedule <ID de la
   ```

```
tâche>|<nom de la tâche> --file <chemin d'accès complet au fichier>.
```

Cf. également

Consultation de l'état de la tâche..... 55

Consultation de l'état de la tâche

Vous pouvez consulter l'état de la tâche.

Les tâches de Kaspersky Endpoint Security peuvent posséder 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 ;

► *Pour consulter l'état de la tâche, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --get-task-state <ID de la tâche>|<nom de la tâche>.
```

Mise à jour des bases de données et des modules de l'application

Cette section contient des informations sur la mise à jour des bases de données et des modules de l'application et des instructions indiquant comment configurer les paramètres de la mise à jour.

Dans cette section

A propos de la mise à jour des bases de données et des modules de l'application

Au cours de la durée de validité de la licence, vous pouvez obtenir les mises à jour des bases de données et des modules de Kaspersky Endpoint Security. Les bases correspondent à des fichiers avec des enregistrements. Ces enregistrements contiennent des informations sur les portions de contrôle du code des menaces et des algorithmes de désinfection des objets qui contiennent ces menaces.

Les experts anti-virus de Kaspersky Lab détectent chaque jour de nombreuses nouvelles menaces. Ils créent pour ces menaces des enregistrements les identifiant et les insèrent dans les mises à jour des bases de données. *Mise à jour des bases de données* : correspond à un ou à plusieurs fichiers avec ces enregistrements. Pour réduire le risque d'infection de l'ordinateur au minimum, téléchargez les mises à jour régulièrement.

Mise à jour des bases de données de l'application

Pendant l'installation, Kaspersky Endpoint Security reçoit les bases actuelles depuis un des serveurs HTTP de mise à jour de Kaspersky Lab. Si la tâche prédéfinie avec les paramètres par défaut (ID=6) est utilisée pour la mise à jour, Kaspersky Endpoint Security met à jour les bases une fois toutes les 60 minutes. Vous pouvez modifier les paramètres de la tâche de mise à jour prédéfinie des bases et des modules de l'application et créer des tâches personnalisées de mise à jour.

Kaspersky Endpoint Security continue à utiliser la version précédente installée des bases si le chargement des mises à jour des bases de données s'interrompt ou se solde par une erreur.

Par défaut l'application inscrit au journal l'événement de *Les bases sont dépassées* (AVBasesAreOutOfDate), si les dernières mises à jour des bases de données installées ont été publiées sur le serveur de Kaspersky Lab il y a plus d'une semaine. Si les bases ne sont pas mises à jour pendant deux semaines, Kaspersky Endpoint Security enregistre l'événement *Les bases sont fortement dépassées* (AVBasesAreTotallyOutOfDate) dans le journal.

A propos des sources de mises à jour

Une *source des mises à jour* est une ressource qui contient les mises à jour des bases de données et des modules de l'application Kaspersky Endpoint Security. Les sources de mises à jour peuvent être des serveurs FTP ou HTTP (par exemple, Kaspersky Security Center, les serveurs de mise à jour de Kaspersky Lab) ou des répertoires locaux ou réseau montés au préalable par l'utilisateur.

Dans la tâche de la mise à jour prédéfinie par défaut en tant que source de mises à jour, les serveurs de mise à jour de Kaspersky Lab sont sélectionnés. Des mises à jour des bases de données et des modules sont installées sur les serveurs de mise à jour pour de nombreuses applications de Kaspersky Lab. Les mises à jour sont chargées selon les protocoles HTTP.

Si, pour une raison quelconque, vous ne pouvez pas utiliser les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour, vous pouvez récupérer les mises à jour à partir de la *source de mises à jour définie par l'utilisateur*, à savoir un répertoire local ou réseau (SMB/NFS) que vous avez désigné et qui a été monté au préalable par l'utilisateur ou un serveur FTP ou HTTP. Vous pouvez indiquer la sources des mises à jour utilisateur dans le fichier de configuration de la tâche de la mise à jour.

Configuration des paramètres de la mise à jour

Vous pouvez configurer les paramètres de la mise à jour suivants :

- source des mises à jour (cf. section "Sélection de la source des mises à jour" p. 59) ;
- activer/désactiver l'utilisation du serveur proxy, si vous utilisez un serveur proxy pour vous connecter à Internet (cf. section "Utilisation du serveur proxy lors de l'accès aux sources de mises à jour" à la page 61).

Les paramètres de la mise à jour se trouvent dans le fichier de configuration qu'utilise la tâche de la mise à jour. La structure du fichier de configuration et la description détaillée des paramètres à utiliser et de leurs valeurs éventuelles sont reprises dans la section Paramètres des tâches de mise à jour (cf. section "Paramètres des tâches de mise à jour et des tâches de copie des mises à jour" à la page 143).

Création de la tâche de la mise à jour

Pour la réception des mises à jour, vous pouvez créer une tâche de mise à jour avec les paramètres par défaut ou avec un ensemble de paramètres spécifié par vous.

► *Pour créer la tâche de la mise à jour avec les paramètres par défaut, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche>
--type Update
```

La tâche créée fonctionne automatiquement avec les paramètres par défaut (cf. section "Paramètres des tâches de mise à jour et des tâches de copie des mises à jour" à la page 143).

► *Pour créer une tâche de la mise à jour avec un ensemble spécifié des paramètres, procédez comme suit :*

1. Créez un fichier de configuration (cf. p. 120) avec les paramètres que vous voulez définir dans la tâche de la mise à jour.

2. Exécutez la commande :

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche> --type Update --file <nom du fichier de configuration>
```

La tâche créée fonctionne automatiquement avec les paramètres spécifiés dans le fichier de configuration.

Sélection de la source des mises à jour

► *Pour sélectionner la source de la mise à jour, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de la mise à jour dans le fichier de configuration à l'aide de la commande suivante :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 6 --file <chemin d'accès complet au fichier>
```

2. Ouvrez le fichier de configuration créé pour l'édition. Renseignez la valeur du paramètre `SourceType` :

   - `KLServers` – pour charger les mises à jour à partir des serveurs de mise à jour de Kaspersky Lab ;

   - `SCServer` – pour charger les mises à jour à partir du Serveur d'administration Kaspersky Security Center;

   - `Custom` – pour charger les mises à jour à partir de la source utilisateur (indiquée par vous-même).

Exemple :

```
SourceType="KLServers"
```

Pour les sources de mise à jour définies par l'utilisateur, configurez les paramètres avancés dans la section `[CustomSources.item_#]` (cf. page 146) :

- `URL` : adresse du serveur HTTP ou du répertoire source des mises à jour.

- `Enabled` : état de la source des mises à jour (`Yes` : la source des mises à jour est utilisée, `No` : la source des mises à jour n'est pas utilisée). Si vous avez choisi la valeur du paramètre `Enabled=No`, l'application n'utilise pas la source des mises à jour définie par le paramètre `URL`.

3. Configurez les paramètres avancés de la mise à jour (facultatif).

4. Enregistrez les modifications dans le fichier de configuration.

5. Importez les paramètres du fichier de configuration dans la tâche de la mise à jour à l'aide de la commande suivante :

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6 --file
<chemin d'accès complet au fichier>
```

Kaspersky Endpoint Security applique immédiatement les nouvelles valeurs des paramètres de la tâche de mise à jour.

Utilisation du serveur proxy lors de l'accès aux sources de mises à jour

► *Pour activer l'utilisation du serveur proxy lors de l'accès aux sources de mises à jour, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de la mise à jour dans le fichier de configuration à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kesl/bin/kesl-control --get-settings 6 --file
   <chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier de configuration créé pour l'édition. Indiquez la source des mises à jour :

   - Pour utiliser le serveur proxy dans le cadre de l'accès aux serveurs de mise à jour de Kaspersky Lab, indiquez `IgnoreProxySettingsForKLServers=No`.

   - Pour utiliser le serveur proxy dans le cadre de l'accès aux sources de mises à jour définies par l'utilisateur, indiquez `IgnoreProxySettingsForCustomSources=No`.

3. Enregistrez les modifications dans le fichier de configuration.

4. Importez les paramètres du fichier de configuration dans la tâche de la mise à jour à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kesl/bin/kesl-control --set-settings 6 --file
   <chemin d'accès complet au fichier>
   ```

Recul de mise à jour des bases

► *Pour revenir à l'état antérieur à la dernière mise à jour des bases antivirus, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --start-task Rollback
```

En conséquence, l'application lancera la tâche prédéfinie d'annulation de la mise à jour des bases de données. Il est possible d'exécuter la tâche d'annulation de la mise à jour des bases de données si au moins deux mises à jour réussies des bases antivirus avaient pu être réalisées.

Copie des mises à jour

Pour copier les mises à jour, vous pouvez créer une tâche de copie des mises à jour avec les paramètres par défaut ou avec un ensemble de paramètres que vous définissez.

► *Pour créer la tâche de copie des mises à jour avec les paramètres par défaut, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche>
-type Retranslate
```

La tâche créée fonctionne automatiquement avec les paramètres par défaut (cf. section "Paramètres des tâches de mise à jour et des tâches de copie des mises à jour" à la page 143).

► *Pour créer une tâche de copie des mises à jour avec un ensemble défini de paramètres, procédez comme suit :*

1. Créez un fichier de configuration (cf. page 120) reprenant les paramètres que vous souhaitez attribuer à la tâche de copie des mises à jour.

2. Exécutez la commande :

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la
tâche> --type Retranslate --file <nom du fichier de configuration>
```

La tâche créée fonctionne automatiquement avec les paramètres spécifiés dans le fichier de configuration.

Protection en temps réel et analyse à la demande

Cette section explique comment Kaspersky Endpoint Security protège et analyse les serveurs. La protection en temps réel et l'analyse à la demande sont exécutées à l'aide des tâches prédéfinies et des tâches personnalisées. La section contient des instructions indiquant comment créer et configurer des tâches de protection en temps réel et d'analyse à la demande :

- former les zones de protection et des zones d'analyse, ainsi que des exclusions de ces zones ;
- choisir les actions de l'application avec les objets infectés ;
- configurer la durée de l'analyse et les autres paramètres.

Dans cette section

A propos de la protection en temps réel

La protection en temps réel permet d'éviter l'infection du système de fichiers de l'ordinateur. La tâche de protection en temps réel est créée selon les paramètres par défaut lors de l'installation de Kaspersky Endpoint Security sur l'ordinateur. La tâche de protection en temps réel est lancée

automatiquement par défaut 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 et la lancer.

Vous ne pouvez pas créer de tâches de protection en temps réel définies par l'utilisateur. Vous pouvez modifier les paramètres de la tâche prédéfinie de la protection en temps réel.

Les paramètres de protection en temps réel se trouvent dans le fichier de configuration utilisé par la tâche de protection en temps réel. La structure du fichier de configuration, la description détaillée des paramètres utilisés et de leurs valeurs possibles se trouvent dans la section "Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande" (cf. page 126).

Par défaut, la tâche de protection en temps réel utilise les paramètres suivants :

- `ScanArchived=No` – ne pas analyser les archives.
- `ScanSfxArchived=No` – ne pas analyser les archives autoextractibles (self-extracting archives).
- `ScanMailBases=No` – ne pas analyser les bases de messagerie.
- `ScanPlainMail=No` – ne pas analyser les messages électroniques au format texte (plain text).
- `UseTimeLimit=Yes` – activer l'application du paramètre `TimeLimit`.
- `TimeLimit=60` – définir la durée maximale de l'analyse de l'objet de 60 secondes.
- `UseSizeLimit=No` – désactiver l'application du paramètre `SizeLimit`.
- `SizeLimit=0` – analyser les objets de n'importe quelle taille.
- `FirstAction=Recommended` – définir `Recommended` (recommandé) comme première action sur l'objet infecté.
- `SecondAction=Block` – définir `Block` (bloquer) comme deuxième action sur l'objet infecté.
- `UseExcludeMasks=No` – ne pas exclure les objets de la zone de protection selon les masques.

- `UseExcludeThreats=No` – ne pas exclure les objets de la zone de protection selon le nom de la menace.
- `ReportCleanObjects=No` – ne pas consigner dans le journal les informations relatives aux objets non infectés.
- `ReportPackedObjects=No` – ne pas consigner dans le journal les informations relatives à l'analyse des objets dans les fichiers composés.
- `ReportUnprocessedObjects=No` – ne pas consigner dans le journal les informations relatives aux objets non analysés.
- `UseAnalyzer=Yes` – activer l'utilisation de l'analyseur heuristique.
- `HeuristicLevel=Recommended` – définir le niveau de l'analyse heuristique recommandé.
- `UseIChecker=Yes` – utiliser la technologie iChecker ™.
- `ScanByAccessType=SmartCheck` – appliquer le mode intellectuel `(SmartCheck)` d'analyse des objets en fonction du type d'accès à ces objets.
- `[ScanScope.item_0000]` – section contenant les paramètres de formation de la zone de protection.
- `AreaDesc=All objects` – description de la zone de protection (tous les objets).
- `UseScanArea=Yes` – analyser la zone indiquée.
- `Path=/` – analyser tous les répertoires locaux de l'ordinateur ; analyser les répertoires montés via les protocoles SMB et NFS.
- `AreaMask.item_0000 =*` – analyser tous les objets de la zone de protection.

A propos de l'analyse à la demande

L'analyse à la demande est une analyse complète ou personnalisée ponctuelle des fichiers de l'ordinateur réalisée par Kaspersky Endpoint Security. Kaspersky Endpoint Security peut exécuter simultanément plusieurs tâches d'analyse à la demande.

Dans Kaspersky Endpoint Security, une seule tâche d'analyse à la demande prédéfinie est créée par défaut : l'analyse complète. L'application analyse tous les objets sur les disques locaux du serveur, ainsi que tous les objets montés et partagés, accessibles via les protocoles Samba et NFS, selon les paramètres de sécurité recommandés.

Vous pouvez créer de nouvelles tâches personnalisées d'analyse à la demande de manière autonome.

Un tâche d'analyse personnalisée prédéfinie est également créée par défaut dans Kaspersky Endpoint Security.

Les paramètres d'analyse à la demande se trouvent dans le fichier de configuration utilisé par la tâche d'analyse à la demande. La structure du fichier de configuration, la description détaillée des paramètres utilisés et de leurs valeurs possibles se trouvent dans la section "Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande" (cf. page 126).

Par défaut, la tâche d'analyse à la demande fonctionne avec les paramètres suivants :

- `ScanArchived=Yes` – analyser les archives ;
- `ScanSfxArchived=Yes` – analyser les archives autoextractibles (self-extracting archives).
- `ScanMailBases=No` – ne pas analyser les bases de messagerie.
- `ScanPlainMail=No` – ne pas analyser les messages électroniques au format texte (plain text).
- `UseTimeLimit=No` – désactiver l'application du paramètre `TimeLimit`.
- `TimeLimit=0` – ne pas définir la durée maximale de l'analyse de l'objet.
- `UseSizeLimit=No` – désactiver l'application du paramètre `SizeLimit`.
- `SizeLimit=0` – ne pas définir la taille maximale de l'objet analysé.

- `FirstAction=Recommended` – définir `Recommended` (recommandé) comme première action sur l'objet infecté.
- `SecondAction=Skip` – définir `Skip` (ignorer) comme deuxième action sur l'objet infecté.
- `UseExcludeMasks=No` – ne pas exclure les objets de la zone d'analyse selon les masques.
- `UseExcludeThreats=No` – ne pas exclure les objets de la zone d'analyse selon le nom de la menace.
- `ReportCleanObjects=No` – ne pas consigner dans le journal les informations relatives aux objets non infectés.
- `ReportPackedObjects=No` – ne pas consigner dans le journal les informations relatives à l'analyse des objets dans les fichiers composés.
- `ReportUnprocessedObjects=No` – ne pas consigner dans le journal les informations relatives aux objets non analysés.
- `UseAnalyzer=Yes` – activer l'utilisation de l'analyseur heuristique.
- `HeuristicLevel=Recommended` – définir le niveau de l'analyse heuristique recommandé.
- `UseIChecker=Yes` – utiliser la technologie iChecker.
- `[ScanScope.item_0000]` – section contenant les paramètres de formation de la zone d'analyse.
- `AreaDesc=All objects` – description de la zone d'analyse (tous les objets).
- `UseScanArea=Yes` – analyser la zone indiquée.
- `Path=/` – analyser tous les répertoires locaux de l'ordinateur ; analyser les répertoires montés via les protocoles SMB et NFS.
- `AreaMask.item_0000 =*` – analyser tous les objets de la zone d'analyse.

A propos des fichiers infectés

Kaspersky Endpoint Security utilise des bases antivirus pour analyser les fichiers. Les bases contiennent des fichiers avec des fragments de code des menaces et des algorithmes de désinfection des objets qui contiennent ces menaces. Les bases antivirus permettent de détecter dans les fichiers analysés les menaces connues.

Si un fichier contient du code qui coïncide entièrement avec le code d'une menace connue, Kaspersky Endpoint Security attribue l'état *Infecté* au fichier.

Création d'une tâche personnalisée d'analyse à la demande

► *Pour créer une tâche d'analyse à la demande avec les paramètres par défaut, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche> --type ODS
```

A la suite de l'exécution de la commande, une nouvelle tâche d'analyse à la demande est créée avec les paramètres de la tâche d'analyse complète prédéfinie.

► *Pour créer une tâche avec votre propre fichier de configuration, procédez comme suit :*

1. Créez un fichier de configuration avec les paramètres (cf. p. 120), que vous voulez définir dans la tâche d'analyse à la demande.

2. Exécutez la commande suivante :

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <nom de la tâche> --type ODS --file <nom du fichier de configuration>
```

En conséquence, une nouvelle tâche d'analyse à la demande est créée avec les paramètres spécifiés dans le fichier de configuration.

Formation d'une zone de protection et d'une zone d'analyse

L'ensemble des objets ouverts, modifiés et enregistrés, analysés par la tâche de protection en temps réel au temps de travail, s'appelle *zone de protection*. La zone de protection est indiquée dans le fichier de configuration de la tâche de protection en temps réel.

Par défaut, la tâche de protection en temps réel analyse tous les objets ouverts, modifiés et enregistrés qui se trouvent sur les disques locaux de l'ordinateur, ainsi que tous les objets montés et partagés accessibles via les protocoles SMB et NFS.

L'ensemble des objets du système de fichiers de l'ordinateur couvert par la tâche d'analyse à la demande s'appelle la *zone d'analyse*. La zone d'analyse est indiquée dans le fichier de configuration de la tâche d'analyse. La zone d'analyse de la tâche d'analyse à la demande prédéfinie correspond à tous les objets qui se trouvent sur les disques locaux de l'ordinateur, ainsi que tous les objets montés et partagés accessibles via les protocoles SMB et NFS.

Vous pouvez modifier les zones de protection et les zones d'analyse dans les tâches prédéfinies et dans les tâches personnalisées.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre dans lequel ces zones sont numérotées dans le fichier de configuration de la tâche.

► *Pour ajouter des objets à analyser à la zone de protection ou à la zone d'analyse, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.

3. Ajoutez la section `[ScanScope.item_#]` au fichier créé. Définissez les valeurs des paramètres suivants dans la section :

   - `AreaMask`, spécifiant le masque des noms des objets à analyser ;

- `AreaDesc`, spécifiant le nom de la zone de protection ou la zone d'analyse.
- `Path`, pour définir le chemin d'accès aux objets à analyser.
- `UseScanArea`, pour activer l'analyse de la zone de protection ou de la zone d'analyse dans la tâche.

Exemple :

`AreaMask.item_0000 =*exe` – analyser tous les objets avec l'extension exe.
`AreaMask.item_0001 =*doc` – analyser tous les objets avec l'extension doc.

4. Enregistrez les modifications dans le fichier de configuration.
5. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

   En conséquence, pendant l'exécution de la tâche de protection en temps réel ou d'analyse à la demande, Kaspersky Endpoint Security analyse les objets qui figurent par défaut dans la zone de protection en temps réel ou d'analyse à la demande.

A propos de l'analyse heuristique

Chaque jour, des objets malveillants apparaissent, dont les enregistrements ne se sont pas encore trouvés dans les bases antivirus. Pour détecter ces objets malveillants dans les fichiers, Kaspersky Endpoint Security *utilise l'analyseur heuristique*.

Analyse heuristique : permet à l'application de reconnaître les nouvelles menaces avant qu'elles soient connues des experts anti-virus. Vous pouvez spécifier le niveau de l'analyse heuristique.
Le niveau de l'analyse heuristique assure un équilibre entre la minutie de la recherche des menaces, le degré de chargement des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique défini est élevé , plus l'analyse demande de ressources et plus cette tâche prend de temps.

Vous pouvez choisir le niveau de l'analyse heuristique en fonction de vos exigences en matière de sécurité et de la vitesse de l'échange de fichiers sur l'ordinateur :

- `Light` (Superficiel) – analyse moins minutieuse, charge minimale du système ;
- `Medium` (Moyen) – niveau moyen de l'analyse heuristique ; charge équilibrée du système ;
- `Deep` (Minutieux) – analyse plus minutieuse, charge maximale du système ;
- `Recommended` (Recommandé) – valeur recommandée par les spécialistes de Kaspersky Lab.

Par défaut, l'analyseur heuristique est activé pour les tâches de protection en temps réel et d'analyse à la demande avec la valeur `Recommended`.

Activation et configuration de l'analyseur heuristique

Dans les tâches prédéfinies de protection en temps réel et d'analyse à la demande, l'analyseur heuristique est activé par défaut. Le niveau de l'analyse heuristique par défaut est le niveau recommandé. Si vous utilisez les tâches de protection en temps réel et d'analyse à la demande avec vos propres ensembles de paramètres, vous devez parfois activer ou désactiver l'analyseur heuristique et configurer le niveau de l'analyse heuristique.

► *Pour activer l'analyseur heuristique et configurer le niveau de l'analyse heuristique, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Attribuez la valeur `Yes` au paramètre `UseAnalyzer` afin d'activer l'analyse heuristique.

   Pour désactiver l'analyse heuristique, le paramètre `UseAnalyzer` doit avoir la valeur `No`.

4. Attribuez une des valeurs suivantes au paramètre `HeuristicLevel` :

   - `Recommended` – pour utiliser le niveau recommandé de l'analyse heuristique ;
   - `Deep` – pour utiliser un niveau élevé d'analyse heuristique ;
   - `Medium` – pour utiliser le niveau moyen de l'analyse heuristique ;
   - `Light` – pour utiliser le niveau bas de l'analyse heuristique.

5. Enregistrez les modifications dans le fichier de configuration.
6. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

Exclusion des objets des zones de protection et d'analyse à la demande

Par défaut, les tâches de protection en temps réel et d'analyse à la demande analysent tous les objets de la zone de protection et de la zone d'analyse. Vous pouvez exclure certains objets de la zone de protection et de la zone d'analyse.

Exclusion des objets de la zone de protection ou de la zone d'analyse

Vous pouvez créer *une zone d'exclusion globale*. Les objets de cette zone sont exclus de la zone de protection ou de toutes les zones d'analyse spécifiées dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande.

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

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

   ```
   /opt/kaspersky/kesl/bin/kesl-control --get-settings <ID de la
   ```

```
tâche> --file <chemin d'accès complet au fichier>
```

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Ajoutez au fichier de configuration créé la section `[ExcludedFromScanScope.item_#]` (cf. à la page 138).
4. Dans la section `[ExcludedFromScanScope.item _ #]`, indiquez les valeurs des paramètres suivants :
   - `AreaDesc` détermine le nom unique de la zone d'exclusion.
   - `UseScanArea` indique, si Kaspersky Endpoint Security va exclure la zone de l'analyse pendant l'exécution de la tâche.
   - `Path` définit le chemin d'accès aux objets exclus de l'analyse.

   A l'aide des masques au format de l'interpréteur de commandes, vous pouvez définir le modèle du nom de fichier à exclure de la zone de protection ou de l'analyse à la demande.
5. Enregistrez les modifications dans le fichier de configuration.
6. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

Exclusion des objets selon la signature de la menace découverte

Quand Kaspersky Endpoint Security détecte un fichier infecté, l'application le traite : elle exécute l'action définie (cf. section"Choix des actions de l'application sur les objets infectés" à la page 77). Si vous considérez ce fichier comme sûr pour l'ordinateur, vous pouvez l'exclure de l'analyse selon le nom de la menace détectée. Dans ce cas, Kaspersky Endpoint Security reconnaît les objets détectés comme sûrs et ne les traite pas.

Le nom complet de la menace détectée dans le fichier contient les informations suivantes :

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

Vous pouvez trouver le nom complet du type de la menace détectée dans le fichier dans le journal de Kaspersky Endpoint Security et sur le site Internet de l'Encyclopédie antivirus (http://www.securelist.fr).

Lorsque vous définissez les modèles des noms des objets à détecter, vous pouvez utiliser les masques au format de l'interpréteur de commande.

► *Pour exclure des objets de la zone de protection ou de la zone d'analyse selon le nom de la menace détectée, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.

3. Attribuez la valeur `Yes` au paramètre `UseExcludeThreats`.

4. Définissez le modèle des noms de menaces à l'aide du paramètre `ExcludeThreats`.

   Pour spécifier quelques clichés de noms des menaces, répétez la valeur du paramètre `ExcludeThreats` autant de fois que nécessaire avec l'indication du numéro d'ordre `item _ #`.

Exemple :

```
ExcludeThreats.item_0000=EICAR-Test-*

ExcludeThreats.item_0001=?rojan.Linux
```

5. Enregistrez les modifications dans le fichier de configuration.

6. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

Choix du mode de protection en temps réel

Le choix du mode de protection des objets est accessible seulement pour la tâche de protection en temps réel (cf. section "A propos de la protection en temps réel" p. 64).

Le mode de protection en temps réel définit le type d'accès aux fichiers selon lequel Kaspersky Endpoint Security va réaliser une analyse.

Vous pouvez choisir un des modes de protection en temps réel :

- *Mode de protection intelligent* : Kaspersky Endpoint Security analyse le fichier en cas de tentative d'ouverture et l'analyse de nouveau en cas de tentative de fermeture s'il a été modifié. Si un processus quelconque s'adresse plusieurs fois au fichier pendant un certain temps et le modifie, Kaspersky Endpoint Security analyse de nouveau le fichier seulement lors de la dernière tentative de fermeture du fichier par ce processus.
- *Mode de protection en cas de tentative d'ouverture et de modification du fichier :* Kaspersky Endpoint Security analyse le fichier en cas de tentative d'ouverture et l'analyse de nouveau lors de la tentative de fermeture, s'il a été modifié.
- *Mode de protection en cas de tentative d'ouverture du fichier* : Kaspersky Endpoint Security analyse le fichier en cas de tentative d'ouverture en lecture, d'exécution ou de modification.

► *Pour choisir le mode de protection en temps réel des objets, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Attribuez une des valeurs suivantes au paramètre `ScanByAccessType` :
   - `SmartCheck` pour activer le mode de protection intelligent.
   - `OpenAndModify` pour activer le mode de protection en cas de tentative d'ouverture du fichier.
   - `Open` pour activer le mode de protection en cas de tentative d'ouverture du fichier.
4. Enregistrez les modifications dans le fichier de configuration.
5. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel à l'aide de la commande suivante :

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

Choix des actions de l'application sur les objets infectés

En cas de détection d'objets *infectés* (cf. section "A propos des fichiers infectés" à la page 69), Kaspersky Endpoint Security les traite : il exécute les actions indiquées dans la tâche de protection en temps réel ou d'analyse à la demande. Kaspersky Endpoint Security peut réparer, supprimer, bloquer les objets (pour la tâche de protection en temps réel) ou les ignorer (pour la tâche d'analyse à la demande).

Vous pouvez définir deux actions que Kaspersky Endpoint Security doit exécuter sur les objets infectés : la première action (exécutée initialement) et la deuxième action (exécutée si la première action a échoué).

► *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 ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Définissez les valeurs des paramètres suivants :
   - `FirstAction` – première action sur l'objet ;
   - `SecondAction` – deuxième action sur l'objet.
4. Enregistrez les modifications dans le fichier de configuration.
5. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

Analyse personnalisée des fichiers et des répertoires (Scan_File)

Kaspersky Endpoint Security permet d'analyser rapidement les fichiers et les répertoires sans devoir composer une zone d'analyse (cf. "Formation d'une zone de protection et d'une zone d'analyse" à la page 70).

> Vous pouvez définir les modèles des noms des fichiers à analyser à l'aide de masques au format de l'interpréteur de commandes. Dans ce cas, Kaspersky Endpoint Security analyse uniquement les fichiers de la zone de protection désignés à l'aide des masques au format de l'interpréteur de commandes.

Kaspersky Endpoint Security lance par défaut l'analyse des fichiers et des répertoires à l'aide de la commande `--scan-file` avec les paramètres par défaut définis pour la tâche d'analyse à la demande (cf. section "A propos de l'analyse à la demande" à la page 67).

► *Pour lancer l'analyse personnalisée des fichiers et des répertoires, exécutez une des commandes suivantes :*

- Si vous voulez analyser un seul fichier ou répertoire, exécutez la commande

```
/opt/kaspersky/kesl/bin/kesl-control --scan-file <chemin d'accès
```

```
au fichier ou au répertoire>
```

- Si vous voulez analyser plusieurs fichiers ou répertoires, exécutez la commande:

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

Analyse des secteurs d'amorçage

Kaspersky Endpoint Security permet d'analyser les secteurs d'amorçage sans devoir composer une zone d'analyse (cf. section "Formation d'une zone de protection et d'une zone d'analyse" à la page 70).

► *Pour analyser les secteurs d'amorçage, lancez la tâche système d'analyse des secteurs d'amorçage (ID=4) :*

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 4
```

Analyse de la mémoire des processus

Kaspersky Endpoint Security permet d'analyser la mémoire des processus sans devoir composer une zone d'analyse (cf. section "Formation d'une zone de protection et d'une zone d'analyse" à la page 70).

► *Pour analyser la mémoire des processus, lancez la tâche système d'analyse de la mémoire des processus (ID=5) :*

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 5
```

Réduction du temps d'analyse

En cas de nécessité, vous pouvez réduire le temps d'analyse des objets par les moyens suivants :

- Limiter la durée d'analyse de l'objet. Kaspersky Endpoint Security cesse l'analyse de l'objet à l'expiration du délai défini.

- Limiter la taille maximale de l'objet analysé. Pendant l'analyse, Kaspersky Endpoint Security ignore les objets dont la taille dépasse la valeur spécifiée.

Les restrictions de durée d'analyse et de taille de l'objet sont appliquées seulement à l'analyse des objets constitutifs (par exemple, les archives ou les bases de données).

► *Pour limiter la durée d'analyse d'un objet constitutif, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Attribuez les valeurs suivantes aux paramètres :
   - la `Yes` pour le paramètre `UseTimeLimit` ;
   - le temps maximal de l'analyse de l'objet constituant (en secondes) pour le paramètre `TimeLimit`.

Exemple :

```
UseTimeLimit=Yes

TimeLimit=120
```

4. Enregistrez les modifications dans le fichier de configuration.
5. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

► *Pour limiter la taille maximale de l'objet constitutif analysé, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel ou de la tâche d'analyse à la demande dans le fichier de configuration à l'aide de la commande suivante :

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

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Attribuez les valeurs suivantes aux paramètres :
   - valeur `Yes` pour le paramètre `UseSizeLimit` ;
   - taille maximale de l'objet constitutif analysé (en mégaoctets) pour le paramètre `SizeLimit`.

Exemple :

```
UseSizeLimit=Yes

SizeLimit=10
```

4. Enregistrez les modifications dans le fichier de configuration.
5. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel ou dans la tâche d'analyse à la demande à l'aide de la commande suivante :

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

Particularités de l'analyse des liens symboliques et matériels

Kaspersky Endpoint Security permet d'analyser les liens symboliques et matériels vers les fichiers.

Analyse des liens symboliques

Kaspersky Endpoint Security analyse les liens symboliques uniquement si le fichier auquel se réfère le lien symbolique entre dans la zone de protection de la tâche de protection en temps réel ou dans la zone d'analyse de la tâche d'analyse à la demande.

Si un fichier accessible via le lien symbolique n'entre pas dans la zone de protection ou dans la zone d'analyse de la tâche, l'application n'analyse pas ce fichier. Si un tel fichier contient un code malveillant, la sécurité de l'ordinateur est menacée.

Analyse des liens matériels

Quand Kaspersky Endpoint Security traite un fichier contenant plusieurs liens matériels, l'application choisit l'action en fonction de l'action à exécuter sur les objets définies :

- Si l'action **Exécuter l'action recommandée** (Recommended) est sélectionnée, Kaspersky Endpoint Security choisit automatiquement l'action et exécute celle-ci sur l'objet sur la base des données relatives au danger de la menace détectée dans l'objet et de la possibilité de désinfection de celui-ci.
- Si l'action **Supprimer** (Remove) est sélectionnée, Kaspersky Endpoint Security supprime le lien matériel traité. Les autres liens matériels vers ce fichier ne seront pas traités.
- Si l'action **Réparer** (Cure) est sélectionnée, Kaspersky Endpoint Security répare le fichier initial. Si la désinfection est impossible, l'application supprime le lien matériel et crée à la place une copie du fichier initial avec le nom du lien matériel supprimé.

Quand vous restaurez un fichier avec un lien matériel depuis la Sauvegarde, Kaspersky Endpoint Security crée la copie du fichier initial avec le nom du lien matériel précédemment placé dans la Sauvegarde. Les liens avec les autres liens matériels sur le fichier initial ne seront pas restaurés.

Configuration de la collaboration : Kaspersky Antivirus for Linux Mail Server

► *Pour configurer la compatibilité entre Kaspersky Endpoint Security 10 et Kaspersky Anti-Virus for Linux Mail Server, procédez comme suit :*

1. Enregistrez les paramètres de la tâche de protection en temps réel dans le fichier de configuration à l'aide de la commande suivante :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 1 --file
```

```
<chemin d'accès complet au fichier>
```

2. Ouvrez le fichier de configuration créé pour l'édition.
3. Ajoutez dans le fichier créé la section suivante :

```
[ExcludedFromScanScope.item_#]
Path=</var/opt/kaspersky/klms>
```

4. Répéter la section indiquée ci-dessus pour tous les agents de messagerie intégrés avec Kaspersky Anti-Virus for Linux Mail Server.
5. 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.item_#]
Path=/tmp/klmstmp
```

6. Enregistrez les modifications dans le fichier de configuration.
7. Importez les paramètres du fichier de configuration dans la tâche de protection en temps réel à l'aide de la commande suivante :

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 1 --file
<chemin d'accès complet au fichier>
```

Utilisation de la Sauvegarde

Avant la désinfection ou la suppression des objets infectés, Kaspersky Endpoint Security enregistre un copie de ceux-ci dans la Sauvegarde.

Si l'objet infecté fait partie d'un objet composé, Kaspersky Endpoint Security enregistre tout l'objet composé dans la Sauvegarde. Par exemple, si Kaspersky Endpoint Security détermine qu'un objet faisant partie de la base de messagerie est infecté, Kaspersky Endpoint Security enregistre une copie de toute la base de messagerie dans la Sauvegarde avant la désinfection.

Cette section contient des instructions sur l'utilisation des objets dans la sauvegarde.

Dans cette section

Cf. également

A propos de la Sauvegarde

Le *dossier de Sauvegarde* est une liste de copies de sauvegarde des fichiers qui ont été supprimés ou modifiés pendant la désinfection. La *copie de sauvegarde* est une copie du fichier créée lors de la

première désinfection ou suppression de ce fichier. Les copies de sauvegarde des fichiers sont conservées dans un format spécial et ne représentent aucun danger.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations critiques partiellement ou complètement perdues suite à la désinfection, l'utilisateur peut tenter de restaurer le fichier depuis sa copie désinfectée dans son dossier d'origine.

Consultation des numéros d'identification des objets dans la sauvegarde

Au moment de placer un objet dans la Sauvegarde, Kaspersky Endpoint Security lui attribue un identifiant numérique. Le numéro d'identification sert pour les actions effectuées sur l'objet, par exemple, la restauration (cf. page 86) ou la suppression (cf. page 87) de l'objet de la sauvegarde.

► *Pour consulter les numéros d'identification des objets dans la Sauvegarde, exécutez la commande :*

```
/opt/kaspersky/kesl/bin/kesl-control -B --query
```

L'identifiant de l'objet apparaît dans la ligne `ObjectId`.

Cf. également

Obtention des informations sur les objets du répertoire de sauvegarde..... 177

A propos de la restauration des objets depuis la Sauvegarde

Kaspersky Endpoint Security conserve les objets dans la Sauvegarde sous forme chiffrée pour protéger le serveur contre d'éventuelles actions malveillantes.

Vous pouvez restaurer les objets depuis la sauvegarde. La restauration des objets peut être

nécessaire dans les cas suivants :

- Lors de la désinfection d'un fichier infecté Kaspersky Endpoint Security n'a pas réussi à l'enregistrer intégralement et les informations contenues dans le fichier ne sont plus accessibles.
- Vous considérez l'objet sûr pour le serveur et souhaitez l'utiliser.

  Vous pouvez exclure un objet de l'analyse pour que l'application ne le détecte pas lors des analyses ultérieures. Pour cela, vous devez exclure l'objet en fonction du nom ou de l'appellation de la menace détectée dans la tâche de protection en temps réel ainsi qu'en fonction du nom ou de l'appellation de la menace détectée dans les tâches d'analyse à la demande.

La restauration des objets infectés peut infecter l'ordinateur.

En cas restauration depuis la Sauvegarde, vous pouvez enregistrer le fichier sous un autre nom.

Cf. également

Restauration des objets depuis la sauvegarde 178

Restauration des objets depuis la Sauvegarde

► *Pour restaurer un objet depuis la sauvegarde, exécutez une des actions suivantes :*

- Pour restaurer l'objet avec le nom initial et à l'emplacement initial, vous devez effectuer l'une des opérations suivantes :

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

  où `ID de l'objet` correspond au numéro d'identification de l'objet dans la sauvegarde.

- Pour restaurer un objet avec un nouveau nom dans le répertoire indiqué, vous devez effectuer l'une des opérations suivantes :

  ```
  /opt/kaspersky/kesl/bin/kesl-control --restore <ID de l'objet>
  --file <nom du fichier et chemin d'accès à celui-ci>
  ```

Si le répertoire indiqué n'existe pas, Kaspersky Endpoint Security le crée.

Suppression des objets de la Sauvegarde

- *Pour supprimer un objet de la sauvegarde, exécutez la commande suivante :*

  ```
  /opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query "ObjectId == 'ID de l'objet>'"
  ```

- *Pour supprimer plusieurs objets de la sauvegarde, exécutez la commande suivante :*

  ```
  /opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query "<champ><opérateur de comparaison> '<valeur>' [and <champ> <opérateur de comparaison>'<valeur>' ]* ]
  ```

- *Pour supprimer tous les objets de la Sauvegarde, exécutez une des commandes suivantes :*

  ```
  /opt/kaspersky/kesl/bin/kesl-control -B --mass-remove
  ```

  ou

  ```
  /opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query
  ```

Configuration des notifications sur les événements

Pendant le fonctionnement de Kaspersky Endpoint Security, des événements se produisent. Ils traduisent une modification de l'état de la protection antivirus du serveur et de l'état de Kaspersky Security dans son ensemble. Si vous administrez l'application via Kaspersky Security Center, vous pouvez configurer la notification de l'administrateur par email pour ces événements.

Pour en savoir plus sur la configuration des notifications relatives aux événements, consultez le *Manuel de l'administrateur de Kaspersky Security Center*.

Participation au Kaspersky Security Network

Cette section contient des informations relatives à la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de Kaspersky Security Network.

Dans cette section

Présentation de la participation au Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet de récolter ces données.

Kaspersky Security Network (KSN) est une infrastructure de services cloud qui permet d'accéder à la base des connaissances de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et des logiciels. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement face aux menaces inconnues. L'efficacité de certains modules de protection est améliorée et la probabilité de faux positifs est réduite.

En fonction de l'infrastructure, on distingue le KSN global (infrastructure implantée sur les serveurs de Kaspersky Lab) ou le KSN privé (infrastructure implantée sur des serveurs tiers, par exemple dans le réseau d'un FAI).

Après la modification de la licence d'utilisation du KSN privé, il faut transmettre les informations relatives à la nouvelle clé au fournisseur de services. Dans le cas contraire, il sera impossible d'échanger des informations avec le KSN privé en raison d'une erreur d'authentification.

La participation des utilisateurs à KSN permet à Kaspersky Lab de recevoir rapidement les informations sur les types et les sources de menaces, d'élaborer les moyens de neutralisation des menaces et de diminuer la quantité de faux positifs des composants de l'application.

Pendant l'utilisation du KSN, l'application envoie automatiquement à KSN les statistiques obtenues dans le cadre de son fonctionnement. L'application peut également envoyer à Kaspersky Lab pour analyse complémentaire des fichiers (ou des parties de fichiers) que des individus malintentionnés pourraient utiliser pour nuire à l'ordinateur et aux données.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour en savoir plus sur l'envoi, la conservation et la suppression des statistiques obtenues pendant l'utilisation du KSN qui sont envoyées à Kaspersky Lab, consultez la Déclaration de Kaspersky Security Network et le site Internet de Kaspersky Lab (http://www.kaspersky.ru/privacy). Le fichier qui reprend la Déclaration de Kaspersky Security Network figure dans le kit de distribution de l'application.

Les ordinateurs des utilisateurs administrés via le Serveur d'administration Kaspersky Security Center peuvent interagir avec KSN à l'aide du service KSN Proxy.

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur peut interroger KSN et transmettre des informations à KSN, même en l'absence d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Pour en savoir plus sur le service KSN Proxy, lisez le *Manuel de l'administrateur de Kaspersky Security Center*.

La configuration des paramètres d'utilisation du service KSN Proxy s'opère via les propriétés de stratégie de *Kaspersky Security Center* (cf. section "*Administration des stratégies*" à la page 110).

La participation au Kaspersky Security Network est volontaire. L'application propose de participer au KSN pendant l'installation. Vous pouvez décider de participer au KSN ou de retirer votre participation à tout moment.

Activation et désactivation de l'utilisation de Kaspersky Security Network

► *Pour activer l'utilisation de Kaspersky Security Network, exécutez la commande suivante :*

```
kesl-control --set-app-settings UseKSN=Yes
```

► *Pour désactiver l'utilisation de Kaspersky Security Network, exécutez la commande suivante :*

```
kesl-control --set-app-settings UseKSN=No
```

► *Pour activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide du fichier de configuration, exécutez la commande suivante :*

```
kesl-control --set-app-settings --file <nom du fichier de configuration>
```

Si Kaspersky Endpoint Security, installé sur l'ordinateur, fonctionne sous une stratégie définie dans Kaspersky Security Center, la valeur du paramètre `UseKSN` peut être modifiée uniquement à l'aide de Kaspersky Security Center.

Si Kaspersky Endpoint Security, installé sur l'ordinateur, n'est plus soumis à la stratégie, la valeur du paramètre devient `UseKSN=No`.

Le fichier contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire `/opt/kaspersky/kesl/doc/ksn_license.<ID de la langue>`.

Vérification de la connexion à Kaspersky Security Network

► *Pour vérifier la connexion à Kaspersky Security Network, exécutez la commande suivante :*

```
kesl-control --app-info
```

La ligne `KSN state` affiche l'état de la connexion à Kaspersky Security Network :

- Si l'état `On` est affiché, Kaspersky Endpoint Security est connecté à Kaspersky Security Network.
- Si l'état `Off` est affiché, Kaspersky Endpoint Security n'est pas connecté à Kaspersky Security Network.

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- L'ordinateur n'est pas connecté à Internet.
- Vous ne participez pas à Kaspersky Security Network.
- L'application n'est pas activée ou la licence a expiré.
- Des problèmes liés à la clé ont été détectés. Par exemple, la clé figure dans une liste noire de clés.

Protection complémentaire avec l'utilisation de Kaspersky Security Network

Kaspersky Lab offre un niveau complémentaire de protection avec l'utilisation de Kaspersky Security Network. Ce mode de protection permet de lutter efficacement contre les menaces permanentes complexes et les menaces du type zero-day (0jour). Les technologies cloud associées à Kaspersky Endpoint Security et les connaissances approfondies des experts de virus de Kaspersky Lab assurent une protection puissante contre les menaces les plus complexes.

Pour en savoir plus sur la protection complémentaire dans Kaspersky Endpoint Security, visitez le site Internet de Kaspersky Lab.

Administration à distance via Kaspersky Security Center

Cette section présente l'administration à distance de Kaspersky Endpoint Security via Kaspersky Security Center. La description présentée concerne Kaspersky Security Center SP2.

Dans cette section

A propos de l'administration de Kaspersky Endpoint Security à l'aide de Kaspersky Security Center

Kaspersky Security Center permet d'installer, de supprimer, de lancer et d'arrêter Kaspersky Endpoint Security à distance, de configurer les paramètres de fonctionnement de l'application et de lancer les tâches sur les ordinateurs administrés.

L'application est administrée via Kaspersky Security Center à l'aide du plug-in d'administration de Kaspersky Endpoint Security.

> Avant l'installation du plug-in d'administration de Kaspersky Endpoint Security, il faut s'assurer que Kaspersky Security Center et Redist C ++ 2015 (Microsoft Visual C ++ 2015 Redistributable) sont installés.

Vous pouvez exécuter les actions suivantes dans la Console de gestion de Kaspersky Security Center :

- consulter l'état de protection des ordinateurs ;
- configurer les paramètres généraux de protection des ordinateurs ;
- administrer les politiques ;
- administrer les tâches :
  - ajout d'une clé ;
  - copie des mises à jour ;
  - mises à jour ;
  - annulation de la mise à jour ;
  - analyse des secteurs d'amorçage ;
  - analyse de la mémoire des processus ;

- analyse à la demande.

Lancement et arrêt de Kaspersky Endpoint Security sur un ordinateur client

► *Pour lancer ou arrêter Kaspersky Endpoint Security sur un ordinateur client, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Dans la liste des appareils administrés, sélectionnez l'ordinateur sur lequel vous voulez lancer ou arrêter l'application.
5. Ouvrez le menu contextuel de l'ordinateur d'un clic-droit. Sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de l'ordinateur s'ouvre.
6. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.

   La liste des applications de Kaspersky Lab installées sur l'ordinateur s'affiche à droite de la fenêtre des propriétés de l'ordinateur.
7. Choisissez l'application Kaspersky Endpoint Security 10 for Linux.
8. Procédez comme suit :

   - Si vous souhaitez démarrer l'application, cliquez à droite de la liste des applications Kaspersky Lab sur le bouton  ou procédez comme suit :

     a. Ouvrez le menu contextuel de l'application Kaspersky Endpoint Security 10 for Linux d'un clic-droit et choisissez l'option **Propriétés** ou cliquez sur le bouton **Propriétés** situé sous la liste des applications de Kaspersky Lab.

La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** s'ouvre sous l'onglet **Général**.

b. Cliquez sur le bouton **Lancer**.

- Si vous souhaitez arrêter l'application, cliquez à droite de la liste des applications Kaspersky Lab sur le bouton  ou procédez comme suit :

a. Ouvrez le menu contextuel de l'application Kaspersky Endpoint Security 10 for Linux d'un clic-droit et choisissez l'option **Propriétés** ou cliquez sur le bouton **Propriétés** situé sous la liste des applications.

La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** s'ouvre sous l'onglet **Général**.

b. Cliquez sur le bouton **Arrêter**.

Configuration des paramètres de Kaspersky Endpoint Security

► *Pour configurer les paramètres de Kaspersky Endpoint Security, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Dans la liste des ordinateurs, client, choisissez l'ordinateur pour lequel vous souhaitez configurer les paramètres de Kaspersky Endpoint Security.
5. Ouvrez le menu contextuel de l'ordinateur d'un clic-droit. Sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de l'ordinateur s'ouvre.
6. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.

La liste des applications de Kaspersky Lab installées sur l'ordinateur s'affiche à droite de la fenêtre des propriétés de l'ordinateur.

7. Choisissez l'application Kaspersky Endpoint Security 10 for Linux.

8. Ouvrez le menu contextuel de l'application Kaspersky Endpoint Security 10 for Linux d'un clic-droit et sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** s'ouvre.

9. Dans la section **Paramètres avancés**, configurez les paramètres de fonctionnement de Kaspersky Endpoint Security ainsi que les paramètres des rapports et des stockages.

   Les autres sections de la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** sont standard pour l'application Kaspersky Security Center. Elles sont décrites dans le *Manuel de l'administrateur de Kaspersky Security Center*.

   Si une stratégie est créée dans laquelle la modification de certains paramètres est interdite pour l'application, vous n'avez pas accès à la modification de la configuration des paramètres de l'application.

10. Dans la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux**, cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

Consultation de l'état de protection de l'ordinateur

► *Pour consulter l'état de la protection de l'ordinateur, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez l'entrée **Appareils administrés** et sélectionnez le groupe auquel appartient l'ordinateur protégé.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Ouvrez le menu contextuel de l'ordinateur protégé d'un clic-droit et sélectionnez l'option **Propriétés**.

4. Dans la fenêtre **Propriétés**, sélectionnez l'onglet **Protection**.

Les informations suivantes relatives à l'ordinateur protégé s'affichent sous l'onglet **Protection** :

- **Etat de l'ordinateur** : informations sur la sécurité antivirus de l'ordinateur protégé, par exemple, *Les bases sont dépassées*, *La durée de validité de la licence a expiré* ;
- **Etat de la protection en temps réel** : l'état de la protection en temps réel, par exemple, *En cours*, *Arrêtée*, *Suspendue* ;
- **Dernière analyse à la demande** : date et heure de la dernière exécution de la tâche d'analyse à la demande ;
- **Virus détectés** : total des applications malveillantes détectées sur l'ordinateur protégé (compteur des menaces détectées) depuis l'installation de Kaspersky Endpoint Security ou depuis la remise à zéro du compteur. Pour réinitialiser le compteur, cliquez sur le bouton **Remettre à zéro**.
- **Nombre d'objets non désinfectés** : nombre d'objets infectés que Kaspersky Endpoint Security n'a pas pu désinfecter.

Consultation des paramètres de Kaspersky Endpoint Security

► *Pour consulter les paramètres de Kaspersky Endpoint Security, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez l'entrée **Appareils administrés** et sélectionnez le groupe auquel appartient l'ordinateur protégé.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Ouvrez le menu contextuel de l'ordinateur protégé d'un clic-droit et sélectionnez l'option **Propriétés**.

4. Dans la fenêtre **Propriétés : <Nom de l'ordinateur>**, sélectionnez la section **Applications**.

5. Dans la section **Applications**, choisissez **Kaspersky Endpoint Security 10 for Linux** dans la liste des applications installées et dans le menu contextuel de l'application, sélectionnez l'option **Propriétés**.

   Cela entraîne l'ouverture de la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** à la section **Général**.

La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 for Linux** affiche les informations suivantes sur Kaspersky Endpoint Security :

Section **Général**

- **Numéro de version** : le numéro de la version de Kaspersky Endpoint Security ;
- **Installé** : la date et l'heure de l'installation de Kaspersky Endpoint Security sur l'ordinateur protégé ;
- **Etat en cours** : l'état de la protection en temps réel, par exemple *En cours*, *Suspendue* ;
- **Dernière mise à jour logicielle** : la date et l'heure de la dernière mise à jour des modules de l'application Kaspersky Endpoint Security ;
- **Mises à jour installées** : la liste des modules dont les mises à jour ont été installées ;
- **Bases de l'application** : la date et l'heure de la dernière mise à jour des bases antivirus et nombre d'enregistrements dans les bases.

Section **Clés**

- **Type de licence** : le type de licence, *commerciale* ou *évaluation* ;
- **Date d'activation** (le champ est disponible uniquement pour la clé active) : la date d'ajout de la clé active ;
- **Date d'expiration du délai** (le champ est accessible seulement pour la clé active) : la date d'expiration de la validité de la clé active ;
- **Durée de validité** : la durée de validité de la clé, en jours ;

- **Restriction** : le nombre d'ordinateurs sur lesquels vous pouvez utiliser la clé.

Section **Evénements**

Cette section permet de consulter les événements que Kaspersky Endpoint Security consigne dans le stockage des événements.

Section **Avancé**

Cette section permet de consulter les informations sur le plug-in d'administration de l'application.

Administration des tâches

Cette section contient des informations sur l'administration des tâches de Kaspersky Endpoint Security.

Pour en savoir plus sur la méthode d'administration des tâches via Kaspersky Security Center, consultez le *Manuel de l'administrateur de Kaspersky Security Center.*

A propos des tâches de Kaspersky Endpoint Security

Kaspersky Security Center utilise des tâches pour administrer le fonctionnement de Kaspersky Endpoint Security sur les ordinateurs. Les tâches assurent les principales fonctions générales d'administration, par exemple, l'ajout d'une clé, l'analyse des objets, la mise à jour des bases et des modules de l'application.

En utilisant Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez créer les types de tâches suivants :

- tâches locales définies pour un ordinateur distinct ;
- tâches de groupe définies pour les ordinateurs qui font partie de groupes d'administration ;
- tâches pour des ensembles d'ordinateurs ne faisant pas partie de groupes d'administration.

> Les tâches pour les ensembles d'ordinateurs ne faisant pas partie de groupes d'administration sont exécutées seulement pour les ordinateurs indiqués dans les paramètres de la tâche. Si de nouveaux ordinateurs sont ajoutés à un ensemble d'ordinateurs pour lequel une tâche a été créée, cette tâche ne s'applique pas à ceux-ci. Dans ce cas, il faut créer une autre tâche ou modifier les paramètres de la tâche existante.

Vous pouvez créer des tâches des types suivants :

- **Mise à jour**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security met à jour les bases antivirus conformément aux paramètres de mise à jour définis.
- **Remise à l'état initial de la mise à jour**. Pendant l'exécution de cette tâche, Kaspersky Endpoint Security restaure l'état antérieur à la dernière mise à jour des bases antivirus.
- **Copie des mises à jour**. Pendant l'exécution de cette tâche, Kaspersky Endpoint Security télécharge les bases antivirus dans le répertoire indiqué sans les installer.
- **Analyse à la demande**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security recherche la présence éventuelle de virus et d'autres programmes dangereux dans les secteurs de l'ordinateur définis via les paramètres de la tâche.
- **Analyse des secteurs d'amorçage**. Pendant l'exécution de cette tâche, Kaspersky Endpoint Security analyse les secteurs d'amorçage de l'ordinateur.
- **Analyse de la mémoire système**. Pendant l'exécution de cette tâche, Kaspersky Endpoint Security analyse la mémoire système de l'ordinateur.
- **Ajout d'une clé**. Pendant l'exécution de cette tâche, Kaspersky Endpoint Security ajoute une clé, notamment une clé additionnelle, pour l'activation de l'application.

Vous pouvez réaliser les opérations suivantes sur les tâches :

- démarrer, arrêter, suspendre ou reprendre l'exécution de la tâche ;
- créer de nouvelles tâches ;
- modifier les paramètres des tâches.

Les autorisations d'accès aux paramètres des tâches de Kaspersky Endpoint Security (lecture, modification, exécution) sont définies pour chaque utilisateur qui a accès au Serveur d'administration Kaspersky Security Center via les paramètres d'accès aux zones de fonction de Kaspersky Endpoint Security. Pour configurer les autorisations d'accès aux paramètres des zones de fonction de Kaspersky Endpoint Security, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration Kaspersky Security Center.

Les informations générales sur les tâches disponibles dans Kaspersky Security Center figurent dans le *Manuel de l'administrateur de Kaspersky Security Center*.

Création d'une tâche locale

► *Pour créer une tâche locale, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Dans la liste des ordinateurs, client, choisissez l'ordinateur pour lequel vous souhaitez créer une tâche locale.
5. Ouvrez le menu contextuel de l'ordinateur d'un clic-droit. Sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de l'ordinateur s'ouvre.
6. Choisissez la section **Tâches**.
7. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.
8. Suivez les instructions de l'Assistant de création de tâche.

Création d'une tâche de groupe

► *Pour créer une tâche de groupe, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Ouvrez le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Créer une tâche**.
   - Choisissez l'option **Créer** → **Tâche** dans le menu contextuel de Kaspersky Security Center.

   L'Assistant de création de tâche démarre.
5. Suivez les instructions de l'Assistant de création de tâche.

Création d'une tâche pour un ensemble d'ordinateurs

► *Pour créer une tâche pour un ensemble d'ordinateurs, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Ouvrez le dossier **Tâches pour les ensembles d'appareils** de l'arborescence de la Console d'administration Kaspersky Security Center.
3. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Créer une tâche**.
   - Choisissez l'option **Créer** → **Tâche** dans le menu contextuel de Kaspersky Security Center.

   L'Assistant de création de tâche démarre.

4. Suivez les instructions de l'Assistant de création de tâche.

Démarrage, arrêt, suspension et reprise manuel(le) d'une tâche

Si l'application Kaspersky Endpoint Security (cf. section "Lancement et arrêt de Kaspersky Security sur un ordinateur client" à la page 96) est lancée sur l'ordinateur, vous pouvez lancer / arrêter / suspendre / reprendre l'exécution d'une tâche sur cet ordinateur via Kaspersky Security Center. Si Kaspersky Endpoint Security est arrêté, les tâches en cours d'exécution sont arrêtées et il n'est plus possible de gérer le lancement, l'arrêt, la suspension et la reprise des tâches via Kaspersky Security Center.

► *Pour démarrer / arrêter / suspendre / reprendre l'exécution d'une tâche locale, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Choisissez dans la liste des ordinateurs client celui sur lequel vous souhaitez lancer, arrêter, suspendre ou reprendre une tâche locale.
5. Choisissez l'option **Propriétés** dans le menu contextuel de l'ordinateur.

   La fenêtre des propriétés de l'ordinateur s'ouvre.
6. Choisissez la section **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.
7. Choisissez la tâche locale que vous voulez démarrer / arrêter / suspendre / reprendre.
8. Exécutez une des actions suivantes :

- Cliquez-droit sur le menu contextuel de la tâche. Choisissez l'option **Démarrer** / **Arrêter** / **Arrêter** / **Reprendre**.

- Cliquez sur le bouton  ou  à droite de la liste des tâches locales pour lancer ou arrêter la tâche locale.

- Cliquez sur le bouton **Propriétés** sous la liste des tâches locales. La fenêtre **Propriétés de la tâche <Nom de la tâche>**. Ensuite sous l'onglet **Général** de la fenêtre **Propriétés de la tâche <Nom de la tâche>**, cliquez sur le bouton **Démarrer** / **Arrêter** / **Suspendre** / **Reprendre**.

► *Pour démarrer / arrêter / suspendre / reprendre l'exécution d'une tâche de groupe, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous voulez démarrer / arrêter / suspendre / reprendre l'exécution de la tâche de groupe.

3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

   La liste des tâches de groupe dans la partie droite de la fenêtre.

4. Dans la liste des tâches de groupe, sélectionnez la tâche de groupe que vous voulez démarrer / arrêter / suspendre / reprendre.

5. Exécutez une des actions suivantes :

   - Cliquez-droit sur le menu contextuel de la tâche de groupe. Choisissez l'option **Démarrer** / **Arrêter** / **Arrêter** / **Reprendre**.

   - Cliquez sur le bouton  /  à droite de la liste des tâches de groupe pour démarrer ou arrêter la tâche de groupe.

► *Pour lancer / arrêter / suspendre / reprendre l'exécution d'une tâche d'un ensemble d'ordinateurs, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Tâches pour un ensemble d'ordinateurs** de l'arborescence de la console, sélectionnez la tâche pour l'ensemble d'ordinateurs que vous voulez lancer / arrêter / suspendre/ recommencer.

3. Exécutez une des actions suivantes :

- Cliquez-droit pour ouvrir le menu contextuel de la tâche pour l'ensemble d'ordinateurs.

  Choisissez l'option **Démarrer** / **Arrêter** / **Arrêter** / **Reprendre**.

- Cliquez sur le bouton  /  à droite de la liste des tâches pour les ensembles d'ordinateurs pour lancer ou arrêter la tâche pour l'ensemble d'ordinateurs.

Modification des paramètres de la tâche

► *Pour modifier les paramètres d'une tâche locale, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration Kaspersky Security Center, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur requis.

3. Dans la zone de travail, sélectionnez l'onglet **Ordinateurs**.

4. Dans la liste des ordinateurs, client, choisissez l'ordinateur pour lequel vous voulez configurer les paramètres de l'application.

5. Exécutez une des actions suivantes :

   - Ouvrez le menu contextuel de l'ordinateur d'un clic-droit. Sélectionnez l'option **Propriétés**.

   - Dans le menu **Actions**, choisissez l'option **Propriété de l'ordinateur**.

   La fenêtre des propriétés de l'ordinateur s'ouvre.

6. Choisissez la section **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.

7. Sélectionnez la tâche locale requises dans la liste.
8. Exécutez une des actions suivantes :
   - Ouvrez le menu contextuel de la tâche d'un clic-droit. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés**.

   La fenêtre **Propriétés : <Nom de la tâche locale>** s'ouvre.
9. Dans la fenêtre **Propriétés : <Nom de la tâche locale>**, sélectionnez la section **Paramètres**.
10. Modifiez les paramètres de la tâche locale.
11. Dans la fenêtre **Propriétés : <Nom de la tâche locale>**, cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

► *Pour modifier les paramètres d'une tâche de groupe, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés**, ouvrez le dossier comportant le nom du groupe d'administrations souhaité.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

   La liste des tâches de groupe apparaît dans la partie inférieure de la barre des tâches.
4. Sélectionnez la tâche de groupe requise dans la liste.
5. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel de la tâche. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Modifier les paramètres de la tâche** situé à droite de la liste des tâches de groupe.

   La fenêtre **Propriétés : <Nom de la tâche de groupe>** s'ouvre.

6. Dans la fenêtre **Propriétés : <Nom de la tâche de groupe>**, sélectionnez la section **Paramètres**.

7. Modifiez les paramètres de la tâche de groupe.

8. Dans la fenêtre **Propriétés : <Nom de la tâche de groupe>**, cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

► *Pour modifier les paramètres d'une tâche pour un ensemble d'ordinateurs, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Tâche pour un ensemble d'ordinateurs** de l'arborescence de la console, sélectionnez la tâche pour l'ensemble d'ordinateurs dont vous voulez modifier les paramètres.

3. Exécutez une des actions suivantes :

   - Ouvrez le menu contextuel de la tâche pour l'ensemble d'ordinateurs d'un clic-droit. Sélectionnez l'option **Propriétés**.

   - Cliquez sur le bouton **Modifier les paramètres de la tâche** situé à droite de la liste des tâches pour les ensembles d'ordinateurs.

   La fenêtre **Propriétés : <Nom de la tâche pour un ensemble d'ordinateurs>** s'ouvre.

4. Dans la fenêtre **Propriétés : <Nom de la tâche pour un ensemble d'ordinateurs>**, sélectionnez la section **Paramètres**.

5. Modifiez les paramètres de la tâche pour l'ensemble d'ordinateurs.

6. Dans la fenêtre **Propriétés : <Nom de la tâche pour un ensemble de serveurs>**, cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

Toutes les sections de la fenêtre des propriétés des tâches, exceptée la section **Paramètres**, sont standard pour l'application Kaspersky Security Center. Ils sont décrits en détail dans le *Manuel de l'administrateur de Kaspersky Security Center*. La section **Paramètres** contient les paramètres spécifiques de Kaspersky Endpoint Security 10 ; son contenu varie en fonction du type de tâche choisi.

Administration des stratégies

Cette section contient des informations sur la création et la configuration des stratégies pour Kaspersky Endpoint Security. Vous pouvez obtenir des informations plus détaillées sur le concept d'administration de l'application Kaspersky Endpoint Security à l'aide des stratégies de Kaspersky Security Center dans le *Manuel de l'administrateur de Kaspersky Security Center*.

A propos des stratégies

Les stratégies permettent de définir des valeurs identiques pour les paramètres de fonctionnement de Kaspersky Endpoint Security sur tous les postes clients appartenant au groupe d'administration.

Vous pouvez modifier localement les paramètres spécifiés par la stratégie pour des ordinateurs distincts dans le groupe d'administration à l'aide de Kaspersky Endpoint Security. Vous pouvez modifier localement seulement les paramètres dont la modification n'est pas interdite par la stratégie.

La possibilité de modifier le paramètre de l'application sur un ordinateur client est défini par l'état du "cadenas" du paramètre dans la stratégie :

- Si le paramètre est fermé par un "cadenas" (), cela signifie que vous ne pouvez pas modifier la valeur du paramètre localement. Pour tous les ordinateurs client du groupe d'administration, la valeur du paramètre spécifiée par la stratégie est utilisée.

- Si le paramètre n'est fermé par un "cadenas" (), cela signifie que vous pouvez modifier la valeur du paramètre localement. Pour tous les ordinateurs client du groupe d'administration, les valeurs du paramètre spécifiées par la stratégie sont utilisées. La valeur du paramètre définie dans la stratégie n'est pas appliquée.

Les paramètres locaux de l'application changent conformément aux paramètres de la stratégie après la première application de la stratégie.

Les stratégies vous permettent de configurer les paramètres de la tâche de protection en temps réel de Kaspersky Endpoint Security.

Les droits d'accès aux paramètres d'une stratégie (lecture, modification, exécution) sont précisés pour chaque utilisateur ayant accès au Serveur d'administration Kaspersky Security Center et

séparément pour chaque zone fonctionnelle de Kaspersky Endpoint Security. Pour configurer les droits d'accès aux paramètres d'une stratégie, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration de Kaspersky Security Center.

Vous pouvez réaliser les opérations suivantes sur les stratégies :

- créer une stratégie.
- modifier les paramètres d'une stratégie.

  > Si le compte utilisateur sous lequel vous avez accédé au Serveur d'administration n'est pas autorisé à modifier les paramètres de certaines zones fonctionnelles, les paramètres de ces zones ne peuvent pas être modifiés.

- supprimer une stratégie.
- modifier l'état d'une stratégie.

Les informations relatives aux stratégies qui ne concernent pas l'interaction avec Kaspersky Endpoint Security sont reprises dans le *Manuel de l'administrateur de Kaspersky Security Center*.

Création d'une stratégie

► *Pour créer une stratégie, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
   - Sélectionnez le dossier **Ordinateurs administrés** de l'arborescence de la console si vous souhaitez créer une stratégie pour tous les ordinateurs administrés par Kaspersky Security Center.
   - Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier portant le nom du groupe d'administration dont font partie les ordinateurs qui vous intéressent.
3. Dans la zone de travail, sélectionnez l'onglet **Stratégies**.

4. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Créer une stratégie**.
   - Ouvrez le menu contextuel d'un clic-droit. Sélectionnez l'option **Créer** → **Stratégie**.

   L'Assistant de création de stratégie démarre.

5. Suivez les instructions de l'Assistant de création de stratégie.

Modification des paramètres de la stratégie

► *Pour modifier les paramètres de la stratégie, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration dont vous souhaitez modifier les paramètres de la stratégie.
3. Dans la zone de travail, sélectionnez l'onglet **Stratégies**.
4. Sélectionnez la stratégie souhaitée.
5. Exécutez une des actions suivantes :

   - Ouvrez le menu contextuel de la stratégie d'un clic-droit. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Modifier la stratégie** situé à droite de la liste des stratégies.

   La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

   Les paramètres de la stratégie pour Kaspersky Endpoint Security 10 comprennent les paramètres des tâches et les paramètres de l'application. Les sections **Protection** et **Contrôle** de la fenêtre **Propriétés : <Nom de la stratégie>** reprennent les paramètres des tâches, tandis que la section **Paramètres complémentaires** contient les paramètres de l'application.

6. Modifiez les paramètres de la stratégie.

7. Dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

Affichage des messages des utilisateurs dans le stockage des événements Kaspersky Security Center

Kaspersky Endpoint Security donne aux utilisateurs du réseau local de l'organisation la possibilité d'envoyer des messages à l'administrateur depuis les ordinateurs où est installée l'application.

L'utilisateur peut envoyer un message à l'administrateur de deux moyens différents :

- sous forme d'un événement dans le stockage des événements de Kaspersky Security Center. L'événement de l'utilisateur est transmis dans le stockage des événements de Kaspersky Security Center, si l'application Kaspersky Endpoint Security installée sur l'ordinateur de l'utilisateur fonctionne avec une stratégie active.

- sous forme d'un message électronique. Les informations de l'utilisateur sont transmises sous forme d'un message électronique si l'application Kaspersky Security installée sur l'ordinateur de l'utilisateur ne fonctionne pas avec une stratégie ou s'il est couvert par une stratégie mobile.

► *Pour consulter le message de l'utilisateur dans le stockage des événements de Kaspersky Security Center, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Ouvrez le dossier **Rapports et notifications \ Événements** \ **Avertissements** de l'arborescence de la console.

   Dans la zone de travail de Kaspersky Security Center, s'affiche la liste de tous les événements-avertissements, y compris les messages adressés à l'administrateur provenant des utilisateurs du réseau local de l'organisation. La zone de travail de Kaspersky Security Center se trouve à droite de l'arborescence de la console.

3. Sélectionnez dans la liste des événements le message adressé à l'administrateur.

4. Ouvrez la liste des événements via l'un des moyens suivants :

- Double-cliquez sur l'événement dans la liste.
- Ouvrez le menu contextuel de l'événement d'un clic-droit. Dans le menu contextuel de l'événement, sélectionnez l'option **Propriétés**.
- Cliquez sur le bouton **Ouvrir les propriétés de l'événement** à droite de la liste des événements.

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

La distribution de l'Agent d'administration comprend l'utilitaire *klnagchk* destiné à contrôler la connexion au Serveur d'administration.

Après l'installation de l'Agent d'administration, l'utilitaire est installé dans le répertoire /opt/kaspersky/klnagent/bin et, au démarrage, en fonction des clés utilisées, exécute les actions suivantes :

- affiche à l'écran ou consigne dans le fichier journal des événements les valeurs des paramètre de connexion de l'Agent d'administration installé sur l'ordinateur client au Serveur d'administration ;
- consigne dans le fichier journal des événements les statistiques de l'Agent d'administration (à compter du dernier démarrage du composant en question) et les résultats de l'exécution de l'utilitaire ou affiche les informations à l'écran ;
- essaie d'établir la connexion de l'Agent d'administration au Serveur d'administration ;
- si la connexion ne parvient pas à être établie, envoie le paquet ICMP pour vérifier l'état de l'ordinateur sur lequel est installé le Serveur d'administration.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nom du fichier>] [-sp] [-savecert <chemin d'accès au fichier du certificat>] [-restart]
```

Description des clés :

- `-logfile <nom du fichier>` – consigner les paramètres de connexion de l'Agent d'administration au Serveur et les résultats de l'exécution de l'utilitaire dans le fichier journal ; par défaut les informations sont enregistrées dans le fichier stdout.tx ; si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur s'affichent à l'écran.

- `-sp` – afficher le mot de passe d'authentification de l'utilisateur sur le serveur proxy ; le paramètre est utilisé si la connexion au Serveur d'administration est établie via le serveur proxy.

- `-savecert <nom du fichier>` – enregistrer le certificat d'authentification de l'accès au Serveur d'administration dans le fichier indiqué.

- `-restart` – redémarrer l'Agent d'administration une fois l'utilitaire terminé.

Connexion manuelle au Serveur d'administration. Utilitaire klmover

La distribution de l'Agent d'administration comprend l'utilitaire *klmover* destiné à administrer la connexion au Serveur d'administration.

Après l'installation de l'Agent d'administration, l'utilitaire est installé dans le répertoire /opt/kaspersky/klnagent/bin et, au démarrage, en fonction des clés utilisées, exécute 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 affiche à l'écran.

Syntaxe de l'utilitaire :

```
klmover [-logfile <nom du fichier>] {-address <adresse du serveur>} [-pn
<numéro de port>] [-ps <numéro de port SSL>] [-nossl] [-cert <chemin
d'accès au fichier du certificat>] [-silent] [-dupfix]
```

Description des clés :

- `-logfile <nom du fichier>` – enregistrer les résultats de l'exécution de l'utilitaire dans le fichier indiqué ; si la clé n'est pas utilisée, les résultats et les messages d'erreur sont affichés sur stdout.

- `-address <adresse du serveur>` – adresse du Serveur d'administration pour la connexion ; l'adresse indiquée peut être l'adresse IP, NetBIOS ou le nom DNS de l'ordinateur.

- `-pn <numéro de port>` – numéro du port qui servira à la connexion non protégée au Serveur d'administration ; le port 14000 est utilisé par défaut.

- `-ps <numéro de port SSL>` – numéro de port SSL qui servira à la connexion protégée au Serveur d'administration via le protocole SSL. Par défaut, le port 13000 est utilisé.

- `-nossl` – utiliser la connexion non protégée au Serveur d'administration ; si la clé n'est pas indiquée, la connexion de l'Agent au Serveur est établi via le protocole SSL de chiffrement.

- `-cert <chemin d'accès au fichier du certificat>` – utiliser le fichier indiqué du certificat pour l'authentification de l'accès à un nouveau Serveur d'administration. Si la clé n'est pas utilisée, l'Agent d'administration obtient le certificat à la première connexion au Serveur d'administration.

- `-silent` – démarrer l'utilitaire en mode non interactif ; l'utilisation de la clé peut être utile, par exemple, au démarrage de l'utilitaire à partir du scénario de démarrage au moment de l'enregistrement de l'utilisateur.

- `-dupfix` – la clé donnée est utilisée si l'installation de l'Agent d'administration a été exécutée de manière inhabituelle, non à l'aide du distributif, mais, par exemple, par restauration à partir de l'image du disque.

Contacter le service du Support Technique

Cette section contient des informations sur les modes et les conditions d'obtention de l'assistance technique.

Dans cette section

Modes d'obtention du Support Technique

Si vous n’avez pas trouvé la solution à votre problème dans la documentation ou dans une des sources d’informations sur l’application (cf. section "Sources d’informations sur l’application" à la page 14), veuillez contacter le Support technique. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

L'assistance technique est fournie uniquement aux utilisateurs de l'application qui ont acheté une licence commerciale. Les utilisateurs qui disposent d'une licence d'évaluation n'ont pas droit au support technique.

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

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- contacter le Support Technique par téléphone (http://support.kaspersky.com/fr/b2b) ;
- envoyer une demande au Support Technique de Kaspersky Lab du portail Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Assistance technique par téléphone

Vous pouvez téléphoner aux experts du Support Technique dans la plupart des régions du monde. Les informations sur les moyens de bénéficier de l'aide de l'assistance technique dans votre région ainsi que les coordonnées du Support Technique figurent sur le site Internet du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/b2c#region1).

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

Support Technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un portail à disposition des entreprises qui utilisent les applications de Kaspersky Lab. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Il permet de suivre le traitement des requêtes par les experts de Kaspersky Lab et de conserver un historique de ces requêtes.

Vous pouvez enregistrer tous les employés de votre entreprise dans un seul compte utilisateur Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de centraliser l'administration des requêtes électroniques envoyées à Kaspersky Lab et provenant des employés enregistrés. Il vous permet également d'administrer les privilèges de ces employés Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;
- français ;
- japonais.

Pour en savoir plus sur Kaspersky CompanyAccount, veuillez consulter le site Internet du Support technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

Appendices

Cette section contient des renseignements qui viennent compléter le contenu principal du document.

Dans cette section

Paramètres des fichiers de configuration

Cette section décrit les structures et les paramètres des fichiers de configuration de Kaspersky Endpoint Security au format INI ainsi que les règles de mise au point des fichiers de configuration.

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

Lors de la mise au point du fichier de configuration, veuillez respecter les règles suivantes :

- Il faut définir une valeur pour tous les paramètres obligatoires du fichier de configuration. Pour définir des paramètres distincts d'une tâche, vous pouvez opter pour la ligne de commande qui permet de réaliser l'opération sans fichier.
- Si le paramètre fait partie d'une section, ne le placez que dans cette section. Au sein d'une section, vous pouvez placer les paramètres dans tout ordre.
- 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.item_0000]

AreaDesc=Home

AreaMask.item_0000=*doc

Path=/home
```

Les symboles "espace" et "tabulation" sont ignorés avant le premier guillemet et après le dernier guillemet d'une valeur de ligne, ainsi qu'au début et à la fin d'une de ligne ne figurant pas entre guillemets.

- 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.item_0000=*xml

AreaMask.item_0001=*doc
```

- Respectez le registre lors de la saisie des valeurs des paramètres des types suivants :
  - noms (masques) des objets analysés et des objets d'exclusion ;
  - noms (masque) des menaces ;

  Lors de la saisie des autres valeurs des paramètres, il n'est pas nécessaire de respecter le registre.
- Indiquez les valeurs des paramètres de type booléen comme suit : `Yes – No`.

- 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, contenant date et heure au format AAAA-MM-DD HH:MM:SS).

  Exemple :

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

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

  Un guillemet solitaire en début ou en fin de ligne est une erreur.

Paramètres généraux de Kaspersky Endpoint Security

Après avoir modifié les paramètres généraux de Kaspersky Endpoint Security, relancez l'application.

Les paramètres généraux du fichier de configuration ont les valeurs suivantes :

SambaConfigPath

Répertoire dans lequel se trouve le fichier de configuration Samba. Le fichier de configuration Samba est nécessaire pour garantir le fonctionnement des valeurs `AllShared` ou `Shared:SMB` de l'option `Path`.

Le répertoire standard du fichier de configuration Samba sur l'ordinateur est indiqué par défaut.

Valeur par défaut : `/etc/samba/smb.conf`.

NfsExportPath

Répertoire dans lequel se trouve le fichier de configuration NFS. Le fichier de configuration NFS est nécessaire pour garantir le fonctionnement des valeurs `AllShared` ou `Shared:NFS` de l'option `Path`.

Le répertoire standard du fichier de configuration NFS sur l'ordinateur est indiqué par défaut.

Valeur par défaut : `/etc/exports`.

TraceFolder

Répertoire dans lequel Kaspersky Endpoint Security enregistre les fichiers du journal de trace.

Si vous indiquez un autre répertoire, veillez à ce que le compte utilisateur sous les autorisations duquel Kaspersky Endpoint Security fonctionne puisse y accéder en lecture et en écriture.

Valeur par défaut : `/var/log/kaspersky/kesl`.

TraceLevel

Niveau de détail du journal des traces.

Valeurs possibles :

`Detailed`. Journal de trace le plus détaillé.

`NotDetailed`. Le journal de trace contient des notifications sur les erreurs.

`None`. Aucun journal de trace n'est créé.

Valeur par défaut : `None`.

BlockFilesGreaterMaxFileNamePath

Blocage de l'accès aux fichiers dont la longueur du chemin d'accès complet dépasse la valeur du paramètre définie en octets.

Si la longueur le chemin complet d'accès au fichier analysé excède la valeur de ce paramètre, les tâches d'analyse à la demande ignorent ce fichier lors de l'analyse.

Valeurs possibles : `4096 – 33554432`.

Valeur par défaut : `16384`.

DetectOtherObjects

La case active/désactive la détection des applications légitimes qui pourraient être détournées par des individus malintentionnés pour nuire aux ordinateurs ou aux données de l'utilisateur.

Valeurs possibles :

`Yes`. Active la détection des applications légitimes qui pourraient être détournées par des individus malintentionnés pour nuire aux ordinateurs ou aux données de l'utilisateur.

`No`. Désactive la détection des applications légitimes qui pourraient être détournées par des individus malintentionnés pour nuire aux ordinateurs ou aux données de l'utilisateur.

Valeur par défaut : `No`.

UseKSN

Active/désactive la participation à Kaspersky Security Network.

Valeurs possibles :

`Yes`. Active la participation à Kaspersky Security Network

`No`. Désactive la participation à Kaspersky Security Network

Valeur par défaut : `No`.

UseProxy

Active/désactive l'utilisation d'un proxy pour Kaspersky Security Network, l'activation de l'application et les mises à jour.

Valeurs possibles :

`Yes`. Active l'utilisation d'un proxy.

`No`. Désactive l'utilisation d'un proxy.

Valeur par défaut : `No`.

ProxyServer

Les paramètres du serveur proxy au format `[utilisateur[:mot_de_passe]@]hôte[:port]`.

MaxEventsNumber

Quantité maximale d'événements qui sera enregistrée dans Kaspersky Endpoint Security. Quand la quantité maximale d'événements définie est atteinte, Kaspersky Endpoint Security supprime les événements les plus anciens.

Valeur par défaut : `500000`.

LimitNumberOfScanFileTasks

Quantité maximale des tâches de type `Scan_File` que l'utilisateur privé de privilèges peut lancer simultanément sur l'ordinateur. Ce paramètre ne limite pas la quantité de tâches que l'utilisateur doté des autorisations root peut lancer. Si la valeur `0` est attribuée, l'utilisateur privé de privilèges ne peut pas lancer les tâches de type `Scan_File`.

Valeurs possibles : `0 – 4294967295`.

Valeur par défaut : `0`.

UseSysLog

Active/désactive l'enregistrement des informations relatives aux événements dans syslog.

`Yes`. Active l'enregistrement des informations relatives aux événements dans syslog.

`No`. Désactive l'enregistrement des informations relatives aux événements dans syslog.

Valeur par défaut : `No`.

EventsStoragePath

Fichier de la base de données dans lequel Kaspersky Endpoint Security enregistre les informations relatives aux événements.

Valeur par défaut : `/var/opt/kaspersky/kesl/events.db`.

Cf. également

Paramètres de la tâche de protection en temps réel et des tâches d'analyse à la demande. .. 126

Règles de mise au point des fichiers de configuration de Kaspersky Endpoint Security 120

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

Vous pouvez configurer le fonctionnement des tâches de protection en temps réel et d'analyse à la demande en modifiant les paramètres dans les fichiers de configuration de ces tâches.

Pour modifier une tâche, il faut exécuter la séquence d'actions suivante :

1. Exportez les paramètres de la tâche dans le fichier de configuration (cf. page 171).
2. Dans le fichier de configuration, modifiez les paramètres de la tâche en fonction de vos exigences (cf. page 120).
3. Importez dans la tâche le fichier de configuration avec les paramètres modifiés (cf. page 172).

Cette section décrit les sections et les paramètres des fichiers de configuration de la tâche de protection en temps réel et des tâches d'analyse à la demande.

Structure du fichier de configuration ini de la tâche de protection en temps réel et de la tâche d'analyse à la demande

Le fichier de configuration de la tâche de protection en temps réel et de la tâche d'analyse à la demande comprend différents paramètres et sections. Les sections du fichier de configuration définissent les zones d'analyse et les zones d'exclusion utilisées par Kaspersky Endpoint Security pendant l'exécution de la tâche de protection en temps réel et des tâches d'analyse à la demande.

Le fichier de configuration de la tâche de protection en temps réel et des tâches d'analyse à la demande comprend les sections suivantes :

[ScanScope.item_#]

Dans cette section, vous pouvez indiquer le nom de la zone d'analyse. A l'aide des paramètres de cette section, vous pouvez former la zone d'analyse.

Cette section est obligatoire.

[ExcludedFromScanScope.item_#] (cf. page 138)

Dans cette section, vous pouvez indiquer la zone d'exclusion de l'analyse.

Cette section est facultative.

Si vous voulez définir plusieurs zones d'analyse ou d'exclusions, définissez plusieurs sections `[ScanScope.item_#]` et `[ExcludedFromScanScope.item_#]` (uniquement dans les tâches de protection en temps réel).

Kaspersky Endpoint Security traite les zones dans l'ordre indiqué par l'identifiant de la section.

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

Les fichiers de configuration de la tâche de protection en temps réel et des tâches d'analyse à la demande reprennent les paramètres suivants :

ScanArchived

Active / désactive l'analyse des archives (y compris les archives autoextractibles SFX). Kaspersky Endpoint Security détecte les menaces dans les archives mais ne les désinfecte pas.

Valeurs possibles :

`Yes` : analyser les archives ;

`No` : ne pas analyser les archives.

Valeur par défaut :

dans la tâche de protection en temps réel, `No` ;

dans la tâche d'analyse à la demande, `Yes`.

ScanSfxArchived

Active / désactive l'analyse uniquement des archives autoextractibles (archives comprenant un décompresseur exécutable d'archives autoextractibles).

Valeurs possibles :

`Yes` : analyser les archives autoextractibles ;

`No` : ne pas analyser les archives autoextractibles.

Valeur par défaut :

dans la tâche de protection en temps réel, `No` ;

dans la tâche d'analyse à la demande, `Yes`.

ScanMailBases

Active/désactive l'analyse des bases de messagerie des applications Microsoft Outlook®, Outlook Express, The Bat et autres clients de messagerie.

Valeurs possibles :

`Yes` : analyse les fichiers des bases de messagerie ;

`No` : n'analyse pas les fichiers des bases de messagerie.

Valeur par défaut : `No`.

ScanPlainMail

Active/désactive l'analyse des messages électroniques au format texte (plain text).

Valeurs possibles :

`Yes` : analyse les messages électroniques au format texte ;

`No` : n'analyse pas les messages électroniques au format texte.

Valeur par défaut : `No`.

ScanPacked

Active / désactive l'analyse des fichiers exécutables archivés par les compresseurs en codage binaire (par exemple, UPX ou ASPack). Les objets composés de ce type contiennent plus souvent des menaces.

Valeurs possibles :

`Yes` : analyse les fichiers archivés ;

`No` : n'analyse pas les fichiers archivés.

Valeur par défaut : `Yes`.

UseSizeLimit

Active/désactive l'application du paramètre `SizeLimit` (taille maximale de l'objet analysé).

Valeurs possibles :

`Yes` : applique le paramètre `SizeLimit` ;

`No` : n'applique pas le paramètre `SizeLimit`.

Valeur par défaut : `No`.

SizeLimit

Détermine la taille maximale de l'objet analysé (en mégaoctets). Si la taille de l'objet analysé dépasse la valeur indiquée, Kaspersky Endpoint Security ignore l'objet.

Ce paramètre est appliqué avec le paramètre `UseSizeLimit`.

Valeurs possibles : `0 – 999 999`. `0` : Kaspersky Endpoint Security analyse les objets de n'importe quelle taille.

Valeur par défaut : `0`.

UseTimeLimit

Active/désactive l'application du paramètre `TimeLimit` (durée maximale d'analyse de l'objet).

Valeurs possibles :

`Yes` : applique le paramètre `TimeLimit` ;

`No` : n'applique pas le paramètre `TimeLimit`.

Valeur par défaut :

dans la tâche de protection en temps réel, `Yes` ;

dans la tâche d'analyse à la demande, `No`.

TimeLimit

Précise la durée maximale d'analyse de l'objet (en secondes). Kaspersky Endpoint Security interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.

Ce paramètre est appliqué avec le paramètre `UseTimeLimit`.

Valeurs possibles : 0 – 9999. `0` – la durée d'analyse des objets n'est pas limitée.

Valeur par défaut : `0`.

FirstAction

Sélection de la première action exécutée par Kaspersky Endpoint Security sur les objets infectés.

Dans les tâches de protection en temps réel, avant d'exécuter l'action que vous avez choisie, Kaspersky Endpoint Security bloque l'accès de l'application à l'objet qu'elle a sollicité.

Valeurs possibles :

`Cure` (désinfecter) : Kaspersky Endpoint Security tente de désinfecter l'objet après avoir enregistré une copie de celui-ci dans la Sauvegarde. Si la désinfection est impossible

(par exemple, le type de l'objet ou le type de menace ne se prête pas à la désinfection), Kaspersky Endpoint Security laisse l'objet en l'état. Si la première action choisie est `Cure`, il est recommandé de préciser la deuxième action dans le paramètre `SecondAction`.

`Remove` (supprimer) : Kaspersky Endpoint Security supprime l'objet infecté après avoir créé au préalable sa copie de sauvegarde.

`Recommended` (exécuter l'action recommandée) : Kaspersky Endpoint Security choisit automatiquement et exécute l'action sur l'objet en fonction des données relatives à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime tout de suite les chevaux de Troie car ils n'infectent pas d'autres fichiers et ne se prêtent pas à la désinfection.

`Block` (bloquer) : Kaspersky Endpoint Security bloque l'accès à l'objet infecté. Les informations sur l'objet infecté sont conservées dans le journal.

> La valeur est utilisée uniquement dans la tâche de protection en temps réel.

`Skip` (ignorer) : Kaspersky Endpoint Security ne tente pas de désinfecter ou de supprimer l'objet infecté. Les informations sur l'objet infecté sont conservées dans le journal.

> La valeur est utilisée uniquement dans les tâches d'analyse à la demande.

Valeur par défaut : `Recommended`.

SecondAction

Sélection de la deuxième action exécutée par Kaspersky Endpoint Security sur les objets infectés. Kaspersky Endpoint Security exécute la deuxième action s'il ne parvient pas à exécuter la première.

Les valeurs du paramètre `SecondAction` sont les mêmes que celles du paramètre `FirstAction`.

Si l'option `Block` (pour une tâche de protection en temps réel) / `Skip` (pour une tâche d'analyse à la demande) ou `Remove` a été choisie en tant que première action, il n'est pas nécessaire de désigner la deuxième action. Dans les autres cas, il est recommandé d'indiquer deux actions. Si vous n'avez pas défini la deuxième action, Kaspersky Endpoint Security applique en tant que deuxième action `Block` (pour la tâche de protection en temps réel) / `Skip` (pour la tâche d'analyse à la demande).

Valeur par défaut : `Block` (pour la tâche de protection en temps réel) / `Skip` (pour la tâche d'analyse à la demande).

UseExcludeMasks

Active/désactive l'exclusion de l'analyse des objets désignés par le paramètre `ExcludeMasks`.

Valeurs possibles :

`Yes` : exclut les objets désignés par le paramètre `ExcludeMasks`.

`No` : n'exclut pas les objets désignés par le paramètre `ExcludeMasks`.

Valeur par défaut : `No`.

ExcludeMasks

Exclut de l'analyse les objets en fonction des noms ou des masques. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide des masques de l'interpréteur de commandes.

Valeur par défaut : non spécifié.

Exemple :

```
UseExcludeMasks=Yes

ExcludeMasks.item_0000=eicar1.*

ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Active ou désactive l'exclusion de l'analyse les objets contenant les menaces indiquées par le paramètre `ExcludeThreats`.

Valeurs possibles :

`Yes` : exclut de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats` ;

`No` : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats`.

Valeur par défaut : `No`.

ExcludeThreats

Exclut de l'analyse les objets en fonction des noms des menaces détectées dans les objets. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.

Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, une ligne de conclusion pour Kaspersky Security indiquant que l'objet est infecté.

Par exemple, vous utilisez un des utilitaires pour obtenir des informations sur le réseau. Pour que Kaspersky Endpoint Security ne le bloque pas, ajoutez le nom complet de la menace qu'elle comporte à la liste des menaces exclues de l'analyse.

Le nom complet de la menace détectée dans l'objet est repris dans le journal de Kaspersky Endpoint Security. Vous pouvez également trouver le nom complet de la menace sur le site Internet de l'Encyclopédie des virus (http://www.securelist.fr). Pour trouver le nom d'une menace, saisissez le nom de l'application dans le champ **Rechercher**.

La valeur du paramètre est sensible à la casse.

Valeur par défaut : non spécifié.

Exemples :

```
UseExcludeThreats=Yes

ExcludeThreats.item_0000=EICAR-Test-*

ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Active/désactive l'enregistrement dans le journal des informations sur les objets analysés que Kaspersky Endpoint Security a reconnus comme non infectés.

Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par Kaspersky Endpoint Security.

Valeurs possibles :

`Yes` : enregistre les informations relatives aux objets non infectés dans le journal ;

`No` : n'enregistre pas les informations relatives aux objets non infectés dans le journal.

Valeur par défaut : `No`.

ReportPackedObjects

Active / désactive l'enregistrement dans le journal des informations sur les objets analysés qui font partie d'objets composés.

Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet se trouvant dans une archive a bien été analysé par Kaspersky Endpoint Security.

Valeurs possibles :

`Yes` : enregistre les informations relatives à l'analyse des objets des archives dans le journal ;

`No` : n'enregistre pas les informations relatives à l'analyse des objets des archives dans le journal.

Valeur par défaut : `No`.

ReportUnprocessedObjects

Active/ désactive l'enregistrement dans le journal des informations relatives aux objets non analysés.

Valeurs possibles :

`Yes` : enregistre les informations relatives aux objets non analysés dans le journal ;

`No` : n'enregistre pas les informations relatives aux objets non analysés dans le journal.

Valeur par défaut : `No`.

UseAnalyzer

Active / désactive l'analyse heuristique.

Valeurs possibles :

`Yes` : active l'analyse heuristique ;

`No` : désactive l'analyse heuristique.

Valeur par défaut : `Yes`.

HeuristicLevel

Niveau de l'analyse heuristique.

Valeurs possibles :

`Light` – analyse moins minutieuse, charge minimale du système ;

`Medium` – niveau moyen de l'analyse heuristique, charge équilibrée du système ;

`Deep` – analyse plus minutieuse, charge maximale du système ;

`Recommended` – valeur recommandée.

Valeur par défaut : `Recommended`.

UseIChecker

Active/désactive l'utilisation de la technologie iChecker.

Valeurs possibles :

`Yes` : active l'utilisation de la technologie iChecker ;

`No` : désactive l'utilisation de la technologie iChecker.

Valeur par défaut : `Yes`.

ScanByAccessType

A l'aide de ce paramètre, vous pouvez préciser le mode de protection en temps réel. Le paramètre `ScanByAccessType` s'applique seulement aux tâches de protection en temps réel.

Valeurs possibles :

`SmartCheck` : analyser le fichier en cas de tentative d'ouverture et analyser de nouveau le fichier en cas de tentative de fermeture s'il a été modifié. Si un processus quelconque s'adresse plusieurs fois au fichier pendant un certain temps et le modifie, analyser de nouveau le fichier seulement lors de la dernière tentative de fermeture du fichier par ce processus.

`OpenAndModify` : analyser le fichier en cas de tentative d'ouverture et l'analyser de nouveau en cas de tentative de fermeture s'il a été modifié.

`Open` : analyser le fichier en cas de tentative d'ouverture en lecture, ainsi qu'en exécution ou modification.

Valeur par défaut : `SmartCheck`.

[ScanScope.item_#]

La section `[ScanScope.item_#]` contient les paramètres suivants :

AreaDesc

La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne précisée par ce paramètre est de 4096 caractères.

Valeur par défaut : `All objects`.

Exemple :

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

UseScanArea

Ce paramètre active / désactive l'analyse de la zone indiquée. Pour exécuter la tâche, il faut activer l'analyse d'au moins une zone.

Valeurs possibles :

`Yes` : analyse la zone indiquée ;

`No` : n'analyse pas la zone indiquée.

Valeur par défaut : `Yes`.

AreaMask

Ce paramètre permet de limiter la zone d'analyse.

Dans les zones d'analyse, Kaspersky Endpoint Security analyse uniquement les fichiers désignés à l'aide des masques au format de l'interpréteur de commande.

Si le paramètre n'est pas défini, Kaspersky Endpoint Security analyse tous les objets de la zone d'analyse. Vous pouvez indiquer plusieurs valeurs de ce paramètre.

Valeur par défaut : `*` (analyser tous les objets).

Exemple :

```
AreaMask=*doc
```

Path

Ce paramètre permet de désigner le chemin d'accès aux objets à analyser.

La valeur du paramètre `Path` comprend deux éléments : `<type de système de fichiers>:<protocole d'accès>`. Il peut également contenir le chemin d'accès au répertoire dans le système de fichiers local.

Valeurs possibles :

`<chemin d'accès au répertoire local>` : analyse les objets dans le répertoire indiqué ;

`Shared:NFS` : analyse les ressources du système de fichiers de l'ordinateur accessibles via le protocole NFS ;

`Shared:SMB` : analyse les ressources du système de fichiers de l'ordinateur accessibles via le protocole SMB ;

`AllRemoteMounted` : analyse tous les répertoires distants montés sur l'ordinateur via les protocoles SMB et NFS ;

`AllShared` :analyse toutes les ressources du système de fichiers de l'ordinateur accessibles via les protocoles SMB et NFS.

[ExcludedFromScanScope.item_#]

La section `[ExcludedFromScanScope.item_#]` contient les paramètres suivants :

AreaDesc

Description de la zone d'exclusion de l'analyse. Contient des informations complémentaires sur la zone d'exclusion.

Valeur par défaut : non spécifié.

Exemple :

```
AreaDesc="Exclusion des fichiers SAMBA fragmentés"
```

UseScanArea

Ce paramètre active/désactive l'analyse de la zone indiquée.

Valeurs possibles :

`Yes` : exclut la zone indiquée ;

`No` : n'exclut pas la zone indiquée.

Valeur par défaut : `Yes`.

Path

Ce paramètre permet de définir le chemin d'accès aux objets à exclure.

La valeur du paramètre `Path` comprend deux éléments : `<type de système de fichiers>:<protocole d'accès>`. Il peut également contenir le chemin d'accès au répertoire dans le système de fichiers local.

Valeurs possibles :

`<chemin d'accès au répertoire local>` : exclut les objets du répertoire indiqué de l'analyse ;

`Shared:NFS` : exclut les ressources du système de fichiers de l'ordinateur accessibles via le protocole NFS de l'analyse ;

`Shared:SMB` : exclut les ressources du système de fichiers de l'ordinateur accessibles via le protocole SMB de l'analyse ;

`AllRemoteMounted` : exclut tous les répertoires distants montés sur l'ordinateur via les protocoles SMB et NFS de l'analyse ;

`AllShared` : exclut toutes les ressources du système de fichiers de l'ordinateur accessibles via les protocoles SMB et NFS de l'analyse.

Paramètres des tâches d'analyse des secteurs d'amorçage et des tâches d'analyse de la mémoire des processus

Vous pouvez configurer le fonctionnement des tâches d'analyse des secteurs d'amorçage et d'analyse de la mémoire des processus en modifiant les paramètres dans les fichiers de configuration de ces tâches.

Les paramètres des fichiers de configuration ont les valeurs suivantes :

UseExcludeMasks

> Le paramètre n'est pas utilisé dans la tâche d'analyse de la mémoire des processus.

Active/désactive l'exclusion de l'analyse des objets désignés par le paramètre `ExcludeMasks`.

Valeurs possibles :

`Yes` : exclut les objets désignés par le paramètre `ExcludeMasks`.

`No` : n'exclut pas les objets désignés par le paramètre `ExcludeMasks`.

Valeur par défaut : `No`.

ExcludeMasks

> Le paramètre n'est pas utilisé dans la tâche d'analyse de la mémoire des processus.

Exclut de l'analyse les objets en fonction des noms ou des masques. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide des masques de l'interpréteur de commandes.

Valeur par défaut : non spécifié.

UseExcludeThreats

Active ou désactive l'exclusion de l'analyse les objets contenant les menaces indiquées par le paramètre `ExcludeThreats`.

Valeurs possibles :

`Yes` : exclut de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats` ;

`No` : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats`.

Valeur par défaut : `No`.

ExcludeThreats

Exclut de l'analyse les objets en fonction des noms des menaces détectées dans les objets. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.

Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, une ligne de conclusion pour Kaspersky Security indiquant que l'objet est infecté.

Par exemple, vous utilisez un des utilitaires pour obtenir des informations sur le réseau. Pour que Kaspersky Endpoint Security ne le bloque pas, ajoutez le nom complet de la menace qu'elle comporte à la liste des menaces exclues de l'analyse.

Le nom complet de la menace détectée dans l'objet est repris dans le journal de Kaspersky Endpoint Security. Vous pouvez également trouver le nom complet de la menace sur le site Internet de l'Encyclopédie des virus (http://www.securelist.fr). Pour trouver le nom d'une menace, saisissez le nom de l'application dans le champ **Rechercher**.

La valeur du paramètre est sensible à la casse.

Valeur par défaut : non spécifié.

ReportCleanObjects

Active/désactive l'enregistrement dans le journal des informations sur les objets analysés que Kaspersky Endpoint Security a reconnus comme non infectés.

Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par Kaspersky Endpoint Security.

Valeurs possibles :

`Yes` : enregistre les informations relatives aux objets non infectés dans le journal ;

`No` : n'enregistre pas les informations relatives aux objets non infectés dans le journal.

Valeur par défaut : `No`.

UseAnalyzer

> Le paramètre n'est pas utilisé dans la tâche d'analyse de la mémoire des processus.

Active / désactive l'analyse heuristique.

Valeurs possibles :

`Yes` : active l'analyse heuristique ;

`No` : désactive l'analyse heuristique.

Valeur par défaut : `Yes`.

HeuristicLevel

> Le paramètre n'est pas utilisé dans la tâche d'analyse de la mémoire des processus.

Niveau de l'analyse heuristique.

Valeurs possibles :

`Light` – analyse moins minutieuse, charge minimale du système ;

`Medium` – niveau moyen de l'analyse heuristique, charge équilibrée du système ;

`Deep` – analyse plus minutieuse, charge maximale du système ;

`Recommended` – valeur recommandée.

Valeur par défaut : `Recommended`.

Action

Sélection de l'action exécutée par Kaspersky Endpoint Security sur les objets infectés.

Valeurs possibles :

`Cure` (désinfecter) : Kaspersky Endpoint Security tente de désinfecter l'objet après avoir enregistré une copie de celui-ci dans la Sauvegarde. Si la désinfection est impossible (par exemple, le type de l'objet ou le type de menace ne se prête pas à la désinfection), Kaspersky Endpoint Security laisse l'objet en l'état.

`Skip` (ignorer) : Kaspersky Endpoint Security ne tente pas de désinfecter ou de supprimer l'objet infecté. Les informations sur l'objet infecté sont conservées dans le journal.

Valeur par défaut : `Cure`.

Paramètres des tâches de mise à jour et des tâches de copie des mises à jour

Vous pouvez configurer le fonctionnement des tâches de mise à jour et des tâches de copie des mises à jour en modifiant les paramètres dans les fichiers de configuration de ces tâches.

Le fichier de configuration des tâches de mise à jour et des tâches de copie des mises à jour comprend différents paramètres et la section `[CustomSources.item_#]`. Dans cette section, vous pouvez configurer les paramètres des sources utilisateur de mise à jour. Si vous voulez renseigner plusieurs sources de mises à jour définies par l'utilisateur, il faut décrire chacune d'entre elles dans une section `[CustomSources.item_#]` séparée. Kaspersky Endpoint Security utilise ces paramètres au moment de l'accès aux sources de mise à jour définies par l'utilisateur.
Cette section est facultative.

Paramètres généraux des tâches de mise à jour et des tâches de copie des mises à jour

Les fichiers de configuration des tâches de mise à jour et des tâches de copie des mises à jour contiennent les paramètres suivants :

SourceType

Ce paramètre permet de choisir la source sur laquelle Kaspersky Endpoint Security va récupérer les mises à jour.

Valeurs possibles :

KLServers : Kaspersky Endpoint Security reçoit les mises à jour depuis un des serveurs de mise à jour de Kaspersky Lab. Les mises à jour sont chargées selon le protocole HTTP.

`SCServer` : Kaspersky Endpoint Security télécharge les mises à jour sur l'ordinateur protégé à partir du Serveur d'administration de Kaspersky Security Center installé sur le réseau local. Vous pouvez sélectionner cette source si vous utilisez l'application Kaspersky Security Center pour assurer l'administration centralisée de la protection antivirus des ordinateurs de votre entreprise.

`Custom` : Kaspersky Endpoint Security télécharge les mises à jour à partir d'une source définie par l'utilisateur dans la section `[CustomSources.item_#]` (cf. section "`[CustomSources.item_#]`" à la page 146). Vous pouvez désigner des répertoires de serveurs HTTP, des répertoires sur n'importe quel périphérique monté d'un ordinateur protégé, y compris des répertoires sur des ordinateurs distants montés via les protocoles Samba ou NFS.

Valeur par défaut : `KLServers`.

UseKLServersWhenUnavailable

Ce paramètre permet de configurer l'accès de Kaspersky Endpoint Security aux serveurs de mise à jour de Kaspersky Lab si toutes les sources définies par l'utilisateur sont inaccessibles.

Valeurs possibles :

`Yes` : Kaspersky Endpoint Security contacte les serveurs de mise à jour de Kaspersky Lab si toutes les sources de mise à jour définies par l'utilisateur sont inaccessibles ;

`No` : Kaspersky Endpoint Security ne contacte pas les serveurs de mise à jour de Kaspersky Lab si toutes les sources de mise à jour définies par l'utilisateur sont inaccessibles.

Valeur par défaut : `Yes`.

IgnoreProxySettingsForKLServers

A l'aide de ce paramètre, vous pouvez configurer l'utilisation du serveur proxy pour vous connecter aux serveurs de mise à jour de Kaspersky Lab.

Valeurs possibles :

`Yes` : Kaspersky Endpoint Security n'utilise par le serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky Lab ;

`No` : Kaspersky Endpoint Security utilise le serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky Lab.

Valeur par défaut : `No`.

IgnoreProxySettingsForCustomSources

A l'aide de ce paramètre, vous pouvez configurer l'utilisation du serveur proxy pour vous connecter aux sources utilisateur de mise à jour. Vous devez activer ce paramètre si l'accès à un serveur proxy est requis pour établir la connexion à un des serveurs de mise à jour HTTP personnalisé.

Valeurs possibles :

`Yes` : Kaspersky Endpoint Security n'utilise pas le serveur proxy pour se connecter aux sources de mise à jour définies par l'utilisateur ;

`No` : Kaspersky Endpoint Security utilise le serveur proxy pour se connecter aux sources de mise à jour définies par l'utilisateur ;

Valeur par défaut : `No`.

ConnectionTimeout

Ce paramètre permet de définir le délai d'attente (en secondes) de la réponse depuis le serveur HTTP défini comme source de mise à jour en cas de connexion à celle-ci. Si la source de mises à jour n'a pas répondu à l'issue de la période de temps indiquée, Kaspersky Endpoint Security contacte une autre source de mise à jour indiquée.

Vous pouvez indiquer uniquement des nombres entiers compris entre 0 et 120.

Valeur par défaut : `10`.

RetranslationFolder

Le paramètre est accessible uniquement pour les tâches de copie des mises à jour.

Ce paramètre permet de définir le paramètre dans lequel les mises à jour seront copiées. Si le répertoire indiqué n'existe pas, Kaspersky Endpoint Security le crée pendant l'exécution de la tâche de copiage des mises à jour.

[CustomSources.item_#]

La section `[CustomSources.item_#]` contient les paramètres suivants :

URL

A l'aide de ce paramètre, vous pouvez indiquer l'adresse de la source utilisateur de mise à jour sur le réseau local ou sur Internet.

Valeur par défaut : non spécifié.

Exemples :

`URL=http://example.com/bases/` – adresse du serveur HTTP sur lequel se trouve le répertoire contenant les mises à jour.

`URL =/home/bases/` – le répertoire qui contient les bases de l'application sur l'ordinateur protégé.

Enabled

Ce paramètre permet d'activer ou de désactiver l'utilisation de la source de mises à jour désignée par le paramètre `URL`. Pour exécuter la tâche, il faut utiliser au moins une source de mises à jour.

Valeurs possibles :

`Yes` : Kaspersky Endpoint Security utilise la source de mise à jour ;

`No` : Kaspersky Endpoint Security n'utilise pas la source de mise à jour.

Valeur par défaut : non spécifié.

Exemple :

```
Enabled=Yes
```

Paramètres du dossier de la Sauvegarde

Vous pouvez configurer le fonctionnement des tâches pour la Sauvegarde en modifiant les paramètres suivants dans les fichiers de configuration de ces tâches.

BackupFolder

Chemin d'accès à la sauvegarde. Vous pouvez préciser une répertoire de la sauvegarde autre que celui précisé par défaut.

En guise de répertoire de la Sauvegarde, vous pouvez utiliser des répertoires sur n'importe quel périphérique de l'ordinateur. Il est déconseillé de désigner des répertoires qui se trouvent sur des ordinateurs distants, par exemple des répertoires montés via les protocoles Samba et NFS.

Kaspersky Endpoint Security commence à placer les objets dans le répertoire indiqué après l'importation des paramètres du fichier dans la tâche pour la Sauvegarde et le relancement de Kaspersky Endpoint Security.

Si le répertoire précisé n'existe pas ou n'est pas disponible, Kaspersky Endpoint Security utilise le répertoire de sauvegarde par défaut.

Valeur par défaut :

```
/var/opt/kaspersky/kesl/objects-backup/
```

BackupSizeLimit

Taille maximale de la sauvegarde.

Quand la taille de la Sauvegarde atteint la valeur maximale définie, Kaspersky Endpoint Security supprime les objets les plus anciens.

Valeurs possibles : 0 à 999 999 (en mégaoctets).

Pour lever la restriction sur la taille de la Sauvegarde, attribuez la valeur 0.

Valeur par défaut : `0`.

DaysToLive

Durée de conservation des objets dans la Sauvegarde (en jours).

Pour lever la restriction sur la durée de conservation des objets dans la Sauvegarde, attribuez la valeur 0.

Valeur par défaut : 90.

Commandes d'administration de Kaspersky Endpoint Security via la ligne de commande

Cette section contient des informations sur les commandes d'administration de Kaspersky Endpoint Security à partir de la ligne de commande.

A propos de l'administration de Kaspersky Security via la ligne de commande

Vous pouvez modifier les valeurs des paramètres de Kaspersky Endpoint Security

Au moment de saisir les commandes de Kaspersky Endpoint Security, respectez les règles suivantes :

- Respectez le registre.
- Séparez les clés par le caractère " espace ".
- Au moment d'utiliser le nom complet de la commande ou de l'argument, saisissez la valeur après le signe "égal" (=).

Exemple :

Indiquer la valeur du paramètre URL pour la sources de mises à jour personnalisée pour la tâche de mise à jour (ID=6) de la ligne de commande :

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6
SourceType=Custom CustomSources.item_0000.URL=http://site.domain/path
CustomSources.item_0000.Enabled=Yes
```

Affichage de l'aide sur les commandes de Kaspersky Endpoint Security

`--help`

Affiche l'aide sur les commandes de Kaspersky Endpoint Security.

Affichage des événements de Kaspersky Endpoint Security

`-W`

Affiche les événements de Kaspersky Endpoint Security.

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

`-T`

Préfixe ; indique que la commande appartient au groupe des commandes d'administration des paramètres de Kaspersky Endpoint Security / d'administration des tâches (facultatif).

`[-S] --app-info`

Affiche les informations générales relatives à Kaspersky Endpoint Security.

`[-T] --get-app-settings --file <nom et répertoire du fichier>`

Renvoie les paramètres généraux de Kaspersky Endpoint Security.

`[-T] --set-app-settings --file <nom et répertoire du fichier>`

Définit les paramètres généraux de Kaspersky Endpoint Security.

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

Renvoie la liste des tâches existantes de Kaspersky Endpoint Security.

`[-T] --get-task-state <ID de la tâche>|<nom de la tâche>`

Affiche l'état de la tâche indiquée.

`[-T] --create-task <nom de la tâche> --type <type de la tâche> --file <nom et répertoire du fichier>`

Crée la tâche de type spécifié ; importe dans la tâche les paramètres depuis le fichier de configuration spécifié.

`[-T] --delete-task <ID de la tâche>|<nom de la tâche>`

Supprime la tâche.

`[-T] --start-task <ID de la tâche>|<nom de la tâche> [-W] [--progress] [--file <nom et répertoire du fichier>]`

Lance la tâche.

`[-T] --stop-task <ID de la tâche>|<nom de la tâche>`

Arrête la tâche.

`[-T] --suspend-task <ID de la tâche>|<nom de la tâche>`

Suspend la tâche.

`[-T] --resume-task <ID de la tâche>|<nom de la tâche>`

Reprend la tâche.

`[-T] --get-settings <ID de la tâche>|<nom de la tâche> --file <nom_et_répertoire du fichier>`

Fait afficher les paramètres de la tâche.

`[-T] --set-settings <ID de la tâche>|<nom de la tâche> [<paramètres>] [--file <nom et répertoire du fichier>] [--add-path <chemin>] [--del-path <chemin>] [--add-exclusion <exclusion>] [--del-exclusion <exclusion>]`

Installe les paramètres de la tâche.

`[-T] --scan-file <chemin> [--action <action>]`

Crée et lance la tâche temporaire `Scan_File`.

Commandes de gestion des clés

`-L`

Préfixe ; indique que la commande appartient au groupe des commandes de gestion des clés.

`[-L] --install-active-key <code d'activation>|<fichier clé>`

Ajoute la clé active.

`[-L] --install-additional-key <code d'activation>|<fichier clé>`

Ajoute une clé additionnelle.

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

Supprime la clé active.

`[-L] --revoke-additional-key`

Supprime la clé additionnelle.

`[-L] --query`

Affiche les informations relatives à la clé.

Commandes d'administration du répertoire de la Sauvegarde

`-B`

Préfixe ; indique que la commande appartient au groupe des commandes d'administration de la Sauvegarde.

`[-B] --mass-remove --query`

Purge la Sauvegarde complètement ou partiellement.

`[-B] --query --limit --offset`

Affiche les informations sur les objets de la sauvegarde.

`--limit`

Quantité maximale d'objets au sujet desquels des informations seront affichées.

`--offset`

Nombre d'entrées représentant le décalage à partir du début de la sélection.

`[-B] --restore <ID de l'objet> --file <nom et répertoire du fichier>`

Restaure l'objet depuis la Sauvegarde.

Instructions d'administration du journal des événements

`-E`

Préfixe ; indique que la commande appartient au groupe de commandes d'administration du journal des événements.

`[-E] --query --limit --offset --file <nom et répertoire du fichier> --db`

Quantité maximale d'événements au sujet desquels des informations seront affichées.

`--query`

Affiche le nombre d'événement filtrés du journal des événements ou du fichier de rotation indiqué.

`--offset`

Nombre d'entrées représentant le décalage à partir du début de la sélection.

`--db`

Nom du fichier de la base de données.

Commandes d'administration de la planification des tâches

`[-T] --set-schedule <ID de la tâche>|<nom de la tâche> --file <nom et répertoire du fichier>`

Détermine les paramètres de l'horaire de la tâche/les importe dans la tâche depuis le fichier de configuration.

`[-T] --get-schedule <ID de la tâche>|<nom de la tâche> --file <nom et répertoire du fichier>`

Fait afficher les paramètres de l'horaire de la tâche.

`RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR`

Planification du lancement d'une tâche.

`PS` : lance une tâche après le lancement de Kaspersky Endpoint Security.

`BR` : lance une tâche après la mise à jour des bases antivirus.

`StartTime=[année/mois/jour_du_mois] [hh]:[mm]:[ss]; [<jour_du_mois>|<jour_de_la_semaine>]; [<period>]`

Heure de lancement d'une tâche.

`RandomInterval=<min.>`

Intervalle du lancement de la tâche, si plusieurs tâches sont lancées simultanément (en minutes).

`ExecuteTimeLimit=<min.>`

Restriction du temps d'exécution de la tâche (en minutes).

`RunMissedStartRules`

Active/désactive le lancement d'une tâche ignorée après le lancement Kaspersky Endpoint Security.

Affichage de l'aide sur les commandes de Kaspersky Endpoint Security

La commande kesl-control avec l'argument `--help` <sélection de commandes de Kaspersky Endpoint Security> affiche l'aide sur les commandes de Kaspersky Endpoint Security.

Syntaxe de la commande

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

<ensemble de commandes de Kaspersky Endpoint Security>

Valeurs possibles :

`[-T]` :commandes d'administration des tâches et des paramètres généraux de Kaspersky Endpoint Security ;

`[-L]` : commandes de gestion des clés ;

`[-B]` : commandes d'administration de la Sauvegarde ;

`[-E]` : commandes d'administration des événements de Kaspersky Endpoint Security.

Activation de l'affichage des événements

La commande `-W` active le mode d'affichage des événements de Kaspersky Endpoint Security. Vous pouvez utiliser cette commande séparément pour afficher tous les événements de Kaspersky Endpoint Security, mais également avec la commande `--start-task` (lancer la tâche (cf. section "Lancement et arrêt de la tâche" à la page 53)) pour afficher uniquement les événements

relatifs à la tâche exécutée. Vous pouvez utiliser `--query` avec l'attribut -W pour afficher certains événements uniquement.

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

Syntaxe de la commande

```
kesl-control -W
```

Exemples :

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

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

Analyse rapide des fichiers et des répertoires

La commande `--scan-file` crée et lance la tâche temporaire `Scan_File`. Kaspersky Endpoint Security supprime la tâche quand l'exécution de celle-ci est terminée ou après le relancement de l'application.

Syntaxe de la commande

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

Description des arguments et des clés

`--scan-file <chemin d'accès au fichier ou au répertoire>`

Nom du fichier ou du répertoire qui vont être soumis à l'analyse rapide de Kaspersky Endpoint Security. Vous pouvez ajouter jusqu'à 100 fichiers ou répertoires pour l'analyse.

`--action <action>`

Clé facultative.

Valeurs possibles :

`Recommended` – exécuter l'action recommandée.

`Cure` – réparer.

`Remove` – supprimer.

`Skip` – ignorer.

Valeur par défaut : `Skip`.

Consultation des informations sur le programme

La commande `--app-info` affiche les informations relatives à Kaspersky Endpoint Security.

Syntaxe de la commande

```
kesl-control [-S] --app-info
```

Résultat de l'exécution de la commande

`Name`

Nom Kaspersky Endpoint Security.

`License status`

Statut de la licence.

`License expiration date`

Date de fin de validité de la licence.

`Backup state`

Nombre d'objets dans la Sauvegarde.

`Backup usage space`

Taille de la Sauvegarde.

`Scan_My_Computer last run date`

Heure du dernier lancement de la tâche Scan_My_Computer.

`Anti-virus databases loaded`

Indique si les bases antivirus sont chargées ou non.

`Anti-virus databases date`

Indique la date du dernier chargement des bases antivirus.

`Anti-virus databases records`

Nombre d'enregistrements dans les bases antivirus.

`Protection status`

Etat de la protection de l'ordinateur.

`KSN state`

Etat de la connexion à Kaspersky Security Network.

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

Cette section contient des informations sur les commandes d'administration des paramètres de Kaspersky Endpoint Security et des tâches.

Obtention des paramètres généraux de Kaspersky Endpoint Security

La commande `--get-app-settings` permet d'afficher les paramètres généraux de Kaspersky Endpoint Security. Cette commande permet également d'obtenir les paramètres généraux de Kaspersky Endpoint Security définis à l'aide des arguments de la commande.

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 la commande `--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 la commande `--set-app-settings`. Kaspersky Endpoint Security utilise les nouvelles valeurs des paramètres après que vous avez arrêté, puis relancé Kaspersky Endpoint Security.

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

Syntaxe de la commande

```
kesl-control [-T] --get-app-settings [--file <nom du fichier de configuration>] kesl-control [-T] --get-app-settings [<nom du paramètre>]
```

Arguments et clés

`--file <nom du fichier de configuration>`

Nom du fichier de configuration dans lequel les paramètres de Kaspersky Endpoint Security vont être enregistrés. 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.

Exemples :

Exportez les paramètres généraux de Kaspersky Endpoint Security dans un fichier nommé kesl_config.ini. Enregistrer le fichier créé dans le répertoire en cours :

```
/opt/kaspersky/kesl/bin/kesl-control --get-app-settings --file kesl_config.ini
```

Affiche la valeur du paramètre TraceLevel :

```
/opt/kaspersky/kesl/bin/kesl-control --get-app-settings TraceLevel
```

Modification des paramètres généraux de Kaspersky Endpoint Security

La commande `--set-app-settings` détermine à l'aide des clés de la commande ou importe depuis le fichier de configuration indiqué les paramètres généraux de Kaspersky Endpoint Security.

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 la commande `--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 la commande --set-app-settings. Kaspersky Endpoint Security applique les nouvelles valeurs des paramètres après que vous avez arrêté, puis relancé 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

```
kesl-control [-T] --set-app-settings --file <nom du fichier de configuration>
```

```
kesl-control [-T] --set-app-settings <nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre>
```

Arguments et clés

```
--file <nom du fichier de configuration>
```

Le nom du fichier de configuration dont les paramètres vont être importés dans Kaspersky Endpoint Security ; contient le chemin d'accès complet au fichier.

Exemples :

Importez dans Kaspersky Endpoint Security les paramètres généraux depuis le fichier de configuration nommé /home/test/kav_config.ini :

```
/opt/kaspersky/kesl/bin/kesl-control --set-app-settings --file
/home/test/kav_config.ini
```

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

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

Paramètres de planification de la tâche

Cette section contient des informations sur les commandes de gestion de la planification 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. 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 la commande `--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`. Kaspersky Endpoint Security utilise les nouvelles valeurs des paramètres de planification immédiatement.

Syntaxe de la commande

```
kesl-control [-T] --get-schedule <ID de la tâche>|<nom de la tâche> [--file
```

<nom du fichier de configuration>]

kesl-control [-T] --get-schedule <ID de la tâche>|<nom de la tâche> <nom du paramètre>

Arguments et clés

<ID de la tâche>

Le numéro d'identification de la tâche dans Kaspersky Endpoint Security.

<nom de la tâche>

Nom de la tâche.

--file <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.

Exemples :

Enregistrer les paramètres de Kaspersky Endpoint Security dans le fichier nommé on_demand_schedule.ini. Enregistrer le fichier créé dans le répertoire en cours :

```
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 9 --file
on_demand_schedule.ini
```

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

```
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 9 RuleType
```

Modification des paramètres de l'horaire d'une tâche

La commande `--set-schedule` détermine à l'aide des clés de la commande les paramètres de l'horaire d'une tâche ou les importe depuis le fichier de configuration spécifié.

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 la commande `--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 `-T --set-schedule`. Kaspersky Endpoint Security utilise les nouvelles valeurs des paramètres de planification immédiatement.

Syntaxe de la commande

```
kesl-control --set-schedule <ID de la tâche>|<nom de la tâche> --file <nom du fichier de configuration>
kesl-control --set-schedule <ID de la tâche>|<nom de la tâche> <nom du paramètre>=<valeur du paramètre> <nom du paramètre>=<valeur du paramètre>
```

Arguments et clés

`<ID de la tâche>`

Le numéro d'identification de la tâche dans Kaspersky Endpoint Security.

`<nom de la tâche>`

Nom de la tâche.

`--file <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.

Exemple :

Importer dans la tâche portant'ID=9 les paramètres de planification depuis le fichier de configuration nommé /home/test/on_demand_schedule.ini :

```
/opt/kaspersky/kesl/bin/kesl-control --set-schedule 9 --file
/home/test/on_demand_schedule.ini
```

Commandes d'administration des tâches de Kaspersky Endpoint Security

Cette section contient des informations sur les commandes d'administration des tâches de Kaspersky Endpoint Security.

Création d'une tâche

La commande – `create-task` crée une tâche de mise à jour ou d'analyse à la demande.
La commande importe dans la tâche les paramètres du fichier de configuration indiqué et affiche le numéro d'identification de la tâche créée.

Syntaxe de la commande

```
kesl-control [-T] --create-task <nom de la tâche> --type <type de la tâche>
[--file <nom du fichier de configuration>]
```

Description et valeurs possibles des arguments et clés

`--create-task <nom de la tâche>`

Attribuer un nom à la tâche.

Le nom de la tâche doit commencer par une lettre de l'alphabet latin et doit être unique.
Le nom de la tâche peut contenir un nombre illimité de caractères ASCII.

`--type <type de tâche>`

Clé obligatoire.

Précisez le type de tâche à créer. Pour en savoir plus sur les valeurs possibles, consultez la section relative aux tâches de Kaspersky Endpoint Security (cf. section "A propos des tâches de Kaspersky Endpoint Security" à la page 51).

`--file <nom du fichier de configuration>`

Clé facultative.

Préciser le chemin d'accès complet au fichier de configuration existant.

Kaspersky Endpoint Security importe dans la tâche les paramètres définis dans ce fichier de configuration.

Exemple :

Créer une tâche d'analyse à la demande avec le nom Fridayscan. Importer dans la tâche les paramètres depuis le fichier de configuration /home/test/config_kesscanner.ini :

```
/opt/kaspersky/kesl/bin/kesl-control --create-task Fridayscan --type ODS --file /home/test/config_kesscanner.ini
```

Suppression d'une tâche

La commande `--delete-task` supprime la tâche de Kaspersky Endpoint Security portant le numéro d'identification ou le nom indiqué.

Vous ne pouvez pas supprimer les tâches personnalisées.

Syntaxe de la commande

```
kesl-control --delete-task <ID de la tâche>|<nom de la tâche>
```

Description des arguments

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

Exemple :

Supprimer la tâche avec ID=20 :

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

Lancement d'une tâche

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

Vous pouvez lancer les tâches des types OAS, ODS, BootScan, MemoryScan, Rollback, Retranslate et Update.

Cette instruction peut être exécutée avec l'argument -W (cf. page) et les informations relatives aux événements survenus pendant l'exécution de la tâche seront affichées sur la console ou dans un fichier. Après l'achèvement de la tâche, le suivi des événements cesse.

Syntaxe de la commande

```
kesl-control --start-task <ID de la tâche>|<nom de la tâche> --[progress]
```

Description des arguments et des clés

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

`--progress`

Afficher la progression de la tâche (sauf pour la tâche de protection en temps réel).

Exemples :

Lancer la tâche avec ID=6 :

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

Lancer la tâche avec le nom UpdateTask1 et afficher des informations sur les événements apparaissant pendant l'exécution de la tâche :

```
/opt/kaspersky/kesl/bin/kesl-control --start-task UpdateTask1 -W
```

Lancer la tâche d'analyse à la demande et afficher la progression de l'exécution de la tâche :

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 2 --progress
```

Arrêt d'une tâche

La commande `--stop-task` arrête la tâche avec le numéro d'identification ou le nom spécifié.

Vous pouvez arrêter les tâches de tous les types, à l'exception de Backup et License.

Cette instruction peut être exécutée avec l'argument -W (cf. page) et les informations relatives aux événements survenus pendant l'exécution de la tâche seront affichées sur la console ou dans un fichier. Après l'achèvement de la tâche, le suivi des événements cesse.

Syntaxe de la commande

```
kesl-control --stop-task <ID de la tâche>|<nom de la tâche>
```

Description des arguments

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

Exemples :

Arrêter la tâche avec ID=6 :

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

Arrêter la tâche avec le nom ODStask et afficher des informations sur les événements apparaissant pendant l'exécution de la tâche :

```
/opt/kaspersky/kesl/bin/kesl-control --stop-task ODStask -W
```

Suspension d'une tâche

La commande `--suspend-task`suspend la tâche avec le numéro d'identification ou le nom spécifié.

Vous pouvez arrêter les tâches des types Update, Retranslate, Rollback, ODS, BootScan et MemoryScan.

Syntaxe de la commande

```
kesl-control --suspend-task <ID de la tâche>|<nom de la tâche>
```

Description des arguments

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

Exemple :

Suspendre la tâche avec ID=19 :

```
/opt/kaspersky/kesl/bin/kesl-control --suspend-task 19
```

Reprise d'une tâche

La commande `--resume-task` reprend la tâche avec le numéro d'identification indiqué ou le nom spécifiée, tâche précédemment suspendue l'aide de la commande `--suspend-task`.

Vous pouvez reprendre les tâches des types Update, Retranslate, Rollback, ODS, BootScan et MemoryScan.

Syntaxe de la commande

```
kesl-control --resume-task <ID de la tâche>|<nom de la tâche>
```

Description des arguments

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

Exemple :

Reprendre la tâche avec ID=19 :

```
/opt/kaspersky/kesl/bin/kesl-control --resume-task 19
```

Consultation de l'état de la tâche

La commande `--get-task-state` renvoie l'état de la tâche spécifiée.

Syntaxe de la commande

```
kesl-control --get-task-state <ID de la tâche>|<nom de la tâche>
```

Description des arguments

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

Description du résultat de l'exécution de la commande

`Name`

Nom de la tâche.

L'utilisateur attribue à la tâche personnalisée un nom au moment de sa création. Kaspersky Endpoint Security attribue des noms aux tâches prédéfinies.

`ID`

Numéro d'identification de la tâche attribué par Kaspersky Endpoint Security lors de la création de la tâche.

`Type`

Type de tâche de Kaspersky Endpoint Security.

`State`

Etat de la tâche.

Exemple :

Consulter l'état de la tâche avec l'ID=1 :

```
/opt/kaspersky/kesl/bin/kesl-control --get-task-state 1
```

Exemple de résultat de l'exécution de la commande :

```
Name: File_Monitoring
ID: 1
Type: OAS
State: Started
```

Consultation de la liste des tâches de Kaspersky Endpoint Security

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

Syntaxe de la commande

```
kesl-control --get-task-list
```

Description du résultat de l'exécution de la commande

`Name`

Nom de la tâche.

L'utilisateur attribue à la tâche personnalisée un nom au moment de sa création. Kaspersky Endpoint Security attribue des noms aux tâches prédéfinies.

`ID`

Numéro d'identification de la tâche attribué par Kaspersky Endpoint Security lors de la création de la tâche.

`Type`

Type de tâche de Kaspersky Endpoint Security.

`State`

Etat de la tâche.

Obtention des paramètres d'une tâche

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 le fichier de configuration sur un ordinateur et importer les paramètres depuis ce fichier de configuration dans la tâche du type correspondant sur un autre ordinateur.

Syntaxe de la commande

```
kesl-control --get-settings <ID de la tâche>|<nom de la tâche> [--file <nom du fichier de configuration>]
kesl-control --get-settings <ID de la tâche>|<nom de la tâche> <nom de la section du fichier INI>.<nom du paramètre>
```

Description et valeurs possibles des arguments et clés

`<ID de la tâche>`

Numéro d'identification de la tâche.

`<nom de la tâche>`

Nom de la tâche.

`--file <nom du fichier de configuration>`

Nom du fichier de configuration dans lequel seront enregistrés les paramètres de la tâche. Si vous ne spécifiez pas le chemin d'accès au fichier, celui-ci 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 INI.

Exemples :

Extraire les valeurs des paramètres de la tâche d'analyse à la demande :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2
```

Exporter les paramètres de la tâche d'analyse à la demande dans le fichier /home/test/configkesscanner.ini :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2 --file
/home/test/configkesscanner.ini
```

Exporter les paramètres de la tâche d'analyse à la demande dans le fichier configkesscanner.ini situé dans le répertoire actif :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2
--file configkesscanner.ini
```

Afficher la valeur du paramètre Path défini dans la tâche d'analyse à la demande :

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2 Path
```

Modification des paramètres de la tâche

La commande `--set-settings` définit les paramètres de la tâche à l'aide des clés ou les importe depuis le fichier de configuration.

Vous pouvez importer les paramètres du fichier de configuration dans tous les types de tâches (utilisateur et prédéfinies). Kaspersky Endpoint Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche de protection en temps réel. Dans autres types de tâches, Kaspersky Endpoint Security applique les nouvelles valeurs des paramètres au prochain lancement de la tâche.

Syntaxe de la commande

```
kesl-control --set-settings <ID de la tâche>|<nom de la tâche>}
[<paramètre>] [--file <nom du fichier de configuration>] [--add-path
<chemin>] [--del-path <chemin>] [--add-exclusion <chemin>]
[--del-exclusion <chemin>]
```

Description et valeurs possibles des arguments et clés

`<ID de la tâche>`

Le numéro d'identification de la tâche (ID). Pour consulter les numéros d'identification des tâches de Kaspersky Endpoint Security, utilisez la commande `--get-task-list` (cf. page 170).

`<nom de la tâche>`

Nom de la tâche.

`--file <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.

`--add-path <chemin>`

Ajoute la section `[ScanScope.item_#]` au fichier de configuration de la tâche avec le paramètre défini `Path=<chemin>` et `UseScanArea=Yes`.

`--del-path <chemin>`

Supprime la section `[ScanScope.item_#]` du fichier de configuration de la tâche pour le chemin indiqué.

`--add-exclusion <chemin>`

Ajoute la section `[ExcludedFromScanScope.item_#]` au fichier de configuration de la tâche avec le paramètre défini `Path=<chemin>` et `UseScanArea=Yes`.

`--del-exclusion <chemin>`

Supprimer la section `[ExcludedFromScanScope.item_#]` du fichier de configuration de la tâche pour le chemin indiqué.

Exemples :

Définir la valeur URL pour la source de mises à jour personnalisée dans la tâche de la mise à jour portant l'ID=6 :

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6
SourceType=Custom CustomSources.item_0000.URL=http://site.domain/pa
th CustomSources.item_0000.Enabled=Yes
```

Ajouter une zone d'analyse au fichier de configuration de la tâche d'analyse à la demande :

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 2 --add-path
/home
```

Suite à l'exécution de la commande, la section suivante est ajoutée au fichier de configuration :

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Commandes de gestion des clés

Cette section contient des instructions sur l'affichage des informations sur les licences et les actions à effectuer sur les clés.

Ajout d'une clé active

La commande `--install-active-key` ajoute une clé active. Pour en savoir plus sur les clés, lisez la section "A propos de la clé" (cf. section "A propos de la clé" à la page 43).

Syntaxe de la commande

```
kesl-control [-L] --install-active-key <chemin d'accès au fichier clé>|<code d'activation>
```

Arguments et clés

```
<chemin d'accès au fichier clé>
```

Chemin d'accès au fichier clé ; si le fichier clé se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

Exemple :

Ajouter une clé depuis le fichier /home/test/00000001.key en tant que clé active :

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

Ajout d'une clé additionnelle

La commande `--install-additional-key` ajoute une clé active. Pour en savoir plus sur les clés, lisez la section "A propos de la clé" (cf. section "A propos de la clé" à la page 43).

Si la clé active n'est pas installée, la clé additionnelle est installée comme clé principale.

Syntaxe de la commande

```
kesl-control [-L] --install-additional-key <chemin d'accès au fichier clé>
```

Arguments et clés

```
<chemin d'accès au fichier clé>
```

Chemin d'accès au fichier clé ; si le fichier clé se trouve dans le répertoire actuel, il suffit de saisir seulement le nom du fichier.

Exemple :

Installer la clé additionnelle depuis le fichier /home/test/00000002.key :

```
/opt/kaspersky/kesl/bin/kesl-control --install-additional-key
/home/test/00000002.key
```

Suppression d'une clé active

La commande `--revoke-active-key` supprime la clé active.

Syntaxe de la commande

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

Suppression d'une clé additionnelle

La commande `--revoke-additional-key` supprime la clé additionnelle.

Syntaxe de la commande

```
kesl-control [-L] --revoke-additional-key
```

Saisie d'un code d'activation supplémentaire

La commande `--install-additional-key` saisie un code d'activation supplémentaire.

Pour plus d'informations sur les codes d'activation, lisez la section "A propos du code d'activation" (cf. page 42).

Syntaxe de la commande

```
kesl-control [-L] --install-additional-key <code d'activation>
```

Commandes d'administration du répertoire de la Sauvegarde

Cette section contient des informations sur les commandes de gestion de la Sauvegarde.

Obtention des informations sur les objets du répertoire de sauvegarde

La commande `--query` affiche des informations sur les objets actuellement situés dans la Sauvegarde. Vous pouvez utiliser des filtres.

Syntaxe de la commande

```
kesl-control [-B] --query "<expression logique>" [--limit=<nombre d'entrée maximum>] [--offset=<écart du début de la sélection>]
```

Arguments et clés

`"<expression logique>"`

Installe le filtre : expression logique.

`--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.

Exemples :

Consulter les informations relatives aux objets dont le nom de fichier ou le chemin contiennent le mot test dans la Sauvegarde :

```
/opt/kaspersky/kesl/bin/kesl-control -B --query "FileName like '%test%'"
```

Restauration des objets depuis le répertoire de sauvegarde

La commande `--restore` restaure depuis la sauvegarde l'objet avec le numéro d'identification indiqué.

> La date et l'heure de création du fichier restauré à partir de la sauvegarde sont différentes de la date et de l'heure de création du fichier source.

Syntaxe de la commande

```
kesl-control [-B] --restore <identifiant de l'objet dans la Sauvegarde>
[--file <nom du fichier et chemin d'accès au fichier>]
```

Arguments et clés

`<numéro d'identification de l'objet>`

Pour obtenir l'identifiant de l'objet, vous pouvez exécuter la commande `-B --query`.

`--file <nom du fichier>`

Le nom sous lequel Kaspersky Endpoint Security enregistre l'objet lors de la restauration. Inclut le chemin d'accès au fichier.

Si le chemin d'accès au fichier n'est pas indiqué, Kaspersky Endpoint Security enregistre le fichier dans le répertoire actif.

Si le répertoire indiqué n'existe pas, Kaspersky Endpoint Security le crée.

Si cette clé n'est pas définie, Kaspersky Endpoint Security enregistre l'objet dans l'emplacement d'origine, dans un fichier portant le nom d'origine.

Exemples :

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

```
/opt/kaspersky/kesl/bin/kesl-control -[B] --restore 1
```

Pour restaurer l'objet avec ID=1 dans le répertoire en cours, dans le fichier avec le nom restored.exe :

```
/opt/kaspersky/kesl/bin/kesl-control --restore 1 --file restored.exe
```

Restaurer l'objet avec l'indication du nouveau nom et de l'emplacement :

```
/opt/kaspersky/kesl/bin/kesl-control --restore 1 --file
/newpath/newfile
```

Codes de retour de la ligne de commande

Cette section décrit les codes de retour de la ligne de commande.

0 : réussite de l'exécution de la commande/de la tâche ;

1 : erreur générale dans les arguments de la commande ;

2 : erreur dans les configurations de l'application transmises ;

64 : Kaspersky Endpoint Security n'est pas lancé ;

66 : les bases antivirus ne sont pas chargées (utilisé uniquement par la commande `--app-info`) ;

67 : échec de l'activation 2.0 suite à des problèmes de réseau ;

68 : impossible d'exécuter la commande car l'application est couverte par une stratégie ;

128 : erreur inconnue ;

65 : toutes les autres erreurs.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre diverses menaces dont les virus et autres programmes malveillants, le courrier indésirable (spam), les attaques de réseau et les attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie ("IDC Endpoint Tracker 2014").

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est un groupe international d'entreprises avec 38 bureaux dans 33 pays. La société emploie plus de 3000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection de l'information sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des équipements gérés par l'automatisation industrielle et la prévention des escroqueries financières. L’utilisation de ces solutions combinée à des outils d’administration centralisés permet de mettre en place et d’exploiter une protection efficace et automatisée de toute organisation, quelle que soit sa taille, contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, créent les outils de détection et de

désinfection de ces menaces et ajoutent les signatures de ces menaces aux bases utilisées par les applications de Kaspersky Lab.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu ou ZyXEL. De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 400 millions d'utilisateurs. Elle compte également plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.fr
L'Encyclopédie des virus :	https://securelist.fr/
Laboratoire antivirus :	http://newvirus.kaspersky.com/fr (pour l'analyse des fichiers et des sites suspects)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

Informations sur le code tiers

Les informations sur le code tiers se trouvent dans le fichier legal_notices.txt, situé dans le répertoire d'installation de l'application.

Notice sur les marques de commerce

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Core est une marque d'Intel Corporation déposée aux Etats-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans autres pays.

Microsoft, Outlook, Visual C++ et Windows sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Novell est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

Red Hat, Red Hat Enterprise Linux et CentOS sont des marques de Red Hat Inc., déposées aux Etats-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc.

SUSE est une marque de SUSE LLC déposée aux Etats-Unis et dans d'autres pays.

Glossaire

A

Agent d'administration

Module de l'application Kaspersky Security Center et qui réalise l'interaction entre le Serveur d'administration et les applications de Kaspersky Lab installées sur un nœud spécifique du réseau (poste de travail ou serveur). Ce composant est unique pour toutes les applications de Kaspersky Lab qui tournent sous le système d'exploitation Windows®. Pour les applications qui tournent sous d'autres systèmes d'exploitation, il existe des versions dédiées de l'Agent d'administration.

Analyse heuristique

Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky Lab. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.

Les fichiers dans lesquels un code malveillant pendant l'analyse heuristique a été détecté sont à l'état infecté.

Analyse sur la base de signatures

Technologie d'identification des menaces qui utilise les bases de Kaspersky Endpoint Security contenant les descriptions des menaces connues et les méthodes de leur élimination. La protection à l'aide de cette méthode offre le niveau de sécurité admissible minimal. Conformément aux recommandations des spécialistes de Kaspersky Lab, cette méthode d'analyse est toujours activée.

Analyseur heuristique

Module de Kaspersky Endpoint Security qui exécute l'analyse heuristique.

B

Bases antivirus

Bases de données contenant des informations sur les menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les enregistrements dans les bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les bases antivirus sont créées par les experts de Kaspersky Lab et actualisées chaque heure.

C

Certificat de licence

Document fourni par Kaspersky Lab avec le fichier clé ou le code d'activation. Il contient des informations concernant la licence octroyée.

Clé active

Clé utilisée actuellement pour faire fonctionner l'application.

Clé complémentaire

Clé qui confirme le droit d'utilisation de l'application, mais non utilisée au moment présent.

Code d'activation

Code octroyé par Kaspersky Lab lors de la réception d'une licence d'évaluation ou lors de l'acquisition d'une licence commerciale d'utilisation de Kaspersky Endpoint Security. Ce code est indispensable pour activer l'application.

Le code d'activation est une suite de 20 caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

D

Désinfection d'objets

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Certains objets infectés ne peuvent pas être désinfectés.

E

Etat de la protection

Etat actuel de la protection. Il caractérise le niveau de la protection du périphérique.

Exclusion

L'exclusion est un objet exclu de l'analyse par une application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon le masque, une certaine zone (par exemple, un dossier ou un application), des processus d'applications ou des objets selon leur nom conformément à la classification de l'encyclopédie antivirus. Pour chaque tâche, vous pouvez spécifier les exclusions.

F

Faux positif

Situation où un objet non infecté est considéré par l'application de Kaspersky Lab comme infecté car son code évoque celui d'un virus.

Fichier de licence

Fichier présentant l'aspect xxxxxxxx.key, fourni par Kaspersky Lab lors de la réception de la licence d'évaluation ou de l'acquisition de la licence commerciale d'utilisation de Kaspersky Endpoint Security. Le fichier clé est nécessaire pour l'activation de l'application.

Fichier infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "coffre-fort" pour déployer et diffuser un objet malveillant. En règle générale, il s'agit de fichiers exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est assez élevé pour ces fichiers.

Fichier infecté

Fichier qui contient un code malveillant (pendant l'analyse, le code d'une application connue et présentant une menace a été détecté). Les experts de Kaspersky Lab vous déconseillent de manipuler de tels fichiers car ils risquent d'infecter votre ordinateur.

G

Groupe d'administration

Ensemble d'ordinateurs regroupés selon les fonctions exécutées et selon l'ensemble d'applications de Kaspersky Lab installé sur ces ordinateurs. Les ordinateurs sont regroupés pour en faciliter la gestion comme un tout unique. Un groupe peut contenir d'autres groupes. Des stratégies de groupe et des tâches de groupe peuvent être créées pour chaque application installée dans le groupe.

L

Le niveau de sécurité

Le niveau de sécurité est un ensemble prédéfini de paramètres de fonctionnement du composant.

M

Masque de fichier

Représentation du nom et de l'extension d'un fichier par des symboles génériques.

Pour créer un masque de fichier, vous pouvez utiliser tous les symboles autorisés dans les noms des fichiers y compris des symboles spéciaux :

- * : symbole qui remplace zéro symbole ou plus de n'importe quel type ;
- ? : symbole qui remplace n'importe quel symbole unique.

Rappelez-vous que le nom et l'extension d'un fichier sont toujours séparés par un point.

Mise à jour

Procédure du remplacement de fichiers/d'ajout de nouveaux fichiers (bases ou modules d'applications) reçus des serveurs de mise à jour de Kaspersky Lab.

P

Paramètres de l'application

Paramètres de fonctionnement de l'application, valables pour tous les types de ses tâches et servant au fonctionnement de l'application dans son ensemble, par exemple : paramètres de performances de l'application, paramètres de gestion des rapports, paramètres de la sauvegarde.

Paramètres de la tâche

Paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches.

Protection en temps réel des fichiers

Mode de fonctionnement pendant lequel l'application analyse des objets en temps réel pour y détecter la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, en écriture et en exécution ; elle analyse l'objet pour y détecter la présence de menaces. Les objets sains sont ignorés pour l'utilisateur ; les objets contenant des menaces, sont traités conformément aux paramètres de la tâche (désinfectés ou supprimés).

S

Sauvegarde de réserve

Dossier spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur première désinfection ou leur suppression.

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction d'enregistrement centralisé des informations sur les applications de Kaspersky Lab installées sur le réseau de la société et de gestion de ces applications.

Serveurs proxy

Service dans les réseaux informatiques qui permet aux clients d'adresser des requêtes indirectes à d'autres services du réseau. Le client se connecte d'abord au serveur proxy et envoie une requête à une ressource quelconque (par exemple, un fichier) située sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou renvoie la ressource à partir de son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peuvent être modifiées par le serveur proxy à des fins déterminées.

Source des mises à jour

Ressource contenant les mises à jour des bases antivirus de l'application Kaspersky Endpoint Security. Les serveurs des mises à jour de Kaspersky Lab, ainsi que le serveur HTTP, le serveur FTP, le dossier local ou de réseau peuvent servir de sources de mises à jour des bases antivirus.

Stratégie

La stratégie définit les paramètres de fonctionnement de l'application et l'accès à la configuration de l'application installée sur les ordinateurs d'un groupe d'administration. Pour chaque application, il est nécessaire de créer une stratégie. Vous pouvez créer un nombre illimité de stratégies différentes pour les applications installées sur les ordinateurs de chaque groupe d'administration mais, à l'intérieur d'un groupe d'administration, il n'est possible d'appliquer qu'une seule stratégie à la fois à chaque application.

T

Tâche

Fonctions exécutées par une application de Kaspersky Lab et réalisées sous la forme de tâches, par exemple : protection en temps réel des fichiers, analyse complète du périphérique et mise à jour des bases de données.

Tâche de groupe

Tâche définie pour un groupe d'administration et exécutée sur tous les périphériques clients de ce groupe d'administration.

Tâche pour un ensemble de périphériques

Tâche définie pour un ensemble de périphériques clients provenant de groupes d'administration aléatoires et exécutée sur ceux-ci.

Index

A

B

C

E

C

L

S

M

N

S

T

Z