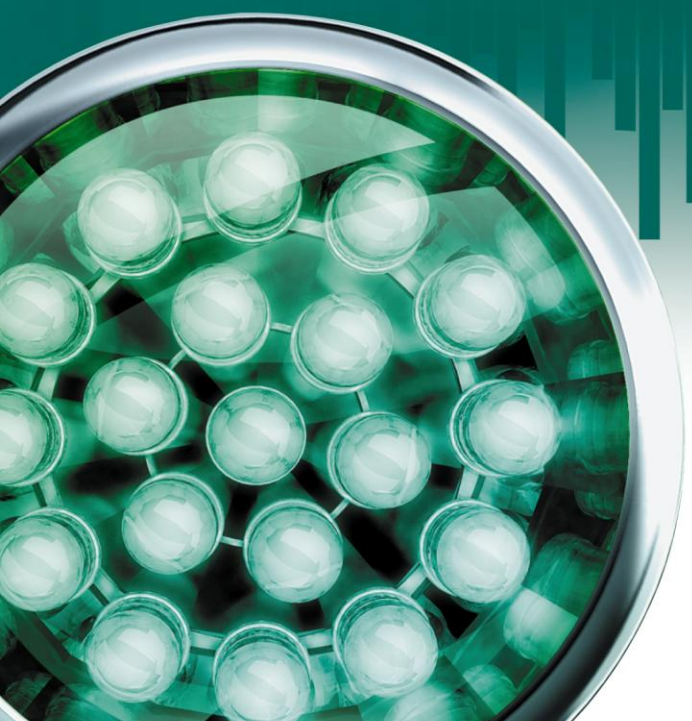
Kaspersky Endpoint Security 8 for Linux

MANUEL D'INSTALLATION

VERSION DU LOGICIEL: 8.0



KASPERSKY lab

Chers utilisateurs!

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

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

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

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

TABLE DES MATIÈRES

INTRODUCTION

Ce manuel décrit l'installation de l'application Kaspersky Endpoint Security 8 for Linux (ci-après — *Kaspersky Endpoint Security* ou *application*).

Tous les exemples d'instruction repris ci-après dans ce document sont pour les systèmes Linux.

DANS CETTE SECTION

FONCTIONS DE L'APPLICATION

L'application Kaspersky Endpoint Security 8 for Linux est destinée à la protection antivirus des postes de travail fonctionnant sous un système d'exploitation Linux.

Kaspersky Endpoint Security permet les points suivants:

- assurer la protection en temps réel du système de fichiers du postes de travail contre un code malveillant – intercepter les requêtes aux fichiers; les analyser; réparer ou supprimer les objets infectés;
- analyser à la demande les objets sur le poste de travail: rechercher les objets infectés ou suspects dans des secteurs d'analyse prédéterminés; les analyser; réparer ou supprimer les objets infectés;
- placer les objets infectés et suspects en quarantaine;
- créer des copies des objets infectés dans le répertoire de sauvegarde avant leur réparation ou suppression en vue d'une éventuelle réparation des objets qui sont importants du point de vue du contenu informatique;
- actualiser les bases (les serveurs de mise à jour ou le Serveur d'administration de Kaspersky Lab sont des sources pour les mises à jour; de même, il est possible de configurer Kaspersky Endpoint Security de sorte que les bases soient mises à jour depuis le répertoire local);
- administrer l'application et configurer son fonctionnement à l'aide de l'utilitaire d'administration, Kaspersky Administration Kit.

CONFIGURATION MATÉRIELLE ET LOGICIELLE REQUISES

Pour le fonctionnement de Kaspersky Endpoint Security, le système doit être conforme aux exigences matérielle et logicielle suivantes:

- Configuration matérielle requise:
  - processeur Intel Pentium® II 400 MHz ou supérieur;
  - 512 Mo de mémoire vive;

- rubrique de téléchargement avec au moins 1 Go d'espace libre;
- 2 Go du disque dur pour l'installation de Kaspersky Endpoint Security et sauvegarde des fichiers temporaires et des fichiers des registres.

- Configuration logicielle:
  - pour la plate-forme de 32 bits, un des systèmes d'exploitation suivants:
    - Red Hat Enterprise Linux 5.5 Desktop;
    - Fedora 13;
    - CentOS-5.5;
    - SUSE Linux Enterprise Desktop 10 SP3;
    - SUSE Linux Enterprise Desktop 11 SP1;
    - openSUSE Linux 11.3;
    - Mandriva Linux 2010 Spring;
    - Ubuntu 10.04 LTS Desktop Edition;
    - Debian GNU/Linux 5.0.5.
  - pour la plate-forme de 64 bits, un des systèmes d'exploitation suivants :
    - Red Hat Enterprise Linux 5.5 Desktop;
    - Fedora 13;
    - CentOS-5.5;
    - SUSE Linux Enterprise Desktop 10 SP3;
    - SUSE Linux Enterprise Desktop 11 SP1;
    - openSUSE Linux 11.3;
    - Ubuntu 10.04 LTS Desktop Edition;
    - Debian GNU/Linux 5.0.5.
  - Processeur du langage Perl version 5.0 ou supérieure http://www.perl.org
  - Paquets installés pour la compilation des applications (gcc, binutils, glibc (pour les systèmes d'exploitation de 64 bits, c'est la version glibc de 32 bits qui est utilisée), glibc-devel, make, ld), ainsi que le code du nœud d'origine installé du système d'exploitation: pour la compilation des modules de Kaspersky Endpoint Security.

OBTENTION D'INFORMATIONS SUR KASPERSKY ENDPOINT SECURITY

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

Si vous avez déjà acheté Kaspersky Endpoint Security, vous pouvez vous adresser au service du Support Technique. Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum au http://forum.kaspersky.fr.

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

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

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

La page sur le site Internet de Kaspersky Lab

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

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

Documentation

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

Le **Manuel d'administrateur** contient les informations sur l'administration de Kaspersky Endpoint Security à l'aide de l'utilitaire de la ligne de commande et de Kaspersky Administration Kit.

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

Manuels d'aide

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

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

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

- configuration des paramètres généraux de Kaspersky Endpoint Security:

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

- configuration de la tâche de protection en temps réel:

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

- configuration des tâches d'analyse à la demande:

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

- configuration des tâches de mise à jour:

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

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

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

- configuration des paramètres du référentiel des événements:

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

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

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

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

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

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

Si vous avez déjà acheté Kaspersky Endpoint Security, vous pouvez obtenir des renseignements sur ce produit auprès des ingénieurs du service du Support Technique.

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

Requête électronique adressée au Service du Support Technique

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

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

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

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

L'ingénieur du service du Support Technique, vous enverra sa réponse dans votre Espace personnel(https://support.kaspersky.com/fr/PersonalCabinet), ainsi qu'à l'adresse électronique que vous avez indiquée dans votre demande.

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

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

Assistance technique par téléphone

Si le problème est urgent, vous pouvez toujours téléphoner au service du Support Technique dans votre ville. Lorsque vous contactez les experts du Service du Support Technique russe (http://support.kaspersky.ru/support/support_local) ou international (http://support.kaspersky.com/fr/support/international), n'oubliez pas de fournir les informations relatives à Kaspersky Endpoint Security (http://support.kaspersky.com/fr/support/international) pour que nos experts puissent vous aider dans les délais les plus courts.

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

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

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

NOUVEAUTÉS DE LA VERSION 8

Regardons plus en détail les nouveautés de Kaspersky Endpoint Security 8 for Linux.

Nouveautés au niveau de la protection:

- Kaspersky Endpoint Security 8.0 réunit les fonctionnalités des versions du logiciel précédentes, de Kaspersky Anti-Virus 5.7 pour Linux Workstations et de Kaspersky Anti-Virus 5.5 pour Samba Servers grâce à l'utilisation des intercepteurs des opérations de fichier de deux types: intercepteur du niveau du nœud (kernel module) et intercepteur Samba;
- Les possibilités de l'administration de la quarantaine/du dossier de sauvegarde sont élargies. Elles permettent de:
  - mettre des objets en quarantaine manuellement;
  - chercher des objets mis en quarantaine (suivant les valeurs des propriétés des objets);
  - supprimer des objets trouvés;
  - restaurer des objets trouvés;
  - refaire l'analyse des objets;
  - sauvegarder une partie de la quarantaine/du répertoire de sauvegarde de réserve dans l'archive (pour diminuer le volume occupé);
  - importer des objets dans la quarantaine / le répertoire de sauvegarde de réserve depuis l'archive.

Nouveautés dans l'administration du fonctionnement de Kaspersky Endpoint Security:

- Administration centralisée de Kaspersky Endpoint Security et de l'exécution des tâches d'analyse à la demande, de protection en temps réel et de mise à jour des bases de Kaspersky Endpoint Security.
- Sauvegarde centralisée des paramètres de fonctionnement de Kaspersky Endpoint Security.
- Les paramètres de fonctionnement de Kaspersky Endpoint Security ne sont plus sauvegardés dans les fichiers de configuration texte. Les fichiers texte ne sont utilisés que lors de la sauvegarde et de l'obtention des réglages depuis le répertoire de sauvegarde centralisé des paramètres.
- Il est possible de spécifier plusieurs zones d'analyse pour une seule tâche. Avec cela:

- les paramètres d'analyse peuvent être configurés individuellement pour chaque secteur;
- le secteur d'analyse peut être spécifié:
  - par le chemin d'accès complet dans le système de fichiers;
  - par le nom du dispositif;
  - par le type de l'accès réseau (Shared, Mounted);
  - par le protocole de l'accès réseau (SMB/CIFS, NFS);
  - par le nom de la ressource réseau (SAMBA share name, NFS shared folder);
- dans la spécification du secteur d'analyse, les expressions régulières de type ECMA-262 Extended sont prises en charge;

- Pour un secteur d'analyse, la possibilité de configurer la liste d'utilisateurs / de groupes, les opérations de fichiers au nom desquelles elles sont analysées par la tâche de protection en temps réel.
- La possibilité de configurer plusieurs règles d'exclusion pour un seul secteur d'analyse.
- La possibilité d'administrer à distance à l'aide de Kaspersky Administration Kit.
- La possibilité d'administrer à l'aide de l'interface d'administration locale de l'utilisateur, où vous pouvez effectuer les tâches suivantes:
  - voir l'état de la protection de l'ordinateur sur lequel vous avez installé Kaspersky Endpoint Security;
  - lancer les tâches d'analyse de l'ordinateur sur les virus et les tâches de mise à jour des bases, ainsi qu'administrer ces tâches;
  - voir les statistiques des tâches d'analyse à la demande et les tâches de protection en temps réel;
  - parcourir les événements dans le journal des événements.
- La possibilité de configurer les actions à effectuer sur des objets en fonction du type de la menace détectée.
- La possibilité de configurer en détail l'horaire du lancement/de l'arrêt des tâches.

Nouveautés dans les moyens de surveillance, de rapports et de statistiques du fonctionnement de Kaspersky Endpoint Security:

- Les possibilités de surveillance suivantes du fonctionnement de Kaspersky Endpoint Security sont améliorées:
  - moyens d'obtention des catégories d'information suivantes:
    - informations générales sur l'application;
    - informations sur la version des bases de Kaspersky Endpoint Security;
    - informations sur le statut de la licence;
    - informations sur le statut des composants de Kaspersky Endpoint Security;
    - informations sur les résultats du fonctionnement des tâches;
    - informations sur l'état de la quarantaine/du dossier de sauvegarde;
  - les moyens d'une analyse rétrospective du fonctionnement de Kaspersky Endpoint Security permettant d'effectuer:

- la collecte, le comptage et la sauvegarde des informations statistiques sur le fonctionnement de Kaspersky Endpoint Security;

- l'affichage des informations statistiques sur le fonctionnement de Kaspersky Endpoint Security recueillies durant la période de temps spécifiée par l'utilisateur;

- la recherche d'événements selon la base des critères donnés par l'utilisateur;

- le contrôle des aspects de fonctionnement de Kaspersky Endpoint Security suivants: création/lancement/arrêt des tâches, modification des paramètres du fonctionnement du logiciel, des actions de l'utilisateur à effectuer pour des objets mis en quarantaine/dans le répertoire de stockage de réserve, etc.;

- les moyens de formation des rapports sur le fonctionnement de Kaspersky Endpoint Security à partir des statistiques collectées, moyens d'exportation des rapports (les formats HTML et CSV sont supportés);

- la surveillance du fonctionnement de Kaspersky Endpoint Security et de l'activité de virus. Les informations se trouvent dans le répertoire de sauvegarde centralisé des événements de Kaspersky Endpoint Security. Kaspersky Endpoint Security présente ses propres moyens pour la recherche, l'affichage et l'analyse des données sur son fonctionnement, ainsi que la possibilité d'utiliser des moyens extérieurs.

COMPOSITION DU KIT DE DISTRIBUTION

La composition du kit de distribution de Kaspersky Endpoint Security est donnée dans le tableau ci-dessous.

Le tableau 1. Paquets de Kaspersky Endpoint Security

PAQUET	FONCTION
kes4lwks-<numéro_de_version>.i386.rpm **kes4lwks_<numéro_de_version>_i386.deb**	Contient des fichiers de base de Kaspersky Endpoint Security. Le paquet peut être installé sous les systèmes d'exploitation de 32 bits et 64 bits.
klnagent-<numéro_de_version>.i386.rpm **klnagent_<numéro_de_version>_i386.deb**	Contient l'Agent d'administration (utilitaire de communication de Kaspersky Endpoint Security avec Kaspersky Administration Kit).
kes4lwks-rpm.tar.gz **kes4lwks-deb.tar.gz**	Contient des fichiers kes4lwks.kpd et akinstall.sh qui sont utilisés par le mode d'installation à distance de Kaspersky Endpoint Security à l'aide de Kaspersky Administration Kit.
klnagent-rpm.tar.gz **klnagent-deb.tar.gz**	Contient des fichiers klnagent.kpd et akinstall.sh qui sont utilisés par le mode d'installation à distance de l'Agent d'administration à l'aide de Kaspersky Administration Kit.

INSTALLATION DE KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security est distribué aux formats *.deb* et *.rpm*.

Le processus d'installation comprend plusieurs étapes:

1. Installation du paquet de Kaspersky Endpoint Security.
2. Installation de l'Agent d'administration (ce paquet doit être installé pour l'administration de Kaspersky Endpoint Security à l'aide de Kaspersky Administration Kit).

DANS CETTE SECTION

ETAPE 1. INSTALLATION DU PAQUET DE KASPERSKY ENDPOINT SECURITY

Avant d'installer Kaspersky Endpoint Security 8 for Linux, supprimez Kaspersky Anti-Virus 5.5 for Samba Servers ou Kaspersky Anti-Virus 5.7 for Linux qui sont installés sur l'ordinateur.

Le lancement du processus d'installation du paquet de Kaspersky Endpoint Security doit être effectué avec les droits du compte **root**.

Avant de procéder à l'installation de Kaspersky Endpoint Security, il faut installer le paquet glibc (pour les systèmes d'exploitation de 64 bits, c'est la version de 32 bits glibc qui est demandée).

- *Pour installer Kaspersky Endpoint Security depuis le paquet .rpm, exécutez la commande suivante:*

```
# rpm -i kes4lwks-<numéro_de_version>.i386.rpm
```

- *Pour installer Kaspersky Endpoint Security depuis le paquet .deb, exécutez la commande suivante:*

```
# dpkg -i kes4lwks_<numéro_de_version>_i386.deb
```

- *Endpoint Security depuis le paquet .deb sur un système d'exploitation de 64 bits, exécutez la commande suivante:*

```
# dpkg -i --force-architecture kes4lwks_<numéro_de_version>_i386.deb
```

Une fois la commande lancée, le processus d'installation sera exécuté automatiquement.

A la fin d'installation de Kaspersky Endpoint Security à partir du paquet rpm , il faut procéder au lancement du script de la configuration de post-installation (cf. rubrique "Configuration initiale de Kaspersky Endpoint Security" à la page 23).

ETAPE 2. INSTALLATION DE L'AGENT D'ADMINISTRATION

L'Agent d'administration doit être installé si vous envisagez d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Administration Kit.

Le lancement du processus d'installation de l'Agent d'administration doit être effectué avec les droits du compte **root**.

- *Pour installer l'Agent d'administration depuis le paquet .rpm, saisissez l'instruction suivante:*

  ```
  # rpm -i klnagent-<numéro_de_version>.i386.rpm
  ```

- *Pour installer l'Agent d'administration depuis le paquet .deb, saisissez l'instruction suivante:*

  ```
  # dpkg -i klnagent_<numéro_de_version>_i386.deb
  ```

- *Pour installer l'Agent d'administration depuis le paquet .deb sur un système d'exploitation de 64 bits, exécutez la commande suivante:*

  ```
  # dpkg -i --force-architecture klnagent_<numéro_de_version>_i386.deb
  ```

Une fois la commande lancée, le processus d'installation sera exécuté automatiquement.

A la fin d'installation de l'Agent d'administration à partir du paquet rpm, il faut procéder au lancement du script de la configuration de post-installation.

INSTALLATION DE KASPERSKY ENDPOINT SECURITY

Vous pouvez installer Kaspersky Endpoint Security à distance via la Console d'administration de Kaspersky Administration Kit. Pour pouvoir installer Kaspersky Endpoint Security à distance, créez la tâche d'installation à distance (voir section "Création de la tâche d'installation à distance" à la page 15) pour un groupe d'ordinateurs.

L'installation du logiciel à distance est effectuée par le mode *d'installation forcée* (voir Manuel de mise en œuvre de Kaspersky Administration Kit 8.0). L'installation forcée permet de réaliser l'installation à distance du logiciel sur les postes clients spécifiés du réseau logique. Lors de l'exécution de la tâche, le Serveur d'administration copie un groupe de fichiers pour l'installation de l'application depuis le dossier partagé vers chaque client dans un dossier temporaire, et lance le programme d'installation sur chacun d'entre eux.

L'Agent d'administration assure le lien entre le Serveur d'administration et le poste client. C'est pourquoi il doit être installé et configuré. Pour que l'installation à distance soit réussie, l'Agent d'administration doit être lancé sur l'ordinateur protégé.

Lors de la création des tâches d'installation à distance, les paquets d'installation (voir section "Création du paquet d'installation" à la page 19) sont utilisés. Le paquet d'installation est un ensemble de fichiers nécessaires pour l'installation du logiciel; ce paquet comprend les paramètres qui concernent le processus d'installation ainsi que la configuration initiale (voir page 23) du logiciel à installer. Le paquet d'installation peut être créé avant la création de la tâche d'installation à distance ou durant la création de cette dernière. Le même paquet d'installation peut être utilisé à plusieurs reprises.

Pour les systèmes d'exploitation utilisant dpkg, veillez à ce que le paquet d'installation soit créé à la base du paquet deb; pour les systèmes d'exploitation utilisant RPM, il doit être à la base du paquet rpm.

Tous les paquets d'installation formés pour les Serveurs d'administration se placent dans l'arborescence de la console dans le dossier **Stockages** → **Paquets d'installation**.

DANS CETTE SECTION

CRÉATION D'UNE TÂCHE D'INSTALLATION À DISTANCE

Afin de créer une tâche d'installation à distance pour la sélection d'ordinateurs à l'aide de l'installation forcée, procédez comme suit:

1. Connectez-vous au Serveur d'administration nécessaire.
2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de console.
3. Ouvrez le menu contextuel et sélectionnez **Nouveau** → **Tâche** ou sélectionnez la même action dans le menu **Action**.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.

ETAPES DE L'ASSISTANT

ETAPE 1. DÉFINITION DU NOM DE LA TÂCHE

Saisissez le nom de la tâche dans le champ **Nom**.

ETAPE 2. SÉLECTION DU TYPE DE LA TÂCHE

Dans le rubrique **Kaspersky Administration Kit**, sélectionnez le type de tâche **Installation à distance de l'application**.

ETAPE 3. SÉLECTION DU PAQUET D'INSTALLATION

Indiquez le paquet d'installation dont l'installation sera réalisée lors de l'exécution de cette tâche. Sélectionnez le paquet nécessaire parmi les paquets formés pour ce Serveur d'administration, ou saisissez un nouveau paquet à l'aide du bouton **Nouveau**. La création d'un nouveau paquet d'installation (voir section "Création du paquet d'installation" à la page 19) est effectuée à l'aide de l'Assistant de création du paquet d'installation.

ETAPE 4. SÉLECTION DU MODE D'INSTALLATION À DISTANCE

Sélectionnez l'option **Installation forcée**.

ETAPE 5. DÉFINITION DES PARAMÈTRES DE LA TÂCHE

A cette étape, il vous est proposé de définir s'il faut réinstaller l'application au cas où elle serait déjà installée sur l'ordinateur client. Cochez la case **Ne pas installer l'application sur des postes déjà équipés** afin de ne pas réinstaller l'application sur ces postes.

ETAPE 6. SÉLECTION DU PAQUET D'INSTALLATION POUR UNE INSTALLATION EN PARALLELE

Si vous voulez installer l'Agent d'administration avec l'application, cochez la case **Installer l'Agent d'administration avec cette application**, puis sélectionnez le paquet d'installation nécessaire.

➧ *Pour créer le nouveau paquet d'installation de l'Agent d'administration,*

cliquez sur **Créer**.

Finalement, l'Assistant de création d'un paquet d'installation s'ouvre (cf. section "Création du paquet d'installation" à la page 19). Suivez les instructions de l'Assistant.

ETAPE 7. CONFIGURATION DES PARAMÈTRES DE REDÉMARRAGE DES ORDINATEURS

Définissez les actions qu'il faut suivre s'il faut redémarrer l'ordinateur après l'installation du programme. Les options suivantes sont accessibles:

- **Ne pas redémarrer l'ordinateur**;
- **Redémarrer l'ordinateur** – lors de la sélection de cette option, le système d'exploitation n'est redémarré que si cela s'avère nécessaire;
- **Confirmer auprès de l'utilisateur** – en cas de sélection de cette variante, vous devez configurer les paramètres de notification de l'utilisateur sur le redémarrage.

Sélectionnez la variante **Ne pas redémarrer l'ordinateur**.

ETAPE 8. DÉFINITION DU MOYEN DE LA SÉLECTION D'ORDINATEURS

Définissez le mode de sélection des ordinateurs pour lesquels la tâche sera créée:

- **Sur la base des données obtenues lors du sondage du réseau Windows** – dans ce cas, les ordinateurs seront sélectionnés en fonction des données recueillies par le Serveur d'administration pendant son exploration du réseau Windows;
- **A la base des adresses (IP, NetBIOS ou nom DNS) saisies manuellement** – dans ce cas, le nom ou l'adresse IP des ordinateurs client doit être sélectionné ou saisi manuellement.

ETAPE 9. SÉLECTION DE POSTES CLIENTS

Lorsque les ordinateurs sont sélectionnés à la base des données reçues lors du sondage du réseau, la création de la liste est effectuée dans la fenêtre de l'Assistant. Pour la sélection, cochez les cases en regard du nom des postes clients des groupes d'administration (rubrique **Ordinateurs administrés**) ou des ordinateurs qui n'en font pas encore partie (rubrique **Ordinateurs non définis**).

Si la sélection d'ordinateurs s'effectue manuellement, alors la formation de la liste des adresses se réalise grâce à la saisie du nom NetBIOS ou du nom DNS, des adresses IP (ou de la plage des adresses IP) des ordinateurs, ou grâce à l'importation de la liste du fichier txt, dont chaque adresse doit être spécifiée par une nouvelle ligne (cf. ill. ci-après). Créez la liste des adresses en cliquant sur **Rajouter**, **Supprimer** et **Rajouter l'intervalle IP**, ou importez la liste depuis le fichier texte en cliquant sur **Importer**. À titre d'adresse de l'ordinateur, vous pouvez indiquer l'adresse IP (ou la plage d'adresses IP), un nom NetBIOS ou DNS. Pour importer la liste à partir d'un fichier, parcourez vos dossiers pour retrouver le fichier .txt contenant les adresses des ordinateurs ajoutés.

ETAPE 10. SÉLECTION DU COMPTE POUR LANCER LA TÂCHE

Vu que les fichiers sont copiés sur les ordinateurs clients par l'Agent d'administration, il n'est pas nécessaire de configurer le compte. Toutes les opérations de copie et d'installation des fichiers seront effectuées par l'Agent d'administration sous les droits du compte **Système local**.

ETAPE 11. PROGRAMMATION DE L'EXÉCUTION DE LA TÂCHE

Définissez la fréquence et l'heure de démarrage de la tâche.

- Dans la liste déroulante **Planification**, sélectionnez le régime nécessaire de la mise en marche de la tâche:
  - **Mode manuel**;
  - **Toutes les N heures**;
  - **Chaque jour**;
  - **Chaque semaine**;
  - **Chaque mois**;
  - **Une fois** – dans ce cas, le lancement de la tâche d'installation à distance sur les ordinateurs sera réalisé seulement une fois quel que soit le résultat de son exécution;
  - **Immédiatement** – démarrera la tâche immédiatement après avoir terminé l'Assistant;
  - **A la fin d'une autre tâche** – dans ce cas, la tâche d'installation à distance sur les ordinateurs sera lancée seulement à la fin de fonctionnement de la tâche indiquée.
- Configurez les paramètres de l'horaire dans le groupe des champs correspondant au mode sélectionné.
- Configurez les paramètres avancés d'exécution de la tâche (ils varient en fonction du mode d'exécution). Pour ce faire, exécutez les opérations suivantes:
  - La procédure que la tâche doit démarrer si le poste client n'est pas disponible (éteint, déconnecté du réseau, etc.) ou si l'application n'est pas lancée à l'heure programmée.
  - Cochez la case **Lancer les tâches non exécutées** pour que le système essaie d'exécuter une tâche lors de la prochaine ouverture de l'application sur ce poste client. Si l'option **Mode manuel**, **Une fois** ou **Immédiatement** a été sélectionnée, la tâche sera exécutée dès l'apparition de l'ordinateur sur le réseau.
  - Si cette case n'est pas cochée, l'exécution de la tâche sur les postes clients aura lieu uniquement selon la programmation et pour les options **Manuel**, **Une fois** et **Immédiatement**, uniquement pour les postes clients visibles dans le réseau. Par défaut, cette case n'est pas cochée.

ETAPE 12. FIN DE LA CRÉATION D'UNE TÂCHE

Après la fin de l'Assistant, la tâche créée sera ajoutée au dossier **Tâches pour les sélections d'ordinateurs** et affichée dans le panneau des résultats. Vous pouvez, si nécessaire, modifier ses paramètres (voir page 19).

LANCEMENT DE LA TÂCHE D'INSTALLATION À DISTANCE

Pour lancer manuellement la tâche d'installation à distance pour l'ensemble des ordinateurs, effectuez les actions suivantes:

1. Connectez-vous au Serveur d'administration.
2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de console.
3. Dans la barre des résultats, sélectionnez la tâche appropriée de la liste.
4. Ouvrez le menu contextuel et sélectionnez **Démarrer** ou sélectionnez la même action dans le menu **Action**.

CONSULTATION ET PARAMÉTRAGE DE LA TÂCHE D'INSTALLATION À DISTANCE

Pour consulter les propriétés de la tâche d'installation à distance et modifier ses paramètres, effectuez les actions suivantes:

1. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de console.
2. Dans la barre des résultats, sélectionnez la tâche appropriée de la liste.
3. Ouvrez le menu contextuel et sélectionnez **Propriétés**, ou sélectionnez la même action dans le menu **Action**.

La fenêtre **Propriétés <Nom de la tâche>** s'affichera, comprenant les onglets suivants: **Général**, **Notifications**, **Ordinateurs client**, **Horaire**, **Paramètres**, **Compte** et **Redémarrage SE**.

La configuration de la tâche d'installation à distance est effectuée de la même manière que celle des propriétés de toute tâche. Examinons en détail les paramètres spécifiques, fournis à l'onglet **Paramètres** pour ce type de tâche. Cet onglet vous permet de déterminer:

- le moyen de remise des fichiers (nécessaires pour l'installation de l'application) sur les postes clients, et pour indiquer le nombre maximum de connexions simultanées;
- le nombre de tentatives d'installation au lancement de la tâche programmée;
- s'il faut installer à nouveau l'application au cas où elle serait déjà installée sur le poste client;
- s'il est nécessaire de fermer les applications en cours avant l'installation;
- s'il faut vérifier avant l'installation de l'application la version du système d'exploitation sur la conformité des exigences au système.

CRÉATION DU PAQUET D'INSTALLATION

Avant de procéder à la création du paquet d'installation, il faut effectuer la préparation paquet d'installation de Kaspersky Endpoint Security.

Pour pouvoir préparer le paquet d'installation de Kaspersky Endpoint Security à l'installation, effectuez les actions suivantes:

1. Effectuez l'extraction de l'archive kes4lwks-rpm.tar.gz ou kes4lwks-deb.tar.gz (en fonction du manager des paquets qui est utilisé dans le système d'exploitation de l'ordinateur protégé) dans le dossier accessible au Serveur d'administration de Kaspersky Administration Kit.

2. Copiez dans ce même dossier le paquet kes4lwks-<référence_de_la_version>.i386.rpm ou kes4lwks_<référence_de_la_version>_i386.deb (en fonction du manager des paquets qui est utilisé dans le système d'exploitation de l'ordinateur protégé).

Afin de créer le paquet d'installation, procédez comme suit:

1. Connectez-vous au Serveur d'administration.

2. Sélectionnez le dossier **Stockages** → **Paquets d'installation** dans l'arborescence de la console.

3. Ouvrez le menu contextuel et sélectionnez **Nouveau** → **Paquet d'installation** ou sélectionnez la même action dans le menu **Action**.

Ceci ouvre l'Assistant de création d'un paquet d'installation. Suivez les instructions de l'Assistant.

ETAPES DE L'ASSISTANT

ETAPE 1. DÉFINITION DU NOM DU PAQUET D'INSTALLATION

Saisissez le nom du paquet d'installation dans le champ **Nom**.

ETAPE 2. SÉLECTION DU DISTRIBUTIF DE L'APPLICATION

A cette étape, il vous est proposé de spécifier le logiciel à installer.

Dans la liste déroulante, sélectionnez la variante: **Créer le paquet d'installation pour le logiciel de "Kaspersky Lab"**. Cliquez sur **Sélectionner** et sélectionnez le fichier avec l'extension .kpd. Finalement, les champs se remplissent automatiquement avec le nom et le numéro de version de l'application.

Les paramètres du paquet d'installation sont créés par défaut, en fonction de l'application à installer. Vous pouvez les modifier (voir page 22) après avoir créé le paquet, dans la fenêtre des propriétés de ce dernier.

ETAPE 3. CHARGEMENT DU PAQUET D'INSTALLATION

Pour télécharger le paquet d'installation créé sur le Serveur d'administration, cliquezr sur **Suivant**.

ETAPE 4. CONFIGURATION DES PARAMÈTRES DE LA TÂCHE DE PROTECTION EN TEMPS RÉEL

A cette étape, il vous est proposé de lancer la compilation du module du noyau du système d'exploitation. En faisant cela, le module nécessaire pour le fonctionnement de la tâche de protection en temps réel est compilé. Vous avez le choix parmi les options suivantes:

- **Ne pas compiler le module de protection en temps réel**;
- **Compiler le module, chercher les codes d'origine en automatique**: lorsque cette variante est sélectionnée, les codes d'origine du noyau seront trouvés automatiquement;
- **Compiler le module, spécifier le chemin d'accès aux codes d'origine**: lorsque cette variante est sélectionnée, vous devez spécifier manuellement le chemin d'accès complet aux codes d'origine du noyau du système d'exploitation (par exemple, */lib/modules/2.6.27.39-0.2-default*). Cliquez sur **Options** pour spécifier le chemin d'accès complet aux codes d'origine du noyau.

Puis à cette étape, il vous est proposé de déterminer les paramètres d'intégration avec le Serveur Samba. Vous avez le choix parmi les options suivantes:

- **Ne pas installer l'intercepteur Samba**;
- **Intégration automatique avec le serveur Samba:** lorsque cette variante est sélectionnée, l'intégration de Kaspersky Endpoint Security avec le serveur Samba sera effectuée automatiquement;
- **Intégration avec le serveur Samba, spécifier les paramètres manuellement:** lorsque cette variante est sélectionnée, vous devez spécifier les paramètres d'intégration avec le serveur Samba manuellement. Cliquez sur **Options** pour spécifier les paramètres d'intégration avec le serveur Samba suivants:
  - chemin d'accès complet au fichier de configuration du serveur Samba (par exemple, */etc/samba/smb.conf*);
  - répertoire pour les modules VFS Samba (par exemple, */usr/lib/samba/vfs*);
  - nom du module VFS à installer (par exemple, */opt/kaspersky/kes4lwks/lib/samba/kes4lwks-smb-vfs21.so*).

Cochez la case **Lancer la tâche de protection en temps réel après l'installation**, si vous voulez que la tâche soit lancée immédiatement après l'installation.

ETAPE 5. CONFIGURATION DES PARAMÈTRES DE LA TÂCHE DE MISE À JOUR

A cette étape, il vous est proposé de spécifier les paramètres de la tâche de mise à jour. Vous pouvez sélectionner une des sources de mise à jour suivantes:

- **Ne pas modifier**;
- **Serveur d'administration de Kaspersky Administration Kit**;
- **Les serveurs de mise à jour de Kaspersky Lab**;
- **Autres sources de mise à jour**.

  Si vous avez sélectionné cette variante, cliquez sur **Options** pour configurer la source de mise à jour d'utilisateur. Les serveurs HTTP ou FTP, les répertoires locaux ou de réseau peuvent être utilisés en tant que source de mise à jour.

Cochez la case **Lancer la mise à jour après l'installation** si vous voulez que la tâche de mise à jour soit lancée immédiatement après l'installation.

ETAPE 6. FIN DE CRÉATION DU PAQUET D'INSTALLATION

Finalement, le paquet d'installation sera formé et présenté dans la barre des résultats dans le dossier **Stockages** → **Paquets d'installation**. Vous pouvez modifier les paramètres du paquet d'installation dans la fenêtre de ses propriétés.

CONSULTATION ET CONFIGURATION DES PARAMÈTRES DU PAQUET D'INSTALLATION

Pour consulter les propriétés du paquet d'installation et modifier ses paramètres, effectuez les actions suivantes:

1. Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Paquets d'installation**.
2. Dans la barre des résultats, sélectionnez le paquet d'installation approprié.
3. Ouvrez le menu contextuel et sélectionnez **Propriétés**, ou sélectionnez la même action dans le menu **Action**.
4. La fenêtre **Propriétés <Nom du paquet d'installation>** s'affichera et comprendra les onglets suivants: **Général**, **Protection en temps réel**, **Mise à jour** et **Licence**.

L'onglet **Général** contient les renseignements généraux sur le paquet. Les données suivantes le composent:

- Nom du paquet d'installation (vous pouvez le modifier).
- Nom et version de l'application pour laquelle un paquet est créé.
- Taille du paquet.
- Date de création.
- Chemin d'accès au dossier de placement du paquet d'installation.

L'onglet **Protection en temps réel** comprend les paramètres de la tâche de protection en temps réel: paramètres de compilation du module du noyau du système d'exploitation nécessaire pour le fonctionnement de la tâche de protection en temps réel, ainsi que paramètres d'intégration avec le serveur Samba. Ces paramètres sont spécifiés à l'étape de création du paquet d'installation (voir section "Création du paquet d'installation" à la page 19). Vous pouvez les modifier si nécessaire.

L'onglet **Mise à jour** comprend les paramètres de la tâche de mise à jour: sélection de la source de mise à jour et configuration de la source de mise à jour d'utilisateur. Ces paramètres sont spécifiés à l'étape de création du paquet d'installation (voir section "Création du paquet d'installation" à la page 19). Vous pouvez les modifier si nécessaire.

L'onglet **Licence** comprend les renseignements généraux sur la licence relative au logiciel pour l'installation duquel le paquet d'installation est créé. A cet onglet, vous pouvez rajouter ou modifier le fichier de clé.

CONFIGURATION INITIALE DE KASPERSKY ENDPOINT SECURITY

Une fois Kaspersky Endpoint Security installé sur le serveur, vous devez effectuer la configuration initiale de Kaspersky Endpoint Security.

Si la procédure de configuration initiale de Kaspersky Endpoint Security n'a pas été faite, la protection antivirus de l'ordinateur ne sera pas opérationnelle.

Le processus de configuration initiale de l'application est une suite d'étapes qui, pour la convivialité de l'utilisateur, est réalisée sous forme de script. Le script de la configuration initiale est lancé automatiquement, une fois que l'application est installée sur l'ordinateur. Si le manager de paquets qui est utilisé dans le système d'exploitation n'admet pas l'utilisation des scripts interactifs, le script de la configuration initiale doit être lancé manuellement.

Une fois que le processus de configuration initiale est terminé, la tâche de protection en temps réel est lancée. Pour cela, il est nécessaire d'effectuer les actions suivantes:

- installation du fichier de licence,
- téléchargement des bases de Kaspersky Endpoint Security,
- compilation des modules du noyau.

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

pour Linux:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl
```

Les actions nécessaires pour le lancement de la tâche de protection en temps réel peuvent être effectuées à l'aide des moyens d'administration de Kaspersky Endpoint Security. Pour de plus amples informations, consultez le Manuel d'administrateur de Kaspersky Endpoint Security 8 for Linux.

DANS CETTE SECTION

ETAPE 1. CONSULTATION DU TEXTE DU CONTRAT DE LICENCE

Au cours de cette étape, vous devez accepter ou rejeter les termes du contrat de licence.

Vous pouvez consulter le texte à l'aide de l'utilitaire *less*. Pour se déplacer sur le texte, utilisez les touches de commande du curseur, ou les touches **b** (pour revenir à l'écran précédent) et **f** (pour passer à l'écran suivant). Pour obtenir un renseignement, utilisez la touche **h**. Pour terminer la consultation, utilisez la touche **q**.

Après avoir quitté le mode de consultation, saisissez **yes** (ou **y**) pour accepter les conditions de la convention de licence. Si vous n'acceptez pas les termes de la convention de licence, saisissez **no** (ou **n**).

Si vous n'acceptez pas les conditions de la convention de licence, le processus de configuration de Kaspersky Endpoint Security sera arrêté.

ETAPE 2. SÉLECTION DU "LOCALE"

A cette étape, il faut spécifier la référence du locale qui sera utilisé en cours du fonctionnement de Kaspersky Endpoint Security.

Le locale est spécifié au format qui est déterminé dans RFC 3066.

- *Pour avoir la liste exhaustive des références des locaux, utilisez la commande suivante:*

```
# locale -a
```

Par défaut, il vous est proposé d'utiliser le locale **en_US.utf8**.

ETAPE 3. INSTALLATION DU FICHIER DE LICENCE

L'installation du fichier de licence est nécessaire à cette étape. Le fichier de licence contient les renseignements à la base desquels la disponibilité des droits à l'utilisation de Kaspersky Endpoint Security est vérifiée et la durée de son utilisation est déterminée.

Pour installer le fichier de licence,

spécifiez le chemin d'accès complet au fichier de licence ou le chemin d'accès au répertoire contenant les fichiers de licence.

Si le répertoire spécifié comprend plusieurs fichiers de licence, le premier fichier conforme à Kaspersky Endpoint Security 8 for Linux.

Si la licence n'est pas installée, Kaspersky Endpoint Security n'assurera pas la protection antivirus de l'ordinateur.

Vous pouvez installer le fichier de licence sans utilisation du script de la configuration initiale. Pour obtenir les informations relatives à l'installation du fichier de licence, consultez la section "Administration des licences" du "Manuel d'administrateur" de Kaspersky Endpoint Security 8 for Linux.

ETAPE 4. CONFIGURATION DES PARAMÈTRES DE CONNEXION

A cette étape, vous pouvez définir les paramètres de connexion à un serveur proxy. Si un serveur proxy est utilisé pour accéder à Internet, il faudra configurer ses paramètres. La connexion à Internet est nécessaire pour pouvoir télécharger les bases de Kaspersky Endpoint Security depuis les serveurs de mises à jour.

Pour configurer les paramètres d'un serveur proxy, procédez comme suit:

- Si, lors de la connexion à Internet, un proxy serveur est utilisé, spécifiez l'adresse du serveur proxy sous un des formats suivants:
  - `IP_adresse_du_serveur_proxy:port`, si l'authentification n'est pas demandée lors de la connexion au serveur proxy;
  - `nom_d'utilisateur:mot de passe@IP_adresse_du_serveur_proxy:port`, si l'authentification est demandée lors de la connexion au serveur proxy.
- Si, lors de la connexion à Internet, le proxy serveur n'est pas utilisé, saisissez **no** comme réponse.

Par défaut, c'est la réponse **no** qui est proposée.

Vous pouvez configurer les paramètres de proxy serveur sans utilisation du script de la configuration initiale. Pour avoir les informations sur la configuration des paramètres du serveur proxy, consultez la section "Mise à jour de Kaspersky Endpoint Security" du "Manuel d'administrateur" de Kaspersky Endpoint Security 8 for Linux.

ETAPE 5. TÉLÉCHARGEMENT DES BASES DE KASPERSKY ENDPOINT SECURITY

A cette étape, il vous est proposé de télécharger sur l'ordinateur les bases de Kaspersky Endpoint Security. La protection des informations sur l'ordinateur est assurée à partir des bases de données qui contiennent la spécification

des signatures des menaces et des moyens de lutte contre celles-là. Kaspersky Endpoint Security les utilise pour la recherche et la neutralisation des objets dangereux. Ces bases sont enrichies régulièrement des définitions de nouvelles menaces et des moyens de lutte contre celles-ci.

- *Pour télécharger les bases de Kaspersky Endpoint Security sur l'ordinateur,*

  saisissez en tant que réponse **yes**.

Si vous ne voulez pas télécharger les bases immédiatement, saisissez **no**.

Par défaut, c'est la réponse **yes** qui est proposée.

Si les bases de Kaspersky Endpoint Security n'ont pas été téléchargées, Kaspersky Endpoint Security n'assurera pas la protection antivirus de l'ordinateur.

Vous pouvez lancer la mise à jour des bases de Kaspersky Endpoint Security sans utilisation du script. Pour avoir des informations sur le lancement de la mise à jour des bases de Kaspersky Endpoint Security, consultez la section "Mise à jour de Kaspersky Endpoint Security" du "Manuel d'administrateur" de Kaspersky Endpoint Security 8 for Linux.

ETAPE 6. ACTIVATION DE LA MISE À JOUR DES BASES EN MODE AUTOMATIQUE

A cette étape, vous pouvez activer la mise à jour des bases de Kaspersky Endpoint Security en mode automatique.

- *Pour activer la mise à jour des bases automatiquement,*

  saisissez **yes**.

Par défaut, les bases de Kaspersky Endpoint Security sont mises à jour toutes les 30 minutes.

Vous pouvez automatiquement activer la mise à jour des bases de Kaspersky Endpoint Security sans utiliser le script de la configuration initiale. Pour avoir des informations sur la configuration de l'horaire de la mise à jour des bases de Kaspersky Endpoint Security, consultez les sections "Modification des paramètres de l'horaire de la tâche. -T --set-schedule" et "Paramètres de l'horaire" du "Manuel d'administrateur" de Kaspersky Endpoint Security 8 for Linux.

ETAPE 7. COMPILATION DU MODULE DU NOYAU

A cette étape, il vous est proposé de lancer la compilation du module du noyau. En faisant cela, le module nécessaire pour le fonctionnement de la tâche de protection en temps réel est compilé.

Si le script découvre les codes d'origine du noyau du système d'exploitation dans le répertoire par défaut, le chemin trouvé sera utilisé par défaut. En cas contraire, il vous sera proposé de spécifier le chemin d'accès aux codes d'origine du noyau.

Vous pouvez effectuer la compilation du module du noyau, sans répéter les étapes précédentes du script.

- *Pour compiler le module du noyau sans démarrer le processus de la configuration initiale, exécutez la commande suivante:*

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \

--build=<chemin d'accès aux codes d'origine du noyau>
```

Si la compilation du module du noyau n'a pas été faite, la tâche de protection en temps réel ne traitera pas les opérations sur les objets locaux ou montés du système de fichiers de l'ordinateur.

ETAPE 8. INTÉGRATION AVEC LE SERVEUR SAMBA

A cette étape, l'intégration avec le serveur Samba est effectuée. En faisant cela, les actions suivantes sont exécutées:

- recherche du serveur Samba distant et vérification de sa version qui doit être conforme à la configuration logicielle requise;
- recherche et modification du fichier de configuration du serveur Samba;
- vérification du fichier de configuration du serveur Samba au sujet de la disponibilité des modules VFS.

Si dans le fichier de configuration du serveur Samba, les modules VFS sont spécifiés au moment de l'installation de Kaspersky Endpoint Security, ces modules seront désactivés.

Le script de la configuration initiale effectue la recherche des serveurs Samba installés. Après cela, il vous sera proposé de configurer la protection des serveurs trouvés en mode automatique ou manuel. Saisissez **Y** pour configurer la protection du serveur Samba en mode automatique. Ce mode est utilisé par défaut. Saisissez **N** si le serveur Samba est trouvé avec erreur, ou si vous voulez configurer la protection du serveur Samba en mode manuel.

➧ *Pour configurer la protection du serveur Samba en mode manuel, effectuez les actions suivantes:*

Si vous laissez une ligne vide pour la réponse à la demande du script de la configuration initiale, le processus de protection du serveur Samba est arrêté.

1. Spécifiez le chemin d'accès au répertoire qui contient le fichier *smbd*.
2. Spécifiez le chemin d'accès au répertoire qui contient le fichier de configuration du serveur Samba (*smb.conf*).
3. Spécifiez le chemin d'accès au répertoire qui contient les modules VFS du serveur Samba.

Une fois que l'intégration est terminée, il faut redémarrer le service du serveur Samba manuellement.

Si la tâche de protection en temps réel a été arrêtée après l'intégration avec le serveur Samba, l'accès aux ressources Samba sera bloqué.

➧ *Pour que l'accès aux ressources Samba ne soit pas bloqué après l'arrêt de la tâche de protection en temps réel,*

ajoutez dans la section `[global]` du fichier de configuration */etc/samba/smb.conf* la ligne suivante:

```
kavsamba:access_on_error = yes
```

Vous pouvez effectuer l'intégration avec le serveur Samba sans répéter les étapes précédentes du script.

➧ *Pour exécuter l'intégration avec le serveur Samba sans démarrer le processus de la configuration initiale, exécutez la commande suivante:*

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl --samba
```

ETAPE 9. LANCEMENT AUTOMATIQUE DE L'INTERFACE GRAPHIQUE

A ce stade, précisez s'il faut démarrer automatiquement l'interface graphique pour l'utilisateur au démarrage du système.

- *Pour démarrer automatiquement l'interface graphique pour l'utilisateur au démarrage du système*

  saisissez en tant que réponse **yes**.

Si vous ne voulez pas accepter le démarrage automatique de l'interface graphique pour l'utilisateur, saisissez **no**.

Par défaut, c'est la réponse **yes** qui est proposée.

ETAPE 10. LANCEMENT DE LA TÂCHE DE PROTECTION EN TEMPS RÉEL

A cette étape, la tâche de protection en temps réel est lancée si les actions suivantes ont été effectuées:

- installation de la licence;
- téléchargement des bases de Kaspersky Endpoint Security;
- compilation du module du noyau ou intégration avec le serveur Samba.

Pour obtenir les informations relatives à l'administration d'une tâche, consultez la section "Administration des tâches" du "Manuel d'administrateur" de Kaspersky Endpoint Security 8 for Linux.

ETAPE 11. CONFIGURATION DES PARAMÈTRES DE L'AGENT D'ADMINISTRATION

Si vous envisagez d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Administration Kit, il convient de configurer les paramètres de l'Agent d'administration. Le processus de configuration est réalisé sous forme de script.

- *Pour lancer le script de la configuration de l'Agent d'administration, effectuez la commande suivante:*

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

Lors du fonctionnement du script, il vous sera proposé d'effectuer les actions suivantes:

1. Spécifier le nom DNS ou l'adresse IP du Serveur d'administration.
2. Spécifier les numéros du port du Serveur d'administration ou utiliser le port par défaut (14000).
3. Spécifier les numéros du port SSL du Serveur d'administration ou utiliser le port par défaut (13000).
4. Spécifier s'il faut utiliser la connexion SSL pour le transfert des données. Par défaut, la connexion SSL est activée.

Pour de plus amples informations sur la configuration de l'Agent d'administration, consultez le "Manuel d'administrateur" de Kaspersky Administration Kit.

LANCEMENT DE LA CONFIGURATION INITIALE AUTOMATIQUE

La configuration initiale de Kaspersky Endpoint Security peut être réalisée en mode automatique.

Pour lancer la configuration initiale en mode automatique, procédez comme suit:

pour Linux:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \
--auto-install=<chemin d'accès complet au fichier de configuration de la configuration initiale>
```

pour FreeBSD:

```
/usr/local/bin/kes4lwks-setup.pl \
--auto-install=<chemin d'accès complet au fichier de configuration de la configuration initiale>
```

Le tableau ci-après reprend les paramètres du fichier de configuration de la configuration initiale.

Le tableau 2. Paramètres du fichier de configuration de configuration initiale

PARAMÈTRE	DESCRIPTION	VALEURS POSSIBLES
EULA_AGREED	Paramètre obligatoire. Acceptation des termes du contrat de licence	**yes**
SERVICE_LOCALE	Locale utilisée par Kaspersky Endpoint Security	La locale au format qui est déterminé dans la norme RFC 3066
INSTALL_KEY_FILE	Chemin d'accès complet au fichier	
UPDATER_SOURCE	Source des mises à jour	• **AKServer** – le serveur d'administration de Kaspersky Administration Kit sera la source des mises à jour; • **KLServers** – les serveurs de Kaspersky Lab seront la source des mises à jour; • URL source des mises à jour;
UPDATER_PROXY	Adresse du serveur proxy utilisé pour la connexion à Internet.	• URL du serveur proxy; • **no** – ne pas utiliser le serveur proxy;
UPDATER_EXECUTE	Lancement de la tâche de mise à jour des bases antivirus pendant la configuration.	• **yes** – lance la mise à jour des bases; • **no** – ne lance pas la tâche de mise à jour;
UPDATER_ENABLE_AUTO	Active/désactive le lancement automatique de la tâche de mise à jour.	• **yes** – active le lancement automatique de la tâche de mise à jour; • **no** – désactive le lancement automatique de la tâche de mise à jour;
RTP_BUILD_KERNEL_MODULE	Paramètre obligatoire. Lancement de la compilation du noyau du module	• **yes** – compile le noyau du module; • **no** – ne compile pas le noyau du module;
RTP_BUILD_KERNEL_SRCS	Chemin d'accès aux codes d'origine du noyau	• **auto** – recherche automatique; • chemin d'accès au code source;

PARAMÈTRE	DESCRIPTION	VALEURS POSSIBLES
RTP_SAMBA_ENABLE	Paramètre obligatoire. Intégration avec le serveur Samba	• **yes** – réalise l'intégration à l'aide des valeurs des paramètres RTP_SAMBA_CONF, RTP_SAMBA_VFS, RTP_SAMBA_VFS_MODULE; • **no** – ne réalise pas l'intagration; • **auto** – détermine automatiquement les chemins d'accès aux composants du serveur Samba;
RTP_SAMBA_CONF	Chemin d'accès complet au fichier de configuration du serveur Samba (*smb.conf*)	
RTP_SAMBA_VFS	Chemin d'accès au répertoire qui contient les modules VFS du serveur Samba	
RTP_SAMBA_VFS_MODULE	Chemin d'accès complet au module VFS de Kaspersky Endpoint Security qui sera installé en guise de module de traitement	
RTP_START	Lancement de la tâche de protection en temps réel à la fin de la configuration	• **yes** – lance la protection en temps réel; • **no** – ne lance pas la protection en temps réel;
GUI_ENABLE	Lancement automatique de l'interface graphique lors de l'entrée dans le système.	• **yes** – démarrer automatiquement l'interface graphique; • **no** – ne pas démarrer automatiquement l'interface graphique;

Saisissez les valeurs au format **nom du paramètre=valeur** (les espaces entre le nom du paramètre et sa valeur ne sont pas traités).

CONFIGURATION DES RÈGLES D'AUTORISATION DANS LES SYSTÈMES SELINUX ET APPARMOR

Kaspersky Endpoint Security n'est pas compatible avec SELinux et Novell AppArmor.

- *Pour placer SELinux dans le mode d'autorisation, saisissez l'instruction suivante:*

```
# setenforce Permissive
```

- *Pour placer toutes les règles AppArmor en mode "protection", saisissez les instructions suivantes:*

```
# aa-complain /etc/apparmor.d/*
# /etc/init.d/apparmor reload
```

SUPPRESSION DE KASPERSKY ENDPOINT SECURITY

Si vous voulez restaurer les fichiers qui se trouvent en quarantaine, faites-le avant de supprimer Kaspersky Endpoint Security. Sinon, il ne sera plus possible de restaurer les fichiers depuis la quarantaine.

- *Pour supprimer Kaspersky Endpoint Security depuis le paquet .rpm, exécutez la commande suivante:*

  ```
  # rpm -e kes4lwks
  ```

- *Pour supprimer Kaspersky Endpoint Security depuis le paquet deb, exécutez la commande suivante:*

  ```
  # dpkg -r kes4lwks
  ```

- *Pour supprimer Kaspersky Endpoint Security installé sur l'ordinateur administré par le système d'exploitation FreeBSD, accomplissez la commande suivante:*

  ```
  # pkg_delete kes4lwks
  ```

En faisant cela, toutes les tâches de Kaspersky Endpoint Security seront arrêtées.

- *Pour supprimer l'Agent d'administration depuis le paquet .rpm, saisissez l'instruction suivante:*

  ```
  # rpm -e klnagent
  ```

- *Pour supprimer l'Agent d'administration depuis le paquet deb, saisissez l'instruction suivante:*

  ```
  # dpkg -r klnagent
  ```

La procédure de suppression est effectuée automatiquement. Une fois la procédure de suppression terminée, le message approprié sera affiché.

DÉSINSTALLATION DE KASPERSKY ENDPOINT SECURITY À DISTANCE

La désinstallation de Kaspersky Endpoint Security à l'aide de Kaspersky Administration Kit est effectuée par le lancement de la tâche de désinstallation à distance.

- *Pour créer la tâche de désinstallation à distance de Kaspersky Endpoint Security, procédez comme suit:*

1. Connectez-vous au Serveur d'administration nécessaire.
2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de console.
3. Ouvrez le menu contextuel et sélectionnez **Nouveau** → **Tâche** ou sélectionnez la même action dans le menu **Action**.

   Ceci permet de lancer l'assistant de création de tâche.
4. Dans la fenêtre **Nom de la tâche**, saisissez le nom de la tâche dans le champ **Nom**.
5. Dans la fenêtre **Type de la tâche**, dans le nœud **Kaspersky Administration Kit**, ouvrez le sous-dossier **Options** et sélectionnez **Désinstallation du logiciel à distance**.
6. Dans la fenêtre **Paramètres**, indiquez l'application à supprimer. Pour le faire, dans la liste déroulante **Supprimer le logiciel supporté par Kaspersky Administration Kit**, sélectionnez la variante **Kaspersky Endpoint Security 8 for Linux**.
7. Dans la fenêtre **Mode de désinstallation à distance**, sélectionnez la variante **Désinstallation forcée**.
8. Dans la fenêtre **Paramètres**, dans le bloc des paramètres **Forcer le téléchargement de l'utilitaire de désinstallation,** cochez la case **A l'aide de l'Agent d'administration**.
9. Terminez la création de la tâche de la même façon que pour la tâche d'installation à distance (voir page 15).

La tâche formée sera exécutée selon sa programmation.

- *Pour lancer manuellement la tâche de désinstallation à distance de Kaspersky Endpoint Security, procédez comme suit:*

1. Connectez-vous au Serveur d'administration.
2. Sélectionnez le dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de la console.
3. Dans la barre des résultats, sélectionnez la tâche appropriée de la liste.
4. Ouvrez le menu contextuel et sélectionnez **Démarrer** ou sélectionnez la même action dans le menu **Action**.

ACTIONS APRÈS LA SUPPRESSION DE KASPERSKY ENDPOINT SECURITY

Après avoir supprimé Kaspersky Endpoint Security (cf. page 31) les informations suivantes restent sur l'ordinateur:

- les bases de Kaspersky Endpoint Security;
- les bases de données du répertoire de sauvegarde des licences;
- les bases de données du répertoire de sauvegarde des événements;
- les bases de données des paramètres du fonctionnement de Kaspersky Endpoint Security;
- les fichiers dans le répertoire de sauvegarde et dans la quarantaine;
- les fichiers du registre.

Kaspersky Endpoint Security comprend les scripts qui suppriment ces fichiers et les répertoires qui restent après la désinstallation de Kaspersky Endpoint Security sur l'ordinateur.

Pour lancer ces scripts, effectuez les actions suivantes:

1. Effectuez la commande suivante:
   - pour Linux: `# /var/opt/kaspersky/kes4lwks/cleanup.sh`
   - pour FreeBSD: `# /var/db/kaspersky/kav4fs/cleanup.sh`
2. Confirmez la suppression des informations qui restent après la suppression de Kaspersky Endpoint Security en saisissant **yes**. Pour ne pas supprimer les informations et arrêter le fonctionnement du script, saisissez **no**.

VÉRIFICATION DU FONCTIONNEMENT DES TÂCHES DE PROTECTION EN TEMPS RÉEL ET D'ANALYSE À LA DEMANDE

Après avoir installé et effectué la configuration initiale de Kaspersky Endpoint Security, vous pouvez vous assurer que les tâches de protection en temps réel et d'analyse à la demande sont configurées correctement.

DANS CETTE SECTION

VÉRIFICATION DU FONCTIONNEMENT DE LA TÂCHE DE PROTECTION EN TEMPS RÉEL

Cette section décrit comment s'assurer qu'à l'aide de la tâche de protection en temps réel, Kaspersky Endpoint Security découvre des objets infectés et suspects lorsqu'il y accède et effectue sur ces objets les actions spécifiées dans la tâche.

➧ *Pour vérifier le fonctionnement de la tâche de protection en temps réel, procédez comme suit:*

1. Téléchargez le fichier *eicar.com* eicar.com depuis la page du site EICAR http://www.eicar.org/anti_virus_test_file.htm. Sauvegardez-le sur l'ordinateur protégé.

   Si vous voulez vérifier comment Kaspersky Endpoint Security découvre des objets suspects, rajoutez le préfixe SUSP– à la ligne de texte dans le fichier (pour de plus amples informations, consultez la section "Virus d'essai EICAR et ses modifications").

2. Si la tâche de protection en temps réel a été arrêtée, lancez-la à l'aide de la commande suivante:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 8
   ```

3. Ouvrez le fichier *eicar.com* en lecture à l'aide de la commande suivante:

   ```
   # cat <chemin_d'accès_complet_à_eicar.com>
   ```

4. Kaspersky Endpoint Security interceptera l'appel au fichier, l'analysera et bloquera son accès. En faisant cela, le message suivant est affiché sur la console:

   ```
   "cat: <chemin_d'accès_complet_à_eicar.com>: Permission denied"
   ```

5. Effectuez la commande suivante:

   ```
   # echo $?
   ```

   La tâche de protection en temps réel traite avec succès la requête au fichier *eicar.com*, si le résultat de l'exécution de cette commande est une valeur qui n'est pas égale à zéro.

VÉRIFICATION DU FONCTIONNEMENT DE LA TÂCHE D'ANALYSE À LA DEMANDE

Cette section décrit comment s'assurer que Kaspersky Endpoint Security découvre des objets infectés et suspects dans la tâche d'analyse à la demande spécifiée du secteur d'analyse, et effectue des actions sur ceux-ci comme spécifiées dans la tâche.

Vous pouvez vérifier la fonction "Analyse à la demande" lors de l'exécution de la tâche prédéterminée **Analyse complète de l'ordinateur**, ainsi que celle de la tâche d'analyse à la demande d'utilisateur.

Vous devez sauvegarder le fichier *eicar.com* sur l'ordinateur protégé.

Pour vérifier le fonctionnement de la tâche d'analyse à la demande, procédez comme suit:

1. Arrêtez la tâche de protection en temps réel à l'aide de la commande suivante:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task 8
   ```

2. Téléchargez le fichier *eicar.com* depuis la page du site EICAR http://www.eicar.org/anti_virus_test_file.htm et enregistrez-le sur l'ordinateur protégé.

   Lors de l'analyse, Kaspersky Endpoint Security attribuera au fichier le statut **Infecté**, si vous laissez le fichier eicar.com intact. Kaspersky Endpoint Security attribuera au fichier le statut **Suspect**, si vous rajoutez le préfixe SUSP- à la ligne de texte dans le fichier *eicar.com* (pour plus d'informations, consultez la section "Virus de test EICAR et ses modifications" (voir page 35)).

3. Créez la tâche d'analyse à la demande à l'aide de la commande suivante:

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

   --create-task <nom_de_la_tâche> --use-task-type=ODS
   ```

   ID de la tâche créée sera affiché sur la console.

4. Rajoutez le répertoire qui contient le fichier *eicar.com* dans le secteur d'analyse de la tâche créée à l'aide de la commande suivante:

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

   --set-settings <ID_de_la_tâche_créée> \

   ScanScope.AreaPath.Path=<chemin_d'accès_au_fichier_ contenant_eicar.com>
   ```

5. Lancez la tâche créée à l'aide de la commande suivante:

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

   --start-task <ID_de_la_tâche_créée> -W
   ```

6. Consultez les résultats du fonctionnement de la tâche sur la console.

La tâche d'analyse à la demande est configurée correctement si le fichier *eicar.com* est supprimé de l'ordinateur protégé (si dans les paramètres de la tâche, l'action à exécuter sur des objets infectés **Réparer est spécifiée; si cela n'est pas possible, supprimer**).

VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

Le virus d'essai est destiné pour la vérification du fonctionnement des applications antivirus. Il a été créé par l'organisation The European Institute for Computer Antivirus Research (EICAR).

Le virus "test" n'est pas une application malveillante. Il ne contient pas de code de programme qui peut endommager votre ordinateur. En revanche, les applications antivirus de la majorité des fabricants identifient une menace en lui.

Le fichier qui contient le virus d'essai est dénommé eicar.com. Vous pouvez le télécharger depuis la page http://www.eicar.org/anti_virus_test_file.htm du site officiel de l'organisation EICAR.

Avant de sauvegarder le fichier dans le répertoire sur l'ordinateur, assurez-vous que la protection en temps réel des fichiers dans ce répertoire est désactivée.

Le fichier eicar.com contient la ligne de texte. Lors de la vérification du fichier, l'Anti-Virus détecte la "menace" dans cette ligne de texte, attribue au fichier le statut **Infecté** et exerce sur ce fichier l'action qui est spécifiée dans la tâche.

De même, vous pouvez utiliser le fichier eicar.com pour vérifier la réaction de Kaspersky Endpoint Security lors de la détection des objets d'autres types. Pour cela, ouvrez le fichier à l'aide du programme de traitement de texte, rajoutez au contenu du fichier un des préfixes énumérés dans le tableau suivant, et enregistrez le fichier sous un autre nom.

Le tableau 3. Préfixes

PRÉFIXE	STATUT DU FICHIER APRÈS L'ANALYSE ET ACTION DE KASPERSKY ENDPOINT SECURITY
Sans préfixe	Kaspersky Endpoint Security attribue à l'objet le statut **Infecté**.
WARN-	Kaspersky Endpoint Security attribue à l'objet le statut **Avertissement** (le code de l'objet correspond partiellement au code d'une menace connue).
ERRO-	Une erreur s'est produite lors de l'analyse de l'objet. Kaspersky Endpoint Security ne peut pas accéder à l'objet, car l'intégrité de celui-ci a été violée (par exemple: il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau).
SUSP-	Kaspersky Endpoint Security attribue à l'objet le statut **Suspect** (détecté à l'aide de l'analyseur heuristique).
CURE-	Kaspersky Endpoint Security attribue à l'objet le statut **Infecté** et essaie de le réparer. Si la réparation est réussie, le corps du virus est remplacé par le mot "CURE".
CORR-	Kaspersky Endpoint Security attribue à l'objet le statut **Corrompus**.

SCHÉMA DE DISPOSITION DES FICHIERS DE KASPERSKY ENDPOINT SECURITY

Après avoir installé Kaspersky Endpoint Security sur le poste de travail sous l'administration du système d'exploitation Linux, les fichiers du kit de distribution seront disposés par défaut de la façon suivante:

/opt/kaspersky/kes4lwks/ – répertoire de base de Kaspersky Endpoint Security comprenant :

bin/ – répertoire des fichiers exécutables de tous les composants de Kaspersky Endpoint Security:

kes4lwks-control – fichier exécutable du composant d'administration de Kaspersky Endpoint Security;

kes4lwks-qtgui – fichier exécutable de l'interface graphique;

kes4lwks-setup.pl – script de la configuration de post-installation de Kaspersky Endpoint Security.

lib/ – répertoire de sauvegarde des modules supplémentaires de Kaspersky Endpoint Security:

samba/ — répertoire de sauvegarde des modules compilés Samba.

lib64/ — répertoire de sauvegarde des modules supplémentaires de 64 bits de Kaspersky Endpoint Security:

samba/ — répertoire de sauvegarde des modules 64 bits compilés Samba.

libexec/ — répertoire de sauvegarde des fichiers auxiliaires de Kaspersky Endpoint Security;

src/ — répertoire de sauvegarde du code d'origine des modules de Kaspersky Endpoint Security:

kernel/ — répertoire de sauvegarde des bibliothèques du module du noyau antivirus de Kaspersky Endpoint Security;

samba/ — répertoire de sauvegarde des bibliothèques du module Samba de Kaspersky Endpoint Security.

/opt/kaspersky/kes4lwks/share/doc/ – fichiers de la documentation de Kaspersky Endpoint Security:

LICENSE — convention de licence.

LICENSE.GPL — convention de licence pour les modules du noyau et de Samba.

/opt/kaspersky/kes4lwks/share/man/ — répertoire de sauvegarde des fichiers man.

/etc/init.d/ — répertoire qui contient les scripts d'administration des services Kaspersky Lab Framework:

kes4lwks-supervisor — script d'administration du service Kaspersky Lab Framework.

/etc/opt/kaspersky/ — répertoire qui contient les fichiers de configuration Kaspersky Lab Framework:

kes4lwks-supervisor.conf — fichier de configuration de Kaspersky Lab Framework.

/var/opt/kaspersky/kes4lwks/ — répertoire des données de Kaspersky Endpoint Security:

db/ — bases de données de Kaspersky Endpoint Security;

update/ — répertoire de sauvegarde des mises à jour de Kaspersky Endpoint Security;

quarantine/ — répertoire de la quarantaine.

/var/log/kaspersky/kes4lwks/ — répertoire de sauvegarde des fichiers log de Kaspersky Endpoint Security;

/var/run/kes4lwks/ — répertoire de sauvegarde des fichiers auxiliaires de Kaspersky Endpoint Security.

Pour connecter le système de renseignements de Kaspersky Anti-Virus (manuels d'aide), rajoutez dans le fichier de configuration de l'enveloppe les lignes suivantes:

```
MANPATH="$MANPATH:/opt/kaspersky/kes4lwks/share/man/:"

export MANPATH
```

KASPERSKY LAB ZAO

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes en chef en matière de virus siègent en tant que membres de l'organisation pour la recherche antivirus en informatique Computer Anti-virus Researcher's Organization (CARO).

La valeur principale de la société: c'est une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à une analyse continue de l'activité de virus, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirus les plus exigeants. Kaspersky Anti-Virus, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus: postes de travail, serveurs de fichiers, systèmes de messagerie, pare-feu et passerelles Internet, ordinateurs de poche. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus: Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirus pour entreprise. Les bases antivirus de Kaspersky Lab sont mises à jour en temps réel toutes les heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez une réponse complète à vos questions.

Site Web de Kaspersky Lab:	http://www.kaspersky.fr
L'Encyclopédie des virus:	http://www.securelist.com/fr/
Laboratoire antivirus:	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive) http://support.kaspersky.com/fr/virlab/helpdesk.html (pour les questions aux experts antivirus)