



Kaspersky Security for Virtualization 4.0 Light Agent

Manuel de l'administrateur

Version de l'application : 4.0

Cher utilisateur,

Nous vous remercions de votre confiance. Nous espérons que ce document vous sera utile et qu'il répondra à la majorité des questions que vous pourrez vous poser.

Attention ! Ce document demeure la propriété de Kaspersky Lab AO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous un format quelconque et la diffusion, y compris la traduction, de tout document ne sont admises que par autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et à titre d'information.

Ce document peut être modifié sans avertissement préalable.

Kaspersky Lab ne peut être tenue responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. Kaspersky Lab n'assume pas non plus de responsabilité en cas de dommages liés à l'utilisation de ces textes.

Date d'édition : 20/01/2017

© 2017 AO Kaspersky Lab. Tous droits réservés.

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

Table des matières

Présentation du manuel	9
Dans ce document.....	9
Conventions.....	12
Sources d'informations sur l'application	14
Sources pour des consultations indépendantes	14
Discussion sur les logiciels de Kaspersky Lab sur le forum.....	16
Kaspersky Security for Virtualization 4.0 Light Agent	17
A propos de Kaspersky Security for Virtualization 4.0 Light Agent	17
Nouveautés	22
Distribution.....	23
Configurations logicielle et matérielle	23
Architecture de l'application	29
Présentation de l'architecture de l'application	29
Variantes de déploiement des SVM	32
A propos de la connexion Light Agent à la SVM.....	34
A propos de la détection des SVM	35
A propos de l'algorithme de choix des SVM	36
A propos du Serveur d'intégration	37
Licence de l'application	39
A propos du Contrat de Licence Utilisateur Final.....	40
A propos de la licence	40
A propos du Certificat de licence	42
A propos de la clé.....	42
A propos du code d'activation.....	44
Présentation du fichier clé	44
A propos de l'abonnement.....	45
A propos de l'activation de l'application	46
Conditions pour activer l'application à l'aide d'un code d'activation	48
Particularités de l'activation de l'application avec plusieurs types de clés	49
Procédure d'activation de l'application.....	50

Ajout d'une clé dans le stockage des clés de Kaspersky Security Center.....	51
Création d'une tâche d'activation de l'application	53
Etape 1. Sélection de l'application et du type de tâche	54
Etape 2. Ajout d'une clé	54
Etape 3. Choix de la SVM	56
Etape 4. Définition des paramètres de programmation de la tâche.....	57
Etape 5. Définition du nom de la tâche	58
Etape 6. Fin de la création de la tâche	58
Renouvellement de la licence	59
Renouvellement de l'abonnement	60
Consultation des informations relatives aux clés utilisées	61
Consultation des informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab.....	62
Consultation des informations relatives à la clé dans les propriétés de l'application.....	65
Consultation des informations relatives à la clé dans les propriétés de la tâche d'activation de l'application	68
Consultation du rapport sur l'utilisation des clés.....	70
Lancement et arrêt de l'application	75
Etat de la protection de la machine virtuelle	77
Concept de l'administration de l'application via le Kaspersky Security Center.....	78
Protection en temps réel et analyse de la machine virtuelle	80
A propos de la protection en temps réel et de l'analyse de la machine virtuelle	80
Particularités de l'analyse des liens symboliques et fixes	81
Administration des stratégies	83
Présentation des stratégies pour Kaspersky Security	83
Affichage des paramètres des stratégies.....	86
Création de la stratégie pour le Serveur de protection	86
Etape 1. Définition du nom de la stratégie de groupe pour l'application	87
Etape 2. Sélection de l'application pour la création de la stratégie du groupe.....	87
Etape 3. Configuration des paramètres KSN.....	87
Etape 4. Configuration de la mise à jour	90
Etape 5. Configuration des paramètres de détection des SVM	90

Etape 6. Configuration des paramètres supplémentaires de fonctionnement des SVM.....	92
Etape 7. Création de la stratégie de groupe pour l'application	93
Configuration de l'affichage des paramètres de contrôle dans la Console d'administration.....	93
Création de la stratégie pour le Light Agent for Windows	94
Etape 1. Définition du nom de la stratégie de groupe pour l'application	95
Etape 2. Sélection de l'application pour la création de la stratégie du groupe.....	96
Etape 3. Importation des paramètres du Light Agent	96
Etape 4. Configuration des paramètres du contrôle	96
Etape 5. Configuration des paramètres de protection	98
Etape 6. Configuration des paramètres de détection des SVM	102
Etape 7. Configuration de la zone de confiance	104
Etape 8. Configuration de l'interface du Light Agent.....	106
Etape 9. Protection de l'accès aux fonctions et aux paramètres du Light Agent	108
Etape 10. Création de la stratégie de groupe pour l'application	109
Création de la stratégie pour le Light Agent for Linux.....	110
Etape 1. Définition du nom de la stratégie de groupe pour l'application	111
Etape 2. Sélection de l'application pour la création de la stratégie du groupe.....	111
Etape 3. Importation des paramètres du Light Agent	111
Etape 4. Configuration des paramètres de protection	111
Etape 5. Configuration des paramètres de détection des SVM	114
Etape 6. Création de la stratégie de groupe pour l'application	116
Modification des paramètres des stratégies	117
Création de la stratégie pour le Serveur de protection	117
Modification des paramètres d'une stratégie pour le Light Agent for Windows ...	118
Modification des paramètres d'une stratégie pour un Light Agent for Linux	119
Administration des tâches.....	121
Présentation des tâches pour Kaspersky Security	121
Création des tâches exécutées sur les machines virtuelles protégées.....	125
Lancement et arrêt des tâches dans Kaspersky Security Center	128
Mise à jour des bases de données et des modules de l'application.....	129
A propos de la mise à jour des bases et des modules de l'application	129

Activation et désactivation de la mise à jour des modules de Light Agent for Windows	132
Récupération automatique des paquets de mises à jour des bases et des modules de l'application.....	134
Création d'une tâche de mise à jour sur le Serveur de protection	135
Mise à jour des bases de données et des modules du Light Agent for Windows sur le modèle de machine virtuelle	137
Remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application	138
Création de la tâche de restauration d'une mise à jour sur le Serveur de protection.....	140
Configuration des paramètres du Light Agent for Linux via Kaspersky Security Center.....	142
Configuration de l'Antivirus Fichiers via Kaspersky Security Center.....	142
Activation et désactivation de l'Antivirus Fichiers	144
Modification du niveau de sécurité des fichiers	145
Modification de l'action de l'Antivirus Fichiers sur les fichiers infectés	146
Formation de la zone de protection de l'Antivirus Fichiers	148
Analyse des fichiers composés avec l'Antivirus Fichiers	150
Configuration de l'utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Fichiers.....	152
Modification du mode d'analyse des fichiers	153
Configuration de l'utilisation de la technologie iChecker lors du fonctionnement de l'Antivirus Fichiers	155
Configuration des exclusions de la protection via Kaspersky Security Center.....	156
Création d'une exclusion	158
Lancement et suspension de l'utilisation d'une exclusion.....	160
Modification d'une exclusion.....	161
Suppression d'une exclusion	162
Configuration des paramètres de la tâche de recherche des virus pour Light Agent for Linux.....	163
Modification du niveau de sécurité	164
Modification de l'action sur les fichiers infectés	165
Constitution de la zone d'analyse	167
Analyse des fichiers composés	169
Configuration de l'utilisation de l'analyse heuristique	171
Configuration de l'utilisation de la technologie iChecker.....	172

Configuration des paramètres du Light Agent for Windows via Kaspersky Security Center.....	174
Configuration du Contrôle du lancement des applications via le Kaspersky Security Center.....	174
Passage du mode "Liste noire" au mode "Liste blanche"	176
Etape 1. Réception des informations concernant les applications installées sur les machines virtuelles protégées	177
Etape 2. Composition des catégories d'applications	178
Etape 3. Définition des règles d'autorisation du Contrôle du lancement des applications	179
Etape 4. Test des règles d'autorisation du Contrôle du lancement des applications	180
Etape 5. Passage au mode "Liste blanche"	181
Modification de l'état de la règle de contrôle du lancement des applications	182
Configuration du contrôle des périphériques via le Kaspersky Security Center.....	183
Ajout de périphériques de confiance à la liste en fonction de leur modèle ou de leur identifiant	184
Ajout de périphériques de confiance à la liste selon le masque de leur identifiant.....	186
Technologie de réparation de l'infection active	188
Présentation de la technologie de réparation de l'infection active	188
Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur	190
Participer au Kaspersky Security Network	192
A propos de la participation à Kaspersky Security Network.....	192
A propos de l'approvisionnement des données	194
Configuration de l'utilisation de Kaspersky Security Network	195
Administration du Light Agent for Linux via la ligne de commande.....	199
Affichage d'aide sur les commandes de Kaspersky Security	199
Consultation des informations sur l'état de la protection de la machine virtuelle	201
Consultation des informations sur les SVM	201
Consultation des informations sur la licence.....	202
Lancement de la tâche d'analyse	203
Sélection des actions sur les fichiers infectés	204
Analyse des fichiers composés	206
Utilisation de la technologie iChecker lors de l'analyse	207

Lancement et arrêt de la tâche de mise à jour.....	207
Lancement de la tâche de mise à jour avec des paramètres supplémentaires ...	208
Consultation de l'état de la tâche de mise à jour	209
Consultation des statistiques du fonctionnement de la tâche de mise à jour.....	209
Sauvegarde	210
A propos de la sauvegarde.....	211
Consultation de la liste des fichiers dans la sauvegarde	211
Restauration des fichiers depuis la sauvegarde	212
Contacter le Support Technique	213
Modes d'obtention du Support Technique	213
Support Technique par téléphone	214
Support Technique via Kaspersky CompanyAccount.....	214
Obtention d'informations pour le Support Technique.....	215
A propos de la composition des fichiers de trace	217
Composition des fichiers de trace des SVM.....	218
Composition des fichiers de trace du Light Agent for Windows.....	219
Composition des fichiers de trace du Light Agent for Linux	220
Utilisation des fichiers de trace des SVM	221
Utilisation des fichiers de trace sur le Light Agent for Windows	222
Utilisation des fichiers de trace sur le Light Agent for Linux	223
A propos des journaux du Serveur d'intégration.....	225
Glossaire.....	226
AO Kaspersky Lab.....	231
Informations sur le code tiers.....	233
Avis de marques déposées.....	234
Index.....	235

Présentation du manuel

Le manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent (ci-après “ Kaspersky Security ”) est adressé aux spécialistes qui réalisent l'installation et l'administration de Kaspersky Security et aux spécialistes qui réalisent l'assistance technique des organisations utilisant Kaspersky Security.

Ce manuel est destiné aux experts techniques possédant de l'expérience dans l'utilisation de l'infrastructure virtuelle Microsoft® Windows Server® avec le rôle Hyper-V® (ci-après, “ Microsoft Windows Server (Hyper-V)”), Citrix XenServer, VMware ESXi™ ou KVM (Kernel-based Virtual Machine), et du système d'administration centralisée à distance des applications de Kaspersky Lab Kaspersky Security Center. Pour l'utilisation de Kaspersky Security, l'utilisateur doit être aussi familier avec les systèmes d'exploitation Microsoft Windows® et Linux® et posséder les droits généraux d'utilisation de ces systèmes.

Dans ce manuel, vous trouverez des informations sur la configuration et l'utilisation de Kaspersky Security.

Ce manuel indique également les sources d'informations relatives à l'application et les différents moyens d'obtenir le Support Technique.

Dans cette section

Dans ce document	9
Conventions	12

Dans ce document

Ce document 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 Security for Virtualization 4.0 Light Agent (cf. page [17](#))

Cette rubrique décrit les fonctions, les composants et la distribution de Kaspersky Security ainsi que la configuration matérielle et logicielle requise pour l'application.

Architecture de l'application (cf. page [29](#))

Cette section décrit les composants de Kaspersky Security et leur interaction.

Licence de l'application (cf. page [39](#))

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

Lancement et arrêt de l'application (cf. page [75](#))

Cette section contient des informations sur le lancement et l'arrêt de l'application.

Etat de la protection de la machine virtuelle (cf. page [77](#))

Cette section fournit des informations sur l'évaluation de l'état de la protection de la machine virtuelle.

Concept de l'administration de l'application via le Kaspersky Security Center (cf. page [78](#))

Cette section fournit des informations sur l'administration de l'application via l'administration centralisée à distance des applications de Kaspersky Lab Kaspersky Security Center.

Protection permanente et analyse de la machine virtuelle (cf. page [80](#))

Cette section contient des informations sur la manière dont Kaspersky Security protège et analyse la machine virtuelle protégée.

Administration des stratégies (cf. page [83](#))

Cette section fournit des informations sur l'élaboration et la configuration des stratégies pour l'application Kaspersky Security for Virtualization 4.0 Light Agent.

Administration des tâches (cf. page [121](#))

Cette section détaille l'administration des tâches configurables dans Kaspersky Security Center pour l'application Kaspersky Security for Virtualization 4.0 Light Agent.

Mise à jour des bases de données et des modules de l'application (cf. page [129](#))

Cette section contient des informations sur la mise à jour des bases de données et des modules de l'application et des instructions sur la configuration de la mise à jour.

Configuration des paramètres du Light Agent for Linux dans Kaspersky Security Center (cf. p. [142](#))

Cette section contient des informations sur la configuration des paramètres généraux de la protection du Light Agent for Linux et des paramètres du composant Antivirus Fichiers du Light Agent for Linux via Kaspersky Security Center.

Configuration des paramètres du Light Agent for Windows via Kaspersky Security Center (cf. p. [174](#))

Cette section contient des informations sur la configuration de certains paramètres du composant Contrôle du lancement des applications et du composant Contrôle des périphériques du Light Agent for Windows via Kaspersky Security Center.

Technologie de réparation de l'infection active (cf. page [188](#))

Cette section fournit des informations sur la technologie de réparation de l'infection active et des instructions concernant son activation pour le système d'exploitation de serveur Windows sur les machines virtuelles protégées.

Participation au Kaspersky Security Network (cf. page [192](#))

Cette section présente la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de ce service.

Administration du Light Agent for Linux via la ligne de commande (cf. p. [199](#))

Cette section contient des informations sur l'administration du composant Light Agent for Linux à l'aide des commandes de la ligne de commande et sur la configuration des paramètres des commandes.

Contacter le Support Technique (cf. page [213](#))

Cette section explique comment bénéficier des services du Support Technique et des conditions à remplir.

Glossaire (cf. page [226](#))

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

AO Kaspersky Lab (cf. page [231](#))

Cette section contient des informations sur AO Kaspersky Lab.

Information sur le code tiers (cf. page [233](#))

Cette section contient des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page [234](#))

Cette section contient des informations sur les marques de commerce utilisées dans le document.

Index

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

Conventions

Des conventions sont utilisées dans ce document (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. Les avertissements contiennent des informations sur les actions qui peuvent avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations supplémentaires et de l'aide.
Exemple : ...	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".

Exemple du texte	Description de la convention
<p>La <i>mise à jour</i>, c'est...</p> <p>L'événement <i>Bases dé-passées</i> survient.</p>	<p>Les éléments de texte suivants sont en italique :</p> <ul style="list-style-type: none"> • nouveaux termes ; • noms des états et des événements de l'application.
<p>Appuyez sur la touche ENTER.</p> <p>Appuyez sur la combinaison des touches ALT+F4.</p>	<p>Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.</p> <p>Deux noms de touche unis par le caractère “ + ” eprésentent une combinaison de touches. Il convient d'appuyer simultanément sur ces touches.</p>
<p>Cliquez sur le bouton Activer.</p>	<p>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.</p>
<p>► <i>Pour planifier une tâche, procédez comme suit :</i></p>	<p>Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".</p>
<p>Dans la ligne de commande, saisissez le texte <code>help</code></p> <p>Les informations suivantes s'affichent :</p> <p>Indiquez la date au format <code>JJ:MM:AA</code>.</p>	<p>Les types suivants du texte apparaissent dans un style spécial :</p> <ul style="list-style-type: none"> • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir au clavier.
<p><Type de la tâche></p>	<p>Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.</p>
<p>[Command]</p>	<p>Les paramètres non obligatoires sont inclus entre crochets.</p>

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 des consultations indépendantes	14
Discussion sur les logiciels de Kaspersky Lab sur le forum.....	16

Sources pour des consultations indépendantes

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

- page de Kaspersky Security sur le site de Kaspersky Lab ;
- page de Kaspersky Security sur le site du Support Technique (banque de solutions) ;
- l'aide électronique ;
- la documentation.

Si vous ne trouvez pas de solution aux problèmes qui se présentent, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support Technique" à la page [213](#)).

La consultation des sources d'informations en ligne requiert une connexion Internet.

Page de Kaspersky Security sur le site de Kaspersky Lab

La page Kaspersky Security (<http://www.kaspersky.fr/business-security/virtualization-light-agent>) fournit des informations générales sur l'application, ses possibilités et ses particularités.

Page de Kaspersky Security dans la base de connaissances

La *Base de connaissances* est une section du site du Support Technique.

La page de Kaspersky Security dans la Base des connaissances (<http://support.kaspersky.com/fr/ksv4>) permet de trouver les articles qui proposent des informations utiles, des recommandations et une foire aux questions sur l'achat, l'installation et l'utilisation de l'application.

Les articles publiés dans la base de connaissances peuvent répondre à des questions qui portent sur d'autres applications de Kaspersky Lab également. Les articles de la base de connaissances peuvent contenir des nouvelles du Support Technique.

Aide électronique

L'aide électronique de l'application contient l'ensemble des fichiers de l'aide relative à l'interface locale de l'application ainsi que les fichiers de l'aide contextuelle.

Dans l'aide complète, vous trouverez des informations sur la configuration et l'utilisation de Kaspersky Security.

Dans l'aide contextuelle, vous trouverez des informations concernant les fenêtres de l'interface locale de Kaspersky Security et les fenêtres du plug-in d'administration de Kaspersky Security : liste et description des paramètres.

Documentation

La documentation du programme contient les fichiers des manuels.

Dans le manuel d'implantation, vous trouverez des informations sur les tâches suivantes :

- planification de l'installation de Kaspersky Security (avec prise en compte des principes de fonctionnement de Kaspersky Security et des exigences système) ;
- préparation de l'installation, installation et activation de Kaspersky Security.

Dans le manuel de l'administrateur, vous trouverez des informations sur la configuration et l'utilisation de Kaspersky Security.

Le manuel de l'utilisateur contient des renseignements concernant les tâches les plus fréquentes pouvant être effectuées par un utilisateur sur l'application, avec un compte disposant des droits d'accès à l'application Kaspersky Security.

Discussion sur les logiciels 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 dans notre forum (<http://forum.kaspersky.fr>).

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

Kaspersky Security for Virtualization 4.0 Light Agent

Cette rubrique décrit les fonctions, les composants et la distribution de Kaspersky Security ainsi que la configuration matérielle et logicielle requise pour l'application.

Dans cette section

A propos de Kaspersky Security for Virtualization 4.0 Light Agent	17
Nouveautés.....	22
Distribution.....	23
Configurations logicielle et matérielle	23

A propos de Kaspersky Security for Virtualization 4.0 Light Agent

Kaspersky Security for Virtualization 4.0 Light Agent est une solution intégrée assurant une protection avancée des machines virtuelles régies par les hyperviseurs VMware ESXi, Citrix XenServer, Microsoft Windows Server avec Hyper-V ou KVM (Kernel-based Virtual Machine) contre différents types de menaces pour la sécurité de l'information, contre les escroqueries et les attaques réseau.

L'application Kaspersky Security est optimisée pour assurer des performances maximales aux machines virtuelles que vous souhaitez protéger.

L'application permet de protéger les machines virtuelles avec les systèmes d'exploitation de bureau et serveur.

Protection des machines virtuelles

Chacune de ces menaces est traitée par un module particulier de l'application. Vous pouvez activer ou désactiver les composants indépendamment les uns des autres et configurer leurs paramètres de fonctionnement.

Vous pouvez installer les modules de la protection et les modules de contrôle sur une machine virtuelle dotée d'un système d'exploitation hôte pour poste de travail Microsoft Windows®. Les modules de contrôle ne peuvent pas être installés sur une machine virtuelle dotée d'un système d'exploitation hôte Microsoft Windows pour serveur.

Sur la machine virtuelle avec le système d'exploitation hôte Linux®, vous pouvez installer le composant de protection Antivirus Fichiers.

En complément *de la protection en temps réel*, réalisée par les composants de l'application, il est recommandé d'exécuter périodiquement *l'analyse* des machines virtuelles et de leurs modèles pour y détecter des virus et d'autres logiciels malveillants (cf. section "A propos de la protection en temps réel et de l'analyse de la machine virtuelle" à la p. [80](#)).

Afin de maintenir le niveau d'actualisation de l'application Kaspersky Security, il est nécessaire d'effectuer une *Mise à jour* des bases qu'elle exploite pour détecter les menaces (cf. section "Mise à jour des bases de données et des modules de l'application" page [129](#)).

Les modules suivants de l'application sont les modules de contrôle :

- **Contrôle du lancement des applications.** Ce composant recense les tentatives de lancement des applications par les utilisateurs et régule ce processus.
- **Contrôle de l'activité des applications.** Ce module enregistre les actions réalisées par les applications sous le système d'exploitation de la machine virtuelle protégée et gère l'activité des applications en fonction du groupe dans lequel le module place chaque application. Il existe un ensemble de règles défini pour chaque groupe. Ces règles gèrent l'accès des applications aux données personnelles de l'utilisateur et aux ressources du système d'exploitation. Ces données personnelles comprennent les fichiers de l'utilisateur (dossier Mes documents, fichiers cookie, informations sur l'activité de l'utilisateur), ainsi que les fichiers, les dossiers et les clés de registre contenant les paramètres de fonctionnement et les informations importantes sur les applications les plus utilisées.

- **Contrôle des périphériques.** Ce composant permet d'établir en toute souplesse des restrictions d'accès aux périphériques tenants lieux de sources de données (tels que les disques durs, les disques amovibles, les CD/DVD), d'outils de transmission des informations (tels que les modems), d'outils de conversion des données en copie physique (tels que les imprimantes) et d'interfaces permettant aux périphériques de se connecter à la machine virtuelle protégée (USB, Bluetooth).
- **Contrôle Internet.** Ce module permet de configurer en toute souplesse des restrictions d'accès aux ressources Web pour différents groupes d'utilisateurs.

Le fonctionnement des modules du contrôle est géré par les règles suivantes :

- Le Contrôle du lancement des applications utilise lors de son exécution les règles de contrôle du lancement des applications.
- Le Contrôle de l'activité des applications utilise lors de son exécution les règles de contrôle des applications.
- Le Contrôle des périphériques utilise lors de son exécution les règles d'accès aux périphériques et les règles d'accès aux bus de connexion.
- Le Contrôle Internet utilise lors de son exécution les règles d'accès aux ressources Web.

Les modules de protection sont les modules suivants :

- **Antivirus Fichiers.** Ce module permet d'éviter l'infection du système de fichiers du système d'exploitation de la machine virtuelle protégée. Le module est lancé au démarrage de Kaspersky Security. Il se trouve en permanence dans la mémoire opérationnelle et il analyse tous les fichiers ouverts, enregistrés et exécutés sous le système d'exploitation de la machine virtuelle protégée. L'Antivirus Fichiers intercepte toute tentative de s'adresser au fichier et recherche dans ce fichier les virus et d'autres applications malveillantes.
- **Surveillance du système.** Ce composant obtient des données sur les activités des applications sous le système d'exploitation de la machine virtuelle protégée et transmet ces informations aux autres composants afin de garantir une protection plus efficace.
- **Antivirus Courrier.** Ce module analyse l'ensemble des messages électroniques entrants et sortants à la recherche de virus et d'autres applications malveillantes.
- **Antivirus Internet.** Ce module analyse le trafic qui arrive sur la machine virtuelle protégée via les protocoles HTTP et FTP et définit si un lien appartient à la base des adresses Internet dangereuses ou de phishing.

- **Antivirus IM.** Ce composant analyse le trafic qui arrive sur la machine virtuelle protégée via les protocoles clients IM. Ce composant fonctionne en toute sécurité avec de nombreux clients IM.
- **Pare-feu.** Ce module assure la protection des données personnelles stockées dans le système d'exploitation de la machine virtuelle protégée de l'utilisateur en bloquant toutes les menaces éventuelles pour le système d'exploitation lorsque la machine virtuelle protégée est connectée à Internet ou au réseau local. Le module filtre toute activité réseau conformément à deux types de règles : règles réseau de l'application et règles pour les paquets réseau.
- **Surveillance du réseau.** Ce module est prévu pour consulter en temps réel les informations sur l'activité réseau de la machine virtuelle protégée.
- **Prévention des intrusions.** Ce composant recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre la machine virtuelle protégée de l'utilisateur, Kaspersky Security bloque l'activité réseau de l'ordinateur attaquant.

Pour en savoir plus sur le fonctionnement des modules de contrôle et des modules de la protection, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Fonctionnalités supplémentaires de l'application

Kaspersky Security propose plusieurs fonctions supplémentaires. Les fonctions supplémentaires servent à maintenir le logiciel à jour, à élargir les fonctions de l'application et à fournir de l'aide pendant l'utilisation de l'application.

- **Sauvegarde.** Si, au cours de l'analyse du système d'exploitation de la machine virtuelle protégée à la recherche de virus et d'autres logiciels malveillants, l'application Kaspersky Security détecte un fichier infecté, elle bloque ce fichier, le supprime du dossier du placement initial, place sa copie dans la *sauvegarde* et tente de le désinfecter. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger. Si le fichier est réparé, l'état de la copie de sauvegarde devient *Réparé*. Ensuite, vous pouvez restaurer le fichier à partir de sa copie de sauvegarde réparée dans son dossier d'origine.
- **Mise à jour.** Kaspersky Security charge les mises à jour de la base et des modules de l'application. Ceci garantit que la protection du système d'exploitation de la machine virtuelle protégée est à jour contre les nouveaux virus et autres applications malveillantes.

- **Rapports.** Pendant le fonctionnement de l'application, celle-ci génère un rapport pour chaque module et chaque tâche de l'application. Le rapport contient la liste des événements survenus pendant le fonctionnement de Kaspersky Security et de toutes les opérations exécutées par l'application. En cas de problème, vous pouvez envoyer ces rapports aux experts du Support Technique de Kaspersky Lab afin qu'ils analysent la situation plus en détail.
- **Notifications.** Grâce aux notifications, Kaspersky Security tient l'utilisateur informé sur l'état de la protection du système d'exploitation de la machine virtuelle protégée. L'application peut afficher les notifications à l'écran ou les envoyer par email.
- **Kaspersky Security Network.** La participation à Kaspersky Security Network permet d'améliorer l'efficacité de la protection du système d'exploitation de la machine virtuelle protégée grâce à une collecte productive des informations sur la réputation des fichiers, des ressources Web et des applications obtenues auprès des utilisateurs du monde entier.
- **Licence.** L'utilisation de l'application via une licence commerciale permet l'utilisation de l'ensemble des fonctions de l'application, l'accès à la mise à jour de ses bases et de ses modules, l'obtention d'informations détaillées et le recours aux experts du Support Technique de Kaspersky Lab.
- **Support Technique.** Tous les utilisateurs inscrits de Kaspersky Security peuvent bénéficier de l'aide des experts du Support Technique de Kaspersky Lab. Vous pouvez envoyer une requête via le portail Kaspersky CompanyAccount (http://support.kaspersky.com/fr/faq/companyaccount_help) sur le site du Support Technique ou recevoir une assistance téléphonique par nos agents.

Administration du logiciel

La configuration et la gestion du fonctionnement de l'application s'effectuent :

- à distance via Kaspersky Security Center (cf. "Conception de l'administration de l'application dans Kaspersky Security Center" à la p. [78](#)) ;
- via la ligne de commande pour Light Agent for Linux (cf. section "Administration du Light Agent for Linux via la ligne de commande" à la p. [199](#)) ;

- via l'interface locale du Light Agent for Windows (informations détaillées dans le *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
- via la ligne de commande pour Light Agent for Windows (voir détails dans la Base de connaissances (<http://support.kaspersky.fr/13177>)).

Nouveautés

L'application Kaspersky Security for Virtualization 4.0 Light Agent introduit les fonctionnalités suivantes :

- Le composant Light Agent est conçu pour la protection des machines virtuelles avec le système d'exploitation Linux (appelé ensuite aussi “ Light Agent for Linux ”). Le composant Light Agent for Linux permet de protéger les objets du système de fichiers situés sur les disques locaux de la machine virtuelle protégée. Il est aussi possible de créer une tâche de recherche de virus et des stratégies pour le Light Agent for Linux dans Kaspersky Security Center.
- Le système d'exploitation Windows Server 2016 est également pris en charge en tant que système d'exploitation hôte des machines virtuelles protégées.
- Le système d'exploitation Microsoft Windows Server 2016 est également pris en charge avec le rôle installé Hyper-V.
- Le serveur d'administration de l'infrastructure virtuelle Microsoft System Center Virtual Machine Manager peut en outre être utilisé pour le déploiement des SVM.
- La SVM est administrée par le système d'exploitation CentOS 7.2 (64 bits).
- La liste des applications et les entreprises qui les produisent est élargie. Vous pouvez les inclure dans la zone d'analyse et de protection ou les exclure de l'analyse et de la protection dans les paramètres de Light Agent for Windows. Ces applications sont utilisées pour l'administration et la protection antivirus des réseaux informatiques.

- Vous avez en outre la possibilité d'arrêter le lancement de l'interface locale de Light Agent for Windows sur la machine virtuelle protégée. L'arrêt du lancement de l'interface permet de diminuer l'utilisation de la mémoire, y compris lors de l'utilisation des machines virtuelles avec le système d'exploitation pour serveur dans les modes avec plusieurs sessions utilisateur.
- Le rapport sur l'utilisation des clés contient des informations sur les machines virtuelles dont la protection nécessite ces clés.

Distribution

Vous pouvez obtenir des informations sur l'achat de l'application sur le site <http://www.kaspersky.com/fr> ou auprès de nos partenaires.

La distribution contient les éléments suivants :

- les fichiers de l'application, y compris l'image de SVM (machine virtuelle de protection) avec le système d'exploitation installé CentOS 7.2 ;
- les fichiers de documentation sur l'application ;
- Le Contrat de licence utilisateur final reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction du pays où l'application est distribuée.

Les informations indispensables à l'activation de l'application vous seront envoyées par email après le paiement.

Configurations logicielle et matérielle

Pour que Kaspersky Security fonctionne sur le réseau local de l'organisation, une des versions suivantes de l'application Kaspersky Security Center doit être installée :

- Kaspersky Security Center 10 Service Pack 2;
- Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

Configuration requise pour l'infrastructure virtuelle

Le fonctionnement de Kaspersky Security dans l'infrastructure virtuelle exige l'installation de l'un des hyperviseurs suivants :

- Microsoft Windows Server 2016 Hyper-V (en mode d'installation complète ou en mode Server Core) avec les mises à jour les plus récentes ;
- Microsoft Windows Server 2012 R2 Hyper-V (en mode d'installation complète ou en mode Server Core) avec les mises à jour les plus récentes ;
- Citrix XenServer 7 ;
- Citrix XenServer 6.5 Service Pack 1 ;
- VMware ESXi 6.5 avec les mises à jour les plus récentes ;
- VMware ESXi 6.0 avec les mises à jour les plus récentes ;
- VMware ESXi 5.5 avec les mises à jour les plus récentes ;
- VMware ESXi 5.1 avec les mises à jour les plus récentes ;
- KVM (Kernel-based Virtual Machine) sur la base d'un des systèmes d'exploitation suivants :
 - Ubuntu Server 14.04 LTS ;
 - Red Hat Enterprise Linux® Server 7 correctif 1 ;
 - CentOS 7.

Pour pouvoir déployer et utiliser la SVM (machine virtuelle de protection) sous un hyperviseur VMware ESXi, le serveur VMware vCenter™ 5.1, VMware vCenter 5.5, VMware vCenter 6.0 ou VMware vCenter 6.5 doit être installé dans l'infrastructure virtuelle avec toutes les mises à jour accessibles. Le serveur VMware vCenter est un serveur d'administration de l'infrastructure virtuelle qui intervient dans le déploiement des SVM et la fourniture de données sur l'infrastructure virtuelle aux SVM.

Pour le déploiement de la SVM sous les hyperviseurs Microsoft Windows Server Hyper-V, VMware ESXi et Citrix XenServer vous pouvez utiliser le serveur de gestion de l'infrastructure virtuelle Microsoft SCVMM d'une des versions suivantes :

- Microsoft SCVMM 2012 R2 avec les dernières mises à jour ;
- Microsoft SCVMM 2016 avec les dernières mises à jour.

Pour le déploiement de la SVM sur les hyperviseurs KVM sous le système d'exploitation CentOS il est nécessaire de supprimer ou de mettre en commentaire la ligne Defaults requiretty dans le fichier de configuration /etc/sudoers du système d'exploitation de l'hyperviseur.

Configuration requise pour les ressources de la SVM dotée du module Serveur de protection de Kaspersky Security

Pour le fonctionnement de Kaspersky Security pour la SVM, il est nécessaire de prévoir la quantité minimale de ressources système suivante :

- 2 Go de mémoire vive disponible ;
- 30 Go de volume d'espace libre sur le disque ;
- interface réseau virtualisée avec bande passante de 100 Mbit/s.

Configurations requises pour la machine virtuelle dotée du module Light Agent for Windows

L'application XenTools doit être installée sur la machine virtuelle administrée par l'hyperviseur Citrix XenServer avant l'installation du module Light Agent for Windows.

Le paquet VMware™ Tools doit être installé sur la machine virtuelle administrée par l'hyperviseur VMware ESXi avant l'installation du module Light Agent for Windows.

Le paquet de services d'intégration (Integration Services) doit être installé sur la machine virtuelle administrée par Microsoft Windows Server (Hyper-V).

Pour l'installation et le fonctionnement du composant Light Agent for Windows sur la machine virtuelle, vous devez installer un des systèmes d'exploitation invités suivants :

- Windows 7 Professional / Enterprise Service Pack 1 (version 32 / 64 bits) ;
- Windows 8.1 Update 1 Pro / Enterprise (version 32 / 64 bits) ;
- Windows 10 Pro / Enterprise / Enterprise LTSC / RS1 (version 32 / 64 bits) ;

- Windows Server 2008 Service Pack 2 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2008 R2 Service Pack 1 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2012 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2012 R2 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2016 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits).

Le Light Agent for Windows peut protéger les machines virtuelles qui font partie de l'infrastructure utilisant les solutions suivantes pour la virtualisation :

- Citrix XenDesktop 7.9 ou Citrix XenDesktop 7.11 ;
- Citrix Provisioning Services 7.9 ou Citrix Provisioning Services 7.11 ;
- VMware Horizon™ View 7.

Configurations requises pour la machine virtuelle dotée du module Light Agent for Linux

Configuration logicielle requise pour l'installation et le fonctionnement du composant Light Agent for Linux :

- interprète de la langage Perl à la version 5.0 ou ultérieure <http://www.perl.org> ;
- utilitaire installé which ;
- paquets installés pour la compilation des applications (gcc, binutils, glibc, glibc-devel, make, ld), code initial du noyau du système d'exploitation – pour la compilation des modules Kaspersky Security ;
- Le package de 32 bits libc doit être installé sur les versions 64 bits des systèmes d'exploitation pour serveur hôte Linux avant l'installation de Kaspersky Security ;
- paquet installé dmidecode.

Pour l'installation et le fonctionnement du composant Light Agent for Linux sur la machine virtuelle, vous devez installer un des systèmes d'exploitation serveurs hôtes suivants :

- Debian GNU / Linux 8.5 (version 32 / 64 bits) ;
- Ubuntu Server 14.04 LTS (version 32 /64 bits) ;
- Ubuntu Server 16.04 LTS (version 64 bits) ;
- CentOS 6.8 (version 64 bits) ;
- CentOS 7.2 (version 64 bits) ;
- Red Hat Enterprise Linux Server 6.7 (version 64 bits) ;
- Red Hat Enterprise Linux Server 7.2 (version 64 bits) ;
- SUSE Linux Enterprise Server 12 Service Pack 1 (version 64 bits).

Sur la machine virtuelle, où Light Agent for Linux sera installé, vous devez installer le composant Agent d'administration version 10.1.1.-X. L'agent d'administration version 10.1.1-X fait partie de la suite de l'application Kaspersky Security for Virtualization 4.0 Light Agent.

Configuration logicielle et matérielle requise par le composant Serveur d'intégration

Pour l'installation et le fonctionnement du composant Serveur d'intégration sur l'ordinateur, vous devez installer un des systèmes d'exploitation suivants :

- Windows Server 2008 R2 Service Pack 1 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2012 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2012 R2 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits) ;
- Windows Server 2016 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 64 bits).

Pour le fonctionnement du Serveur d'intégration, de la Console de gestion du Serveur d'intégration et des plug-ins d'administration de Kaspersky Security, la plateforme Microsoft.NET Framework 4.6 est requise. La plateforme sera automatiquement installée au cours de l'installation du Serveur d'intégration, de la Console de gestion du Serveur d'intégration et des plug-ins d'administration de Kaspersky Security.

Pour l'installation et le fonctionnement du Serveur d'intégration, l'ordinateur doit respecter la configuration matérielle minimale suivante :

- volume d'espace libre sur le disque de 40 Mo ;
- volume de mémoire vive :
 - pour le fonctionnement de la Console de gestion du Serveur d'intégration : 50 Mo ;
 - pour le fonctionnement du Serveur d'intégration qui ne sert pas plus de 30 hyperviseurs et 2000-2500 machines virtuelles protégées : 300 Mo. Le volume de mémoire vive peut changer en fonction de la taille de l'infrastructure virtuelle.

Architecture de l'application

Cette section décrit les composants de Kaspersky Security et leur interaction.

Dans cette section

Présentation de l'architecture de l'application	29
Variantes de déploiement des SVM	32
A propos de la connexion de Light Agent aux SVM	34
A propos du Serveur d'intégration	37

Présentation de l'architecture de l'application

Kaspersky Security for Virtualization 4.0 Light Agent est une solution intégrée offrant une protection avancée des machines virtuelles fonctionnant sous les hyperviseurs VMware ESXi, Microsoft Windows Server (Hyper-V), Citrix XenServer ou KVM contre les virus et autres applications malveillantes, et contre les escroqueries et les attaques réseau.

Modules de l'application

Les composants suivants font partie du programme :

- *Serveur de protection de Kaspersky Security* (ci-après “ Serveur de protection ”).
- *Light Agent de Kaspersky Security* (ci-après “ Light Agent ”).
- *Serveur d'intégration* (cf. section "A propos du Serveur d'intégration" à la page [37](#)).

Le serveur de protection se présente sous la forme d'une image de SVM (machine virtuelle de protection).

La SVM (*secure virtual machine, machine virtuelle de protection*) est une machine virtuelle située sur un hyperviseur et dotée d'un composant Serveur de protection. La SVM doit être déployée sur chaque hyperviseur dont vous souhaitez protéger les machines virtuelles à l'aide de Kaspersky Security.

Le déploiement d'une SVM s'effectue via le système d'administration centralisée à distance des applications de Kaspersky Lab Kaspersky Security Center. Le déploiement manuel d'une SVM via l'hyperviseur n'est pas pris en charge.

Light Agent est installé sur les machines virtuelles disposant du système d'exploitation Windows (y compris sur les modèles de machines virtuelles et sur le disque virtuel chargé depuis le serveur PVS sur les machines virtuelles du réseau) et sur les machines virtuelles disposant du système d'exploitation Linux. *Machine virtuelle protégée* : machine virtuelle dotée du composant Light Agent de l'application. Le Light Agent doit être installé sur chaque machine virtuelle à protéger à l'aide de Kaspersky Security. Le Light Agent for Windows s'installe en local sur la machine virtuelle ou à distance via le Kaspersky Security Center ou l'éditeur d'administration des stratégies de groupe des services de catalogue (Active Directory® Group Policies). Light Agent for Linux s'installe localement à partir de la ligne de commande ou à distance via le Kaspersky Security Center.

Administration du logiciel

La configuration et la gestion du fonctionnement de l'application s'effectuent :

- à distance via Kaspersky Security Center (cf. section "Conception de l'administration de l'application dans Kaspersky Security Center" à la p. [78](#)) ;
- via la ligne de commande pour Light Agent for Linux (cf. section "Administration du Light Agent for Linux via la ligne de commande" à la p. [199](#)) ;
- via l'interface locale du Light Agent for Windows (informations détaillées dans le *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

L'interaction entre Kaspersky Security et l'application Kaspersky Security Center est assurée par l'Agent d'administration, le composant Kaspersky Security Center. L'Agent d'administration figure dans l'image de la SVM de Kaspersky Security. Si vous souhaitez gérer le fonctionnement du Light Agent installé sur les machines virtuelles protégées à l'aide de Kaspersky Security Center, vous devez installer l'Agent d'administration sur ces machines virtuelles. Si l'Agent d'administration n'est pas installé sur la machine virtuelle protégée, l'administration du fonctionnement du Light Agent sur cette machine virtuelle s'effectue via l'interface locale de Light Agent for Windows ou via la ligne de commande de Light Agent for Linux.

L'interface d'administration de l'application Kaspersky Security via le Kaspersky Security Center est assurée par les plug-ins d'administration. Les plug-ins d'administration de Kaspersky Security font partie de la suite d'installation de Kaspersky Security. Les plug-ins d'administration de Kaspersky Security doivent être installés sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center.

Fonctions du Serveur de protection

Lors du lancement, le Light Agent met en place et assure la connexion au Serveur de protection. Par défaut, le Light Agent se connecte au Serveur de protection installé sur la SVM située sur l'hyperviseur comportant la machine virtuelle protégée (cf. section "A propos de la connexion du Light Agent à la SVM" à la page [34](#)).

Le Serveur de protection remplit les fonctions suivantes :

- Identifie le Light Agent installé sur la machine virtuelle protégée.
- Reçoit les informations en temps réel sur l'état de l'infrastructure virtuelle et les transmet au Light Agent et à l'application Kaspersky Security Center.
- Analyse les fichiers de toutes les machines virtuelles sur lesquels le Light Agent est installé pour y détecter des virus et d'autres applications malveillantes.
- Utilisation de la technologie SharedCache qui permet d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers ayant déjà été analysés sur une autre machine virtuelle. Pendant son fonctionnement, Kaspersky Security conserve dans le cache de la SVM les informations relatives aux fichiers analysés afin de ne pas les analyser une nouvelle fois. Si les informations relatives au fichier à analyser ne figurent pas dans le cache de la SVM, Kaspersky Security peut utiliser KSN lors de l'analyse. Les services KSN sont utilisés par l'application si vous avez accepté de participer au programme Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page [192](#)).
- Charge le paquet de mise à jour depuis le stockage du Serveur d'administration de Kaspersky Security Center dans le dossier de la SVM et met à jour les bases de l'application sur cette dernière. Les mises à jour des bases et des modules de l'application indispensables au bon fonctionnement du Light Agent se chargent à partir du dossier de la SVM vers la machine virtuelle protégée (cf. section "Mise à jour des bases de données et des modules de l'application" à la page [129](#)).
- Gestion des clés et contrôle des conditions de licence (cf. section " Licence de l'application " à la page [39](#)).

Variantes de déploiement des SVM

Les SVM doivent être déployées sur les hyperviseurs de l'infrastructure virtuelle comportant les machines virtuelles que vous souhaitez protéger à l'aide de l'application Kaspersky Security.

Hyperviseurs VMware ESXi

Options de déploiement des SVM sur les hyperviseurs VMware ESXi :

- Déploiement sur l'hyperviseur autonome VMware ESXi connecté au serveur VMware vCenter.
- Déploiement sur les hyperviseurs VMware ESXi entrant dans la composition du cluster DRS ou d'un pool de ressources.

Une fois déployée, la SVM se connecte automatiquement à l'hyperviseur. Autrement dit, elle ne migre pas vers d'autres hyperviseurs VMware ESXi dans le cadre d'un cluster DRS ou d'un pool de ressources conformément aux règles de migration de VMware DRS.

Hyperviseurs Citrix XenServer

Variantes de déploiement des SVM sur les hyperviseurs Citrix XenServer :

- Déploiement sur un hyperviseur autonome Citrix XenServer.
- Déploiement sur un hyperviseur entrant dans la composition du pool d'hyperviseurs Citrix XenServer.

Il est possible de déployer la SVM dans le stockage local de l'hyperviseur ou dans la sauvegarde commune du pool d'hyperviseurs Citrix XenServer.

Après son lancement, la SVM déployée dans le stockage commun est activée sur l'hyperviseur qui fait partie d'un pool d'hyperviseurs Citrix XenServer présentant le plus de ressources et/ou étant le moins chargé. Si la SVM possède une clé avec des restrictions selon le nombre de cœurs, lors du contrôle des restrictions de licence, le décompte additionne le nombre de cœurs de processeurs présents sur l'hyperviseur où ces machines sont utilisées. Si vous utilisez un schéma de licence en fonction du nombre de cœurs, le serveur de protection peut envoyer à Kaspersky Security Center un événement reprenant les informations relatives à la violation des conditions de la licence. Vous pouvez ignorer cet événement.

Hyperviseurs Microsoft Windows Server (Hyper-V)

Options de déploiement des SVM sur des hyperviseurs Microsoft Windows Server (Hyper-V) :

- Déploiement sur un hyperviseur autonome Microsoft Windows Server (Hyper-V).
- Déploiement sur les hyperviseurs Microsoft Windows Server (Hyper-V) entrant dans la composition du cluster d'hyperviseurs administré par le service Windows Failover Clustering.

Lors du déploiement d'une SVM sur l'hyperviseur Microsoft Windows Server (Hyper-V), tous les fichiers nécessaires au fonctionnement de la SVM figurent dans un dossier distinct. Le nom de la SVM est attribué à ce dossier.

► *Pour déployer une SVM sur un cluster d'hyperviseurs Microsoft Windows Server (Hyper-V), procédez comme suit :*

1. Déployer la SVM sur chaque hyperviseur entrant dans la composition du cluster d'hyperviseurs. Si vous souhaitez effectuer une migration à chaud de la SVM entre les nœuds du cluster, placez le dossier avec les fichiers de la SVM sur le volume partagé de cluster.
2. À l'aide de la console Failover Cluster Manager, transformez chaque SVM en machine virtuelle de cluster.
3. Indiquez l'hyperviseur sur lequel la SVM doit fonctionner dans les propriétés des rôles du cluster de chaque SVM, dans le champ **Possible Owners**. Pour cela, vous pouvez utiliser la console Failover Cluster Manager ou Microsoft System Center Virtual Machine Manager.

Pour en savoir plus sur l'utilisation d'un cluster d'hyperviseurs Microsoft Windows Server (Hyper-V), consultez la documentation de l'infrastructure virtuelle.

Hyperviseurs KVM

Variantes de déploiement des SVM sur les hyperviseurs KVM :

- Déploiement sur un hyperviseur autonome KVM.
- Déploiement sur les hyperviseurs KVM entrant dans la composition du cluster d'hyperviseurs.

Lors du déploiement d'une SVM sur les hyperviseurs KVM entrant dans la composition HA du cluster, vous devez configurer l'association de la SVM et des nœuds du cluster. Pour en savoir plus, consultez la documentation du logiciel utilisé pour gérer les ressources du cluster.

A propos de la connexion Light Agent à la SVM

Le fonctionnement du composant Light Agent implique la connexion du Light Agent à la SVM dotée d'un Serveur de protection.

L'analyse des fichiers qui doit être conforme aux paramètres de protection et au cours de l'exécution des tâches d'analyse lancées s'effectue sur le Serveur de protection. Le Light Agent transmet les fichiers pour analyse au Serveur de protection après la connexion à la SVM.

Si le Light Agent n'est connecté à aucune SVM, le Serveur de protection ne vérifie pas les fichiers des machines virtuelles en question. Si au cours de l'exécution des tâches d'analyse lancées, le Light Agent perd la connexion à la SVM pendant plus de 5 minutes, l'exécution des tâches d'analyse s'arrête et celles-ci s'achèvent par une erreur.

Si le Light Agent n'est connecté à aucune SVM pendant plus de 5 minutes, l'état de la protection de la machine virtuelle protégée dans Kaspersky Security Center devient *Suspendue*. Si vous souhaitez que dans ce cas, l'état de la machine virtuelle dans Kaspersky Security Center passe à *Critique*, définissez la condition d'attribution de l'état *Critique* de la manière suivante : définissez "Le niveau de protection en temps réel est différent du niveau défini par l'administrateur" sur "En cours". Pour plus d'informations sur la configuration des conditions d'attribution des états, consultez la documentation de Kaspersky Security Center.

Pour choisir la SVM à connecter, le Light Agent doit recevoir les informations sur les SVM fonctionnant sur le réseau (cf. section "A propos de la détection des SVM" à la p. [35](#)).

Le Light Agent choisit la SVM optimale pour la connexion conformément à l'algorithme du choix des SVM (cf. section "A propos de l'algorithme de choix des SVM" sur p. [36](#)).

Dans cette section

A propos de la détection des SVM	35
A propos de l'algorithme de choix des SVM	36

A propos de la détection des SVM

Le Light Agent peut détecter les SVM fonctionnant sur le réseau par une des méthodes suivantes :

- À l'aide de la diffusion multipoint (Multicast). Les SVM pour lesquelles cette méthode d'octroi d'informations est sélectionnée exécutent la diffusion multipoint (Multicast) des informations les concernant. Les Light Agents reçoivent ces informations et créent la liste des SVM accessibles pour la connexion. Cette méthode est utilisée par défaut.

Pour pouvoir utiliser cette méthode de transmission des informations, la diffusion multipoint doit être autorisée sur le réseau.

- À l'aide du Serveur d'intégration (cf. section "A propos du Serveur d'intégration" à la page [37](#)). Les SVM transmettent des informations les concernant au serveur d'intégration. Le serveur d'intégration crée la liste des SVM accessibles pour la connexion et la transmet au Light Agent.

Pour pouvoir utiliser cette méthode de transmission des informations, vous devez configurer la connexion des SVM et des Light Agents au Serveur d'intégration.

- A l'aide de la liste d'adresses de SVM. Vous pouvez indiquer la liste des SVM auxquelles peuvent se connecter les Light Agents.

Le mode adopté par les SVM pour transférer les informations à leur sujet peut être défini dans la stratégie pour le Serveur de protection (cf. section "Étape 5. Configuration des paramètres de détection des SVM" à la p. [90](#)). La SVM peut transmettre les informations simultanément la concernant à l'aide de la diffusion multiadresse et du Serveur d'intégration.

Vous pouvez choisir la méthode qu'utilise le Light Agent for Windows pour la détection des SVM dans la stratégie pour le Light Agent for Windows (cf. section "Etape 6. Configuration des paramètres de détection des SVM" à la p. [102](#)) ou dans l'interface locale.

Vous pouvez choisir la méthode qu'utilise le Light Agent for Linux pour la détection des SVM dans la stratégie pour le Light Agent pour Linux (cf. section "Etape 5. Configuration des paramètres de détection des SVM" à la p. [114](#)).

Pour le Light Agent vous pouvez choisir seulement une de trois méthodes possibles de détection des SVM.

Après la réception des informations sur les SVM accessibles pour la connexion, le Light Agent choisit la SVM conformément à l'algorithme de choix celle-ci et s'y connecte (cf. section "A propos de l'algorithme de choix des SVM" p. [36](#)).

Vous pouvez recevoir les informations sur la SVM à laquelle le Light Agent est connecté :

- Pour Light Agent for Windows – dans l'interface locale du Light Agent for Windows dans la fenêtre **Support Technique** ;
- Pour Light Agent for Linux – à l'aide de la commande `svminfo` (cf. section "Consultation des informations sur les SVM" à la p. [201](#)).

A propos de l'algorithme de choix des SVM

Lors du choix de la SVM pour la connexion, les Light Agents utilisent un algorithme de choix tenant compte de l'emplacement de la SVM par rapport à l'hyperviseur sur lequel est installé le Light Agent et du nombre actuel de Light Agents connectés à la SVM :

1. Après l'installation et le lancement sur la SVM, le Light Agent se connecte à celle déployée sur l'hyperviseur où il est installé. Si plusieurs SVM sont déployées sur l'hyperviseur, le Light Agent choisit celle à laquelle les Light Agents connectés sont les moins nombreux.
2. Si la SVM de l'hyperviseur du Light Agent n'est pas accessible, le Light Agent choisit la SVM desservant le moins de Light Agents parmi celles accessibles sur d'autres hyperviseurs.
3. Dès que la SVM située sur le même hyperviseur que la machine virtuelle protégée devient accessible, le Light Agent s'y connecte.

Le Light Agent ne se connecte pas à une SVM sur laquelle l'application n'est pas activée (clé non ajoutée) si l'infrastructure virtuelle comporte une SVM sur laquelle l'application est activée. Si l'application n'est activée sur aucune SVM, le Light Agent se connecte à l'une de ces SVM en fonction de l'algorithme de choix. Après l'activation de l'application sur une ou plusieurs SVM, le Light Agent se connecte à l'une d'elles en fonction de l'algorithme de choix.

A propos du Serveur d'intégration

Le *Serveur d'intégration* est un composant de l'application Kaspersky Security qui transmet des informations issues des SVM disposant d'un Serveur de protection aux Light Agents installés sur les machines virtuelles protégées. Les SVM transmettent au Serveur d'intégration les informations nécessaires à leur connexion aux Light Agents. Les Light Agents reçoivent ces informations du Serveur d'intégration. Vous pouvez utiliser le Serveur d'intégration pour détecter des SVM et pour recevoir des informations les concernant via les Light Agents s'il est impossible de faire appel à la diffusion multipoint (Multicast).

Si vous souhaitez utiliser le Serveur d'intégration, procédez comme suit :

1. Installer le Serveur d'intégration et sa Console d'administration.
2. Configurer les paramètres de connexion des SVM au Serveur d'intégration.
La configuration des paramètres de connexion s'opère lors de la création d'une stratégie pour le Serveur de protection (cf. "Étape 5. Configuration des paramètres de détection des SVM " à la p. [90](#)) ou dans les propriétés de la stratégie.

3. Configurer les paramètres de connexion des Light Agents au Serveur d'intégration.

La configuration des paramètres de connexion du Light Agent for Windows au Serveur d'intégration est exécutée dans la stratégie pour le Light Agent pour Windows (cf. section "Etape 6. Configuration des paramètres de détection des SVM" à la p. [102](#)) ou dans l'interface locale du Light Agent for Windows.

La configuration des paramètres de connexion du Light Agent for Linux au Serveur d'intégration est exécutée dans la stratégie pour le Light Agent for Linux (cf. section "Etape 5. Configuration des paramètres de détection des SVM" à la p. [114](#)).

Les SVM pour lesquelles les paramètres de connexion au Serveur d'intégration sont configurés transmettent des informations à ce serveur toutes les 5 minutes.

Les SVM transmettent au Serveur d'intégration les informations suivantes :

- adresse IP et numéro de port pour la connexion à la SVM ;
- nom de l'hyperviseur sur lequel fonctionne la SVM ;
- informations à partir desquelles Light Agent peut déterminer quelle SVM est déployée sur l'hyperviseur où il est installé ;

- informations sur la licence ;
- durée moyenne des requêtes d'analyse des fichiers dans la file d'attente.

Les Light Agents pour lesquels les paramètres de connexion au Serveur d'intégration sont configurés essaient de se connecter au Serveur d'intégration toutes les 5 minutes si :

- Le Light Agent ne dispose d'informations sur aucune des SVM ;
- la dernière tentative de connexion du Light Agent au Serveur d'intégration s'est soldée par un échec.

Une fois que les Light Agents ont reçu du Serveur d'intégration des informations sur les SVM, l'intervalle de connexion du Light Agent au Serveur d'intégration augmente jusqu'à 30 minutes.

Le Serveur d'intégration envoie aux Light Agents la liste des SVM auxquelles ils peuvent se connecter ainsi que les informations les concernant. À partir des informations reçues, les Light Agents sélectionnent la SVM à laquelle ils se connectent.

Lors de son fonctionnement, le Serveur d'intégration enregistre les informations suivantes :

- informations nécessaires à la connexion au Serveur d'intégration des SVM, des Light Agents et de la Console de gestion du Serveur d'intégration ;
- paramètres exigés pour la connexion des Light Agents aux SVM.

Toutes les données sont protégées. Les informations sont enregistrées sur l'ordinateur hébergeant le Serveur d'intégration et ne sont pas automatiquement envoyées à Kaspersky Lab.

Vous pouvez configurer les paramètres du Serveur d'intégration dans la Console de gestion du Serveur d'intégration.

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 Utilisateur Final.....	40
A propos de la licence.....	40
A propos du Certificat de licence.....	42
A propos de la clé	42
A propos du code d'activation	44
Présentation du fichier clé.....	44
A propos de l'abonnement.....	45
A propos de l'activation de l'application	46
Procédure d'activation de l'application.....	50
Renouvellement de la licence	59
Renouvellement de l'abonnement	60
Consultation des informations relatives aux clés utilisées	61

A propos du Contrat de Licence Utilisateur Final

Le Contrat de Licence Utilisateur Final est l'accord légal conclu entre vous et Kaspersky Lab AO qui précise les conditions d'utilisation du logiciel.

Veuillez lire attentivement les conditions du Contrat de licence utilisateur final avant d'utiliser l'application.

Vous pouvez prendre connaissance des conditions du contrat de licence utilisateur final par les moyens suivants :

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

Vous acceptez les conditions du contrat de licence utilisateur final, 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 utilisateur final, 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 utilisateur final.

La licence vous donne droit aux types de service suivants :

- utilisation de l'application conformément aux conditions du Contrat de Licence Utilisateur Final ;
- accès au 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.

Les types de licences suivants sont prévus :

- *Evaluation* : une licence gratuite conçue pour faire découvrir l'application.

La durée de validité de la licence d'évaluation est courte. Une fois que la licence d'évaluation a expiré, Kaspersky Security arrête de remplir toutes ses fonctions. Pour continuer à utiliser l'application, il est nécessaire d'acheter une licence commerciale.

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

- *Commerciale* : licence payante octroyée à l'achat de l'application.

A l'expiration de la licence commerciale, l'application continue à fonctionner, mais avec des fonctionnalités limitées (par exemple, la mise à jour des bases de données de Kaspersky Security n'est pas disponible). Pour pouvoir profiter de toutes les fonctionnalités de Kaspersky Security, vous devez renouveler la licence commerciale.

Il est conseillé de renouveler la licence avant son expiration afin de garantir une protection maximale contre les menaces informatiques.

Les *schémas de licence* suivants sont prévus pour Kaspersky Security :

- Licence selon le nombre de machines virtuelles protégées par l'application. Ce schéma de licence repose sur des clés pour serveur ou pour poste de travail (en fonction du système d'exploitation des machines virtuelles protégées). En fonction des restrictions imposées par la licence, l'application intervient dans la protection d'un nombre défini de machines virtuelles sur lesquelles le composant Light Agent est installé.
- Licence en fonction du nombre de cœurs utilisés dans les processeurs physiques sur les hyperviseurs comportant des machines virtuelles protégées. Dans ce schéma, la licence utilise des clés avec limitation en fonction du nombre de cœurs. En fonction des restrictions imposées par la licence, l'application intervient dans la protection de toutes les machines virtuelles dotées du module Light Agent et installées sur les hyperviseurs dans lesquels un nombre défini de cœurs de processeurs physique est utilisé.

Il est recommandé d'utiliser uniquement l'un des deux schémas de licence prévus pour l'ensemble des SVM et des machines virtuelles protégées rattachées.

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.

Si vous utilisez l'application avec un abonnement, aucun Certificat de licence n'est fourni.

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

- numéro de licence ;
- informations sur l'utilisateur titulaire de la licence ;
- informations sur l'application qu'il est possible d'activer grâce à la licence ;
- restrictions sur le nombre d'unités de licences (par exemple, nombre de périphériques sur lesquels il est possible d'utiliser l'application grâce à la licence) ;
- date de début de validité de la licence ;
- date de fin de validité de la licence ou durée de validité de la licence ;
- type de licence.

A propos de la clé

La *clé* est une séquence de bits qui permet d'activer, puis d'utiliser l'application dans le respect des conditions du Contrat de licence utilisateur final. Cette clé est générée par les experts de Kaspersky Lab.

Vous pouvez ajouter la clé à l'application de l'une des manières suivantes : appliquer le *fichier clé* ou saisir le *code d'activation*. La clé s'affiche dans l'interface de l'application sous la forme d'une séquence unique de chiffres et de lettres après que vous l'avez ajoutée à l'application.

Une fois les clés ajoutées, vous pouvez les remplacer par d'autres.

Kaspersky Lab est en mesure de bloquer la clé en cas de violation des dispositions du Contrat de licence utilisateur final. Si la clé est bloquée, vous pouvez contacter le Support Technique ou ajouter une autre clé pour l'application.

Kaspersky Security accepte les types de clés suivants :

- *Clé pour serveur* : clé de l'application destinée à la protection des machines virtuelles dotées d'un système d'exploitation pour serveurs.
- *Clé pour poste de travail* : clé de l'application destinée à la protection des machines virtuelles dotées d'un système d'exploitation pour poste de travail.
- *Clé avec limitation en fonction du nombre de cœurs du processeur* : clé de l'application destinée à la protection des machines virtuelles, quel que soit le type de système d'exploitation dont elles disposent. En fonction des restrictions imposées par la licence, l'application intervient dans la protection de toutes les machines virtuelles fonctionnant sur les hyperviseurs dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

La clé peut être active ou complémentaire.

Clé active : clé utilisée lors du fonctionnement de l'application. Une clé pour licence d'évaluation, une clé pour licence commerciale ou une clé d'abonnement peut être ajoutée en tant que clé active. Une seule et même SVM ne peut pas compter plus d'une clé active de chaque type (clé pour serveur, clé pour poste de travail et clé avec restrictions par nombre de cœurs de processeur). Si la SVM intervient dans l'infrastructure virtuelle de protection des machines virtuelles avec système d'exploitation pour serveurs ou poste de travail, il convient d'ajouter deux clés : une clé de type serveur et une clé pour poste de travail.

Clé complémentaire : clé confirmant le droit d'utilisation de l'application mais qui ne s'utilise pas au moment donné. Une clé additionnelle devient automatiquement une clé active à l'échéance de la durée de validité de la clé active en cours.

Une clé additionnelle peut être ajoutée uniquement en présence d'une clé active du même type. La clé active et la clé additionnelle doivent correspondre au même type de licence.

Les clés de licence d'évaluation ou d'abonnement ne peuvent être ajoutées qu'en tant que clé active. Il est impossible d'ajouter une clé de licence d'évaluation ou une clé d'abonnement en tant que clé additionnelle. Une clé de licence d'évaluation ne peut pas remplacer une clé commerciale active.

A propos du code d'activation

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

Pour activer l'application avec un code d'activation, il est nécessaire de disposer d'un accès Internet en vue de se connecter aux serveurs d'activation de 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 restaurer le code d'activation, il est nécessaire d'envoyer une demande au Support Technique de Kaspersky Lab (cf. section "Modes d'obtention du Support Technique" à la page [213](#)).

Présentation 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.

Vous recevez le fichier clé à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security ou après la commande d'une version d'essai de Kaspersky Security.

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

Pour restaurer le fichier clé, il est nécessaire d'envoyer une demande au Support Technique (cf. section "Modes d'obtention du Support Technique" à la page [213](#)).

A propos de l'abonnement

L'abonnement à *Kaspersky Security* constitue une commande pour l'utilisation de l'application selon des paramètres sélectionnés (date d'expiration, nombre de périphériques protégés). Il est possible de souscrire un abonnement à Kaspersky Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur d'accès à Internet). Vous pouvez accepter ou refuser un abonnement.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour continuer à utiliser Kaspersky Security après la date d'expiration d'un abonnement limité, vous devez le renouveler (cf. section "Renouvellement de l'abonnement" à la page [60](#)). L'abonnement illimité se renouvelle automatiquement selon les conditions en vigueur au moment du paiement au prestataire de services.

Si un abonnement est suspendu, il est possible que vous bénéficiiez d'une période de renouvellement à tarif préférentiel à son expiration afin de le renouveler. Toutes les fonctions de l'application demeurent opérationnelles durant cette période. La proposition d'une période de grâce et, le cas échéant, sa durée, dépendent du fournisseur de services.

Si un abonnement n'est pas prolongé, à l'expiration de la période de grâce, Kaspersky Security continue à fonctionner mais arrête de mettre à jour les bases de l'application et d'utiliser Kaspersky Security Network.

Pour utiliser Kaspersky Security sur abonnement, vous devez modifier le code d'activation fourni par le prestataire de services. Suite à l'enregistrement du code d'activation, une clé d'abonnement est ajoutée à l'application. Il s'agit d'une clé active correspondant à la licence d'utilisation de l'application par abonnement. Les informations concernant cette clé figurent sur l'interface de Kaspersky Security Center (cf. section "Consultation des informations relatives aux clés utilisées" à la page [61](#)).

Les SVM sur lesquelles l'application est utilisée sur abonnement envoient un événement à Kaspersky Security Center en cas de modification de l'état et des paramètres de l'abonnement par le prestataire de service. Si l'abonnement est terminé, l'état de la SVM dans Kaspersky Security Center passe à *Critique*.

Si vous souhaitez résilier l'abonnement et continuer à utiliser l'application avec une licence commerciale, vous pouvez ajouter cette licence commerciale en tant que clé additionnelle (cf. section "Renouvellement de la licence" à la page [59](#)) avant la fin de l'abonnement.

Cette clé prendra automatiquement le statut de clé active après la fin de l'abonnement limité ou après le refus de l'abonnement illimité. Pour résilier l'abonnement, vous devez contacter le prestataire de services auprès de qui vous avez acheté Kaspersky Security.

Une clé d'abonnement ne peut être ajoutée qu'en tant que clé active. Il est impossible d'ajouter une clé par abonnement en tant que clé additionnelle.

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

A propos de l'activation de l'application

Activation de l'application : cette procédure d'activation de la licence permet l'utilisation de l'ensemble des fonctions de la version de l'application tout au long de la durée de validité de la licence.

L'activation de l'application doit être effectuée sur une SVM sur laquelle la date et l'heure du système sont correctes. Si vous avez modifié la date et l'heure du système après l'activation de l'application, la clé sera inutilisable. L'application ne met plus à jour les bases et Kaspersky Security Network n'est pas accessible. La clé n'est de nouveau utilisable qu'après une réinstallation du système d'exploitation.

Pour activer l'application, il est nécessaire d'ajouter la clé à toutes les SVM. Pour ajouter une clé sur les SVM, la *tâche d'activation de l'application* est utilisée.

Lors de la création de la tâche d'activation de l'application, une clé du stockage des clés de Kaspersky Security Center est utilisée.

Vous pouvez ajouter une clé au stockage de Kaspersky Security Center d'une des manières suivantes :

- via un fichier clé ;
- via un code d'activation.

Vous pouvez ajouter une clé au stockage de Kaspersky Security Center lorsque vous créez la tâche d'activation de l'application sur les SVM (cf. section "Procédure d'activation de l'application" à la page [50](#)).

Après l'activation de l'application sur les SVM, le composant Serveur de protection transmet les informations sur la licence au composant Light Agent installé sur les machines virtuelles protégées. Si le statut de la clé change, la SVM transmet les informations au Light Agent.

Vous pouvez consulter des informations sur la licence d'activation de l'application sur la machine virtuelle protégée :

- pour le Light Agent for Windows : dans l'interface locale du Light Agent for Windows dans la fenêtre **Licence** ;
- pour le Light Agent for Linux à l'aide de la commande license (cf. section "Consultation des informations sur la licence" à la p. [202](#)).

Vous pouvez consulter les informations sur les clés ajoutées sur la SVM dans la Console d'administration de Kaspersky Security Center (cf. section "Consultation des informations sur les clés utilisées" à la p. [61](#)).

Si les informations sur la licence ne sont pas transmises à la machine virtuelle protégée avec le composant Light Agent for Windows, celui-ci fonctionne en mode de fonctionnalité réduite :

- seuls les composants Antivirus Fichiers et Pare-feu du Light Agent fonctionnent ;
- seules les tâches d'analyse complète, d'analyse personnalisée et d'analyse rapide peuvent être réalisées ;
- la mise à jour des bases de données et des composants de l'application servant au fonctionnement du Light Agent n'a lieu qu'une seule fois.

Si les informations sur la licence ne sont pas transmises à la machine virtuelle protégée avec le composant Light Agent for Linux, celui-ci fonctionne en mode de fonctionnalité réduite : la mise à jour des bases de l'application indispensables au fonctionnement du Light Agent est exécutée une seule fois.

Si votre infrastructure comprend plusieurs exemplaires de l'application Kaspersky Security gérées par plusieurs serveurs d'administration Kaspersky Security Center non hiérarchisés, vous pouvez activer les différents exemplaires de l'application Kaspersky Security par l'ajout d'une seule clé.

Une clé ajoutée auparavant sur une SVM gérée par un Serveur d'administration Kaspersky Security Center peut être ajoutée à une SVM gérée par un autre Serveur d'administration Kaspersky Security Center si la licence associée à la clé n'a pas expiré.

Lors du contrôle des restrictions imposées par la licence, on détermine le nombre d'unités couvertes par la licence, pour lesquelles une clé est utilisée, sur tous les Serveurs d'administration Kaspersky Security Center.

► *Pour utiliser une clé ajoutée auparavant sans violer les conditions de la licence, procédez comme suit :*

1. Supprimez les SVM sur lesquelles l'application est activée à l'aide de l'ajout de cette clé sur un seul Serveur d'administration de Kaspersky Security Center.
2. Créez et exécutez la tâche d'activation de l'application sur un autre Serveur d'administration Kaspersky Security Center. Vous pouvez préalablement exporter la clé ajoutée au stockage des clés de Kaspersky Security Center d'un Serveur d'administration vers un autre (pour en savoir plus, consulter la documentation sur Kaspersky Security Center).

Dans cette section

Conditions pour activer l'application à l'aide d'un code d'activation	48
Particularités de l'activation de l'application avec plusieurs types de clés.....	49

Conditions pour activer l'application à l'aide d'un code d'activation

Pour ajouter une clé au stockage des clés de Kaspersky Security Center et activer l'application avec un code d'activation, il convient de se connecter aux serveurs d'activation Kaspersky Lab. L'Assistant d'ajout de clé dans le stockage transmet les données au serveur d'activation Kaspersky Lab pour qu'il vérifie le code d'activation saisi. La connexion aux serveurs d'activation est assurée par le service Activation Proxy. Il est impossible d'ajouter une clé dans le stockage avec un code d'activation si le service Activation Proxy est déconnecté. Si l'accès Internet s'effectue via le serveur proxy, les paramètres du serveur proxy doivent être configurés dans les propriétés du Serveur d'administration de Kaspersky Security Center.

Vous pouvez consulter les informations détaillées sur le service Activation Proxy et sur les paramètres du serveur proxy dans la documentation de Kaspersky Security Center.

Particularités de l'activation de l'application avec plusieurs types de clés

Si vous utilisez un schéma de licence en fonction du nombre de machines virtuelles protégées, le type de clé avec lequel vous activez l'application doit correspondre au système d'exploitation invité des machines virtuelles :

- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour serveur, il faut ajouter à la SVM une clé pour serveur ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour poste de travail, il faut ajouter à la SVM une clé pour poste de travail ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour serveur et d'un système pour poste de travail, il faut ajouter à la SVM une clé pour serveur et une clé pour poste de travail.

Si vous utilisez un schéma de licence en fonction du nombre de cœurs de processeurs, vous aurez besoin d'une clé avec des restrictions en fonction du nombre de cœurs ; ceci quel que soit le système d'exploitation des machines virtuelles.

Pour la protection des machines virtuelles avec le système d'exploitation hôte Linux, vous pouvez utiliser seulement les clés pour serveur et les clés avec limitation selon le nombre de cœurs.

Si vous ajoutez une clé avec des restrictions selon le nombre de cœurs et qu'une clé pour serveur et/ou poste de travail avait été ajoutée à la SVM, les clés active et additionnelle (le cas échéant) pour poste de travail et/ou serveur sont supprimées suite à l'exécution de la tâche. Elles sont remplacées par une clé active avec restrictions en fonction du nombre de cœurs.

Si vous ajoutez une clé pour serveur ou poste de travail et qu'une clé avec des restrictions selon le nombre de cœurs avait été ajoutée à la SVM, la clé active et additionnelle (le cas échéant) avec des restrictions selon le nombre de cœurs est supprimée suite à l'exécution de la tâche. Elle est remplacée par une clé active pour serveur ou poste de travail.

Si vous achetez une clé commerciale et qu'une clé d'abonnement avait déjà été ajoutée sur la SVM, la clé d'abonnement est supprimée. La clé commerciale la remplacera.

Si vous ajoutez une clé d'abonnement et qu'une ou plusieurs clés commerciales avaient déjà été ajoutées sur la SVM, toutes les clés actives et, le cas échéant, les clés additionnelles, sont supprimées. La clé d'abonnement les remplacera.

Procédure d'activation de l'application

► *Pour activer l'application, procédez comme suit :*

1. Créez une tâche d'activation de l'application pour les SVM sur lesquelles vous souhaitez activer l'application (cf. section "Création d'une tâche d'activation de l'application" à la page [53](#)).

Lors de la création de la tâche d'activation de l'application, une clé du stockage des clés de Kaspersky Security Center est utilisée. Vous pouvez ajouter une clé au stockage des clés de Kaspersky Security Center au préalable (cf. section "Ajout d'une clé dans le stockage des clés de Kaspersky Security Center" à la page [51](#)) ou lorsque vous créez la tâche d'activation de l'application.

2. Lancez la tâche d'activation de l'application (cf. section "Lancement et arrêt des tâches dans Kaspersky Security Center" sur p. [128](#)).

Si vous ajoutez la clé active, la tâche active l'application sur les SVM auxquelles il manque une clé active et remplace l'ancienne clé par la nouvelle sur les SVM où l'application est déjà activée :

- Si vous ajoutez une clé avec des restrictions selon le nombre de cœurs et qu'une clé pour serveur et/ou poste de travail avait été ajoutée à la SVM, les clés active et additionnelle (le cas échéant) pour poste de travail et/ou serveur sont supprimées suite à l'exécution de la tâche. Elles sont remplacées par une clé active avec restrictions en fonction du nombre de cœurs.
- Si vous ajoutez une clé pour serveur ou poste de travail et qu'une clé avec des restrictions selon le nombre de cœurs avait été ajoutée à la SVM, la clé active et additionnelle (le cas échéant) avec des restrictions selon le nombre de cœurs est supprimée suite à l'exécution de la tâche. Elle est remplacée par une clé active pour serveur ou poste de travail.

- Si vous achetez une clé commerciale et qu'une clé d'abonnement avait déjà été ajoutée sur la SVM, l'exécution de la tâche de la clé d'abonnement sera annulée. La clé commerciale la remplacera.
- Si vous ajoutez une clé d'abonnement et qu'une ou plusieurs clés commerciales avaient déjà été ajoutées sur la SVM, l'exécution des tâches des clés actives et, le cas échéant, des clés complémentaires, sera annulée. La clé d'abonnement les remplacera.

Si une clé de type serveur et une clé pour poste de travail ont été ajoutées à votre SVM, le délai d'utilisation de l'application est la plus longue de ces deux durées : délai d'utilisation de l'application avec la clé de type serveur ou délai d'utilisation de l'application avec la clé pour poste de travail.

Si le nombre de machines virtuelles protégées ou le nombre de cœurs de processeur utilisés dans l'infrastructure virtuelle dépasse la valeur indiquée dans les conditions du Certificat de licence, Kaspersky Security envoie au Serveur d'administration de Kaspersky Security Center un événement reprenant les informations relatives à la violation des conditions de la licence (cf. Documentation de Kaspersky Security Center).

Dans cette section

Ajout d'une clé dans le stockage des clés de Kaspersky Security Center.....	51
Création d'une tâche d'activation de l'application	53

Ajout d'une clé dans le stockage des clés de Kaspersky Security Center

► *Pour ajouter une clé au stockage des clés de Kaspersky Security Center, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, dans le dossier **Avancé/Administration des applications**, sélectionnez le sous-dossier **Licences pour une application Kaspersky Lab**.

3. Cliquez sur le lien **Ajouter une clé** de l'espace de travail et lancez l'Assistant d'ajout de clé dans le stockage.
4. Dans la fenêtre de l'Assistant **Sélection d'une méthode d'ajout de la clé**, sélectionnez une méthode d'ajout de la clé dans le stockage :
 - Cliquez sur le bouton **Entrer un code d'activation** si vous souhaitez ajouter la clé via un code d'activation.
 - Cliquez sur le bouton **Indiquer un fichier clé** si vous souhaitez ajouter la clé via un fichier clé.
5. Selon le mode sélectionné pour l'ajout de la clé, effectuez l'une des actions ci-dessous dans l'étape suivante de l'Assistant :
 - Saisissez le code d'activation.
 - Indiquez le chemin d'accès au fichier clé. Pour ce faire, cliquez sur le bouton **Sélectionner** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier avec l'extension key.
6. Décochez la case **Diffuser automatiquement la clé aux ordinateurs administrés**.
Passez à l'étape suivante de l'Assistant.
7. Quittez l'Assistant d'ajout de clé dans le stockage.

La clé ajoutée s'affiche dans la liste des clés, dans le dossier **Avancé/Administration des applications** de l'arborescence de la console, dans le sous-dossier **Licences pour une application Kaspersky Lab**.

Les clés ajoutées dans le stockage des clés de Kaspersky Security Center peuvent être utilisées lors de la création d'une tâche d'activation de l'application sur les SVM (cf. section "Création d'une tâche d'activation de l'application" à la page [53](#)).

Création d'une tâche d'activation de l'application

► Pour créer une tâche d'activation de l'application, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Si vous souhaitez créer une tâche d'activation de l'application pour toutes les SVM du groupe d'administration choisi, sélectionnez le dossier **Ordinateurs administrés** dans l'arborescence de la console, puis choisissez le dossier portant le nom de ce groupe d'administration. Dans l'espace de travail choisissez l'onglet **Tâches** et cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de la création de la tâche.
 - Si vous voulez créer la tâche d'activation de l'application pour une ou plusieurs SVM, lancez l'assistant de la création de la tâche par une des méthodes suivantes :
 - Ouvrez le dossier **Tâches** de l'arborescence de la console et cliquez sur le bouton **Créer une tâche**.
 - Dans l'arborescence de la console, dans le dossier **Avancé / Administration des applications**, choisissez le dossier joint **Licences pour les logiciels de Kaspersky Lab** et cliquez sur le bouton **Répandre la clé aux ordinateurs administrés**.
3. Suivez les instructions de l'Assistant de création d'une tâche.

Dans cette section

Etape 1. Sélection de l'application et du type de tâche.....	54
Etape 2. Ajout d'une clé	54
Etape 3. Choix de la SVM	56
Etape 4. Définition des paramètres de programmation de la tâche	57
Etape 5. Définition du nom de la tâche.....	58
Etape 6. Fin de la création de la tâche	58

Etape 1. Sélection de l'application et du type de tâche

Si vous avez lancé l'Assistant de création d'une tâche à partir du dossier **Ordinateurs administrés** ou du dossier **Tâches**, indiquez l'application pour laquelle la tâche est créée et le type de tâche à cette étape. Pour ce faire, dans la liste **Kaspersky Security for Virtualization 4.0 Light Agent – Serveur de protection**, sélectionnez **Activation de l'application**.

Si vous avez lancé l'Assistant de création d'une tâche à partir du dossier **Licence pour les logiciels de Kaspersky Lab**, à cette étape, indiquez l'application pour laquelle la tâche est créée : **Kaspersky Security for Virtualization 4.0 Light Agent - Serveur de protection**.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

Etape 2. Ajout d'une clé

Cette étape permet de sélectionner une clé dans le stockage de clés Kaspersky Security Center.

Si vous avez ajouté une clé au stockage des clés de Kaspersky Security Center au préalable (cf. section "Ajout d'une clé dans le stockage des clés de Kaspersky Security Center" à la page [51](#)), appuyez sur le bouton **Ajouter**. La fenêtre **Stockage de clés du Kaspersky Security Center** s'ouvre. Sélectionnez la clé, puis cliquez sur le bouton **OK**.

► *Pour ajouter une clé au stockage des clés de Kaspersky Security Center, procédez comme suit :*

1. Cliquez sur le bouton **Ajouter**.

La fenêtre **Stockage de clés du Kaspersky Security Center** s'ouvre.

2. Appuyez sur le bouton **Ajouter** situé en bas de la fenêtre. L'Assistant d'ajout d'une clé dans le stockage des clés de Kaspersky Security Center se lance.
3. Suivez les indications de l'assistant pour ajouter une clé dans le stockage des clés (cf. section "Ajout d'une clé dans le stockage des clés de Kaspersky Security Center" à la p. [51](#)).
4. Quittez l'Assistant d'ajout de clé dans le stockage.

Lorsque l'Assistant est terminé, sélectionnez la clé ajoutée dans la fenêtre **Stockage de clés du Kaspersky Security Center** et appuyez sur le bouton **OK**.

Si vous souhaitez utiliser la clé sélectionnée en tant que clé complémentaire, cochez la case **Utiliser la clé en tant que clé complémentaire**.

La case n'est pas accessible si vous ajoutez une clé par abonnement. Il est impossible d'ajouter la clé d'abonnement en tant que clé additionnelle.

Après que vous avez sélectionné la clé, les informations suivantes s'affichent dans la partie inférieure de la fenêtre :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Type de licence** : évaluation, commerciale ou par abonnement.
- **Durée de validité de la licence** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé. Par exemple, 365 jours. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Indisponible>*.
- **Date d'expiration** : date de fin de l'utilisation de l'application activée par cette clé. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Illimité>*.
- La **Période de grâce** définit le nombre de jours suivant la suspension de l'abonnement au cours desquels l'application continue à fonctionner pleinement. Ce champ s'affiche si vous utilisez l'application par abonnement et que votre fournisseur de services propose une période de renouvellement à tarif préférentiel.
- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

Etape 3. Choix de la SVM

Cette étape est accessible si vous avez lancé l'assistant de la création d'une tâche à partir du dossier **Tâche** ou du dossier **Licences pour une application de Kaspersky Lab**.

Indiquez le mode de sélection des SVM pour lesquelles vous créez la tâche :

- Cliquez sur le bouton **Sélectionner les ordinateurs détectés sur le réseau par le Serveur d'administration** si vous souhaitez sélectionner des SVM à partir de la liste des machines virtuelles détectées par le Serveur d'administration lors du balayage du réseau de l'entreprise.
- Cliquez sur le bouton **Définir manuellement les adresses des ordinateurs ou les importer à partir de la liste** si vous souhaitez définir manuellement les adresses des SVM ou en importer la liste à partir du fichier. L'importation se base sur un fichier au format TXT comportant la liste des adresses des SVM, et où une seule adresse doit figurer sur chaque ligne.

Si vous importez la liste d'adresses des SVM à partir d'un fichier ou que vous définissez manuellement ces adresses et que les SVM sont identifiées en fonction de leur nom, seules les SVM dont les informations ont été entrées dans la base de données du Serveur d'administration (lors de la connexion à ces machines ou suite au balayage du réseau local de l'entreprise) peuvent être ajoutées à la liste des SVM pour lesquelles la tâche est créée.

- Appuyez sur le bouton **Ordinateurs d'un ensemble d'ordinateurs précis** si vous souhaitez créer une tâche pour sélectionner des SVM en fonction d'un critère prédéfini.

En fonction du mode choisi pour la sélection des SVM, procédez comme suit dans la fenêtre qui s'ouvre :

- Dans la liste des machines virtuelles détectées, indiquez les SVM sur lesquelles vous souhaitez activer l'application. Pour ce faire, cochez la case à gauche, en regard du nom de la SVM.
- Cliquez sur le bouton **Ajouter** ou **Ajouter un intervalle IP** et définissez manuellement les adresses des SVM.

- Cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier au format TXT contenant la liste des adresses des SVM.
- Appuyez sur le bouton **Sélectionner**, et dans la fenêtre qui s'ouvre, indiquez le nom de l'ensemble contenant les SVM sur lesquelles vous souhaitez activer l'application.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

Etape 4. Définition des paramètres de programmation de la tâche

Cette étape correspond à la configuration du mode de lancement pour la tâche d'activation de l'application :

- **Lancement programmé.** Dans la liste déroulante, sélectionnez le mode de lancement de la tâche. Les paramètres affichés dans la fenêtre dépendent du mode de lancement sélectionné.
- **Lancer les tâches non exécutées.** Cochez la case si vous voulez que l'application lance la tâche ignorée tout de suite après l'apparition de la SVM dans le réseau.

Si la case est décochée, le lancement de la tâche pour le mode **Manuel** est exécuté uniquement sur les SVM visibles dans le réseau.

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche.**
Par défaut, le lancement des tâches sur les SVM s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de SVM couvertes par la tâche :
 - De 0 à 200 SVM : le lancement de la tâche est immédiat ;
 - De 200 à 500 SVM : le lancement de la tâche s'étale sur 5 minutes ;
 - De 500 à 1000 SVM : le lancement de la tâche s'étale sur 10 minutes ;
 - De 1000 à 2000 SVM : le lancement de la tâche s'étale sur 15 minutes ;
 - De 2000 à 5000 SVM : le lancement de la tâche s'étale sur 20 minutes ;
 - De 5000 à 10000 SVM : le lancement de la tâche s'étale sur 30 minutes ;
 - De 10000 à 20000 SVM : le lancement de la tâche s'étale sur 1 heure ;

- De 20000 à 50000 SVM : le lancement de la tâche s'étale sur 2 heures ;
- Plus de 50000 SVM : le lancement de la tâche s'étale sur 3 heures.

S'il n'est pas nécessaire d'étaler le lancement de la tâche sur une période calculée automatiquement, décochez la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, la case est cochée.

- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué depuis le moment du lancement manuel, cochez cette case et, dans le champ de saisie, indiquez le temps de retard maximal de lancement de la tâche. Dans ce cas, la tâche se lancera en mode aléatoire dans l'intervalle indiqué après le lancement manuel. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

Etape 5. Définition du nom de la tâche

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

Passez à l'étape suivante de l'Assistant de création d'une tâche.

Etape 6. Fin de la création de la tâche

Si vous souhaitez que la tâche se lance directement après la fin de l'Assistant de création d'une tâche, cochez la case **Démarrer la tâche après la fin de l'Assistant**.

Fermez l'Assistant. La tâche d'activation de l'application créée apparaît dans la liste des tâches pour le groupe d'administration sélectionné dans l'onglet **Tâches** ou dans le dossier **Tâches**.

Si vous avez défini dans la fenêtre **Programmation de l'exécution de la tâche** une planification pour l'exécution de la tâche, celle-ci sera exécutée conformément à la programmation.

Vous pouvez également lancer manuellement à n'importe quel moment la tâche d'activation de l'application manuellement (cf. section "Lancement et arrêt des tâches dans Kaspersky Security Center" à la page [128](#)).

Renouvellement de la licence

Quand une licence est sur le point d'expirer, vous pouvez la renouveler en ajoutant une clé additionnelle. Ainsi, les fonctionnalités de l'application ne seront pas limitées après l'expiration de la licence active et avant l'activation de l'application à l'aide d'une nouvelle licence.

Pour ajouter une clé supplémentaire sur les SVM, la tâche d'activation de l'application est utilisée.

Le type de la clé additionnelle doit correspondre au type de la clé active ajoutée.

Si vous utilisez le schéma de licence en fonction du nombre de machines virtuelles protégées, le type de fichier clé complémentaire doit correspondre au système d'exploitation invité des machines virtuelles : une clé complémentaire de type serveur est nécessaire pour les machines virtuelles avec système d'exploitation serveur et une clé complémentaire de type poste de travail est nécessaire pour les machines virtuelles avec système d'exploitation pour postes de travail.

Si la SVM intervient dans l'infrastructure virtuelle de protection de machines virtuelles avec système d'exploitation invité pour serveur et poste de travail, il est recommandé d'ajouter la clé complémentaire correspondante à chaque type de système d'exploitation.

Si vous utilisez le schéma de licence en fonction du nombre de cœurs de processeurs, vous aurez besoin d'une clé complémentaire avec des restrictions en fonction du nombre de cœurs ; ceci quel que soit le système d'exploitation des machines virtuelles.

► Pour renouveler une licence, procédez comme suit :

1. Créez une tâche d'activation de l'application pour les SVM sur lesquelles vous souhaitez ajouter une clé additionnelle (cf. section "Création d'une tâche d'activation de l'application" à la page [53](#)).

Lors de la création de la tâche d'activation de l'application, une clé du stockage des clés de Kaspersky Security Center est utilisée. Vous pouvez ajouter une clé au stockage des clés de Kaspersky Security Center au préalable (cf. section "Ajout d'une clé dans le stockage des clés de Kaspersky Security Center" à la page [51](#)) ou lorsque vous créez la tâche d'activation de l'application.

2. Cochez la case **Utiliser la clé en tant que clé complémentaire** à l'Etape 2 de l'Assistant de création d'une tâche (cf. section "Etape 2. Ajout d'une clé" à la page [54](#)).
3. Lancez la tâche d'activation de l'application (cf. section "Lancement et arrêt des tâches dans Kaspersky Security Center" sur p. [128](#)).

A la suite de l'exécution de la tâche, la clé supplémentaire est ajoutée aux SVM sur lesquelles la clé active l'a déjà été. Cette clé supplémentaire est utilisée automatiquement en tant que clé active à l'expiration de la licence de Kaspersky Security.

Si vous utilisez un code d'activation pour activer l'application, cette dernière se connecte automatiquement aux serveurs d'activation de Kaspersky Lab à la fin de la durée de validité de la clé active pour assurer le relais. Si la connexion automatique de l'application aux serveurs d'activation de Kaspersky Lab aboutit à une erreur, il est nécessaire de lancer manuellement la tâche d'activation de l'application afin de prolonger la durée de validité de la licence d'utilisation de Kaspersky Security.

La tâche d'activation de l'application se termine avec une erreur et la clé additionnelle n'est pas ajoutée si une des conditions suivantes est remplie :

- La clé active est absente sur la SVM.
- le type de la clé additionnelle ajoutée ne correspond pas au type de la clé active ajoutée antérieurement.

Si une clé active et une clé additionnelle sont ajoutées à la SVM et que vous remplacez la clé active, Kaspersky Security vérifie la date de fin de validité de la clé additionnelle. Si la clé additionnelle expire avant le renouvellement de la validité de la licence, Kaspersky Security supprime automatiquement la clé additionnelle. Dans ce cas, vous pourrez ajouter une autre clé additionnelle après l'ajout de la clé active.

Renouvellement de l'abonnement

Au moment de l'utilisation de l'application par abonnement, Kaspersky Security se connecte automatiquement au serveur d'activation de Kaspersky Lab à des intervalles définis jusqu'à la fin de l'abonnement.

Si vous utilisez l'application avec un abonnement illimité, Kaspersky Security vérifie en arrière-plan la présence d'une nouvelle clé sur les serveurs d'activation de Kaspersky Lab. Si cette opération est possible, il remplace la clé antérieure par la nouvelle. C'est ainsi que l'abonnement illimité à Kaspersky Security se renouvelle sans votre participation.

Si votre abonnement a pris fin, Kaspersky Security en informe le Serveur d'administration du Kaspersky Security Center et interrompt les tentatives de renouvellement automatique. Kaspersky Security arrête de mise à jour les bases de l'application et d'utiliser Kaspersky Security Network.

Pour renouveler l'abonnement, vous devez contacter le prestataire de services auprès de qui vous avez acheté Kaspersky Security.

Après le renouvellement de l'abonnement, vous devrez relancer la tâche d'activation de l'application que vous avez créée pour l'activation de l'application par abonnement.

Consultation des informations relatives aux clés utilisées

Les informations relatives aux clés utilisées sont accessibles :

- dans le dossier **Avancé / Administration des applications** de l'arborescence de la console, dans le sous-dossier **Licence pour une application Kaspersky Lab** ;
- dans les propriétés de l'application installée sur la SVM ;
- dans les propriétés de la tâche d'activation de l'application ;
- dans le rapport sur l'utilisation des clés.

Dans cette section

Consultation des informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab	62
Consultation des informations relatives à la clé dans les propriétés de l'application	65
Consultation des informations relatives à la clé dans les propriétés de la tâche d'activation de l'application	68
Consultation du rapport sur l'utilisation des clés	70

Consultation des informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab

- Pour consulter les informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Avancé / Administration des applications** de l'arborescence de la console, sélectionnez le dossier **Licence pour une application Kaspersky Lab**.

L'espace de travail affiche les clés ajoutées dans le stockage des clés du Kaspersky Security Center.

3. Sélectionnez dans la liste la clé dont vous souhaitez consulter les informations.

Les informations suivantes relatives à la clé apparaissent à droite de la liste :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Type de licence** : évaluation, commerciale ou par abonnement.
- **Application** : nom de l'application activée par l'ajout de cette clé et informations sur la licence.
- **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé. Par exemple, 365 jours. Si vous utilisez l'application avec un abonnement, le champ affiche <N/A>.
- **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle peut être utilisée uniquement jusqu'à l'échéance de sa durée de validité.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de la clé ajoutée. Si la clé a été plusieurs fois ajoutée à différentes SVM, ce champ affiche les données de la SVM sur laquelle la durée de validité de l'application expire en premier. Si vous utilisez l'application avec un abonnement illimité, le champ affiche <Sans restriction>.

- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.
- **Ordinateurs sur lesquels la clé est active** : en fonction du type de clé :
 - pour une clé pour serveur ou poste de travail : nombre de machines virtuelles protégées pour lesquelles la clé est utilisée en tant que clé active ;
 - pour une clé avec limitation du nombre de noyaux du processeur : la quantité de SVM sur les quelle la clé est ajoutée comme active.
- **Ordinateurs sur lesquels la clé est complémentaire** : nombre de SVM sur lesquelles la clé a été ajoutée en tant que clé complémentaire.
- **Informations de service** : ce champ reprend les informations de service liées à la clé et à la licence.

Si vous avez sélectionné une clé d'abonnement dans la liste, les informations suivantes s'affichent également à droite de la liste des clés :

- La **Période de grâce** définit le nombre de jours suivant la suspension de l'abonnement au cours desquels l'application continue à fonctionner pleinement.
- **Adresse Internet du fournisseur** : adresse Internet du fournisseur de services auprès duquel l'abonnement est souscrit.
- **Etat de l'abonnement** : état actuel de l'abonnement (*actif, suspendu, arrêté, résilié*).
- **Raison de l'état de l'abonnement** : raison expliquant le passage de l'abonnement à cet état.

Les informations relatives à l'abonnement s'affichent également dans la fenêtre des propriétés de la clé d'abonnement, dans la section **A propos de l'abonnement**. Cliquez sur le lien **Ouvrir la fenêtre des propriétés de la clé** situé à droite de la liste des clés pour ouvrir la fenêtre des propriétés de la clé.

Si une clé pour serveur et une clé pour poste de travail ont été ajoutées à votre SVM, dans le dossier **Licence pour une application Kaspersky Lab**, Kaspersky Security Center affiche des informations sur ces clés, ainsi que les informations suivantes concernant l'association d'une clé de type serveur et d'une clé pour poste de travail :

- Séquence unique de chiffres et de lettres : combinaison de la clé pour serveur ou poste de travail. Vous pouvez utiliser la combinaison de la clé pour serveur ou poste de travail pour rechercher des informations sur la SVM sur laquelle ces types de clé ont été ajoutés (pour les détails, reportez-vous à la Documentation de Kaspersky Security Center).
- **Durée de validité** : durée la plus longue entre les deux durées d'utilisation de l'application : durée d'utilisation de l'application avec la clé de type serveur ou durée d'utilisation de l'application avec la clé pour poste de travail.
- **Date de fin de validité** : date la plus éloignée entre les deux dates suivantes d'expiration de la validité de la clé : date d'expiration de la validité de la clé pour serveur ou date d'expiration de la validité de la clé pour poste de travail.
- **Date d'expiration de la validité de la licence** : date la plus éloignée entre les deux dates suivantes : la date de fin d'utilisation de l'application avec la clé de type serveur ou la date de fin d'utilisation de l'application avec la clé pour poste de travail.
- **Restriction** : somme des valeurs suivantes : nombre maximal de machines virtuelles avec système d'exploitation pour postes de travail et nombre maximal de machines virtuelles avec système d'exploitation pour serveurs que vous pouvez protéger à l'aide de l'application.
- **Ordinateurs sur lesquels la clé est active** : nombre de SVM sur lesquelles la clé a été ajoutée en tant que clé active.

- **Période de grâce** : période de grâce la plus longue des deux entre celle correspondant à la clé pour serveur et celle correspondant à la clé pour poste de travail.
- **État de l'abonnement** : le champ indique l'état *actif* si l'abonnement correspondant à au moins l'une des clés (serveur ou poste de travail), se trouve à l'état *actif*. Si les deux abonnements sont inactifs, le champ indique le meilleur état (par exemple, si un abonnement est *suspendu* et le deuxième *résilié*, le champ indique l'état *suspendu*).

Consultation des informations relatives à la clé dans les propriétés de l'application

► Pour consulter les informations relatives à la clé dans les propriétés de l'application, 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, choisissez le dossier portant le nom du groupe d'administration comprenant les SVM pour lesquelles vous souhaitez consulter les informations concernant la clé.
3. Dans l'espace de travail, sélectionnez l'onglet **Ordinateurs**.
4. Dans la liste, choisissez la SVM pour laquelle vous voulez consulter des informations sur la clé.
5. Ouvrez la fenêtre des propriétés de la SVM par une des méthodes suivantes :
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.

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

6. Dans la liste de gauche, choisissez l'option **Applications**.

La liste des applications installées sur cette SVM apparaît dans la partie droite de la fenêtre.

7. Choisissez **Kaspersky Security for Virtualization 4.0 Light Agent – Serveur de protection** et ouvrez la fenêtre des paramètres de l'application par une des méthodes suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
 - Cliquez sur le bouton **Propriétés**.

La fenêtre **Kaspersky Security for Virtualization 4.0 Light Agent - Serveur de protection** s'ouvre.

8. Dans la liste de gauche, choisissez la section **Clés**.

La partie droite de la fenêtre comprend des informations sur la clé ajoutée sur la SVM.

Le champ **Clé active** reprend les informations relatives à la clé active, tandis que le groupe **Clé complémentaire** reprend les informations relatives à la clé additionnelle. Si aucune clé additionnelle n'a été ajoutée, le groupe **Clé complémentaire** affiche la ligne *<Non ajoutée>*.

Le groupe **Clé active** reprend les informations suivantes relatives à la clé :

- Séquence unique de chiffres et de lettres (clé).
- **Type de licence** : évaluation, commerciale ou par abonnement.
- **Date d'activation** : date d'activation de l'application via l'ajout de cette clé.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de la clé ajoutée. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Sans restriction>*.
- **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé. Par exemple, 365 jours. Si vous utilisez l'application avec un abonnement, le champ affiche *<N/A>*.
- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.

Le groupe **Clé complémentaire** reprend les informations suivantes relatives à la clé :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Type de licence** : type de licence : commerciale.
- **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé. Par exemple, 365 jours.
- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique sur tous les hyperviseurs où des SVM sont déployées.

Si une clé pour serveur et une clé pour poste de travail ont été ajoutées à votre SVM, la fenêtre des propriétés de l'application Kaspersky Security Center affiche les informations suivantes concernant l'association d'une clé pour serveur et d'une clé pour poste de travail :

- Séquence unique de chiffres et de lettres : combinaison de la clé pour serveur ou poste de travail. Vous pouvez utiliser la combinaison de la clé pour serveur ou poste de travail pour rechercher des informations sur la SVM sur laquelle ces types de clé ont été ajoutés (pour les détails, reportez-vous à la Documentation de Kaspersky Security Center).
- **Date d'expiration de la validité de la licence** : date la plus éloignée entre les deux dates suivantes : la date de fin d'utilisation de l'application avec la clé de type serveur ou la date de fin d'utilisation de l'application avec la clé pour poste de travail.

- **Durée de validité** : durée la plus longue entre les deux durées d'utilisation de l'application : durée d'utilisation de l'application avec la clé de type serveur ou durée d'utilisation de l'application avec la clé pour poste de travail.
- **Restriction** : somme des valeurs suivantes : nombre maximal de machines virtuelles avec système d'exploitation pour postes de travail et nombre maximal de machines virtuelles avec système d'exploitation pour serveurs que vous pouvez protéger à l'aide de l'application.

Consultation des informations relatives à la clé dans les propriétés de la tâche d'activation de l'application

► *Pour consulter les informations relatives à la clé dans les propriétés de la tâche d'activation de l'application, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du groupe d'administration comprenant les SVM pour lesquelles vous souhaitez consulter les propriétés de la tâche d'activation de l'application. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Choisissez le dossier **Tâches** de l'arborescence de la console si vous voulez consulter les propriétés de la tâche de l'activation d'application créée pour une ou plusieurs SVM.
3. Dans la liste des tâches, choisissez celle dont vous voulez consulter les propriétés et exécutez une des actions suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
 - Cliquez sur le lien **Modifier les paramètres de la tâche** pour ouvrir la fenêtre des propriétés de la tâche. Le lien se trouve à droite de la liste des tâches.

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

4. Dans la liste de gauche, choisissez la section **Ajouter une clé**.

La partie droite de la fenêtre affiche alors les informations relatives à la clé ajoutée sur les SVM à l'aide de cette tâche :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Type de licence** : évaluation, commerciale ou par abonnement.
- **Durée de validité de la licence** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé. Par exemple, 365 jours. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Indisponible>*.
- **Date d'expiration** : date de fin de l'utilisation de l'application activée par cette clé. Si la clé a été plusieurs fois ajoutée à différentes SVM, ce champ affiche les données de la SVM sur laquelle la durée de validité de l'application expire en premier. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Illimité>*.
- La **Période de grâce** définit le nombre de jours suivant la suspension de l'abonnement au cours desquels l'application continue à fonctionner pleinement. Ce champ s'affiche si vous utilisez l'application par abonnement et que votre fournisseur de services propose une période de renouvellement à tarif préférentiel.
- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.

Consultation du rapport sur l'utilisation des clés

► Pour consulter le rapport sur l'utilisation des clés, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'espace de travail du nœud **Serveur d'administration** passez à l'onglet **Rapports** et choisissez le cliché du rapport sur l'utilisation des clés.

Le rapport créé selon le modèle de rapport sur l'utilisation des clés apparaît dans l'espace de travail.

Les informations suivantes relatives à l'utilisation de la clé apparaissent dans le diagramme de la partie supérieure de la fenêtre pour chaque clé :

- le nombre d'unités de licence pour lesquelles la clé est déjà utilisée ;
- le nombre d'unités de licence pour lesquelles la clé peut être utilisée en fonction des restrictions imposées par la licence ;
- le nombre d'unités de licence pour lesquelles les restrictions imposées par la licence à propos de l'utilisation de la clé sont dépassées.

Le rapport d'utilisation des clés se compose de deux tableaux :

- Le tableau des informations récapitulatives contient des informations sur les clés utilisées.
- Le tableau des informations détaillées contient des informations sur les SVM sur les clés sont ajoutées ou sur les machines virtuelles protégées pour lesquelles une clé est utilisée.

Vous pouvez configurer le contenu des champs de chaque tableau. Pour en savoir plus sur l'ajout ou la suppression de champs dans les tableaux du rapport, consultez la documentation du Kaspersky Security Center.

Le tableau des informations récapitulatives contient les informations suivantes sur les clés utilisées :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Utilisé en tant que clé active** : en fonction du type de clé :
 - pour une clé pour serveur ou poste de travail : nombre de machines virtuelles protégées pour lesquelles la clé est utilisée en tant que clé active ;

- pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.
- **Utilisée en tant que clé complémentaire** : nombre de SVM sur lesquelles la clé a été ajoutée en tant que clé complémentaire.
- **Restriction** : dépend du type de clé :
 - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
 - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps et pour lesquelles la protection est activée ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de la clé ajoutée. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Sans restriction>*.
- **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle peut être utilisée uniquement jusqu'à l'échéance de sa durée de validité.
- **Autres informations** : paramètres avancés de la clé.
- **Utilisé en tant que clé active pour postes de travail** : nombre de machines virtuelles protégées avec système d'exploitation pour poste de travail pour lesquelles la clé est utilisée en tant que clé active.
- **Utilisé en tant que clé active pour serveurs** : nombre de machines virtuelles protégées avec système d'exploitation pour serveur pour lesquelles la clé est utilisée en tant que clé active.
- **Autres informations** : informations de service liées à la clé et à la licence.

La ligne en dessous reprend les informations de synthèse suivantes :

- **Clés** : nombre total de clés utilisées.
- **Clés utilisées à plus de 90 %** : nombre total de clés utilisées à plus de 90 % de la restriction de la licence. En fonction du type de clé, les restrictions reprennent le nombre maximal de machines virtuelles avec système d'exploitation pour serveur ou poste de travail qui peuvent être exécutées simultanément et pour lesquelles la protection est activée, ou le nombre maximal de cœurs de processeurs physiques déployés sur tous les hyperviseurs comportant des SVM. Par exemple, la restriction inclut 100 machines virtuelles. La clé est utilisée sur deux SVM dont la première protège 42 machines virtuelles et la deuxième 53 machines virtuelles. Par conséquent, cette clé est utilisée à 95% et est incluse dans le nombre de clés indiquées dans ce champ.
- **Clés avec restriction dépassée** : le nombre total de clés pour lesquelles la restriction est dépassée par rapport au nombre de lancements simultanés des machines virtuelles dotées d'un système d'exploitation pour serveurs ou pour postes de travail, ou par rapport au nombre de cœurs de processeurs physique utilisés sur tous les hyperviseurs (en fonction du type de clé).

Le tableau des informations détaillées affiche en fonction du type de clé des informations sur la SVM où la clé est ajoutée (pour la clé avec limitation en fonction du nombre de cœurs) ou des informations sur la machine virtuelle protégée pour laquelle la clé est utilisée (pour la clé de serveur ou la clé pour poste de travail) :

- **Serveur virtuel** : nom du Serveur d'administration virtuel administrant la SVM ou la machine virtuelle protégée.
- **Groupe** : groupe d'administration dont fait partie la SVM ou la machine virtuelle protégée.
- **Ordinateur client** : nom de la SVM ou de la machine virtuelle protégée.
- **Application** : nom du composant Kaspersky Security installé sur la SVM ou sur la machine virtuelle protégée.
- **Numéro de version** : numéro de la version de l'application.
- **Clé active** : clé ajoutée en tant que clé active.

- **Clé complémentaire** : clé ajoutée en tant que clé complémentaire.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application à l'aide de cette clé. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *<Sans restriction>*.
- **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle peut être utilisée uniquement jusqu'à l'échéance de sa durée de validité.
- **Adresse IP** : adresse IP de la SVM ou de la machine virtuelle protégée sur laquelle la clé est ajoutée.
- **Visible dans le réseau** : date et heure auxquelles la SVM ou la machine virtuelle protégée était visible sur le réseau local de l'entreprise pour la dernière fois.
- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la SVM ou de la machine virtuelle protégée au Serveur d'administration de Kaspersky Security Center.
- **Domaine** domaine associé à la SVM ou à la machine virtuelle protégée.
- **Nom de domaine, nom NetBIOS** : nom de la SVM ou de la machine virtuelle protégée.
- **Domaine DNS** : domaine DNS associé à la SVM ou à la machine virtuelle protégée (indiqué seulement si le nom de la SVM ou de la machine virtuelle protégée contient le nom du domaine DNS).
- **Utilisé** : dépend du type de clé active :
 - pour une clé pour serveur ou poste de travail : nombre de machines virtuelles protégées avec système d'exploitation pour serveur ou poste de travail ;
 - pour une clé avec limitation en fonction du nombre de cœurs du processeur : correspond au nombre de cœurs de processeur physique utilisés sur tous les hyperviseurs où des SVM sont déployées.
- **Utilisé pour postes de travail** : pour la clé de bureau, nombre de machines virtuelles protégées dotées d'un système d'exploitation pour postes de travail.
- **Utilisé pour serveurs** : pour la clé de serveur, nombre de machines virtuelles protégées dotées d'un système d'exploitation pour serveurs.

Si une clé de type serveur et une clé pour poste de travail ont été ajoutées à votre SVM, dans le rapport sur l'utilisation des clés, Kaspersky Security Center affiche des informations sur ces clés, ainsi que les informations suivantes concernant l'association d'une clé de type serveur et d'une clé pour poste de travail :

- **Clé, Clé active, Clé complémentaire** : combinaison unique de la clé de type serveur ou de la clé pour poste de travail. Vous pouvez utiliser la combinaison de la clé pour serveur ou poste de travail pour rechercher des informations sur la SVM sur laquelle ces types de clé ont été ajoutés (pour les détails, reportez-vous à la Documentation de Kaspersky Security Center).
- **Date d'expiration de la validité de la licence** : date la plus éloignée entre les deux dates suivantes : la date de fin d'utilisation de l'application avec la clé de type serveur ou la date de fin d'utilisation de l'application avec la clé pour poste de travail.
- **Date de fin de validité** : date la plus éloignée entre les deux dates suivantes d'expiration de la validité de la clé : date d'expiration de la validité de la clé pour serveur ou date d'expiration de la validité de la clé pour poste de travail.
- **Restriction** : somme des valeurs suivantes : nombre maximal de machines virtuelles avec système d'exploitation pour postes de travail et nombre maximal de machines virtuelles avec système d'exploitation pour serveurs que vous pouvez protéger à l'aide de l'application.
- **Restriction pour postes de travail** : nombre maximum de machines virtuelles dotées d'un système d'exploitation pour postes de travail lancées simultanément que vous pouvez protéger à l'aide de l'application.
- **Restriction pour serveurs** : nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs lancées simultanément que vous pouvez protéger à l'aide de l'application.

Lancement et arrêt de l'application

Le composant Serveur de protection de Kaspersky Security se lance automatiquement au démarrage du système d'exploitation sur la SVM. Le Serveur de protection gère les processus de travail qui correspondent à l'exécution de la protection des machines virtuelles, des tâches d'analyse, des tâches de mise à jour des bases et des composants de l'application et de la remise à l'état antérieur à la mise à jour.

La SVM déployée sur l'hyperviseur VMware ESXi est lancée automatiquement après l'activation de l'hyperviseur. L'activation automatique de la SVM peut ne pas fonctionner si la fonction n'est pas activée au niveau de l'hyperviseur ou si cet hyperviseur se trouve dans un cluster VMware HA (pour les détails, consultez la banque de connaissances de VMware (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=850)).

Le composant Light Agent est lancé automatiquement par défaut au démarrage du système d'exploitation sur la machine virtuelle protégée.

Pour le Light Agent for Windows, vous pouvez activer ou désactiver le lancement automatique de l'application dans l'interface locale du Light Agent (cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

Le composant Serveur d'intégration se lance automatiquement au démarrage du système d'exploitation de l'ordinateur sur lequel est installé le Serveur d'intégration.

La protection des machines virtuelles est activée automatiquement lors du démarrage des composants Light Agent et Serveur de protection. Si les informations sur la licence ne sont pas transmises à la machine virtuelle protégée, le Light Agent fonctionne en mode restreint (cf. section "À propos de l'activation de l'application" à la page [46](#)).

Les tâches de Kaspersky Security sont lancées conformément à la programmation.

Les composants Serveur de protection et Light Agent s'arrêtent automatiquement lors de l'arrêt du système d'exploitation de la SVM et de la machine virtuelle protégée. Vous pouvez également effectuer des opérations manuelles pour : arrêter les composants Serveur de protection et Light Agent sur les machines virtuelles, démarrer l'application et suspendre ou rétablir la protection et le contrôle des machines virtuelles protégées via le Kaspersky Security Center (cf. la documentation de Kaspersky Security Center).

Vous pouvez aussi arrêter et lancer le Light Agent for Windows dans son interface locale (voir *Guide de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

Vous pouvez arrêter et lancer le Light Agent for Linux par les méthodes standard du système d'exploitation Linux. Si vous arrêtez le Light Agent for Linux, toutes les tâches exécutées seront interrompues. Après le redémarrage du Light Agent for Linux, les tâches interrompues ne reprennent pas automatiquement. Vous pouvez lancer les tâches manuellement (cf. section "Lancement et arrêt de la tâche de la mise à jour" à la p. [207](#)).

Le composant Serveur d'intégration s'arrête automatiquement lors de l'arrêt du système d'exploitation de l'ordinateur sur lequel est installé le Serveur d'intégration.

Etat de la protection de la machine virtuelle

La machine virtuelle dotée du composant Light Agent de Kaspersky Security Center est identique à un poste client. Les informations relatives à l'état de protection du poste client dans Kaspersky Security Center sont présentées via l'état du poste client.

Lors de la détection d'une menace, l'état de la machine virtuelle protégée affiche *Critique* ou *Avertissement*. Si le Light Agent ne peut se connecter à aucune SVM, l'état de la machine virtuelle protégée passe à *Protection non activée*. Pour en savoir plus sur les états du poste client, cf. la Documentation de Kaspersky Security Center.

Les informations relatives au fonctionnement de chaque composant de Kaspersky Security, à l'exécution de tâches et au fonctionnement de l'application dans son ensemble sont consignées dans des rapports.

Les informations concernant l'état de la protection de chaque SVM sur laquelle est installé le composant Light Agent peuvent également être consultées dans l'interface locale du Light Agent for Windows (cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*) ou à l'aide des commandes de la ligne de commande du Light Agent for Linux (cf. p. [201](#)).

Concept de l'administration de l'application via le Kaspersky Security Center

Kaspersky Security Center vous permet d'administrer à distance l'application Kaspersky Security. Le Kaspersky Security Center permet de réaliser les opérations suivantes :

- installer l'application dans l'infrastructure virtuelle ;
- lancer et arrêter l'application Kaspersky Security sur les machines virtuelles protégées ;
- administrer de façon centralisée le fonctionnement de l'application :
 - administrer la protection des machines virtuelles ;
 - administrer avec les tâches d'analyse ;
 - administrer les clés de l'application ;
- mettre à jour les bases et les modules de l'application ;
- créer des rapports sur les événements survenus pendant le fonctionnement de l'application ;
- supprimer l'application de l'infrastructure virtuelle.

L'administration de l'application Kaspersky Security via Kaspersky Security Center s'opère à l'aide de stratégies et de tâches :

- Les *Stratégies* permettent de définir les paramètres de protection des machines virtuelles et les paramètres de fonctionnement des modules Light Agent et Serveur de protection (cf. section "A propos des stratégies de Kaspersky Security" à la page [83](#)).
- Les *Tâches* permettent de mettre en œuvre des fonctions de l'application telles que l'activation de l'application, l'analyse des machines virtuelles, la mise à jour des bases de données et des modules de l'application (cf. section "A propos des tâches de Kaspersky Security" à la page [121](#)).

Les stratégies et les tâches vous permettent d'installer les mêmes paramètres de l'application Kaspersky Security pour l'ensemble des machines virtuelles protégées ou SVM figurant dans le groupe d'administration.

Vous pouvez consulter les informations détaillées sur les stratégies et les tâches dans la documentation de Kaspersky Security Center.

Protection en temps réel et analyse de la machine virtuelle

Cette section contient des informations sur la manière dont Kaspersky Security protège et analyse la machine virtuelle protégée.

Dans cette section

A propos de la protection en temps réel et de l'analyse de la machine virtuelle.....	80
Particularités de l'analyse des liens symboliques et fixes	81

A propos de la protection en temps réel et de l'analyse de la machine virtuelle

La *protection en temps réel* est automatiquement activée avec l'application Kaspersky Security au démarrage de la machine virtuelle protégée et continue à fonctionner sans interruption.

La protection en temps réel consiste en l'analyse des fichiers de la machine virtuelle protégée lors de l'accès à ces derniers pour y détecter la présence des applications malveillantes.

Quand l'utilisateur ou une application s'adresse à un fichier sur la machine virtuelle protégée (par exemple, en lecture ou en écriture), Kaspersky Security intercepte l'appel à ce fichier.

En plus de la protection en temps réel, il est indispensable d'effectuer à intervalle régulier l'*analyse* de la machine virtuelle protégée pour y détecter les virus et d'autres applications présentant une menace afin d'éviter la propagation d'applications malveillantes non détectées par l'application, par exemple en raison d'un niveau de protection trop faible ou pour toute autre raison.

Sur la machine virtuelle avec le composant Light Agent for Linux installé, les objets du système de fichiers /dev, /sys et /proc sont exclus de l'analyse et de la protection.

Kaspersky Security analyse le fichier pour y détecter la présence des menaces en utilisant les bases antivirus (cf. section "A propos de la mise à jour des bases et des modules de l'application" à la p. [129](#)). Si Kaspersky Security détecte dans le fichier un code malveillant, il exécute dessus lui les actions choisies par vos soins. Par exemple, il tente de désinfecter ou supprime le fichier. L'application qui s'est adressée au fichier peut l'utiliser seulement si ce fichier n'est pas infecté ou désinfecté avec succès.

Avant l'exécution de l'action, Kaspersky Security bloque l'accès au fichier indépendamment de l'action choisie.

Particularités de l'analyse des liens symboliques et fixes

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

Analyse des liens symboliques

La tâche de protection en temps réel analyse le fichier accessible par un lien symbolique seulement si ce fichier fait partie de la zone de protection de la tâche de protection en temps réel.

Si le fichier accessible par un lien symbolique ne fait pas partie de la zone de protection de la tâche de protection en temps réel, l'application ne l'analyse pas. Si un tel fichier contient un code malveillant, la sécurité de la machine virtuelle est menacée.

La tâche d'analyse vérifie le fichier accessible par un lien symbolique, indépendamment de son emplacement. Lors de la détection d'un fichier infecté accessible par un lien symbolique, l'application désinfecte le fichier source. Si la désinfection est impossible, l'application supprime le fichier infecté et conserve le lien symbolique.

Analyse des liens fixes par le composant Light Agent for Linux

Lors de la détection d'un fichier infecté accessible par un lien rigide, le Light Agent for Linux répare le fichier source. Si la désinfection est impossible, le Light Agent for Linux supprime le lien fixe traité vers le fichier. De plus, les autres liens rigides vers ce fichier ne seront pas traités.

Lors de la restauration du fichier avec le lien fixe, l'application crée à partir de la sauvegarde une copie du fichier source avec le nom du lien fixe qui était placé dans la sauvegarde. Les liens avec les autres liens fixes sur le fichier source ne seront pas restaurés.

Analyse des liens fixes par le composant Light Agent for Windows

Quand le Light Agent for Windows traite le fichier contenant plusieurs liens fixes, en fonction de l'action spécifiée sur ces fichiers, les scénarios suivants sont possibles :

- Si l'action **Supprimer** est sélectionné, Kaspersky Security supprime le lien fixe traité. Les autres liens fixes vers ce fichier ne seront pas traités.
- Si l'action **Réparer** est sélectionnée, Kaspersky Security répare le fichier source. Si la désinfection est impossible, l'application supprime le lien fixe traité et crée à la place une copie du fichier source avec le nom du lien fixe supprimé. De plus, les autres liens rigides vers ce fichier ne seront pas traités.

Administration des stratégies

Cette section fournit des informations sur l'élaboration et la configuration des stratégies pour l'application Kaspersky Security for Virtualization 4.0 Light Agent. Pour plus d'informations sur les stratégies, consultez la documentation de Kaspersky Security Center.

Dans cette section

Présentation des stratégies pour Kaspersky Security.....	83
Affichage des paramètres des stratégies	86
Création de la stratégie pour le Serveur de protection.....	86
Configuration de l'affichage des paramètres de contrôle dans la Console d'administration	93
Création d'une stratégie pour un Light Agent for Linux	94
Création de la stratégie pour le Light Agent for Linux	110
Modification des paramètres des stratégies	117

Présentation des stratégies pour Kaspersky Security

L'administration de Kaspersky Security for Virtualization 4.0 Light Agent s'appuie sur les stratégies suivantes de Kaspersky Security Center :

- **Stratégie pour le Serveur de protection.** La stratégie est appliquée sur toutes SVM faisant partie du groupe d'administration pour lequel la stratégie est configurée.

Les paramètres de la stratégie pour le Serveur de protection incluent :

- les paramètres généraux de la protection des machines virtuelles et les paramètres des événements (Kaspersky Security Center cf. documentation) ;

- les paramètres d'utilisation de Kaspersky Security Network (KSN) dans le cadre de l'application (cf. section "Participation au Kaspersky Security Network" à la page [192](#)) ;
- les paramètres de mise à jour du module Light Agent for Windows dans le cadre de la mise à jour des bases de données de l'application (cf. section "Activation et désactivation de la mise à jour des modules de Light Agent for Windows" à la page [132](#)) ;
- les paramètres de détection des SVM, c'est-à-dire les paramètres d'envoi aux Light Agents d'informations sur les SVM (cf. section "Etape 5. Configuration des paramètres de détection des SVM" à la p. [90](#)) ;
- les paramètres complémentaires de fonctionnement des SVM (cf. section "Affichage des paramètres des stratégies" à la page [86](#)).
- **Stratégie pour un Light Agent for Windows** Définit les paramètres de fonctionnement des Light Agent installés sur les machines virtuelles protégées avec les systèmes d'exploitation invités Windows. La stratégie s'applique à l'ensemble des machines virtuelles protégées figurant dans le groupe d'administration pour lequel elle est configurée.

Les paramètres de la stratégie pour le Light Agent for Windows incluent :

- les paramètres généraux de la protection des machines virtuelles et les paramètres des événements (Kaspersky Security Center cf. documentation) ;
- les paramètres généraux de protection antivirus ;
- les paramètres de fonctionnement des modules de contrôle et de protection ;
- les paramètres de détection des SVM fonctionnant en réseau et des réceptions des informations les concernant ;
- les paramètres complémentaires de fonctionnement de l'application (paramètres d'autodéfense, mode de fonctionnement, paramètres des rapports et du stockage de données, paramètres d'interface).



L'utilisateur peut modifier les paramètres définis dans la stratégie pour le Light Agent for Windows si celle-ci l'autorise ; ceci en local, sur chaque machine virtuelle protégée, via l'interface de l'application (cf. *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

- **Stratégie pour un Light Agent for Linux** La stratégie définit les paramètres de fonctionnement des Light Agents installés sur les machines virtuelles protégées avec les systèmes d'exploitation invités Linux. La stratégie s'applique à l'ensemble des machines virtuelles protégées figurant dans le groupe d'administration pour lequel elle est configurée.

Les paramètres de la stratégie pour le Light Agent for Linux incluent :

- les paramètres généraux de la protection des machines virtuelles et les paramètres des événements (Kaspersky Security Center cf. documentation) ;
- les paramètres généraux de protection antivirus ;
- les paramètres de fonctionnement du composant Antivirus Fichiers ;
- les paramètres de détection des SVM fonctionnant en réseau et des réceptions des informations les concernant ;
- les paramètres de la sauvegarde.

La possibilité de modifier la configuration de l'application en local, sur la machine virtuelle protégée, est déterminée par l'état du "verrou" du paramètre dans la stratégie :

- Si le paramètre est fermé par un "verrou" () , l'utilisateur ne peut pas modifier sa valeur en local et c'est la valeur définie par la stratégie qui est appliquée à toutes les machines virtuelles protégées du groupe d'administration.
- Si le paramètre n'est pas fermé par un "verrou" () , l'utilisateur peut modifier sa valeur en local sur chaque machine virtuelle protégée du groupe d'administration.

Vous pouvez réaliser les opérations suivantes sur les stratégies :

- créer une stratégie ;
- modifier les paramètres d'une stratégie ;
- supprimer une stratégie ;
- modifier l'état d'une stratégie.

Pour plus d'informations sur l'utilisation des stratégies, consultez la documentation de Kaspersky Security Center.

Affichage des paramètres des stratégies

Par défaut, l'Assistant de création d'une stratégie pour le Serveur de protection et les propriétés de stratégie pour le Serveur de protection n'affichent pas les paramètres complémentaires de fonctionnement des SVM (cf. section "Étape 6. Configuration des paramètres supplémentaires de fonctionnement des SVM" à la p. [92](#)).

Si vous voulez configurer ces paramètres à l'aide de la stratégie, vous devez préalablement créer la clé AdvancedUI de type DWORD et définir la valeur 1 pour cette clé dans la branche suivante du registre du système d'exploitation sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center :

- HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Products\SVM\3.4.0.0\Settings\ (pour le système d'exploitation de 32 bits) ;
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\SVM\3.4.0.0\Settings\ (pour le système d'exploitation 64 bits).

Création de la stratégie pour le Serveur de protection

► *Pour créer une stratégie pour le Serveur de protection, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les SVM pour lesquelles vous souhaitez créer une stratégie.

Sous l'onglet **Ordinateurs** du dossier portant le nom du groupe d'administration, vous pouvez consulter la liste des SVM qui appartiennent à ce groupe d'administration.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Cliquez sur le bouton **Créer une stratégie** pour lancer l'assistant de création de stratégie.
5. Suivez les instructions de l'Assistant de création de stratégie.

Dans cette section

Etape 1. Définition du nom de la stratégie de groupe pour l'application.....	87
Etape 2. Sélection de l'application pour la création de la stratégie du groupe	87
Etape 3. Configuration des paramètres KSN.....	87
Etape 4. Configuration de la mise à jour.....	90
Etape 5. Configuration des paramètres de détection des SVM.....	90
Etape 6. Configuration des paramètres supplémentaires de fonctionnement des SVM.....	92
Etape 7. Création de la stratégie de groupe pour l'application	93

Etape 1. Définition du nom de la stratégie de groupe pour l'application

A cette étape, saisissez le nom de la stratégie dans le champ **Nom**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 2. Sélection de l'application pour la création de la stratégie du groupe

A cette étape, dans la liste **Nom de l'application**, sélectionnez **Kaspersky Security for Virtualization 4.0 Light Agent - Serveur de protection**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 3. Configuration des paramètres KSN

Cette étape vous invite à participer au Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page [192](#)).

Kaspersky Security Network (KSN) est une infrastructure de services de cloud qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Web et des logiciels. Grâce aux données de Kaspersky Security Network,

Kaspersky Security peut réagir plus rapidement face aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

Selon la disposition de l'infrastructure, les distinctions suivantes ont cours :

- Le KSN global est une infrastructure disposée sur les serveurs de Kaspersky Lab ;
- Le KSN privé (Kaspersky Private Security Network) est une infrastructure disposée sur des serveurs secondaires du prestataire, par exemple à l'intérieur d'un réseau d'un fournisseur d'accès à Internet.

La participation au Kaspersky Security Network est volontaire. Avant d'accepter une solution de participation du Kaspersky Security Network, lisez attentivement la Déclaration de Kaspersky Security Network ou la Déclaration de Kaspersky Private Security Network, en fonction du type de KSN utilisé par Kaspersky Security. Pour prendre connaissance de la Déclaration, cliquez sur le bouton **Déclaration de KSN**.

Si vous souhaitez utiliser Kaspersky Security Network avec Kaspersky Security, assurez-vous que le service KSN Proxy est activé dans le Kaspersky Security Center (consulter la documentation du Kaspersky Security Center).

► *Pour configurer les paramètres d'utilisation de KSN dans le cadre du fonctionnement de l'application, procédez comme suit :*

1. Cochez la case **J'accepte les conditions du Contrat de licence et je participe à KSN**.

En cochant la case **J'accepte les conditions du Contrat de licence et je participe à KSN**, vous marquez votre accord avec les dispositions du programme Kaspersky Security Network présentées dans la déclaration de Kaspersky Security Network.

2. Si vous souhaitez que l'application Kaspersky Security utilise KSN lors de l'analyse des fichiers, cochez la case **Utiliser pour l'analyse des fichiers et des catégories**.

La case active ou désactive l'utilisation des services KSN dans le fonctionnement des modules suivants de Light Agent et des tâches :

- Contrôle du lancement des applications.
- Contrôle de l'activité des applications.
- Antivirus Fichiers.

- Surveillance du système.
- Tâches d'analyse.

Si la case est cochée, lors de l'utilisation des modules de Light Agent énumérés et des tâches, l'application Kaspersky Security reçoit des informations envoyées par les services KSN concernant la catégorie et la réputation des fichiers analysés.

Si la case est décochée, Kaspersky Security ne reçoit pas d'informations envoyées par les services KSN concernant la réputation et la catégorie des fichiers.

Cette case est accessible si la case **J'accepte les Conditions du contrat de licence et je participe à KSN** est cochée.

3. Si vous souhaitez que l'application Kaspersky Security utilise KSN pour l'analyse des adresses Internet, cochez la case **Utiliser pour l'analyse des URL**.

La case active ou désactive l'utilisation des services KSN dans le fonctionnement des modules suivants de Light Agent for Windows :

- Antivirus Internet.
- Contrôle Internet.
- Antivirus IM.

Si la case est cochée, lors de l'utilisation des modules de Light Agent for Windows énumérés, Kaspersky Security reçoit des informations envoyées par les services KSN concernant la réputation des adresses Internet analysées.

Si la case est décochée, Kaspersky Security ne reçoit pas d'informations envoyées par les services KSN concernant la réputation des adresses Internet.

Cette case est accessible si la case **J'accepte les Conditions du contrat de licence et je participe à KSN** est cochée.

4. Si vous souhaitez interdire ou autoriser la modification des paramètres KSN dans les stratégies des niveaux inférieurs (pour les groupes d'administration secondaires), cliquez sur le "verrou" à gauche de la case **J'accepte les conditions du Contrat de licence et je participe à KSN**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 4. Configuration de la mise à jour

Cette étape permet de configurer la mise à jour des modules de l'application (modules du Light Agent for Windows) pendant la mise à jour des bases de l'application sur la machine virtuelle protégée. Par défaut, l'application Kaspersky Security n'inclut pas les mises à jour des modules de l'application dans le paquet de mises à jour.

Si vous souhaitez activer la mise à jour des modules du Light Agent for Windows, cochez la case **Mettre à jour les modules de l'application**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 5. Configuration des paramètres de détection des SVM

À cette étape, indiquez la manière dont les SVM transmettront les informations les concernant aux Light Agents.

- **Utiliser la multidiffusion (Multicast).**

Si la case est cochée, les SVM transmettent les informations les concernant aux Light Agents via la multidiffusion (Multicast).

Si la case est décochée, la multidiffusion n'est pas utilisée.

Par défaut, la case est cochée.

- **Utiliser le Serveur d'intégration.**

Si la case est cochée, les SVM transmettent au Serveur d'intégration toutes les informations nécessaires à la connexion des Light Agents. Si vous souhaitez utiliser le Serveur d'intégration, il faut indiquer les paramètres de connexion des SVM au Serveur d'intégration.

Si la case est décochée, les informations concernant les SVM ne sont pas transmises au Serveur d'intégration.

Par défaut, la case est cochée.

Si la case **Utiliser le Serveur d'intégration** est cochée, indiquez les paramètres de connexion des SVM au Serveur d'intégration.

► *Pour indiquer les paramètres de connexion des SVM au Serveur d'intégration, procédez comme suit :*

1. Par défaut, le champ **Adresse** contient le nom de domaine de l'ordinateur hébergeant la Console d'administration Kaspersky Security Center. Si cet ordinateur n'appartient pas au domaine, si le Serveur d'intégration est installé sur un autre ordinateur, et qu'une adresse incorrecte figure dans le champ, indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) du Serveur d'intégration.
2. Si le port de connexion au Serveur d'intégration est différent de celui utilisé par défaut (7271), indiquez le numéro de port dans le champ **Port**.
3. Si l'ordinateur sur lequel la Console d'administration Kaspersky Security Center n'appartient pas au domaine ou si votre compte n'appartient pas au groupe KAdmins ou au groupe d'administrateurs locaux, la fenêtre **Connexion au Serveur d'intégration** s'ouvre. Indiquez le mot de l'administrateur du Serveur d'intégration (mot de passe du compte admin). Une fois la connexion au Serveur d'intégration établie à l'aide des privilèges d'administrateur, le mot de passe du compte utilisateur est automatiquement transmis à la stratégie pour la connexion des SVM au Serveur d'intégration.

Lors du passage à l'étape suivante de l'assistant, la possibilité de connexion au Serveur d'intégration est analysée. Si cette analyse échoue ou s'il est impossible d'établir une connexion au Serveur d'intégration, vous ne pouvez pas passer à l'étape suivante. Analysez les paramètres de connexion saisis. Les informations sur les erreurs de connexion au Serveur d'intégration sont consignées dans le journal de fonctionnement du Serveur d'intégration (cf. section "A propos des journaux du Serveur d'intégration" à la page [225](#)).

Si vous avez décoché les deux cases **Utiliser la multidiffusion (Multicast)** et **Utiliser le Serveur d'intégration**, vous devez indiquer la liste d'adresses des SVM, auxquelles les Light Agents peuvent se connecter, dans la stratégie pour un Light Agent for Windows (cf. section "Etape 6. Configuration des paramètres de détection des SVM" à la p. [102](#)) et dans la stratégie pour un Light Agent for Linux (cf. section "Etape 5. Configuration des paramètres de détection des SVM" à la p. [114](#)).

Passez à l'étape suivante de l'Assistant.

Etape 6. Configuration des paramètres supplémentaires de fonctionnement des SVM

Cette étape est disponible si vous avez activé l'affichage des paramètres complémentaires de la stratégie pour le Serveur de protection dans le registre du système d'exploitation (cf. section "Affichage des paramètres des stratégies" à la page [86](#)).

Lors de cette étape, indiquez les paramètres de fonctionnement des SVM :

- **Quantité maximale de demandes simultanées d'analyse.**

Nombre maximal de requêtes d'analyse envoyées par les Light Agents et traitées simultanément par la SVM. Les Light Agents envoient des requêtes d'analyse dans le cadre de la protection des machines virtuelles et de l'exécution des tâches d'analyse.

Par défaut, une SVM traite simultanément 75 requêtes d'analyse.

- **Quantité maximale de tâches d'analyse lancées de manière planifiée.**

Nombre maximal de tâches d'analyse exécutées simultanément sur une SVM et lancées en fonction d'une programmation sur le Light Agent.

Pour la SVM, ces tâches d'analyse ont une faible priorité.

Par défaut, cinq tâches d'analyse de priorité faible peuvent être exécutées simultanément.

- **Quantité maximale de tâches d'analyse lancées manuellement.**

Nombre maximal de tâches d'analyse exécutées simultanément sur une SVM et lancées manuellement par l'utilisateur. Pour la SVM, ces tâches d'analyse ont une priorité élevée.

Par défaut, cinq tâches d'analyse de priorité élevée peuvent être exécutées simultanément.

Passez à l'étape suivante de l'Assistant.

Etape 7. Création de la stratégie de groupe pour l'application

Quittez l'Assistant de création de stratégie.

La fenêtre de l'Assistant de création de stratégie se ferme. La stratégie créée apparaît dans la liste des stratégies sous l'onglet **Stratégies**.

Lors de la connexion suivante de la SVM au Serveur d'administration, le Kaspersky Security Center transmet les informations à l'application Kaspersky Security et la stratégie se propage aux SVM. Kaspersky Security commence à protéger les machines virtuelles sur l'hyperviseur, conformément aux paramètres de la stratégie.

Si l'Agent d'administration n'est pas lancé sur la SVM, la stratégie créée ne s'applique pas à cette dernière.

Si vous avez sélectionné l'option **Stratégie inactive**, la stratégie créée ne s'applique pas aux SVM.

Configuration de l'affichage des paramètres de contrôle dans la Console d'administration

Par défaut, l'Assistant de création d'une stratégie pour le Light Agent et les propriétés de la stratégie n'affichent pas les paramètres des modules de contrôle du Light Agent :

- Contrôle du lancement des applications.
- Contrôle de l'activité des applications.
- Contrôle des périphériques.
- Contrôle Internet.

Pour en savoir plus sur le fonctionnement des modules de contrôle du Light Agent, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Si vous souhaitez configurer les paramètres de fonctionnement des modules de contrôle du Light Agent à l'aide d'une stratégie pour le Light Agent, il vous sera d'abord nécessaire de configurer l'affichage des paramètres de contrôle dans l'interface de la Console d'administration de Kaspersky Security Center.

► *Pour configurer l'affichage des paramètres de contrôle dans la Console d'administration, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration et ouvrez la fenêtre **Configuration de l'interface** de l'une des manières suivantes :
 - à l'aide de l'option **Apparence** → **Configuration de l'interface** ;
 - via le lien **Configurer la fonctionnalité affichable dans l'interface utilisateur**. Le lien se trouve dans l'espace de travail dans le groupe **Serveur d'administration**.
3. Dans la fenêtre **Configuration de l'interface**, cochez la case **Afficher les paramètres Endpoint Control**.
4. Cliquez sur le bouton **OK** pour fermer la fenêtre.

Ces modifications sont appliquées dès le redémarrage de la Console d'administration de Kaspersky Security Center.

Création de la stratégie pour le Light Agent for Windows

► *Pour créer une stratégie pour un Light Agent for Windows, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les machines virtuelles protégées pour lesquelles vous souhaitez créer une stratégie.

Sous l'onglet **Ordinateurs** du dossier portant le nom du groupe d'administration, vous pouvez consulter la liste des machines virtuelles protégées qui appartiennent à ce groupe d'administration.

3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Cliquez sur le bouton **Créer une stratégie** pour lancer l'assistant de création de stratégie.
5. Suivez les instructions de l'Assistant de création de stratégie.

Dans cette section

Etape 1. Définition du nom de la stratégie de groupe pour l'application.....	95
Etape 2. Sélection de l'application pour la création de la stratégie du groupe	96
Etape 3. Importation des paramètres du Light Agent.....	96
Etape 4. Configuration des paramètres du contrôle.....	96
Etape 5. Configuration des paramètres de protection.....	98
Etape 6. Configuration des paramètres de détection des SVM.....	102
Etape 7. Configuration de la zone de confiance	104
Etape 8. Configuration de l'interface du Light Agent.....	106
Etape 9. Protection de l'accès aux fonctions et aux paramètres du Light Agent	108
Etape 10. Création de la stratégie de groupe pour l'application	109

Etape 1. Définition du nom de la stratégie de groupe pour l'application

A cette étape, saisissez le nom de la stratégie dans le champ **Nom**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 2. Sélection de l'application pour la création de la stratégie du groupe

A cette étape, dans la liste **Nom de l'application**, sélectionnez **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 3. Importation des paramètres du Light Agent

A cette étape, vous pouvez transférer les paramètres du Light Agent for Windows enregistrés sur la machine virtuelle protégée vers la stratégie en cours de création. Pour le transfert, il faut un fichier de configuration au format CFG que vous pouvez créer dans l'interface locale de Light Agent (informations détaillées dans le *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

Pour le transfert des paramètres, cliquez sur le bouton **Sélectionner** et dans la fenêtre ouverte **Sélection du fichier de configuration**, sélectionnez le fichier avec l'extension cfg.

Le chemin vers le fichier de configuration s'affiche dans le champ **Fichier de configuration**.

Dans les étapes suivantes de l'Assistant de création d'une stratégie, vous pouvez modifier les valeurs des paramètres transférés depuis le fichier de configuration.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 4. Configuration des paramètres du contrôle

Cette étape est accessible si l'affichage des paramètres de contrôle est activé dans les paramètres de l'interface de la Console d'administration de Kaspersky Security Center (cf. section "Configuration de l'affichage des paramètres de contrôle dans la Console d'administration", à la page [93](#)).

A cette étape, vous pouvez configurer les paramètres de contrôle des machines virtuelles.
La fenêtre de l'Assistant affiche la liste des modules de contrôle du Light Agent.

Vous pouvez exécuter les opérations suivantes :

- activer ou désactiver les modules de contrôle ;
- configurer les paramètres de chaque module de contrôle ;
- interdire ou autoriser la modification des paramètres de chaque module de contrôle via l'interface locale de Light Agent. Si la modification des paramètres du module via l'interface locale est interdite, Kaspersky Security utilise les paramètres de fonctionnement du module définis par la stratégie sur l'ensemble des machines virtuelles protégées. Si la modification des paramètres du module via l'interface locale est autorisée, Kaspersky Security utilise les valeurs locales des paramètres de fonctionnement du module plutôt que celles définies dans la stratégie.

► *Pour activer ou désactiver les modules de contrôle, procédez comme suit :*

- Si vous souhaitez activer le module de contrôle, cochez la case à gauche, en regard du nom du module figurant dans la liste.
- Si vous souhaitez désactiver le module de contrôle, décochez la case à gauche, en regard du nom du module figurant dans la liste.

Tous les modules de contrôle sont activés par défaut.

► *Pour configurer les paramètres du module de contrôle, procédez comme suit :*

1. Sélectionnez le module de contrôle dans la liste et cliquez sur le bouton **Modifier** situé au-dessus de la liste des modules de contrôle.

La fenêtre **Configuration : <Nom du composant>** s'ouvre.

2. Configurez les paramètres de fonctionnement du module de contrôle sélectionné.
Suite à l'adoption de la stratégie, Kaspersky Security utilise ces paramètres sur les machines virtuelles protégées.

Pour en savoir plus sur la configuration des paramètres de chaque module de contrôle, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

3. Cliquez sur le bouton **OK** dans la fenêtre **Configuration : <Nom du composant>** pour enregistrer les modifications et fermer la fenêtre.

► *Pour interdire ou autoriser la modification des paramètres du module de contrôle dans l'interface locale de Light Agent, choisissez l'une des options suivantes :*

- Si vous souhaitez interdire la modification des paramètres dans l'interface locale de Light Agent, procédez comme suit :
 - Sélectionnez le module de contrôle dans la liste, puis cliquez sur le bouton **Fermer**. Le bouton est situé au-dessus de la liste des modules de contrôle.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de contrôle.
- Si vous souhaitez autoriser la modification des paramètres dans l'interface locale de Light Agent, procédez comme suit :
 - Sélectionnez le module de contrôle dans la liste, puis cliquez sur le bouton **Ouvrir**. Le bouton est situé au-dessus de la liste des modules de contrôle.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de contrôle.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 5. Configuration des paramètres de protection

A cette étape, vous pouvez configurer les paramètres de protection des machines virtuelles. La fenêtre de l'Assistant affiche la liste des modules de la protection du Light Agent for Windows.

Vous pouvez exécuter les opérations suivantes :

- Configurer les paramètres généraux de la protection et y activer la technologie de réparation de l'infection active.
- Activer ou désactiver les composants de la protection.
- Configurer les paramètres de chaque composant de la protection.
- Interdire ou autoriser la modification des paramètres de chaque composant de la protection via l'interface locale du Light Agent for Windows.

Si la modification des paramètres du module via l'interface locale est interdite, Kaspersky Security utilise les paramètres de fonctionnement du module définis par la stratégie sur l'ensemble des machines virtuelles protégées. Si la modification des paramètres du module via l'interface locale est autorisée, Kaspersky Security utilise les valeurs locales des paramètres de fonctionnement du module plutôt que celles définies dans la stratégie.

► *Pour configurer les paramètres généraux de la protection, procédez comme suit :*

1. Dans la liste des modules, choisissez la section **Paramètres généraux**.
2. Cliquez sur le bouton **Modifier** situé au-dessus de la liste d'adresses des composants de protection.

La fenêtre **Configuration : Administration de la protection** s'ouvre.

3. Cochez la case **Lancer Kaspersky Security for Virtualization 4.0 Light Agent à l'insertion de la machine virtuelle** si vous voulez que l'application Kaspersky Security soit lancée après le chargement du système d'exploitation et protège la machine virtuelle pendant toute la session.
4. Si vous souhaitez utiliser une technologie particulière de réparation de l'infection active pour les machines virtuelles du système d'exploitation pour serveur, cochez la case **Appliquer la technologie de réparation de l'infection active**, (cf. section "Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur" à la page [190](#)).

Si le Light Agent fonctionne sur une machine virtuelle temporaire, la technologie de réparation de l'infection active n'est pas utilisée. En cas d'infection active de cette machine virtuelle temporaire, il est nécessaire de s'assurer de l'absence de virus et d'autres applications malveillantes sur le modèle de machine virtuelle à partir duquel elle a été créée, puis de recréer la machine virtuelle temporaire.

La technologie de réparation de l'infection active pour les machines virtuelles dotées d'un système d'exploitation pour serveur est désactivée par défaut. Pour réparer une infection active sur un serveur de fichiers, il est nécessaire de lancer une tâche de groupe pour la recherche de virus (cf. section "Gestion des tâches" à la page [121](#)). Une fois la procédure de réparation de l'infection active terminée, la machine virtuelle est redémarrée.

L'activation et la désactivation de la technologie de réparation de l'infection active pour les machines virtuelles dotées d'un système d'exploitation pour poste de travail s'effectue dans l'interface locale de Light Agent. Pour en savoir plus sur la technologie de réparation de l'infection active, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

5. Dans le groupe **Objets à détecter**, cliquez sur le bouton **Configuration** et dans la fenêtre ouverte **Objets à détecter**, cochez les cases pour les types des objets que doit détecter l'application Kaspersky Security (pour plus de détails, cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

N'oubliez pas que les fichiers détectés peuvent être supprimés par l'application.

6. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration** et, dans la fenêtre ouverte **Zone de confiance**, configurez la liste des exclusions de la protection Kaspersky Security (cf. section "Configuration des exclusions de la protection via Kaspersky Security Center" à la p. [156](#)). Le Kaspersky Security Center transpose ces paramètres sur les machines virtuelles protégées dès l'application de la stratégie.

Si une application est installée sur votre machine virtuelle et qu'elle exécute la collecte et l'envoi d'informations à traiter, Kaspersky Security peut classer cette application comme malveillante. Pour éviter cela, vous pouvez exclure l'application de la protection en l'ajoutant aux exclusions.

7. Dans le groupe **Ports contrôlés**, configurez le mode de contrôle des ports réseau dans lequel l'Antivirus Courrier, l'Antivirus Internet et l'Antivirus Fichiers analyse les flux de données entrants et sortants. Pour en savoir plus sur le contrôle du trafic réseau, cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.
8. Cliquez sur le bouton **OK** dans la fenêtre **Configuration : administration de la protection** pour enregistrer les modifications et fermer la fenêtre.

Kaspersky Security Center transpose les paramètres configurés sur les machines virtuelles protégées lors de l'application de la stratégie.

► *Pour activer ou désactiver les modules de la protection, procédez comme suit :*

- Si vous souhaitez activer le module de la protection, cochez la case à gauche, en regard du nom du module figurant dans la liste.
- Si vous souhaitez désactiver le module de la protection, décochez la case à gauche, en regard du nom du module figurant dans la liste.

Tous les modules de la protection sont activés par défaut.

► *Pour configurer les paramètres du module de la protection, procédez comme suit :*

1. Sélectionnez le module de la protection dans la liste et cliquez sur le bouton **Modifier** situé au-dessus de la liste des modules de protection.

La fenêtre **Configuration : <Nom du composant>** s'ouvre.

2. Configurez les paramètres de fonctionnement du module de la protection sélectionné. Suite à l'adoption de la stratégie, Kaspersky Security utilise ces paramètres sur les machines virtuelles protégées.

Pour en savoir plus sur la configuration des paramètres de chaque module de la protection, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

3. Cliquez sur le bouton **OK** dans la fenêtre **Configuration : <Nom du composant>** pour enregistrer les modifications et fermer la fenêtre.

► *Pour interdire ou autoriser la modification des paramètres du module de la protection dans l'interface locale du Light Agent, choisissez l'une des options suivantes :*

- Si vous souhaitez interdire la modification des paramètres dans l'interface locale du Light Agent, effectuez une des actions suivantes :
 - Sélectionnez le module de la protection dans la liste, puis cliquez sur le bouton **Fermer**. Le bouton est situé au-dessus de la liste des modules de la protection.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de la protection.

- Si vous souhaitez autoriser la modification des paramètres dans l'interface locale du Light Agent, effectuez une des actions suivantes :
 - Sélectionnez le module de la protection dans la liste, puis cliquez sur le bouton **Ouvrir**. Le bouton est situé au-dessus de la liste des modules de la protection.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de la protection.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 6. Configuration des paramètres de détection des SVM

Lors de cette étape, sélectionner la méthode utilisée par les Light Agents pour la détection des SVM du réseau et la réception des informations les concernant.

- **Utiliser la multidiffusion (Multicast).**

Si cette option est sélectionnée, le module Light Agent obtient les informations sur les SVM à l'aide de la multidiffusion (Multicast).

Cette option est sélectionnée par défaut.

- **Utiliser le Serveur d'intégration.**

Si cette option est sélectionnée, le module Light Agent se connecte au Serveur d'intégration pour obtenir la liste des SVM auxquelles il peut se connecter et les informations les concernant. Si vous souhaitez utiliser le Serveur d'intégration, il faut indiquer les paramètres de connexion des Light Agents au Serveur d'intégration.

- **Utiliser une liste d'adresses de SVM établie manuellement.**

Si cette option est sélectionnée, vous pouvez indiquer la liste des SVM auxquelles peuvent se connecter les Light Agents administrés par cette stratégie. Les Light Agents ne se connecteront qu'aux SVM indiquées dans la liste.

Si vous avez sélectionné la variante **Utiliser le Serveur d'intégration**, indiquez les paramètres de connexion des Light Agents au Serveur d'intégration.

► *Pour indiquer les paramètres de connexion des Light Agents au Serveur d'intégration, procédez comme suit :*

1. Par défaut, le champ **Adresse** contient le nom de domaine de l'ordinateur hébergeant la Console d'administration Kaspersky Security Center. Si cet ordinateur n'appartient pas au domaine, si le Serveur d'intégration est installé sur un autre ordinateur, et qu'une adresse incorrecte figure dans le champ, indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) du Serveur d'intégration.
2. Si le port de connexion au Serveur d'intégration est différent de celui utilisé par défaut (7271), indiquez le numéro de port dans le champ **Port**.
3. Si l'ordinateur sur lequel la Console d'administration Kaspersky Security Center n'appartient pas au domaine ou si votre compte n'appartient pas au groupe KAdmins ou au groupe d'administrateurs locaux, la fenêtre **Connexion au Serveur d'intégration** s'ouvre. Indiquez le mot de l'administrateur du Serveur d'intégration (mot de passe du compte admin). Une fois la connexion au Serveur d'intégration établie à l'aide des privilèges d'administrateur, le mot de passe du compte est automatiquement transmis à la stratégie pour la connexion des Light Agents au Serveur d'intégration.

Lors du passage à l'étape suivante de l'assistant, la possibilité de connexion au Serveur d'intégration est analysée. Si cette analyse échoue ou s'il est impossible d'établir une connexion au Serveur d'intégration, vous ne pouvez pas passer à l'étape suivante. Analysez les paramètres de connexion saisis. Les informations sur les erreurs de connexion au Serveur d'intégration sont consignées dans le journal de fonctionnement du Serveur d'intégration (cf. section "A propos des journaux du Serveur d'intégration" à la page [225](#)).

Si vous avez sélectionné l'option **Utiliser une liste d'adresses de SVM établie manuellement**, composez la liste des SVM.

► *Pour composer une liste des SVM, procédez comme suit :*

1. Cliquez sur le bouton **Ajouter** situé au-dessus de la liste d'adresses de SVM.

Ouvre la fenêtre **Adresses des SVM**.

2. Saisissez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM à laquelle pourront se connecter les Light Agents gérés par la stratégie. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine complet auquel correspondent plusieurs adresses IP peut entraîner des erreurs de fonctionnement de l'application.

3. Cliquez sur le bouton **OK** dans la fenêtre **Adresses des SVM**.

L'application analyse les adresses et noms de domaines complets saisis des SVM.

Si certain(e)s adresses ou noms ne sont pas reconnu(e)s, un message apparaît dans une fenêtre séparée avec le nombre d'adresses ou de noms non reconnu(e)s.

Les adresses reconnues et les noms de domaines complets apparaissent dans la liste des adresses des SVM.

4. Si vous souhaitez supprimer de la liste l'adresse IP ou le nom de domaine complet de la SVM, sélectionnez cet élément dans la liste et cliquez sur le bouton **Supprimer** situé au-dessus de la liste.

Passez à l'étape suivante de l'Assistant.

Etape 7. Configuration de la zone de confiance

A cette étape, vous pouvez créer une zone de confiance.

La *zone de confiance* est une liste de fichiers, de dossiers, d'objets et d'applications composée par l'administrateur que Kaspersky Security ne contrôle pas. Pour en savoir plus sur la zone de confiance, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

La liste de la fenêtre **Exclusions** comporte les noms des applications ou des éditeurs d'applications que vous pouvez inclure ou exclure dans la zone de confiance. Les applications répertoriées sont utilisées pour l'administration et la protection antivirus des réseaux informatiques. Vous pouvez configurer les paramètres de la zone de confiance dans les propriétés de la stratégie pour le Light Agent for Windows ou dans les paramètres du Light Agent dans l'interface locale de l'application (voir *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

► *Pour configurer une zone de confiance, procédez comme suit :*

1. Dans la liste, sélectionnez le nom de l'application ou de l'éditeur d'applications concerné.
2. Exécutez une des actions suivantes :
 - si vous souhaitez inclure l'application ou les applications d'un éditeur spécifique dans la zone de confiance, cochez la case à gauche, en regard du nom de l'application ou de l'éditeur ;
 - si vous souhaitez exclure l'application ou l'application d'un éditeur spécifique de la zone de confiance, décochez la case à gauche, en regard du nom de l'application ou de l'éditeur.

Si les cases **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp** et **Citrix XenDesktop** sont cochées, les fichiers, les dossiers et les processus recommandés pour ces applications sont ajoutés à la zone de confiance et les fichiers exécutables de ces applications sont ajoutés automatiquement à la liste des applications de confiance. Ces exclusions s'appliquent aux systèmes d'exploitation pour serveur et pour poste de travail. La liste complète des exclusions recommandées est reprise sur le site Internet de Citrix <http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/>. Les cases **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp** et **Citrix XenDesktop** sont cochées par défaut pour l'amélioration des performances de ces applications.

Outre les applications de la liste, la zone de confiance inclut par défaut les applications recommandées pour les systèmes d'exploitation pour serveur / poste de travail.

Si vous souhaitez exclure les applications recommandées pour les systèmes d'exploitation pour poste de travail de la zone de confiance, décochez la case **Créer les exclusions recommandées pour les postes de travail**.

Si vous souhaitez exclure les applications recommandées pour les systèmes d'exploitation pour serveur de la zone de confiance, décochez la case **Créer les exclusions recommandées pour les systèmes d'exploitation des serveurs**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 8. Configuration de l'interface du Light Agent

A cette étape, vous pouvez réaliser les opérations suivantes :

- Configurer les paramètres d'interaction entre l'interface locale de Light Agent et l'utilisateur.
- Configurer les paramètres des notifications sur les événements survenant au cours du fonctionnement du Light Agent.
- Configurer l'affichage des informations sur le support dans l'interface locale de Light Agent.
- Interdire ou autoriser la modification des paramètres de l'interface, des paramètres des notifications et des paramètres d'affichage des informations sur le support via l'interface locale de Light Agent.

Si la modification des paramètres via l'interface locale est interdite, Kaspersky Security utilise les paramètres définis par la stratégie sur l'ensemble des machines virtuelles protégées. Si la modification des paramètres via l'interface locale est autorisée, Kaspersky Security utilise les valeurs locales des paramètres de fonctionnement de l'application plutôt que celles définies dans la stratégie.

Pour garantir le fonctionnement de l'application Kaspersky Security sur une machine virtuelle qui utilise la technologie Citrix XenApp, il faut décocher la case **Lancer l'interface locale de l'application**.

Si vous utilisez le Light Agent sur les machines virtuelles temporaires, pour l'augmentation des performances de l'infrastructure virtuelle il est recommandé de décocher la case **Lancer l'interface locale de l'application**.

- *Pour configurer les paramètres des notifications sur les événements survenant au cours du fonctionnement du Light Agent, procédez comme suit :*

1. Cliquez sur le bouton **Configuration** dans le groupe **Notifications**.

La fenêtre **Notifications** s'ouvre.

2. Configurez l'utilisation des notifications et l'enregistrement des informations sur les événements dans le journal de l'application et le journal des événements de Windows. Pour en savoir plus la configuration des notifications, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.
3. Cliquez sur le bouton **OK** dans la fenêtre **Notifications** pour enregistrer les modifications et fermer la fenêtre.

- *Pour configurer l'affichage des informations de support dans l'interface locale de Light Agent, procédez comme suit :*

1. Cliquez sur le bouton **Configuration** dans le groupe **Assistance aux utilisateurs**.

La fenêtre **Informations sur le Support Technique** s'ouvre.

2. Composez une liste des liens sur les ressources Web qui s'affichera dans l'interface locale de Light Agent. Utilisez les boutons situés au-dessus de la liste pour l'ajout, la modification, la suppression ou le déplacement de liens.
3. Cliquez sur le bouton **OK** dans la fenêtre **Informations sur le Support technique** pour enregistrer les modifications et fermer la fenêtre.

- *Pour interdire ou autoriser la modification des paramètres de l'interface, des paramètres des notifications et des paramètres d'affichage des informations sur le support de l'utilisateur via l'interface locale de Light Agent,*

cliquez sur le "verrou" à gauche, en regard du groupe de paramètres concerné.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 9. Protection de l'accès aux fonctions et aux paramètres du Light Agent

A cette étape, vous pouvez configurer la protection de l'accès à l'ensemble ou à certains des paramètres et fonctions du Light Agent via un mot de passe. Si la protection de l'accès est activée, l'utilisateur doit saisir un nom d'utilisateur et un mot de passe pour accéder aux fonctions et aux paramètres du Light Agent sur la machine virtuelle protégée. Par défaut, la protection de l'accès est désactivée.

► *Pour activer la protection de l'accès aux fonctions et aux paramètres du Light Agent, procédez comme suit :*

1. Cochez la case **Activer la protection par mot de passe**.
2. Saisissez le nom d'utilisateur dans le champ **Nom d'utilisateur**.
3. Saisissez le mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.
4. Cliquez sur le bouton **Configuration** pour sélectionner les opérations du Light Agent qui doivent être protégées par un mot de passe.

La fenêtre **Paramètres de protection par mot de passe** s'ouvre.

5. Dans la fenêtre qui s'ouvre, indiquez les opérations du Light Agent qui nécessitent la saisie d'un mot de passe pour s'exécuter :
 - toutes les opérations (sauf les notifications de danger) ;
 - modification des paramètres de fonctionnement de l'application ;
 - arrêt de l'application ;
 - activation des modules de protection ;
 - activation des modules de contrôle ;
 - désactivation des modules de protection et arrêt des tâches d'analyse ;
 - désactivation des modules du contrôle ;

- désactivation de la stratégie de Kaspersky Security Center ;
- suppression/modification/restauration de l'application ;
- consultation des rapports.

Par défaut, toutes les opérations du Light Agent sont protégées par un mot de passe.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 10. Création de la stratégie de groupe pour l'application

Quittez l'Assistant de création de stratégie.

La fenêtre de l'Assistant de création de stratégie se ferme. La stratégie créée apparaît dans la liste des stratégies sous l'onglet **Stratégies**.

Lors de la connexion suivante de la machine virtuelle au Serveur d'administration, le Kaspersky Security Center transmet les informations à l'application Kaspersky Security et la stratégie se propage aux machines virtuelles protégées. Kaspersky Security commence à protéger les machines virtuelles sur l'hyperviseur, conformément aux paramètres de la stratégie.

Si l'Agent d'administration n'est pas lancé sur la machine virtuelle protégée, la stratégie créée ne s'applique pas à cette dernière.

Si vous avez sélectionné l'option **Stratégie inactive**, la stratégie créée ne s'applique pas aux machines virtuelles protégées.

Si les informations sur la licence ne sont pas transmises à la machine virtuelle protégée, le module Light Agent fonctionne en mode restreint (cf. section "Activation de l'application" à la page [46](#)).

Création de la stratégie pour le Light Agent for Linux

► Pour créer une stratégie pour le Light Agent for Linux, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les machines virtuelles protégées pour lesquelles vous souhaitez créer une stratégie.

Sous l'onglet **Ordinateurs** du dossier portant le nom du groupe d'administration, vous pouvez consulter la liste des machines virtuelles protégées qui appartiennent à ce groupe d'administration.

3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Cliquez sur le bouton **Créer une stratégie** pour lancer l'assistant de création de stratégie.
5. Suivez les instructions de l'Assistant de création de stratégie.

Dans cette section

Etape 1. Définition du nom de la stratégie de groupe pour l'application.....	111
Etape 2. Sélection de l'application pour la création de la stratégie du groupe	111
Etape 3. Importation des paramètres du Light Agent.....	111
Etape 4. Configuration des paramètres de protection.....	111
Etape 5. Configuration des paramètres de détection des SVM.....	114
Etape 6. Création de la stratégie de groupe pour l'application	116

Etape 1. Définition du nom de la stratégie de groupe pour l'application

A cette étape, saisissez le nom de la stratégie dans le champ **Nom**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 2. Sélection de l'application pour la création de la stratégie du groupe

A cette étape, dans la liste **Nom de l'application**, sélectionnez **Kaspersky Security for Virtualization 4.0 Light Agent for Linux**.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 3. Importation des paramètres du Light Agent

A cette étape, vous pouvez transférer les paramètres du Light Agent for Linux enregistrés précédemment dans un fichier de configuration au format CFG.

Pour ce faire, cliquez sur le bouton **Sélectionner** et, dans la fenêtre **Sélection du fichier de configuration**, sélectionnez le fichier avec l'extension cfg.

Le chemin vers le fichier de configuration s'affiche dans le champ **Fichier de configuration**.

Dans les étapes suivantes de l'Assistant de création d'une stratégie, vous pouvez modifier les valeurs des paramètres transférés depuis le fichier de configuration.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 4. Configuration des paramètres de protection

A cette étape, vous pouvez configurer les paramètres de protection des machines virtuelles. La fenêtre de l'Assistant affiche la liste des modules de la protection du Light Agent for Linux.

Vous pouvez exécuter les opérations suivantes :

- Configurer les paramètres généraux de la protection et y activer la technologie de réparation de l'infection active.
- Activer ou désactiver le composant Antivirus Fichiers.
- Configurer les paramètres du composant Antivirus Fichiers.
- Interdire ou autoriser la modification des paramètres dans les stratégies du niveau joint de la hiérarchie.

Si le "verrou" est coché dans la stratégie, il est impossible de redéfinir la valeur (pour plus de détails, cf. documentation de Kaspersky Security Center).

► *Pour configurer les paramètres généraux de la protection, procédez comme suit :*

1. Dans la liste des modules, choisissez la section **Paramètres généraux**.

La fenêtre **Configuration : Administration de la protection** s'ouvre.

2. Cochez la case **Lancer Kaspersky Security for Virtualization 4.0 Light Agent à l'insertion de la machine virtuelle** si vous voulez que l'application Kaspersky Security soit lancée après le chargement du système d'exploitation et protège la machine virtuelle pendant toute la session.

3. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration** et, dans la fenêtre ouverte **Zone de confiance**, configurez la liste des exclusions de la protection de Kaspersky Security (cf. section "Configuration des exclusions de la protection via Kaspersky Security Center" à la p. [156](#)). Le Kaspersky Security Center transpose ces paramètres sur les machines virtuelles protégées dès l'application de la stratégie.

En dehors des exclusions ajoutées lors de cette étape, les objets du système de fichiers /dev, /sys et /proc sont exclus de la protection.

Si une application est installée sur votre machine virtuelle et qu'elle exécute la collecte et l'envoi d'informations à traiter, Kaspersky Security peut classer cette application comme malveillante. Pour éviter cela, vous pouvez exclure l'application de la protection en l'ajoutant aux exclusions.

4. Cliquez sur le bouton **OK** dans la fenêtre **Configuration : administration de la protection** pour enregistrer les modifications et fermer la fenêtre.

► *Pour activer ou désactiver le composant Antivirus Fichiers, procédez comme suit :*

- Si vous souhaitez activer le composant Antivirus Fichiers, cochez la case à gauche, en regard du nom du composant figurant dans la liste.
- Si vous souhaitez désactiver le composant Antivirus Fichiers, décochez la case à gauche, en regard du nom du composant figurant dans la liste.

► *Pour configurer les paramètres du composant Antivirus Fichiers, procédez comme suit :*

1. Sélectionnez le composant Antivirus Fichiers dans la liste et cliquez sur le bouton **Modifier** situé au-dessus de la liste des composants de protection.

La fenêtre **Configuration : Antivirus Fichiers** s'ouvre.

2. Configurez les paramètres du travail de l'Antivirus Fichiers (cf. section "Configuration de l'Antivirus Fichiers via Kaspersky Security Center" sur p. [142](#)). Suite à l'adoption de la stratégie, Kaspersky Security utilise ces paramètres sur les machines virtuelles protégées.
3. Cliquez sur le bouton **OK** dans la fenêtre **Configuration : Antivirus Fichiers** pour enregistrer les modifications et fermer la fenêtre de configuration.

► *Pour interdire ou autoriser la succession des paramètres de la stratégie, exécutez une des actions suivantes :*

- Si vous voulez interdire la modification des paramètres de la stratégie, exécutez une des actions suivantes :
 - Sélectionnez le composant de protection dans la liste et cliquez sur le bouton **Fermer** situé au-dessus de la liste des composants de protection.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de la protection.
- Si vous voulez autoriser la modification des paramètres de la stratégie, exécutez une des actions suivantes :
 - Sélectionnez le module de la protection dans la liste et cliquez sur le bouton **Ouvrir** situé au-dessus de la liste des modules de protection.
 - Cliquez sur le "verrou" à gauche, en regard du nom du module de la protection.

Passez à l'étape suivante de l'Assistant de création d'une stratégie.

Etape 5. Configuration des paramètres de détection des SVM

Lors de cette étape, sélectionner la méthode utilisée par les Light Agents pour la détection des SVM du réseau et la réception des informations les concernant.

- **Utiliser la multidiffusion (Multicast).**

Si cette option est sélectionnée, le module Light Agent obtient les informations sur les SVM à l'aide de la multidiffusion (Multicast).

Cette option est sélectionnée par défaut.

- **Utiliser le Serveur d'intégration.**

Si cette option est sélectionnée, le module Light Agent se connecte au Serveur d'intégration pour obtenir la liste des SVM auxquelles il peut se connecter et les informations les concernant. Si vous souhaitez utiliser le Serveur d'intégration, il faut indiquer les paramètres de connexion des Light Agents au Serveur d'intégration.

- **Utiliser une liste d'adresses de SVM établie manuellement.**

Si cette option est sélectionnée, vous pouvez indiquer la liste des SVM auxquelles peuvent se connecter les Light Agents administrés par cette stratégie. Les Light Agents ne se connecteront qu'aux SVM indiquées dans la liste.

Si vous avez sélectionné la variante **Utiliser le Serveur d'intégration**, indiquez les paramètres de connexion des Light Agents au Serveur d'intégration.

► *Pour indiquer les paramètres de connexion des Light Agents au Serveur d'intégration, procédez comme suit :*

1. Par défaut, le champ **Adresse** contient le nom de domaine de l'ordinateur hébergeant la Console d'administration Kaspersky Security Center. Si cet ordinateur n'appartient pas au domaine, si le Serveur d'intégration est installé sur un autre ordinateur, et qu'une adresse incorrecte figure dans le champ, indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) du Serveur d'intégration.
2. Si le port de connexion au Serveur d'intégration est différent de celui utilisé par défaut (7271), indiquez le numéro de port dans le champ **Port**.

3. Si l'ordinateur sur lequel la Console d'administration Kaspersky Security Center n'appartient pas au domaine ou si votre compte n'appartient pas au groupe KAdmins ou au groupe d'administrateurs locaux, la fenêtre **Connexion au Serveur d'intégration** s'ouvre. Indiquez le mot de l'administrateur du Serveur d'intégration (mot de passe du compte admin). Une fois la connexion au Serveur d'intégration établie à l'aide des privilèges d'administrateur, le mot de passe du compte est automatiquement transmis à la stratégie pour la connexion des Light Agents au Serveur d'intégration.

Lors du passage à l'étape suivante de l'assistant, la possibilité de connexion au Serveur d'intégration est analysée. Si cette analyse échoue ou s'il est impossible d'établir une connexion au Serveur d'intégration, vous ne pouvez pas passer à l'étape suivante. Analysez les paramètres de connexion saisis. Les informations sur les erreurs de la connexion au Serveur d'intégration sont consignées dans le journal de fonctionnement du Serveur d'intégration (cf. section "A propos des journaux du Serveur d'intégration" à la page [225](#)).

Si vous avez sélectionné l'option **Utiliser une liste d'adresses de SVM établie manuellement**, composez la liste des SVM.

► *Pour composer une liste des SVM, procédez comme suit :*

1. Cliquez sur le bouton **Ajouter** situé au-dessus de la liste d'adresses de SVM.

Ouvre la fenêtre **Adresses des SVM**.

2. Saisissez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM à laquelle pourront se connecter les Light Agents gérés par la stratégie. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine complet auquel correspondent plusieurs adresses IP peut entraîner des erreurs de fonctionnement de l'application.

3. Cliquez sur le bouton **OK** dans la fenêtre **Adresses des SVM**.

L'application analyse les adresses et noms de domaines complets saisis des SVM.

Si certain(e)s adresses ou noms ne sont pas reconnu(e)s, un message apparaît dans une fenêtre séparée avec le nombre d'adresses ou de noms non reconnu(e)s. Les adresses reconnues et les noms de domaines complets apparaissent dans la liste des adresses des SVM.

4. Si vous souhaitez supprimer de la liste l'adresse IP ou le nom de domaine complet de la SVM, sélectionnez cet élément dans la liste et cliquez sur le bouton **Supprimer** situé au-dessus de la liste.

Passez à l'étape suivante de l'Assistant.

Etape 6. Création de la stratégie de groupe pour l'application

Quittez l'Assistant de création de stratégie.

La fenêtre de l'Assistant de création de stratégie se ferme. La stratégie créée apparaît dans la liste des stratégies sous l'onglet **Stratégies**.

Lors de la connexion suivante de la machine virtuelle au Serveur d'administration, le Kaspersky Security Center transmet les informations à l'application Kaspersky Security et la stratégie se propage aux machines virtuelles protégées. Kaspersky Security commence à protéger les machines virtuelles sur l'hyperviseur, conformément aux paramètres de la stratégie.

Si l'Agent d'administration n'est pas lancé sur la machine virtuelle protégée, la stratégie créée ne s'applique pas à cette dernière.

Si vous avez sélectionné l'option **Stratégie inactive**, la stratégie créée ne s'applique pas aux machines virtuelles protégées.

Si les informations sur la licence ne sont pas transmises à la machine virtuelle protégée, le module Light Agent fonctionne en mode restreint (cf. section "Activation de l'application" à la page [46](#)).

Modification des paramètres des stratégies

Cette section explique comment modifier les paramètres d'une stratégie du Serveur de protection et de stratégies pour le Light Agent.

Dans cette section

Modification des paramètres d'une stratégie pour le Serveur de protection.....	117
Modification des paramètres d'une stratégie pour un Light Agent for Windows	118
Modification des paramètres d'une stratégie pour un Light Agent for Linux.....	119

Création de la stratégie pour le Serveur de protection

► *Pour modifier les paramètres de la stratégie pour le Serveur de protection, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les SVM pour lesquelles vous souhaitez modifier les paramètres de la stratégie.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Serveur de protection et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. Modifiez les paramètres de la stratégie.

Si vous voulez configurer des paramètres supplémentaires de fonctionnement des SVM, vous devez activer l'affichage des paramètres supplémentaires de la stratégie pour le Serveur de protection dans le registre du système d'exploitation (cf. section "Affichage des paramètres des stratégies" à la p. [86](#)).

Les sections **Général** et **Notification sur les événements** de la fenêtre **Propriété : <le Nom de la stratégie>** sont standard pour l'application Kaspersky Security Center. Pour plus d'informations sur les sections standards, consultez la documentation de Kaspersky Security Center.

6. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés:<Nom de la stratégie>**.

Modification des paramètres d'une stratégie pour le Light Agent for Windows

► *Pour modifier les paramètres de la stratégie pour le Light Agent for Windows, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les machines virtuelles protégées pour lesquelles vous souhaitez modifier les paramètres de la stratégie.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Windows et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. Modifiez les paramètres de la stratégie.

Les paramètres de contrôle s'affichent dans les propriétés de la stratégie pour le Light Agent for Windows si l'affichage des paramètres de contrôle est activé dans les paramètres de l'interface de la Console d'administration de Kaspersky Security Center (cf. section "Configuration de l'affichage des paramètres de contrôle dans la Console d'administration", à la page [93](#)).

Dans la section **Paramètres généraux**, vous pouvez activer ou désactiver la technologie de réparation de l'infection active pour les machines virtuelles protégées dotées du système d'exploitation pour serveur (cf. section "Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur" à la page [190](#)).

Pour en savoir plus sur la configuration des paramètres de protection et des paramètres de fonctionnement du Light Agent for Windows, consultez le *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Les sections **Général** et **Notification sur les événements** de la fenêtre **Propriété : <le Nom de la stratégie>** sont standard pour l'application Kaspersky Security Center. Pour plus d'informations sur les sections standards, consultez la documentation de Kaspersky Security Center.

6. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés:<Nom de la stratégie>**.

Modification des paramètres d'une stratégie pour un Light Agent for Linux

► Pour modifier les paramètres de la stratégie pour le Light Agent for Linux, 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, choisissez le dossier portant le nom du groupe d'administration qui comprend les machines virtuelles protégées pour lesquelles vous souhaitez modifier les paramètres de la stratégie.

3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Modifiez les paramètres de la stratégie (cf. section "Configuration des paramètres du Light Agent for Linux dans Kaspersky Security Center" à la p. [142](#)).

Les sections **Général** et **Notification sur les événements** de la fenêtre **Propriété : <le Nom de la stratégie>** sont standard pour l'application Kaspersky Security Center. Pour plus d'informations sur les sections standards, consultez la documentation de Kaspersky Security Center.

6. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés:<Nom de la stratégie>**.

Administration des tâches

Cette section fournit des informations sur l'administration des tâches pour l'application Kaspersky Security for Virtualization 4.0 Light Agent.

Dans cette section

Présentation des tâches pour Kaspersky Security.....	121
Création des tâches exécutées sur les machines virtuelles protégées	125
Lancement et arrêt des tâches dans Kaspersky Security Center.....	128

Présentation des tâches pour Kaspersky Security

Vous pouvez administrer le fonctionnement de l'application Kaspersky Security for Virtualization 4.0 Light Agent à l'aide des tâches comme localement sur les machines virtuelles protégées (via l'interface du Light Agent for Windows ou à l'aide de la ligne de commande dans le cas du Light Agent for Linux), et d'une manière centralisée dans Kaspersky Security Center.

Vous pouvez réaliser les opérations suivantes sur les tâches :

- les lancer et de les arrêter ;
- les créer et les supprimer ;
- modifier leurs paramètres ;
- consulter le bilan de leur exécution.

Administration des tâches via Kaspersky Security Center

Le Kaspersky Security Center vous permet de configurer les tâches suivantes :

- Tâches exécutées sur les SVM :
 - **Activation de l'application.** Kaspersky Security Center ajoute sur les SVM une clé d'activation de l'application ou pour la prorogation de la licence (cf. *Manuel d'implantation de Kaspersky Security for Virtualization 4.0 Light Agent*).
 - **Mise à jour des bases de données** (cf. section "**Création d'une tâche de mise à jour sur le Serveur de protection**" à la p. [135](#)). Le module Serveur de protection charge et installe automatiquement les paquets de mises à jour des bases et des modules de l'application sur les SVM.
 - **Restauration de la mise à jour** (cf. section "**Création de la tâche de remise à l'état antérieur à la dernière mise à jour sur le Serveur de protection**" à la p. [140](#)). Le module Serveur de protection annule la dernière mise à jour des bases de données et des modules de l'application sur les SVM.
- Tâches exécutées sur les machines virtuelles protégées avec le composant installé Light Agent for Windows :
 - **Inventaire** (cf. section "**Création des tâches exécutées sur les machines virtuelles protégées**" à la p. [125](#)). Lors de l'exécution de cette tâche, Kaspersky Security collecte des informations à propos de l'ensemble des fichiers exécutables d'applications sauvegardés sur les machines virtuelles protégées.
 - **Recherche de virus** (cf. section "**Création des tâches exécutées sur les machines virtuelles protégées**" à la p. [125](#)). Pendant l'exécution de la tâche, Kaspersky Security analyse les zones de la machine virtuelle protégée indiquées dans les paramètres de la tâche pour y rechercher des virus et d'autres applications malveillantes.
 - **Modification des modules de l'application.** Pendant l'exécution de la tâche, Kaspersky Security installe ou supprime les composants de Light Agent sur les machines virtuelles protégées (cf. *Manuel d'implantation de Kaspersky Security for Virtualization 4.0 Light Agent*).
- La tâche **Recherche de virus** exécutée sur les machines virtuelles protégées avec le composant Light Agent for Linux installé (cf. section "**Création des tâches exécutées sur les machines virtuelles protégées**" à la p. [125](#)). Pendant l'exécution de la tâche, Kaspersky Security analyse les zones de la machine virtuelle protégée indiquées dans les paramètres de la tâche pour y rechercher des virus et d'autres applications malveillantes.

Pour exploiter Kaspersky Security for Virtualization 4.0 Light Agent, vous pouvez créer les types de tâches suivants :

- La *tâche de groupe* est celle exécutée sur les ordinateurs clients du groupe d'administration choisi. Conformément à l'application Kaspersky Security, les tâches de groupe sont exécutées sur les SVM ou sur les machines virtuelles protégées faisant partie du groupe d'administration.
- La *tâche pour une sélection d'ordinateurs* est une tâche pour une ou plusieurs SVM ou machines virtuelles protégées faisant partie ou non de groupes d'administration.

Le Serveur d'administration de Kaspersky Security Center reçoit de Kaspersky Security les informations relatives à tous les événements survenus pendant l'exécution des tâches. Vous pouvez consulter les informations sur le déroulement et les résultats de l'exécution des tâches dans la Console d'administration de Kaspersky Security Center d'une des manières suivantes :

- Dans la fenêtre **Résultats de l'exécution de la tâche**. La fenêtre s'ouvre selon le lien **Consulter les résultats** situé à droite de la liste des tâches qui s'affiche dans le dossier **Tâches** de l'arborescence de la console Kaspersky Security Center ou sur l'onglet **Tâches** dans l'espace de travail du groupe d'administration.
- Dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les SVM. La liste des événements s'affiche sur l'onglet **Événements** dans l'espace de travail du nœud **Serveur d'administration**.

Pour plus d'informations sur l'utilisation des tâches, consultez la documentation de Kaspersky Security Center.

Administration des tâches via l'interface locale de Light Agent for Windows

Outre les tâches que vous pouvez configurer par le biais de Kaspersky Security Center, l'administration de l'application Kaspersky Security for Virtualization 4.0 Light Agent s'appuie sur des tâches configurables via l'interface locale de Light Agent for Windows sur la machine virtuelle protégée.

Pour administrer l'application via l'interface locale de Light Agent for Windows, vous pouvez utiliser les tâches suivantes :

- *Analyse complète.* Kaspersky Security effectue une analyse minutieuse du système d'exploitation de la machine virtuelle protégée, y compris la mémoire système, les objets chargés au démarrage, la sauvegarde du système d'exploitation et tous les disques durs et amovibles.
- *Analyse personnalisée.* Kaspersky Security analyse les objets de la machine virtuelle protégée sélectionnés par l'utilisateur.
- *Analyse des zones critiques.* Kaspersky Security analyse par défaut les objets chargés au démarrage du système d'exploitation de la machine virtuelle protégée (secteurs d'amorçage et objets de démarrage), la mémoire système et les objets potentiellement infectés par les outils de dissimulation d'activité.
- *Mise à jour.* Kaspersky Security télécharge le paquet de mise à jour des bases et des modules de l'application depuis la SVM et l'installe sur la machine virtuelle protégée.

Pour en savoir plus sur ces tâches, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Gestion des tâches du Light Agent for Linux à l'aide de la ligne de commande

Pour l'administration du Light Agent for Linux à l'aide de la ligne de commande, les tâches des types suivants sont accessibles :

- *Analyse complète* (cf. section "*Lancement de la tâche d'analyse*" à la p. [203](#)).
Kaspersky Security effectue une analyse minutieuse du système d'exploitation de la machine virtuelle protégée, y compris la mémoire système, les objets chargés au démarrage, la sauvegarde du système d'exploitation et tous les disques durs et amovibles.
- *Analyse personnalisée* (cf. section "*Lancement de la tâche d'analyse*" à la p. [203](#)).
Kaspersky Security analyse les objets de la machine virtuelle protégée sélectionnés par l'utilisateur.
- *Mise à jour* (cf. section "*Lancement et l'arrêt de la tâche de mise à jour*" à la p. [207](#)).
Kaspersky Security télécharge depuis la SVM le paquet de mises à jour des bases antivirus et installe sur la machine virtuelle protégée.

Création des tâches exécutées sur les machines virtuelles protégées

► Pour créer une tâche d'analyse antivirus pour le *Light Agent for Linux*, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Choisissez le dossier **Ordinateurs administrés** de l'arborescence de la console si vous voulez créer une tâche pour les machines virtuelles faisant partie de tous les groupes d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche pour l'ensemble des machines virtuelles du groupe d'administration : dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche pour une sélection une ou plusieurs machines virtuelles protégées : ouvrez le dossier **Tâches** de l'arborescence de la console.
3. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de création de la tâche.
4. Sélectionnez le type de tâche. Pour ce faire, dans la liste **Kaspersky Security for Virtualization 4.0 Light Agent for Linux**, sélectionnez **Recherche de virus**.
Passez à l'étape suivante de l'Assistant.
5. Dans la fenêtre **Zone d'analyse**, créez la liste des objets analysés par Kaspersky Security.
Passez à l'étape suivante de l'Assistant de création d'une tâche.
6. Dans la fenêtre **Action de Kaspersky Security for Virtualization 4.0 Light Agent**, choisissez l'action exécutée par l'application Kaspersky Security si, à la suite de l'analyse, des fichiers infectés sont détectés. Passez à l'étape suivante de l'Assistant.
7. Suivez encore les instructions de l'Assistant de création d'une tâche.

► *Pour créer une tâche d'analyse contre les virus pour le Light Agent for Windows, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Choisissez le dossier **Ordinateurs administrés** de l'arborescence de la console si vous voulez créer une tâche pour les machines virtuelles faisant partie de tous les groupes d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche pour l'ensemble des machines virtuelles du groupe d'administration : dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche pour une sélection une ou plusieurs machines virtuelles protégées : ouvrez le dossier **Tâches** de l'arborescence de la console.
3. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de création de la tâche.
4. Sélectionnez le type de tâche. Pour ce faire, dans la liste **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**, sélectionnez **Recherche de virus**. Passez à l'étape suivante de l'Assistant.
5. Dans la fenêtre **Zone d'analyse**, créez la liste des objets analysés par Kaspersky Security (pour plus de détails, cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*). Passez à l'étape suivante de l'Assistant de création d'une tâche.
6. Dans la fenêtre **Action de Kaspersky Security for Virtualization 4.0 Light Agent**, choisissez l'action exécutée par l'application Kaspersky Security si, à la suite de l'analyse, des fichiers infectés sont détectés (pour plus de détails, cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
7. Cochez la case **Exécuter la réparation de l'infection active immédiatement** si vous voulez que l'application exécute la procédure de la réparation de l'infection active (cf. section "Présentation de la technologie de réparation de l'infection avancée" à la p. [188](#)) immédiatement après sa détection lors de l'exécution de la tâche de groupe d'analyse contre les virus et redémarre la machine virtuelle après la réparation de l'infection active sans demander la confirmation de l'utilisateur.

8. Cochez la case **Suspendre l'analyse programmée lorsque l'écran de veille est inactif et si la machine virtuelle protégée n'est pas verrouillée** si vous souhaitez que l'application suspende le lancement de la tâche d'analyse lorsque les ressources de la machine virtuelle sont occupées. Passez à l'étape suivante de l'Assistant.

9. Suivez encore les instructions de l'Assistant de création d'une tâche.

► *Pour créer une tâche d'inventaire pour le Light Agent for Windows, procédez comme suit :*

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

2. Exécutez une des actions suivantes :

- Choisissez le dossier **Ordinateurs administrés** de l'arborescence de la console si vous voulez créer une tâche pour les machines virtuelles faisant partie de tous les groupes d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
- Si vous souhaitez créer une tâche pour l'ensemble des machines virtuelles du groupe d'administration : dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
- Si vous souhaitez créer une tâche pour une sélection une ou plusieurs machines virtuelles protégées : ouvrez le dossier **Tâches** de l'arborescence de la console.

3. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de création de la tâche.

4. Sélectionnez le type de tâche. Pour ce faire, dans la liste **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**, sélectionnez **Inventaire**.
Passez à l'étape suivante de l'Assistant.

5. Dans la fenêtre **Zone d'inventaire**, créez la liste des objets pour l'inventaire.
Passez à l'étape suivante de l'Assistant de création d'une tâche.

6. Cochez la case **Suspendre l'analyse programmée lorsque l'écran de veille est inactif et si la machine virtuelle protégée n'est pas verrouillée** si vous souhaitez que l'application suspende l'analyse lorsque les ressources de la machine virtuelle sont occupées.

7. Suivez encore les instructions de l'Assistant de création d'une tâche.

L'utilisation des tâches est décrite de manière plus détaillée dans la documentation de Kaspersky Security Center.

Lancement et arrêt des tâches dans Kaspersky Security Center

► Pour lancer ou arrêter la tâche, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Si vous souhaitez lancer ou arrêter une tâche créée pour les machines virtuelles de tous les groupes d'administration, sélectionnez le dossier **Ordinateurs administrés** de l'arborescence de la console. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration si vous souhaitez lancer ou arrêter une tâche pour les machines virtuelles de ce dossier. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez lancer ou arrêter une tâche créée pour une ou plusieurs machines virtuelles, sélectionnez le dossier **Tâches** de l'arborescence de la console.
3. Dans la liste des tâches, sélectionnez la tâche que vous souhaitez lancer ou arrêter.
4. Si vous souhaitez lancer une tâche, exécutez l'une des actions suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Démarrer**.
 - Cliquez sur le bouton **Démarrer** situé à droite de la liste des tâches.
5. Si vous souhaitez arrêter une tâche, exécutez l'une des actions suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Arrêter**.
 - Cliquez sur le bouton **Arrêter** situé à droite de la liste des tâches.

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 sur la configuration de la mise à jour.

Dans cette section

A propos de la mise à jour des bases et des modules de l'application	129
Activation et désactivation de la mise à jour des modules de Light Agent for Windows	132
Récupération automatique des paquets de mises à jour des bases et des modules de l'application	134
Tâches de mise à jour créées sur le Serveur de protection	135
Mise à jour des bases de données et des modules du Light Agent for Windows sur le modèle de machine virtuelle.....	137
Remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application.	138
Création de la tâche de remise à l'état antérieur à la dernière mise à jour sur le Serveur de protection	140

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

La mise à jour des bases de données et des modules de l'application Kaspersky Security préserve l'actualité de la protection des machines virtuelles. Chaque jour, de nouveaux virus, et autres applications présentant une menace apparaissent dans le monde. Les bases de Kaspersky Security contiennent les données relatives aux menaces et aux méthodes de neutralisation.

Si les bases de l'application n'ont pas été mises à jour depuis longtemps, un message s'affiche dans la fenêtre **Événement** des propriétés de la SVM.

Pour que Kaspersky Security puisse détecter à temps les nouvelles menaces, il faut actualiser les bases et les modules de l'application à intervalle régulier.

Les mises à jour des bases et des modules de l'application peuvent modifier certains paramètres de Kaspersky Security, par exemple les paramètres de l'analyse heuristique qui augmentent l'efficacité de la protection et de l'analyse.

La mise à jour des bases et des modules de l'application requiert une licence valide d'utilisation.

La *source des mises à jour* est une ressource qui contient les mises à jour des bases et des modules des applications de Kaspersky Lab. Le stockage du Serveur d'administration de Kaspersky Security Center tient lieu de source de mise à jour pour Kaspersky Security for Virtualization 4.0 Light Agent.

La mise à jour des bases de données et des modules de l'application Kaspersky Security s'exécute ainsi :

1. Le composant Serveur de protection télécharge un paquet de mises à jour à partir du stockage du Serveur d'administration dans le dossier de la SVM.

Le paquet de mise à jour contient par défaut les mises à jour des bases de l'application indispensables au fonctionnement du Serveur de protection et du Light Agent. Vous pouvez aussi renouveler les modules du composant Light Agent for Windows. Pour cela, vous devez inclure dans le paquet de mises à jour celles des modules du Light Agent for Windows (cf. section "Activation et désactivation de la mise à jour des modules de Light Agent for Windows" à la p. [132](#)).

Le chargement du paquet de mises à jour s'effectue via *les tâches de mise à jour* sur le Serveur de protection. La tâche est lancée à partir de Kaspersky Security Center et s'exécute sur la SVM (cf. section "Récupération automatique des paquets de mises à jour des bases et des modules de l'application" à la page [134](#)).

Pour bien télécharger le paquet de mises à jour depuis le stockage du Serveur d'administration, la SVM doit pouvoir accéder au Serveur d'administration du Kaspersky Security Center.

Si les bases et les modules de l'application n'ont plus été mises à jour depuis longtemps, la taille du paquet de mise à jour peut être importante. Le téléchargement d'un tel paquet peut créer du trafic de réseau supplémentaire (jusqu'à quelques dizaines de mégaoctets).

2. Les mises à jour des bases et des modules de l'application sont installées sur la SVM à partir du dossier :

- Une fois le paquet de mises à jour téléchargé, le composant Serveur de protection installe automatiquement les mises à jour des bases nécessaires à son fonctionnement (bases antivirus) sur la SVM.
- Le composant Light Agent vérifie si un paquet de mises à jour est disponible dans le dossier de la SVM à laquelle il est connecté. En présence d'un paquet de mises à jour, Light Agent installe sur la machine virtuelle protégée les mises à jour des bases indispensables au fonctionnement du module Light Agent for Windows ainsi que les mises à jour des modules du Light Agent (si les mises à jour des modules sont reprises dans le paquet de mises à jour). La mise à jour des bases de données et des modules du Light Agent s'effectue via les *tâches de mise à jour* sur la machine virtuelle protégée. Le lancement de la tâche de mise à jour sur la machine virtuelle protégée est programmé. Par défaut, le mode de lancement des tâches est défini sur "automatique". La tâche se lance toutes les deux heures.

Sur la machine virtuelle protégée avec le composant installé Light Agent for Windows, l'utilisateur peut configurer dans l'interface locale la programmation du lancement de la tâche de mise à jour ou lancer manuellement cette tâche si ces fonctions ne sont pas interdites par la stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*).

Sur la machine virtuelle protégée avec le composant installé Light Agent for Linux, l'utilisateur peut lancer manuellement la tâche de la mise à jour à partir de la ligne de commande (cf. section "Lancement et arrêt de la tâche de la mise à jour" à la p. [207](#)).

Pour garantir une protection à jour des machines virtuelles temporaires, il est recommandé de renouveler régulièrement les bases et les modules du Light Agent sur le modèle de machine virtuelle à partir duquel les machines virtuelles protégées temporaires sont créées (cf. section "Mise à jour des bases et des modules du Light Agent for Windows sur le modèle de machine virtuelle" à la p. [137](#)).

Si lors de l'installation du Light Agent sur le modèle de machine virtuelle, vous avez coché la case **Installation sur un modèle pour pools temporaires VDI**, les mises à jour demandant le redémarrage de la machine virtuelle protégée ne s'installent pas sur les machines virtuelles temporaires. Lors de la récupération de mise à jour qui requiert le redémarrage de la machine virtuelle protégée, le Light Agent installée sur la machine virtuelle temporaire, envoie à Kaspersky Security Center un message sur la nécessité de mise à jour du modèle des machines virtuelles protégées.

La mise à jour des bases et des modules du Light Agent for Windows sur la machine virtuelle protégée doit être exécutée conformément aux conditions suivantes :

- Éléments définis dans les propriétés de la carte réseau de la machine virtuelle protégée :
 - protocole Internet (TCP/IP) (Internet Protocol (TCP/IP)) ;
 - client pour les réseaux Microsoft (Client for Microsoft Networks).
- Service "Poste de travail" (Workstation) lancé sur la machine virtuelle protégée.
- Le trafic réseau via le port 445 selon le protocole TCP est autorisé sur la SVM.

Activation et désactivation de la mise à jour des modules de Light Agent for Windows

L'activation ou la désactivation des mises à jour des modules de Light Agent for Windows s'opère dans les paramètres de la stratégie pour le Serveur de protection. Si la mise à jour des modules de Light Agent for Windows est activée, Kaspersky Security inclut les mises à jour des modules de Light Agent for Windows dans le paquet de mises à jour.

► *Pour activer ou désactiver la mise à jour des modules de Light Agent for Windows, 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 au nom du groupe d'administration dont vous souhaitez modifier la stratégie.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Serveur de protection et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la fenêtre des propriétés de la stratégie pour le Serveur de protection, choisissez dans la liste à gauche la section **Paramètres de la mise à jour**.

Les paramètres de la mise à jour s'affichent dans la partie droite de la fenêtre.
6. Exécutez une des actions suivantes :
 - Cochez la case **Mettre à jour les modules de l'application** si vous souhaitez activer la mise à jour des modules de Light Agent for Windows.
 - Décochez la case **Mettre à jour les modules de l'application** si vous souhaitez désactiver la mise à jour des modules de Light Agent for Windows.
7. Cliquez sur le bouton **OK**.

Récupération automatique des paquets de mises à jour des bases et des modules de l'application

Le Kaspersky Security Center permet de télécharger automatiquement les paquets de mise à jour des bases et des modules de l'application sur les SVM. Pour ce faire, les tâches suivantes sont prévues :

- **Tâche de téléchargement des mises à jour dans le stockage.** La tâche permet de télécharger le paquet de mises à jour depuis la source de mises à jour pour le Kaspersky Security Center, dans le stockage du Serveur d'administration. La tâche de téléchargement des mises à jour dans le stockage est créée automatiquement lors de l'utilisation de l'Assistant de configuration initiale du Kaspersky Security Center. La tâche de téléchargement des mises à jour dans le stockage peut être créée en un exemplaire unique. Par conséquent, vous pouvez créer une tâche de téléchargement des mises à jour dans le stockage uniquement si elle a été supprimée de la liste des tâches du Serveur d'administration. Pour plus d'informations, consultez la documentation de Kaspersky Security Center.
 - **Tâche de mise à jour du Serveur de protection.** Cette tâche permet de charger les paquets de mises à jour des bases et des modules de l'application sur les SVM figurant dans le groupe d'administration sélectionné, conformément à la planification.
- *Pour configurer la récupération automatique des paquets de mises à jour des bases et des modules de l'application, procédez comme suit :*
1. Assurez-vous que la tâche de téléchargement des mises à jour dans le stockage a été créée dans le Kaspersky Security Center. Si cette tâche n'existe pas, créez-la (cf. Documentation de Kaspersky Security Center).
 2. Créez une tâche de mise à jour sur le Serveur de protection pour les SVM sur lesquelles vous souhaitez mettre à jour les bases et les modules de l'application (cf. section "Création d'une tâche de mise à jour sur le Serveur de protection" à la page [135](#)).

Création d'une tâche de mise à jour sur le Serveur de protection

► Pour créer une tâche de mise à jour sur le Serveur de protection, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Si vous souhaitez créer une tâche de mise à jour pour les SVM de tous les groupes d'administration, sélectionnez le dossier **Ordinateurs administrés** de l'arborescence de la console. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche de mise à jour pour l'ensemble des SVM du groupe d'administration : dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Choisissez le dossier **Tâches** de l'arborescence de la console si vous voulez créer une tâche pour une ou plusieurs SVM.
3. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de création de la tâche.
4. Pendant la première étape de l'assistant, choisissez pour l'application **Kaspersky Security for Virtualization 4.0 Light Agent – Serveur de protection** le type de tâche **Actualisation des bases**.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

5. Si vous avez lancé l'assistant de la création d'une tâche du dossier **Tâches**, indiquez la méthode de choix des SVM pour lesquelles vous créez la tâche. En fonction du mode choisi pour la sélection des SVM, procédez comme suit dans la fenêtre qui s'ouvre :
 - Dans la liste des machines virtuelles détectées, indiquez les SVM sur lesquelles vous créez la tâche. Pour ce faire, cochez la case à gauche, en regard du nom de la SVM.
 - Cliquez sur le bouton **Ajouter** ou **Ajouter un intervalle IP** et définissez manuellement les adresses des SVM.

- Cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier au format TXT contenant la liste des adresses des SVM.
- Appuyez sur le bouton **Sélectionner**, et dans la fenêtre qui s'ouvre, indiquez le nom de l'ensemble contenant les SVM pour lesquelles vous créez la tâche.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

6. Dans le champ **Lancement programmé**, choisissez **Lors du chargement des mises à jour dans le stockage**. Configurez les paramètres restants de planification de la tâche. Pour plus d'informations sur les paramètres de planification du lancement d'une tâche, consultez la documentation de Kaspersky Security Center.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

7. Dans le champ **Nom**, saisissez le nom de la tâche de la mise à jour des bases antivirus.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

8. Si vous souhaitez que la tâche se lance directement après la fin de l'Assistant de création d'une tâche, cochez la case **Démarrer la tâche après la fin de l'Assistant**. Quittez l'Assistant de création d'une tâche. La tâche créée apparaît dans la liste des tâches.

La tâche sera lancée chaque fois au chargement du paquet de mises à jour dans le stockage du Serveur d'administration. Vous pouvez également lancer la tâche ou l'arrêter manuellement à tout moment (cf. section "Lancement et arrêt des tâches dans Kaspersky Security Center" à la page [128](#)).

Mise à jour des bases de données et des modules du Light Agent for Windows sur le modèle de machine virtuelle

Modèle de machines virtuelles sur un hyperviseur Microsoft Windows Server (Hyper-V) ou Citrix XenServer

► Pour mettre à jour les bases et les modules de Light Agent sur le modèle de machines virtuelles, procédez comme suit :

1. Sur l'hyperviseur, activez la machine virtuelle protégée tenant lieu de modèle de machine virtuelle protégée temporaire.
2. Par défaut, le Light Agent installé sur la machine virtuelle protégée se lance automatiquement lors du démarrage du système d'exploitation. Si vous avez désactivé le lancement automatique de l'application, lancez le Light Agent sur la machine virtuelle protégée.
3. Mettez à jour les bases et les modules de Light Agent ou attendez le lancement de la tâche de mise à jour des bases et des modules de Light Agent selon la planification (pour les détails, consultez le *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
4. Recréez des machines virtuelles protégées temporaires à partir du modèle mis à jour. Pour plus d'informations, consultez la documentation concernant l'infrastructure virtuelle.

Pour automatiser la procédure de mise à jour des bases de données et des modules du Light Agent sur les modèles de machine virtuelle, vous pouvez utiliser des outils tels que Microsoft Virtual Machine Servicing Tool (pour les modèles sur hyperviseur Microsoft Windows (Hyper-V)), Citrix PowerShell SDK et Citrix Provisioning Services (pour les modèles créés sur la base de Citrix XenDesktop).

Modèle pour les machines virtuelles protégées sur la base de VMware Horizon View

► Pour mettre à jour les bases et les modules de *Light Agent* sur le modèle de machines virtuelles (*linked clones*), procédez comme suit :

1. Activez la machine virtuelle protégée sur la base de la capture qui a servi à créer le pool de machines virtuelles protégées temporaires.
2. Par défaut, le *Light Agent* installé sur la machine virtuelle protégée se lance automatiquement lors du démarrage du système d'exploitation. Si vous avez désactivé le lancement automatique de l'application, lancez le *Light Agent* sur la machine virtuelle protégée et assurez-vous que le *Light Agent* s'est connecté à la SVM.
3. Mettez à jour les bases et les modules de *Light Agent* ou attendez le lancement de la tâche de mise à jour des bases et des modules de *Light Agent* selon la planification (pour les détails, consultez le *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
4. Après la mise à jour des bases, arrêtez la machine virtuelle protégée et réalisez une nouvelle capture de cette machine.
5. Recréez le pool de machines virtuelles protégées temporaires sur la base de la capture réalisée. Pour en savoir plus, reportez-vous à la section *Update Linked-Clone Desktops* du document *VMware Horizon View Administration*.

Pour automatiser la procédure de mise à jour des bases de données et des modules du *Light Agent* sur les machines virtuelles administrées par VMware Horizon View, vous pouvez utiliser le langage de script VMware vSphere™ PowerCLI™. Il permet de créer le script de la mise à jour automatique de la capture de la machine virtuelle protégée et de reconstituer le pool de machines virtuelles protégées temporaires grâce aux constructions *Get-Snapshot* et *Update-AutomaticLinkedClonePool*.

Remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application

Après la première mise à jour des bases et des modules de l'application, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour des bases et des modules de l'application.

Chaque fois que la mise à jour est lancée sur la SVM, Kaspersky Security crée une copie de sauvegarde des bases et des modules de l'application utilisés, puis l'application procède à la mise à jour. Cela permet de revenir, le cas échéant, aux bases et aux modules antérieurs de l'application. La possibilité de revenir à l'état antérieur à la mise à jour est utile, par exemple, si la nouvelle version des bases de l'application contient une signature incorrecte qui fait que Kaspersky Security bloque une application sans danger.

La remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application Kaspersky Security s'exécute selon les étapes suivantes :

1. Remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application sur les SVM Vous pouvez réaliser une remise à l'état antérieur à la dernière mise à jour des bases de données et des modules de l'application sur une ou plusieurs SVM. La remise à l'état antérieur à la dernière mise à jour sur la SVM s'exécute via la *tâche de restauration d'une mise à jour* sur le Serveur de protection. La tâche est lancée à partir de Kaspersky Security Center et s'exécute sur la SVM.
2. Remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application sur les machines virtuelles protégées. Suite à la remise à l'état antérieur à la dernière mise à jour des bases et des modules de l'application sur la SVM, la remise à l'état antérieur à la dernière mise à jour des bases s'exécute automatiquement sur l'ensemble des machines virtuelles protégées connectées à cette SVM. Si la machine virtuelle protégée est déconnectée ou arrêtée, la remise à l'état antérieur à la dernière mise à jour des bases s'y exécutera dès la connexion suivante, conformément à la programmation du lancement des *tâches de mise à jour* sur le Light Agent. Par défaut, le mode de lancement des tâches est défini sur "automatique". La tâche se lance toutes les deux heures.

Sur la machine virtuelle protégée avec le composant installé Light Agent for Windows, l'utilisateur peut configurer dans l'interface locale la programmation du lancement de la tâche de mise à jour ou lancer manuellement cette tâche si ces fonctions ne sont pas interdites par la stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*).

Sur la machine virtuelle protégée avec le composant installé Light Agent for Linux l'utilisateur peut lancer manuellement la tâche de mise à jour à partir de la ligne de commande (cf. section "Lancement de la tâche de mise à jour avec des paramètres supplémentaires" à la p. [208](#)).

► *Pour revenir à l'état antérieur à la dernière mise à jour des bases de données et des modules de l'application sur les SVM, procédez comme suit :*

1. Créez une tâche de restauration d'une mise à jour sur le Serveur de protection pour les SVM sur lesquelles vous souhaitez annuler la mise à jour des bases de données et des modules de l'application (cf. section "Création de la tâche de restauration d'une mise à jour sur mise à jour sur le Serveur de protection" à la page [140](#)).
2. Lancez la tâche de remise à l'état antérieur à la dernière mise à jour sur le Serveur de protection (cf. section "Lancement et arrêt des tâches dans Kaspersky Security Center" à la page [128](#)).

Création de la tâche de restauration d'une mise à jour sur le Serveur de protection

► *Pour créer une tâche de restauration d'une mise à jour sur le Serveur de protection, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
 - Si vous souhaitez créer une tâche de restauration d'une mise à jour pour les SVM faisant partie de tous les groupes d'administration, sélectionnez le dossier **Ordinateurs administrés** de l'arborescence de la console. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Si vous souhaitez créer une tâche de restauration d'une mise à jour pour l'ensemble des SVM du groupe d'administration : dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le dossier au nom du groupe d'administration. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
 - Ouvrez le dossier **Tâches** de l'arborescence de la console, si vous voulez créer une tâche de restauration d'une mise à jour pour une ou plusieurs SVM.
3. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de création de la tâche.

4. Lors de la première étape de l'assistant choisissez pour l'application **Kaspersky Security for Virtualization 4.0 Light Agent Serveur de protection** comme type de tâche **Restauration de la mise à jour**. Passez à l'étape suivante de l'Assistant de création d'une tâche.
5. Si vous avez lancé l'assistant de la création d'une tâche du dossier **Tâches**, indiquez la méthode de choix des SVM pour lesquelles vous créez la tâche. En fonction du mode choisi pour la sélection des SVM, procédez comme suit dans la fenêtre qui s'ouvre :
 - Dans la liste des machines virtuelles détectées, indiquez les SVM sur lesquelles vous créez la tâche. Pour ce faire, cochez la case à gauche, en regard du nom de la SVM.
 - Cliquez sur le bouton **Ajouter** ou **Ajouter un intervalle IP** et définissez manuellement les adresses des SVM.
 - Cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier au format TXT contenant la liste des adresses des SVM.
 - Appuyez sur le bouton **Sélectionner**, et dans la fenêtre qui s'ouvre, indiquez le nom de l'ensemble contenant les SVM pour lesquelles vous créez la tâche.

Passez à l'étape suivante de l'Assistant de création d'une tâche.

6. Dans le champ **Lancement programmé**, choisissez **Manuel**. Configurez les paramètres restants de planification de la tâche Pour plus d'informations sur les paramètres de planification du lancement d'une tâche, consultez la documentation de Kaspersky Security Center. Passez à l'étape suivante de l'Assistant de création d'une tâche.
7. Saisissez le nom de la tâche de remise à l'état antérieur à la dernière mise à jour dans le champ **Nom**. Passez à l'étape suivante de l'Assistant de création d'une tâche.
8. Si vous souhaitez que la tâche se lance directement après la fin de l'Assistant de création d'une tâche, cochez la case **Démarrer la tâche après la fin de l'Assistant**. Quittez l'Assistant de création d'une tâche. La tâche créée apparaît dans la liste des tâches.

Configuration des paramètres du Light Agent for Linux via Kaspersky Security Center

Cette section contient des informations sur la configuration des paramètres généraux de protection et sur l'analyse du Light Agent for Linux via Kaspersky Security Center.

Dans cette section

Configuration de l'Antivirus Fichiers via Kaspersky Security Center	142
Configuration des exclusions de la protection via Kaspersky Security Center	156
Configuration des paramètres de la tâche de recherche des virus pour Light Agent for Linux.	163

Configuration de l'Antivirus Fichiers via Kaspersky Security Center

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de la machine virtuelle protégée. L'Antivirus Fichiers est lancé par défaut au démarrage de Kaspersky Security. Il se trouve en permanence dans la mémoire vive de la machine virtuelle et analyse tous les fichiers ouverts, enregistrés et exécutés sur la machine virtuelle protégée à la recherche de virus et d'autres programmes malveillants.

L'Antivirus Fichiers utilise les méthodes de l'analyse sur la base de signatures et de l'analyse heuristique, ainsi que la technologie iChecker. Si l'analyse du fichier ne révèle aucun virus ou autre programme malveillant, Kaspersky Security octroie l'accès à ce fichier.

Si, suite à l'analyse, l'Antivirus Fichiers détecte une menace dans un fichier, Kaspersky Security attribue au fichier un statut désignant le type d'objet détecté (par exemple, *virus*, *cheval de Troie*). Ensuite, l'application exécute sur le fichier l'action spécifiée dans les paramètres de l'Antivirus Fichiers.

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Fichiers :

- Modifier le niveau de sécurité des fichiers.

Vous pouvez sélectionner un des niveaux de sécurité prédéfinis pour les fichiers ou personnaliser les paramètres du niveau de sécurité des fichiers. Après avoir modifié les paramètres du niveau de sécurité des fichiers, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité des fichiers.

- Modifier l'action que l'Antivirus Fichiers exécute en cas de détection d'un fichier infecté.
- Composer la zone de protection de l'Antivirus Fichiers.

Vous pouvez élargir ou rétrécir la zone de protection après avoir ajouté ou supprimé des objets analysés par l'Antivirus Fichiers.

- Configurer l'utilisation de l'analyse heuristique.

L'Antivirus Fichiers utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, l'Antivirus Fichiers compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, l'Antivirus Fichiers analyse l'activité des objets dans le système d'exploitation. L'Analyse heuristique permet de détecter de nouveaux objets malveillants dont les enregistrements n'ont pas encore été ajoutés aux bases de l'application.

- Configurer l'analyse des fichiers composés.
- Modifier le mode d'analyse des fichiers.
- Configurer l'utilisation de la technologie d'analyse iChecker.

Vous pouvez activer l'utilisation de la technologie iChecker qui permet d'augmenter la vitesse d'analyse en échange de l'exclusion de l'analyse de certains fichiers selon un algorithme spécial. Ce dernier prend en considération la date de publication des bases de Kaspersky Security, la date de l'analyse précédente du fichier, ainsi que la modification des paramètres d'analyse.

Dans cette section

Activation et désactivation de l'Antivirus Fichiers.....	144
Modification du niveau de protection des fichiers	145
Modification de l'action de l'Antivirus Fichiers sur les fichiers infectés	146
Formation de la zone de protection de l'Antivirus Fichiers	148
Analyse des fichiers composés avec l'Antivirus Fichiers	150
Configuration de l'utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Fichiers	152
Modification du mode d'analyse des fichiers	153
Configuration de l'utilisation de la technologie iChecker lors du fonctionnement de l'Antivirus Fichiers	155

Activation et désactivation de l'Antivirus Fichiers

Par défaut, l'Antivirus Fichiers est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Fichiers le cas échéant.

► *Pour activer ou désactiver l'Antivirus Fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.

- Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Exécutez une des actions suivantes :
 - Cochez la case **Antivirus Fichiers** si vous souhaitez activer l'Antivirus Fichiers.
 - Décochez la case **Antivirus Fichiers** si vous souhaitez le désactiver.
7. Cliquez sur le bouton **Appliquer**.

Modification du niveau de sécurité des fichiers

Pour protéger le système de fichiers de la machine virtuelle protégée, l'Antivirus Fichiers utilise différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de sécurité des fichiers*. Trois niveaux de sécurité des fichiers sont prévus : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité des fichiers **Recommandé** sont considérés comme optimaux et ils sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité des fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.

- Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :
- Pour définir un des niveaux prédéfinis de protection des fichiers (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
 - Pour personnaliser le niveau de sécurité des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Fichiers** qui s'ouvre.

Une fois que vous avez personnalisé le niveau de sécurité des fichiers, le nom du niveau de sécurité des fichiers dans le groupe **Niveau de sécurité** devient **Autre**.

- Pour sélectionner le niveau de sécurité des fichiers **Recommandé**, cliquez sur le bouton **Par défaut**.
7. Cliquez sur le bouton **Appliquer**.

Modification de l'action de l'Antivirus Fichiers sur les fichiers infectés

► *Pour modifier l'action que l'Antivirus Fichiers va exécuter sur les fichiers infectés, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.

4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
- En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.

5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :

- **Sélectionner l'action automatiquement.**

Cette option est sélectionnée par défaut. Suite à la détection d'une menace, l'application exécute l'action **Réparer. Supprimer si la désinfection est impossible**.

- **Exécuter l'action : Réparer. Supprimer si la désinfection est impossible.**
- **Exécuter l'action : Réparer.**
- **Exécuter l'action : Supprimer.**
- **Exécuter l'action : Bloquer.**

Lors de la suppression ou de la réparation, des copies des fichiers sont conservées dans la sauvegarde.

7. Cliquez sur le bouton **Appliquer**.

Formation de la zone de protection de l'Antivirus Fichiers

Le terme de *zone de protection* désigne les objets que le composant Antivirus Fichiers analyse pendant son exécution. Par défaut, l'Antivirus Fichiers analyse uniquement les fichiers potentiellement infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques réseau de la machine virtuelle protégée.

► *Pour former la zone de protection de l'Antivirus Fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Antivirus Fichiers** s'ouvre.

7. Dans la fenêtre **Anti-Virus Fichiers**, sélectionnez l'onglet **Général**.

8. Dans le groupe **Types de fichiers**, sélectionnez le type de fichiers que vous souhaitez analyser avec l'Anti-Virus Fichiers :

- Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
- Sélectionnez **Fichiers analysés selon le format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
- Sélectionnez **Fichiers analysés selon l'extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

9. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :

- Si vous souhaitez ajouter un nouvel objet à la liste des objets analysés, cliquez sur le bouton **Ajouter**.

La fenêtre **Sélection de l'objet** s'ouvre.

- Pour modifier le chemin de l'objet, sélectionnez-le dans la liste des objets et cliquez sur le bouton **Modifier**.

La fenêtre **Sélection de l'objet** s'ouvre.

- Pour supprimer un objet de la zone d'analyse, sélectionnez-le dans la liste des objets et cliquez sur **Supprimer**.

La fenêtre de confirmation de suppression s'ouvre.

10. Exécutez une des actions suivantes dans la fenêtre **Sélection de l'objet** :

- Pour ajouter un nouvel objet, dans la fenêtre **Sélection de l'objet**, indiquez le chemin d'accès à cet objet dans le champ **Objet** et cliquez sur le bouton **Ajouter**.

L'objet ajouté dans la fenêtre **Sélection de l'objet** s'affiche dans la liste **Zone de protection** dans la fenêtre **Antivirus Fichiers**.

Cliquez sur le bouton **OK**.

- Si vous souhaitez modifier le chemin vers un objet de la liste des objets analysés, indiquez un autre chemin dans le champ **Objet** et cliquez sur le bouton **OK**.
- Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

11. Le cas échéant, répétez les points 9 et 10 pour ajouter des objets, modifier leur chemin ou les supprimer de la liste des objets de la zone de protection.
12. Si vous souhaitez exclure un objet de la zone de protection, décochez la case en regard de l'objet dans la liste **Zone de protection**. Dans ce cas, l'objet reste dans la liste des objets analysés mais sera exclu de l'analyse par l'Antivirus Fichiers.
13. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.
14. Cliquez sur le bouton **Appliquer**.

Analyse des fichiers composés avec l'Antivirus Fichiers

L'insertion de virus et d'autres applications malveillantes dans des fichiers composés tels que des archives ou les bases de données est une pratique de dissimulation très répandue. Pour détecter les virus dissimulés et les autres applications malveillantes, vous devez décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter le cercle des fichiers composés analysés pour accélérer l'analyse.

► *Pour configurer l'analyse des fichiers composés, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.

5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Antivirus Fichiers** s'ouvre.

7. Dans la fenêtre **Antivirus Fichiers**, sous l'onglet **Performance** du groupe **Analyse des fichiers composés**, indiquez les fichiers composés que vous voulez analyser : les fichiers compactés, les archives, les paquets d'installation, les bases de messagerie ou les fichiers aux formats de messagerie en cochant les cases correspondantes.

8. Cliquez sur le bouton **Avancé**.

La fenêtre **Fichiers composés** s'ouvre.

9. Dans le groupe **Limitées en temps**, exécutez une des actions suivantes :

- Si vous ne voulez pas que l'Antivirus Fichiers ignore les fichiers à l'expiration du temps spécifié, décochez la case **Ignorer les fichiers si l'analyse dure plus de**.
- Si vous voulez que l'Antivirus Fichiers ignore les fichiers à l'expiration du temps spécifié, cochez la case **Ignorer les fichiers si l'analyse dure plus de** et dans le champ **Durée maximale de l'analyse** indiquez la valeur requise.

10. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

- Si vous ne souhaitez que l'Antivirus Fichiers décompresse les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.
- Si vous souhaitez que l'Antivirus Fichiers décompresse les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

L'Antivirus Fichiers analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

11. Cliquez sur le bouton **OK** dans la fenêtre **Fichiers composés**.

12. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.

13. Cliquez sur le bouton **Appliquer**.

Configuration de l'utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Fichiers

► *Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus Fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Antivirus Fichiers** s'ouvre.

7. Dans la fenêtre **Antivirus Fichiers**, sur l'onglet **Performance**, dans le groupe **Méthodes d'analyse**, exécutez une des actions suivantes :

- Si vous voulez que l'Antivirus Fichiers utilise l'analyse heuristique, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.
- Si vous voulez que l'Antivirus Fichiers n'utilise pas l'analyse heuristique, décochez la case **Analyse heuristique**.

8. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.

9. Cliquez sur le bouton **Appliquer**.

Modification du mode d'analyse des fichiers

Le *mode d'analyse* désigne la condition dans laquelle l'Antivirus Fichiers va commencer l'analyse des fichiers. Par défaut, Kaspersky Security utilise le mode intelligent d'analyse des fichiers. Dans ce mode d'analyse des fichiers, l'Antivirus Fichiers prend une décision sur la base de l'analyse des opérations exécutées par vous, par l'application en votre nom ou au nom d'un autre utilisateur (sur la base des données avec lesquelles l'entrée dans le système d'exploitation a eu lieu) ou par le système d'exploitation sur les fichiers. Par exemple, dans le cas d'un fichier Microsoft Office Word, Kaspersky Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.

► *Afin de modifier le mode d'analyse des fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.

3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Antivirus Fichiers** s'ouvre.

7. Dans la fenêtre **Antivirus Fichiers** sur l'onglet **Avancé** dans le groupe **Mode d'analyse**, choisissez le mode nécessaire :
 - **Intelligent**.
 - **A l'ouverture et en cas de modification**.
 - **A l'accès**.
8. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.
9. Cliquez sur le bouton **Appliquer**.

Configuration de l'utilisation de la technologie iChecker lors du fonctionnement de l'Antivirus Fichiers

► Pour configurer l'utilisation de la technologie iChecker dans le fonctionnement de l'Antivirus Fichiers, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la stratégie, puis sélectionnez l'option **Propriétés**.
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
5. Dans la fenêtre des propriétés de la stratégie du Light Agent for Linux, choisissez à gauche dans la liste **Antivirus Fichiers**.

Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Antivirus Fichiers** s'ouvre.

7. Dans la fenêtre **Antivirus Fichiers** sur l'onglet **Avancé** dans le groupe **Technologie d'analyse**, exécutez une des actions suivantes :

- Si vous souhaitez utiliser cette technologie pendant le fonctionnement de l'Antivirus Fichiers, cochez la case **Technologie iChecker**.

- Si vous ne souhaitez pas utiliser cette technologie pendant le fonctionnement de l'Antivirus Fichiers, décochez la case **Technologie iChecker**.
8. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.
 9. Cliquez sur le bouton **Appliquer**.

Configuration des exclusions de la protection via Kaspersky Security Center

Vous pouvez créer la liste des objets que l'application Kaspersky Security ne contrôle pas lors de son exécution, c'est-à-dire un ensemble des exclusions de la protection et l'analyse.

L'*exclusion* est un ensemble de conditions décrivant l'objet. Si l'objet satisfait ces conditions, Kaspersky Security ne l'analyse pas à la recherche de virus ou d'autres applications malveillantes.

Vous pouvez exclure de la protection et de l'analyse les objets des types suivants :

- les fichiers d'un format déterminé ;
- fichiers selon un masque ;
- dossiers ;
- objets selon la classification de l'Encyclopédie des virus de Kaspersky Lab.

En dehors des exclusions ajoutées par vos soins, les objets du système de fichiers /dev, /sys et /proc sont exclus de la protection et de l'analyse.

Certaines applications légitimes peuvent être exploitées par des individus malintentionnés pour nuire à votre machine virtuelle protégée ou à vos données. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes mais pourraient être utilisées en guise d'auxiliaires pour une application malveillante. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, ou les numéroteurs automatiques. Ce genre d'application n'est pas considéré comme un virus. Vous pouvez obtenir

des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'Encyclopédie de virus de Kaspersky Lab en cliquant sur le lien

<http://securelist.com/threats/riskware/>.

Kaspersky Security peut bloquer de telles applications. Pour éviter le blocage, vous pouvez configurer les exclusions de la protection de Kaspersky Security pour les applications utilisées par vous-même. Pour ce faire, il convient d'ajouter aux exclusions le nom de l'objet ou le masque du nom de l'objet conformément au classement de l'Encyclopédie des virus de Kaspersky Lab.

Si une application est installée sur votre machine virtuelle et qu'elle exécute la collecte et l'envoi d'informations à traiter, Kaspersky Security peut classer cette application comme malveillante. Pour éviter cela, vous pouvez exclure l'application de la protection en l'ajoutant aux exclusions.

Vous pouvez exécuter les opérations suivantes pour configurer les exclusions :

- Créer une nouvelle exclusion (cf. section "Création d'une exclusion" à la p. [158](#)).

Vous pouvez créer une exclusion. Lors de son application, Kaspersky Security n'analyse pas les fichiers, les dossiers et/ou les objets indiqués.

- Suspendre l'utilisation d'une exclusion (cf. section "Lancement et suspension de l'utilisation d'une exclusion" à la p. [160](#)).

Vous pouvez suspendre temporairement l'utilisation d'une exclusion sans devoir la supprimer de la liste des exclusions.

- Modifier les paramètres d'une exclusion existante (cf. section "Modification d'une exclusion" à la p. [161](#)).

Après avoir créé une exclusion, vous pouvez toujours revenir à la configuration des paramètres de cette exclusion et modifier les paramètres requis.

- Supprimer une exclusion (voir la section "Suppression d'une exclusion" à la p. [162](#)).

Vous pouvez supprimer une exclusion si vous ne souhaitez pas que l'application Kaspersky Security l'applique pendant la durée d'analyse de la machine virtuelle protégée.

Dans cette section

Création d'une exclusion	158
Lancement et suspension de l'utilisation d'une exclusion	160
Modification d'une exclusion.....	161
Suppression d'une exclusion.....	162

Création d'une exclusion

► *Pour créer une exclusion, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Linux.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Linux, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Linux s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Linux, sélectionnez la section **Paramètres généraux**.

Les paramètres généraux de la protection s'afficheront dans la partie droite de la fenêtre.

7. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

8. Cliquez sur le bouton **Ajouter**.

La fenêtre **Exclusion** s'ouvre.

9. Si vous souhaitez exclure un fichier ou un dossier de la protection, procédez comme suit :

- a. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.
- b. Le lien **sélectionnez un fichier ou un dossier** situé dans le groupe **Description de l'exclusion** permet d'ouvrir la fenêtre **Nom du fichier ou du dossier**. Dans cette fenêtre, vous pouvez saisir le nom du fichier ou du dossier ou le masque du nom du fichier.
- c. Cliquez sur le bouton **OK** dans la fenêtre **Nom du fichier ou du dossier**.

Le lien vers le fichier ou le dossier ajouté apparaîtra dans le groupe **Description de l'exclusion** de la fenêtre **Exclusions**.

10. Si vous souhaitez exclure de la protection les objets portant un nom défini sur la base de la classification des applications malveillantes et autres applications répertoriées dans l'Encyclopédie des virus de Kaspersky Lab, procédez comme suit :

- a. Dans le groupe **Propriétés**, cochez la case **Nom de l'objet**.
- b. Le lien **saisissez le nom de l'objet** situé dans le groupe **Description de l'exclusion** permet d'ouvrir la fenêtre **Nom de l'objet**. Cette fenêtre permet de saisir le nom ou le masque de l'objet conformément au classement de l'Encyclopédie de virus de Kaspersky Lab sur le site Internet www.securelist.fr.
- c. Cliquez sur le bouton **OK** dans la fenêtre **Nom de l'objet**.

11. Si nécessaire, saisissez un bref commentaire sur l'exclusion à créer dans le champ **Commentaires**.

12. Cliquez sur le bouton **OK** dans la fenêtre **Exclusion**.

L'exclusion ajoutée apparaît dans la liste des exclusions de l'onglet **Exclusions** dans la fenêtre **Zone de confiance**. Le groupe **Description de l'exclusion** affiche les paramètres de cette exclusion.

13. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

14. Cliquez sur le bouton **Appliquer**.

Lancement et suspension de l'utilisation d'une exclusion

► Pour lancer ou arrêter une exclusion, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Linux.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Linux, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Linux s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Linux, sélectionnez la section **Paramètres généraux**.

Les paramètres généraux de la protection s'afficheront dans la partie droite de la fenêtre.

7. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

8. Sélectionnez l'exclusion requise dans la liste des exclusions.
9. Exécutez une des actions suivantes :
 - Cochez la case en regard du nom de l'exclusion si vous voulez utiliser cette exclusion.
 - Décochez la case en regard du nom de l'exclusion si vous souhaitez suspendre temporairement l'application de cette exclusion.
10. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.
11. Cliquez sur le bouton **Appliquer**.

Modification d'une exclusion

► Pour modifier une exclusion, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Linux.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Linux, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Linux s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Linux, sélectionnez la section **Paramètres généraux**.

Les paramètres généraux de la protection s'afficheront dans la partie droite de la fenêtre.

7. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

8. Sélectionnez l'exclusion requise dans la liste des exclusions.
9. Cliquez sur le bouton **Modifier**.

La fenêtre **Exclusion** s'ouvre.

10. Modifiez les paramètres de l'exclusion.
11. Cliquez sur le bouton **OK** dans la fenêtre **Exclusion**.

Le groupe **Description de l'exclusion** affiche les modifications des paramètres de cette exclusion.

12. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.
13. Cliquez sur le bouton **Appliquer**.

Suppression d'une exclusion

► Pour supprimer une exclusion, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Linux.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Linux, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Linux s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Linux, sélectionnez la section **Paramètres généraux**.

Les paramètres généraux de la protection s'afficheront dans la partie droite de la fenêtre.

7. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

8. Sélectionnez l'exclusion requise dans la liste des exclusions.

9. Cliquez sur le bouton **Supprimer**.

L'exclusion supprimée disparaît de la liste des exclusions de l'onglet **Exclusions** dans la fenêtre **Zone de confiance**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

11. Cliquez sur le bouton **Appliquer**.

Configuration des paramètres de la tâche de recherche des virus pour Light Agent for Linux

Pour configurer les paramètres des tâches de recherche de virus, vous pouvez exécuter les opérations suivantes :

- Modifier le niveau de sécurité.

Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

- Modifier l'action que Kaspersky Security exécute en cas de détection d'un fichier infecté.
- Créer la zone d'analyse.

Vous pouvez élargir ou rétrécir la zone d'analyse après avoir ajouté ou supprimé des objets analysés par l'application.

- Configurer l'analyse des fichiers composés.
- Configurer l'utilisation de l'analyse heuristique.

Kaspersky Security utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Security analyse l'activité des objets dans le système d'exploitation. L'Analyse heuristique permet de détecter de nouveaux objets malveillants dont les enregistrements n'ont pas encore été ajoutés aux bases de l'application.

- Configurer l'utilisation de la technologie d'analyse iChecker.

Vous pouvez activer l'utilisation de la technologie iChecker, qui permet d'augmenter la vitesse d'analyse en échange de l'exclusion de certains fichiers de l'analyse. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de l'application, de la dernière date d'analyse du fichier et des modifications des paramètres d'analyse.

Dans cette section

Modification du niveau de protection	164
Modification de l'action sur les fichiers infectés	165
Constitution de la zone d'analyse	167
Analyse des fichiers composés	169
Configuration de l'utilisation de l'analyse heuristique	171
Configuration de l'utilisation de la technologie iChecker	172

Modification du niveau de sécurité

Kaspersky Security utilise différents ensembles de paramètres pour exécuter les tâches d'analyse. Ces ensembles de paramètres sont appelés *niveaux de sécurité*. Trois niveaux sont prévus pour la protection : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont considérés comme optimaux et sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :
 - En double-cliquant.

- Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
 - Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.
5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :
- Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
 - Pour personnaliser le niveau de sécurité, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre avec le nom de la tâche d'analyse qui s'ouvre.

Une fois que vous avez personnalisé le niveau de sécurité, le nom du niveau de sécurité dans le groupe **Niveau de sécurité** devient **Autre**.

- Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.
7. Cliquez sur le bouton **Appliquer**.

Modification de l'action sur les fichiers infectés

► Pour modifier l'action à exécuter sur les fichiers infectés, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.

4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :

- En double-cliquant.
- Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
- Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.

5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :

- **Sélectionner l'action automatiquement.**

Cette option est sélectionnée par défaut. Suite à la détection d'une menace, l'application exécute l'action **Réparer. Supprimer si la désinfection est impossible**.

- **Exécuter l'action : Réparer. Supprimer si la désinfection est impossible.**
- **Exécuter l'action : Réparer.**
- **Exécuter l'action : Supprimer.**
- **Exécuter l'action : Informer.**

Lors de la suppression ou de la réparation, des copies des fichiers sont conservées dans la sauvegarde.

7. Cliquez sur le bouton **Appliquer**.

Constitution de la zone d'analyse

Le terme de *zone d'analyse* désigne l'emplacement des fichiers que l'application analyse pendant l'exécution de la tâche d'analyse.

► *Pour former la zone d'analyse, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
 - Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.
5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Zone d'analyse**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone d'analyse** va s'ouvrir.

7. Dans le groupe **Zone d'analyse**, exécutez une des actions suivantes :
 - Si vous souhaitez ajouter un nouvel objet à la liste des objets analysés, cliquez sur le bouton **Ajouter**.

La fenêtre **Sélection de l'objet** s'ouvre.

- Pour modifier le chemin de l'objet, sélectionnez-le dans la liste des objets et cliquez sur le bouton **Modifier**.

La fenêtre **Sélection de l'objet** s'ouvre.

- Pour supprimer un objet de la zone d'analyse, sélectionnez l'objet dans la liste des objets et cliquez sur **Supprimer**.

La fenêtre de confirmation de suppression s'ouvre.

Vous ne pouvez pas supprimer ou modifier les objets ajoutés à la zone d'analyse par défaut.

8. Exécutez une des actions suivantes dans la fenêtre **Sélection de l'objet** :

- Pour ajouter un nouvel objet, dans la fenêtre **Sélection de l'objet**, indiquez le chemin d'accès à cet objet dans le champ **Objet** et cliquez sur le bouton **Ajouter**.

L'objet ajouté dans la fenêtre **Sélection de l'objet** s'affiche dans la liste des objets de la fenêtre **Zone d'analyse**.

Cliquez sur le bouton **OK**.

- Si vous souhaitez modifier le chemin vers un objet, indiquez un autre chemin dans le champ **Objet** et cliquez sur le bouton **OK**.
- Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

9. Le cas échéant, répétez les points 7 et 8 pour ajouter des objets, modifier leur chemin ou les supprimer de la zone d'analyse.

10. Si vous souhaitez exclure un objet de la zone d'analyse décochez la case à côté de cet objet dans la liste des objets de la fenêtre **Zone d'analyse**. Cet objet reste dans la liste des objets analysés mais n'est pas analysé pendant l'exécution de la tâche d'analyse.

11. Cliquez sur le bouton **OK** dans la fenêtre **Zone d'analyse**.

12. Cliquez sur le bouton **Appliquer**.

Analyse des fichiers composés

L'insertion de virus et d'autres applications malveillantes dans des fichiers composés tels que des archives ou les bases de données est une pratique de dissimulation très répandue.

Pour détecter les virus dissimulés et les autres applications malveillantes, vous devez décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse.

Vous pouvez limiter le cercle des fichiers composés analysés pour accélérer l'analyse.

► *Pour configurer l'analyse des fichiers composés, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
 - Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.
5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Recherche de virus** s'ouvre.

7. Dans la fenêtre **Recherche de virus**, sous l'onglet **Zone d'action**, dans le groupe **Analyse des fichiers composés**, indiquez les fichiers composés à analyser : archives, paquets d'installation ou objets OLE incorporés, fichiers au format de messagerie ou fichiers protégés par un mot de passe en cochant les cases correspondantes.

8. Cliquez sur le bouton **Avancé**.

La fenêtre **Fichiers composés** s'ouvre.

9. Dans le groupe **Limitées en temps**, exécutez une des actions suivantes :

- Si vous ne voulez pas que l'application ignore les fichiers à l'expiration du temps spécifié, décochez la case **Ignorer les fichiers si l'analyse dure plus de**.
- Si vous voulez que l'application ignore les fichiers à l'expiration du temps spécifié, cochez la case **Ignorer les fichiers si l'analyse dure plus de** et, dans le champ **Durée maximale de l'analyse**, indiquez la valeur requise.

10. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

- Si vous ne souhaitez pas que l'application décompresse les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.
- Si vous souhaitez que l'application décompresse les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

Kaspersky Security analyse les fichiers de grande taille extraits des archives quel que soit l'état de la case **Ne pas décompresser les fichiers composés de grande taille**.

11. Cliquez sur le bouton **OK** dans la fenêtre **Fichiers composés**.

12. Cliquez sur le bouton **OK** dans la fenêtre **Recherche de virus**.

13. Cliquez sur le bouton **Appliquer**.

Configuration de l'utilisation de l'analyse heuristique

► Pour configurer l'utilisation de l'analyse heuristique, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
 - Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.
5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.
6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Recherche de virus** s'ouvre.

7. Dans la fenêtre **Recherche de virus**, sur l'onglet **Avancé**, dans le bloc **Méthodes d'analyse**, exécutez une des actions suivantes :
 - Si vous souhaitez que l'application utilise l'analyse heuristique au cours de la tâche d'analyse, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.
 - Si vous souhaitez que l'application n'utilise pas l'analyse heuristique au cours de la tâche d'analyse, décochez la case **Analyse heuristique**.
8. Cliquez sur le bouton **OK** dans la fenêtre **Recherche de virus**.
9. Cliquez sur le bouton **Appliquer**.

Configuration de l'utilisation de la technologie iChecker

► *Pour configurer l'utilisation de la technologie iChecker, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des analyses, sélectionnez une tâche de recherche de virus pour le Light Agent for Linux et ouvrez la fenêtre **Propriétés : <Nom de la tâche>** de l'une des manières suivantes :
 - En double-cliquant.
 - Cliquez sur le bouton droit de la souris pour appeler le menu contextuel de la tâche et sélectionnez l'option **Propriétés**.
 - Le lien **Modifier les paramètres de la tâche** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la tâche.

5. Dans la fenêtre des propriétés de la tâche de recherche de virus pour le Light Agent for Linux, choisissez la section **Paramètres** à gauche dans la liste.

Les paramètres de la tâche s'afficheront dans la partie droite de la fenêtre.

6. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre **Recherche de virus** s'ouvre.

7. Dans la fenêtre **Recherche de virus**, sur l'onglet **Avancé** dans le groupe **Technologie d'analyse**, exécutez une des actions suivantes :

- Cochez la case **Technologie iChecker** si vous souhaitez utiliser cette technologie pendant l'analyse.
- Décochez la case **Technologie iChecker** si vous souhaitez utiliser cette technologie pendant l'analyse.

8. Cliquez sur le bouton **OK** dans la fenêtre **Recherche de virus**.

9. Cliquez sur le bouton **Appliquer**.

Configuration des paramètres du Light Agent for Windows via Kaspersky Security Center

La configuration des paramètres du Light Agent for Windows s'effectue en local sur la machine virtuelle protégée via l'interface du Light Agent for Windows (cf. *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

Cette section contient des informations sur la configuration de certains paramètres du composant Contrôle du lancement des applications et du composant Contrôle des périphériques du Light Agent for Windows via Kaspersky Security Center.

Dans cette section

Configuration du Contrôle du lancement des applications via le Kaspersky Security Center ...	174
Configuration du contrôle des périphériques via le Kaspersky Security Center	183

Configuration du Contrôle du lancement des applications via le Kaspersky Security Center

Le module Contrôle du lancement des applications du Light Agent surveille les tentatives de lancement d'applications sur la machine virtuelle et régit ce processus par le biais des *règles de contrôle du lancement des applications* (pour en savoir plus sur les règles de contrôle du lancement des applications, consultez le "*Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*").

Le composant Contrôle du lancement des applications est disponible si l'application Kaspersky Security est installée sur une machine virtuelle dotée d'un système d'exploitation Windows pour poste de travail. Ce module n'est pas disponible si l'application Kaspersky Security est installée sur une machine virtuelle sous système d'exploitation Windows pour serveur.

Le lancement des applications dont aucun paramètre ne respecte les règles de contrôle du lancement des applications est régi par la règle créée par défaut "Tout autoriser". La règle "Tout autoriser" permet à n'importe quel utilisateur de lancer n'importe quelle application. Toutes les tentatives de lancement des applications sur la machine virtuelle sont consignées dans des rapports.

Le module Contrôle du lancement des applications du Light Agent peut fonctionner selon deux modes :

- *Liste noire.* Mode par lequel le Contrôle du lancement des applications autorise tous les utilisateurs à lancer n'importe quelle application sur la machine virtuelle protégée, à l'exception de celles qui figurent dans les règles de refus du Contrôle du lancement des applications.

Il s'agit du mode de fonctionnement du Contrôle du lancement des applications par défaut. L'autorisation du lancement de toutes les applications repose sur la règle du Contrôle du lancement des applications "Tout autoriser" créée par défaut.

- *Liste blanche.* Mode par lequel le Contrôle du lancement des applications interdit à tous les utilisateurs de lancer quelque application que ce soit sur la machine virtuelle protégée, à l'exception de celles qui figurent dans les règles d'autorisation du Contrôle du lancement des applications. Si les règles d'autorisation du Contrôle du lancement des applications sont rédigées complètement, le Contrôle du lancement des applications interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

La configuration du Contrôle du lancement des applications pour le fonctionnement dans ces modes est possible à partir de l'interface locale de Light Agent ou dans le Kaspersky Security Center.

Toutefois, le Kaspersky Security Center offre des outils qui ne sont pas disponibles dans l'interface locale de Light Agent et qui permettent :

- La création de catégories d'applications (cf. section "Etape 2. Création de catégories d'applications" à la page [178](#)). Les règles de contrôle du lancement des applications de Kaspersky Security Center s'appuient sur les catégories d'applications que vous avez créées plutôt que sur des conditions d'inclusion et d'exclusion telles que celles de l'interface locale du Light Agent.
- La réception des informations concernant les applications installées sur les machines virtuelles protégées du réseau local de l'entreprise (cf. section "Etape 1. Collecte des informations concernant les applications installées sur les machines virtuelles protégées" à la page [177](#)).
- L'analyse du fonctionnement du Contrôle du lancement des applications après le changement de mode (cf. section "Etape 4. Test des règles d'autorisation du Contrôle du lancement des applications" à la page [180](#)).

Ainsi, il est conseillé d'effectuer la configuration du mode de fonctionnement du module Contrôle du lancement des applications via le Kaspersky Security Center.

Dans cette section

Passage du mode "Liste noire" au mode "Liste blanche"	176
Modification de l'état de la règle de contrôle du lancement des applications	182

Passage du mode "Liste noire" au mode "Liste blanche"

Cette section contient des informations sur le passage du mode "Liste noire" au mode "Liste blanche" lors du fonctionnement du Contrôle du lancement des applications. Elle comporte également des recommandations pour une utilisation optimale de ce module.

Dans cette section

Etape 1. Réception des informations concernant les applications installées sur les machines virtuelles protégées	177
Etape 2. Composition des catégories d'applications.....	178
Etape 3. Définition des règles d'autorisation du Contrôle du lancement des applications	179
Etape 4. Test des règles d'autorisation du Contrôle du lancement des applications	180
Etape 5. Passage au mode "Liste blanche"	181

Etape 1. Réception des informations concernant les applications installées sur les machines virtuelles protégées

A cette étape, il est important de connaître les applications utilisées sur les machines virtuelles protégées via le réseau local de l'entreprise. Ainsi, il vous est conseillé d'obtenir des informations sur :

- Les éditeurs, les versions et les localisations des applications installées sur les machines virtuelles protégées.
- La régularité des mises à jour des applications.
- Les stratégies d'utilisation des applications de l'entreprise. Il peut s'agir des stratégies relatives à la sécurité ou à l'administration.
- Les emplacements des stockages des paquets d'installation des applications.

Pour obtenir les informations sur les applications utilisées sur les machines virtuelles protégées du réseau local de l'entreprise, vous pouvez utiliser les données figurant dans les dossiers **Registre des applications** et **Fichiers exécutables**. Les dossiers **Registre des applications** et **Fichiers exécutables** des applications figurent dans le dossier **Administration des applications** de l'arborescence de la console de Kaspersky Security Center (pour plus d'informations, consultez la documentation de Kaspersky Security Center).

Le dossier **Registre des applications** comporte une liste des applications détectées sur les machines virtuelles protégées dotées d'un Agent d'administration.

Le dossier **Fichiers exécutables** comporte une liste des fichiers exécutables s'étant déjà lancés au moins une fois sur les machines virtuelles protégées ou ayant été détectés lors de l'exécution de la tâche d'inventaire de Kaspersky Security.

Dans la fenêtre des propriétés de l'application sélectionnée dans le dossier **Registre des applications** ou **Fichiers exécutables**, vous pouvez consulter les informations générales sur l'application, des informations concernant les fichiers exécutables de l'application et la liste des machines virtuelles protégées sur lesquelles cette application est installée.

Etape 2. Composition des catégories d'applications

Cette étape permet de créer les catégories d'applications à partir desquelles il est possible de définir des règles de Contrôle du lancement des applications.

Il est recommandé de créer une catégorie "Applications de travail" qui inclut un ensemble standard d'applications utilisées par l'entreprise. Si plusieurs groupes d'utilisateurs utilisent des ensembles distincts d'applications de travail, vous pouvez créer une catégorie séparée d'applications pour chaque groupe d'utilisateurs.

► *Pour créer une catégorie d'applications, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Ouvrez le dossier **Administration des applications** → **Catégories d'applications** de l'arborescence de la console.
3. Lancez l'Assistant de création d'une catégorie d'utilisateurs en cliquant sur le lien **Créer une tâche** dans l'espace de travail.
4. Suivez les instructions de l'Assistant de création d'une catégorie d'utilisateurs.

Etape 3. Définition des règles d'autorisation du Contrôle du lancement des applications

Cette étape permet de définir les règles de contrôle du lancement des applications qui autorisent les utilisateurs du réseau local de l'entreprise à lancer des applications sur les machines virtuelles protégées figurant dans les catégories créées à l'étape précédente.

► *Pour créer une règle d'autorisation du Contrôle du lancement des applications, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Windows.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Windows, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Windows s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Windows, sélectionnez la section **Contrôle du lancement des applications**.

Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

7. Cliquez sur le bouton **Ajouter**.

La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

8. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée à l'étape précédente et vouée à servir de base à la règle d'autorisation.
9. Composez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés à lancer les applications appartenant à la catégorie sélectionnée. Pour ce faire, dans le champ **Utilisateurs et/ou groupes autorisés**, saisissez les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**. La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

10. Ne remplissez pas la liste des utilisateurs n'étant pas autorisés à lancer les applications de cette catégorie.
11. Cochez la case **Programmes de mise à jour de confiance** si vous souhaitez que l'application Kaspersky Security considère les applications de la catégorie indiquée dans la règle comme des applications de mise à jour de confiance, et qu'elle les autorise à lancer d'autres applications n'étant pas couvertes par des règles de contrôle de leur lancement.
12. Cliquez sur le bouton **OK**.
13. Cliquez sur le bouton **Appliquer** dans la section **Contrôle du lancement des applications** de la fenêtre des propriétés de la stratégie pour le Light Agent for Windows.

Etape 4. Test des règles d'autorisation du Contrôle du lancement des applications

A cette étape, vous devez réaliser les opérations suivantes :

1. Modifier l'état du fonctionnement des règles d'autorisation créées pour le Contrôle du lancement des applications et le régler sur *Test* (cf. section "*Modification de l'état de la règle de contrôle du lancement des applications*" à la page [182](#)).
2. Analyser les tests des règles d'autorisation du Contrôle du lancement des applications.

Pour analyser les tests des règles de contrôle du lancement des applications, il est nécessaire d'étudier les événements concernant le fonctionnement du module Contrôle du lancement des applications du Light Agent transmis au Kaspersky Security Center. Si le lancement de toutes les applications que vous avez incluses dans les catégories est autorisé, cela signifie que les règles ont été correctement définies. Dans le cas contraire, il est conseillé de préciser les paramètres des catégories d'applications que vous avez créées et des règles de contrôle du lancement des applications.

- Pour consulter les événements concernant le fonctionnement du module Contrôle du lancement des applications du Light Agent dans le Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans la zone de travail du nœud **Serveur d'administration**, sélectionnez l'onglet **Événements** dans lequel vous choisirez la sélection d'événements requise : **Événements d'information** ou **Événements critiques** afin de consulter les événements relatifs aux exécutions autorisées et interdites d'applications.

La liste affiche tous les événements du niveau choisi d'importance et transmis à Kaspersky Security Center pendant la période indiquée dans les propriétés du Serveur d'administration.

3. Pour consulter les informations sur ces événements, ouvrez la fenêtre de propriétés de chacun d'entre eux de l'une des manières suivantes :
 - Double-cliquez sur l'événement.
 - Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'événement, puis sélectionnez l'option **Propriétés**.
 - Cliquez sur le lien **Ouvrir la fenêtre des propriétés de l'événement** à droite de la liste des événements.

Etape 5. Passage au mode "Liste blanche"

A cette étape, vous devez réaliser les opérations suivantes :

- Activer les règles de contrôle du lancement des applications que vous avez créées. Pour ce faire, l'état du fonctionnement de ces règles doit passer de *Test* à *Act*.
- Activer les règles "Programmes de mise à jour des applications de confiance" et "Système d'exploitation et ses modules" créées par défaut. Pour ce faire, l'état du fonctionnement de ces règles doit passer de *Dés.* à *Act*.
- Désactiver la règle "Tout autoriser" créée par défaut. Pour ce faire, l'état du fonctionnement de ces règles doit passer de *Act*. à *Dés.*

Pour en savoir plus sur l'état des règles de contrôle du lancement des applications, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Modification de l'état de la règle de contrôle du lancement des applications

► Pour modifier l'état de fonctionnement de la règle de contrôle du lancement des applications, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent for Windows.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent for Windows, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent for Windows s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent for Windows, sélectionnez la section **Contrôle du lancement des applications**.

Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

7. Sélectionnez la règle de contrôle du lancement des applications dont vous souhaitez modifier l'état.
8. Dans la colonne **Etat**, exécutez l'une des actions suivantes :
 - Pour activer l'utilisation de la règle, sélectionnez la valeur *Actif*.
 - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Inactif*.
 - Si vous souhaitez que la règle fonctionne en mode test, sélectionnez la valeur *Test*.
9. Cliquez sur le bouton **Appliquer**.

Configuration du contrôle des périphériques via le Kaspersky Security Center

Le contrôle des périphériques assure la sécurité des données confidentielles via la restriction d'accès des utilisateurs aux périphériques installés ou connectés à une machine virtuelle protégée, à l'aide des *règles de l'accès aux périphériques* et des *règles de l'accès aux bus de connexion* (pour des informations détaillées sur ces règles cf. *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

En outre, vous pouvez configurer la liste des périphériques de confiance. Les *Périphériques de confiance* sont les périphériques que les utilisateurs définis dans les paramètres du périphérique de confiance peuvent accéder librement à tout moment.

Le module Contrôle des périphériques est disponible si l'application Kaspersky Security est installée sur une machine virtuelle dotée d'un système d'exploitation Windows pour poste de travail. Ce module n'est pas disponible si l'application Kaspersky Security est installée sur une machine virtuelle sous système d'exploitation Windows pour serveur.

La configuration du composant le Contrôle des périphériques est possible dans l'interface locale du Light Agent, comme via le Kaspersky Security Center.

Toutefois, le Kaspersky Security Center offre en outre les outils suivants qui ne sont pas disponibles dans l'interface locale du Light Agent for Windows :

- Ajout de périphériques de confiance à la liste selon leur modèle ou leur identifiant (à la p. [184](#)).
- Ajout de périphériques de confiance à la liste selon le masque de leur identifiant (à la p. [186](#)).

Si le périphérique est ajouté à la liste des périphériques de confiance et une règle d'accès qui interdit ou limite l'accès est créée pour ce type de périphérique, lors de la prise de la décision sur l'accès au périphérique la présence du périphérique sur la liste des périphériques de confiance a une priorité plus élevée que la règle d'accès.

Dans cette section

Ajout de périphériques de confiance à la liste en fonction de leur modèle ou de leur identifiant	184
Ajout de périphériques de confiance à la liste selon le masque de leur identifiant	186

Ajout de périphériques de confiance à la liste en fonction de leur modèle ou de leur identifiant

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

L'ajout des périphériques de confiance à la liste selon leur modèle ou selon leur identifiant est possible seulement sur Kaspersky Security Center.

► *Pour ajouter des périphériques de confiance à la liste en fonction de leur modèle ou de leur identifiant, 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 souhaitez créer une liste de périphériques de confiance.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Sélectionnez la stratégie dont vous avez besoin dans la liste.
5. Exécutez une des actions suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
 - Placez-vous sur le lien **Modifier les paramètres de la stratégie** à droite de la liste de stratégies.

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

6. Choisissez la section **Contrôle des périphériques**.

7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

8. Cliquez sur le bouton **Ajouter**.

Le menu contextuel du bouton s'ouvre.

9. Dans le menu contextuel du bouton **Ajouter**, exécutez l'une des actions suivantes :

- Choisissez le point **Périphériques selon identifiant** si vous voulez ajouter à la liste les périphériques de confiance, dont les identifiants uniques sont connus.
- Choisissez le point **Périphériques selon modèle** si vous voulez ajouter à la liste les périphériques de confiance dont les identifiants VID (éditeur) et PID (produit) sont connus.

10. Dans la liste déroulante **Type de périphériques** qui s'ouvre, sélectionnez le type de périphériques à ajouter au tableau plus bas.

11. Cliquez sur le bouton **Mettre à jour**.

Le tableau affiche la liste des périphériques dont les identifiants et/ou les modèles sont connus et qui sont liés au type indiqué dans la liste déroulante **Type de périphériques**.

12. Cochez les cases en regard des noms des périphériques que vous souhaitez ajouter à la liste des périphériques de confiance.

13. Cliquez sur le bouton **Sélectionner**.

La fenêtre **Sélectionnez utilisateurs ou groupes** s'ouvre.

14. Dans la fenêtre **Sélectionnez utilisateurs ou groupes** spécifiez les utilisateurs et/ou les groupes d'utilisateurs pour qui Kaspersky Security reconnaît les périphériques choisis comme de confiance.

Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre **Sélectionnez utilisateurs ou groupes** s'affichent dans le champ **Autoriser les utilisateurs et/ou groupes d'utilisateurs**.

15. Cliquez sur le bouton **OK**.

Les lignes s'affichent dans le tableau, sur l'onglet **Périph. de confiance** avec les paramètres des périphériques de confiance ajoutés.

16. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Ajout de périphériques de confiance à la liste selon le masque de leur identifiant

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

L'ajout de périphériques de confiance à la liste selon le masque de leur identifiant est uniquement possible depuis Kaspersky Security Center.

► *Pour ajouter un périphérique à la liste des périphériques de confiance selon le masque de leur identifiant, 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 souhaitez créer une liste de périphériques de confiance.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Sélectionnez la stratégie dont vous avez besoin dans la liste.
5. Exécutez une des actions suivantes :
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
 - Placez-vous sur le lien **Modifier les paramètres de la stratégie** à droite de la liste de stratégies.

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

6. Choisissez la section **Contrôle des périphériques**.
7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.
8. Cliquez sur le bouton **Ajouter**.

Le menu contextuel du bouton s'ouvre.

9. Dans le menu contextuel **Ajouter**, sélectionnez l'option **Périphériques selon masque d'identificateur**.

La fenêtre **Ajout de périphériques de confiance selon le masque de l'identifiant** s'ouvre.

10. Saisissez le masque de l'identifiant des périphériques dans la fenêtre **Ajout de périphériques de confiance selon le masque d'identifiant** dans le champ **Masque**.
11. Cliquez sur le bouton **Sélectionner**.

La fenêtre **Sélectionnez utilisateurs ou groupes** s'ouvre.

12. Dans la fenêtre **Sélectionnez utilisateurs ou groupes**, spécifiez les utilisateurs et/ou les groupes d'utilisateurs dont Kaspersky Security reconnaît les périphériques, les modèles ou les identifiants dont ils respectent le masque spécifié comme de confiance.

Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre **Sélectionnez utilisateurs ou groupes** s'affichent dans le champ **Autoriser les utilisateurs et/ou groupes d'utilisateurs**.

13. Cliquez sur le bouton **OK**.

La ligne des paramètres de la règle d'ajout de périphériques dans la liste de périphériques de confiance selon le masque de leurs identifiants s'affiche dans le tableau sous l'onglet **Périph. de confiance** de la fenêtre des paramètres du composant **Contrôle des périphériques**.

14. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Technologie de réparation de l'infection active

Cette section fournit des informations sur la technologie de réparation de l'infection active et des instructions concernant son activation pour le système d'exploitation de serveur Windows sur les machines virtuelles protégées.

Dans cette section

Présentation de la technologie de réparation de l'infection active	188
Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur	190

Présentation de la technologie de réparation de l'infection active

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une activité malveillante dans le système d'exploitation Windows, Kaspersky Security exécute une procédure élargie de réparation utilisant une technologie particulière de réparation de l'infection active. La *technologie de réparation de l'infection active* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui empêchent l'application Kaspersky Security de les supprimer à l'aide d'autres méthodes. La menace est supprimée suite à l'application de la technologie de réparation de l'infection active. Pendant la réparation de l'infection active, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registre du système d'exploitation Windows. La technologie de réparation de l'infection active est gourmande en ressources du système d'exploitation Windows et peut ralentir d'autres applications.

Au terme du processus de réparation de l'infection active sur la machine virtuelle sous système d'exploitation pour poste de travail Windows, Kaspersky Security vous demande l'autorisation de redémarrer la machine virtuelle. Après le redémarrage de la machine virtuelle, Kaspersky Security supprime les fichiers de l'application malveillante et lance une analyse complète simplifiée de la machine virtuelle.

La demande de redémarrage de la machine virtuelle sous système d'exploitation pour serveur Windows est indisponible en raison des particularités de l'application Kaspersky Security pour systèmes d'exploitation pour serveur. Le redémarrage non prévu du système d'exploitation pour serveur peut entraîner des problèmes liés à l'accès temporairement refusé aux données du système d'exploitation pour serveur ou à la perte des données non enregistrées. Il est conseillé de redémarrer le système d'exploitation pour serveur en respectant scrupuleusement la planification prévue. Pour cette raison, la technologie de réparation de l'infection active sur une machine virtuelle protégée sous système d'exploitation pour serveur Windows est désactivée par défaut.

En cas de détection d'une infection active sur une machine virtuelle protégée sous système d'exploitation pour serveur Windows, un événement relatif à la nécessité de réparer l'infection active est envoyé au Kaspersky Security Center. Afin de réparer une infection active sur une machine virtuelle protégée dotée du système d'exploitation pour serveur Windows, il est nécessaire d'activer la technologie de réparation d'une infection active pour système d'exploitation pour serveur (cf. section "Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur" à la page [190](#)) et de lancer une tâche de groupe pour la recherche de virus au moment jugé opportun par les utilisateurs de ce système d'exploitation.

Si le Light Agent fonctionne sur une machine virtuelle temporaire, la technologie de réparation de l'infection active n'est pas utilisée. En cas d'infection active de cette machine virtuelle temporaire, il est nécessaire de s'assurer de l'absence de virus et d'autres applications malveillantes sur le modèle de machine virtuelle à partir duquel elle a été créée, puis de recréer la machine virtuelle temporaire.

Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur

► *Pour activer ou désactiver la technologie de réparation de l'infection active pour les systèmes d'exploitation pour serveur Windows, 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 au nom du groupe d'administration contenant les machines virtuelles protégées souhaitées.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie pour le Light Agent.
5. Cliquez-droit pour ouvrir le menu contextuel de la stratégie pour le Light Agent, puis sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie pour le Light Agent s'ouvre.

6. Dans la fenêtre des propriétés de la stratégie pour le Light Agent, sélectionnez la section **Paramètres généraux**.
7. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :
 - Cochez la case **Appliquer la technologie de réparation de l'infection active** si vous souhaitez activer la technologie de réparation de l'infection active.
 - Décochez la case **Appliquer la technologie de réparation de l'infection active** si vous souhaitez désactiver la technologie de réparation de l'infection active.
8. Cliquez sur le bouton **OK** de la fenêtre des propriétés de la stratégie pour enregistrer les modifications apportées. La fenêtre des propriétés de la stratégie se ferme.

9. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
10. Dans la liste des tâches, sélectionnez la tâche **Recherche de virus**.
11. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la tâche, puis sélectionnez l'option **Propriétés**.

La fenêtre **Propriétés : Recherche de virus** s'ouvre.

12. Dans la fenêtre **Propriétés : Recherche de virus**, sélectionnez la section **Paramètres**.

Les paramètres de la tâche de groupe d'analyse contre les virus s'affichent dans la partie droite de la fenêtre.

13. Dans le groupe de paramètres **Action en cas de détection d'une menace**, exécutez l'une des actions suivantes :
 - Cochez la case **Exécuter la réparation de l'infection active immédiatement** si vous souhaitez activer la technologie de réparation de l'infection active.
 - Décochez la case **Exécuter la réparation de l'infection active immédiatement** si vous souhaitez désactiver la technologie de réparation de l'infection active.
14. Cliquez sur le bouton **OK** de la fenêtre **Propriétés : Recherche de virus** pour enregistrer les modifications apportées.

Participer au Kaspersky Security Network

Cette section présente la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de ce service.

Dans cette section

A propos de la participation au Kaspersky Security Network.....	192
A propos de l'approvisionnement des données	194
Configuration de l'utilisation Kaspersky Security Network	195

A propos de la participation à Kaspersky Security Network

Pour renforcer l'efficacité de la protection des machines virtuelles, Kaspersky Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet de collecter ces données.

Kaspersky Security Network (KSN) est une infrastructure de services de cloud qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Web et des logiciels. Grâce aux données de Kaspersky Security Network, Kaspersky Security peut réagir plus rapidement face aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

Selon la disposition de l'infrastructure, les distinctions suivantes ont cours :

- Le KSN global est une infrastructure disposée sur les serveurs de Kaspersky Lab ;
- Le KSN privé (Kaspersky Private Security Network) est une infrastructure disposée sur des serveurs secondaires du prestataire, par exemple à l'intérieur d'un réseau d'un fournisseur d'accès à Internet.

Les informations relatives au type de KSN utilisé par Kaspersky Security s'affichent dans les propriétés de la stratégie pour le Serveur de protection (cf. section "Configuration de l'utilisation de Kaspersky Security Network" à la page [195](#)) et dans l'interface locale de Light Agent for Windows (cf. *Manuel d'utilisation de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

La configuration de l'utilisation du KSN privé s'effectue dans les propriétés du Serveur d'administration de Kaspersky Security Center, dans la section **Serveur proxy KSN**. Pour plus d'informations, consultez la documentation de Kaspersky Security Center.

Pour continuer à utiliser le KSN privé après la modification de la clé, il faut fournir les informations relatives à la clé au prestataire de service. Dans le cas contraire, l'échange d'informations avec KSN est impossible.

Si vous participez au Kaspersky Security Network et utilisez le KSN global, certaines informations obtenues dans le cadre du fonctionnement de Kaspersky Security sur votre machine virtuelle sont transmises automatiquement à Kaspersky Lab (cf. section "À propos de l'approvisionnement des données" à la page [194](#)).

Votre participation au Kaspersky Security Network permet à Kaspersky Lab d'obtenir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des outils de neutralisation et de réduire le nombre de faux positifs de Kaspersky Security.

La participation à Kaspersky Security Network est volontaire. La décision de participer ou non à Kaspersky Security Network est prise lors de la définition de la stratégie pour le Serveur de protection. Vous pouvez changer d'avis à tout moment (cf. section "Configuration de l'utilisation de Kaspersky Security Network" à la page [195](#)).

A propos de l'approvisionnement des données

En acceptant les conditions de participation au programme Kaspersky Security Network, vous autorisez la transmission automatique des renseignements suivants à Kaspersky Lab :

- Informations relatives à l'installation et à la licence de la version de Kaspersky Security installée incluant : des détails sur la version de l'application, des informations sur les fichiers des modules téléchargés et les versions des bases de l'application utilisées.
- Informations relatives à la configuration logicielle et matérielle installée sur les machines virtuelles, dont la version du système d'exploitation, les paquets de mises à jour et les objets téléchargés.
- Informations relatives à la protection antivirus des machines virtuelles, y compris la version des bases antivirus utilisées et les statistiques des mises à jour et des liaisons avec les services Kaspersky Lab.
- Informations relatives à tous les objets et actions malveillants (dont le nom de l'objet détecté, le hash MD5, la date et l'heure de la détection, l'adresse Internet de téléchargement, le nom et la taille des fichiers infectés et le chemin d'accès à ceux-ci, l'adresse IP de l'ordinateur attaqué et le numéro de port victime de l'attaque réseau, la séquence d'actions du programme malveillant et les adresses Internet potentiellement malveillantes) et informations concernant vos prises de décisions et les solutions appliquées face à ces objets et actions.
- Informations relatives aux fichiers que vous avez téléchargés (adresse Internet, adresse IP à partir de laquelle le téléchargement est effectué, attributs, taille du fichier, informations relatives au processus qui a téléchargé le fichier).
- Informations relatives aux applications et aux modules exécutés sur les machines virtuelles (taille, attributs, date de création, informations de l'en-tête PE, noms des fichiers et de leurs modules, compacteurs).
- Informations sur les vulnérabilités détectées sur les machines virtuelles dont : l'identificateur de la vulnérabilité dans la base des vulnérabilités, le niveau de danger de la vulnérabilité et l'état de la détection.

Des fichiers (ou extraits de fichiers) peuvent être envoyés à "Kaspersky Lab" pour analyse, au cas où ils présenteraient un risque d'utilisation malveillante dans le but de nuire à votre machine virtuelle.

Les paramètres définissant la composition des données envoyées à Kaspersky Lab et le destinataire des données se trouvent dans les fichiers de configuration sur la machine virtuelle protégée.

La sécurité des fichiers de configuration sur la machine virtuelle protégée est garantie par un mécanisme d'auto-protection (pour plus de détails, cf. *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*). Si vous avez désactivé le mécanisme d'auto-protection, vous devez garantir la protection de ces fichiers de configuration contre l'accès non autorisé. Pour les détails, vous pouvez contacter les experts du Support Technique.

Si vous ne participez pas à Kaspersky Security Network, les données susmentionnées ne sont pas transmises. Les données sont traitées et enregistrées dans une section protégée à accès restreint de la machine virtuelle. Les données indiquées sont définitivement supprimées lors de la suppression de l'application. Pour plus de détails sur les données transmises par l'application au Kaspersky Security Network, vous pouvez lire la déclaration de Kaspersky Security Network avant de décider d'y participer ou non.

Pour de plus amples informations sur le traitement des données, consultez le site Internet de Kaspersky Lab (<http://www.kaspersky.com/fr/privacy>).

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 données des statistiques générales sont conservées de manière illimitée.

Configuration de l'utilisation de Kaspersky Security Network

La configuration des services de Kaspersky Security Network est définie dans les paramètres de la stratégie pour le Serveur de protection. Si l'utilisation de Kaspersky Security Network est activée dans la stratégie active du groupe d'administration, les services KSN sont utilisés par Kaspersky Security dans le cadre de la protection des machines virtuelles et dans le cadre de l'exécution des tâches d'analyse des machines virtuelles.

Si la stratégie impliquant l'utilisation de Kaspersky Security Network n'est pas active, les services de KSN ne sont pas utilisés par Kaspersky Security.

Si vous souhaitez utiliser Kaspersky Security Network avec Kaspersky Security, assurez-vous que le service KSN Proxy est activé dans Kaspersky Security Center (voir la documentation de Kaspersky Security Center).

► *Pour configurer l'utilisation de Kaspersky Security Network, 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 au nom du groupe d'administration dont vous souhaitez modifier la stratégie.
3. Dans l'espace de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste des stratégies, sélectionnez une stratégie pour le Serveur de protection et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
 - Via le lien **Modifier les paramètres de la stratégie**, à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
 - En double-cliquant.
 - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez la section **Paramètres KSN**.
6. Exécutez une des actions suivantes :
 - Cochez la case **J'accepte les conditions du Contrat de licence et je participe à KSN** si vous souhaitez activer l'utilisation des services de Kaspersky Security Network.
 - Décochez la case **J'accepte les conditions du Contrat de licence et je participe à KSN** si vous souhaitez désactiver l'utilisation des services de Kaspersky Security Network.

En cochant la case **J'accepte les conditions du Contrat de licence et je participe à KSN**, vous marquez votre accord avec les dispositions du programme Kaspersky Security Network présentées dans la déclaration de Kaspersky Security Network.

7. Si vous avez coché la case **J'accepte les conditions du Contrat de licence et je participe à KSN**, indiquez les paramètres d'utilisation des services Kaspersky Security Network dans le cadre du fonctionnement de l'application :

- **Utiliser pour l'analyse des fichiers et la catégorisation.**

La case active ou désactive l'utilisation des services KSN dans le fonctionnement des modules suivants de Light Agent et des tâches :

- Contrôle du lancement des applications.
- Contrôle de l'activité des applications.
- Antivirus Fichiers.
- Surveillance du système.
- Tâches d'analyse.

Si la case est cochée, lors de l'utilisation des modules de Light Agent énumérés et des tâches, l'application Kaspersky Security reçoit des informations envoyées par les services KSN concernant la catégorie et la réputation des fichiers analysés.

Si la case est décochée, Kaspersky Security ne reçoit pas d'informations envoyées par les services KSN concernant la réputation et la catégorie des fichiers.

Cette case est accessible si la case **J'accepte les Conditions du contrat de licence et je participe à KSN** est cochée.

- **Utiliser pour l'analyse des URL.**

La case active ou désactive l'utilisation des services KSN dans le fonctionnement des modules suivants de Light Agent for Windows :

- Antivirus Internet.
- Contrôle Internet.
- Antivirus IM.

Si la case est cochée, lors de l'utilisation des modules de Light Agent for Windows énumérés, Kaspersky Security reçoit des informations envoyées par les services KSN concernant la réputation des adresses Internet analysées.

Si la case est décochée, Kaspersky Security ne reçoit pas d'informations envoyées par les services KSN concernant la réputation des adresses Internet.

Cette case est accessible si la case **J'accepte les Conditions du contrat de licence et je participe à KSN** est cochée.

8. Si vous souhaitez interdire ou autoriser la modification des paramètres KSN dans les stratégies des niveaux inférieurs (pour les groupes d'administration secondaires), cliquez sur le "verrou" à gauche de la case **J'accepte les conditions du Contrat de licence et je participe à KSN**.
9. Cliquez sur le bouton **OK**.

Administration du Light Agent for Linux via la ligne de commande

Cette section contient des informations sur l'administration du composant Light Agent for Linux à l'aide des commandes de la ligne de commande et sur la configuration des paramètres des commandes.

L'administration de Light Agent for Linux via la ligne de commande est aussi décrite dans la Base de connaissances (<http://support.kaspersky.ru/13170>).

Dans cette section

Affichage d'aide sur les commandes de Kaspersky Security	199
Consultation des informations sur l'état de la protection de la machine virtuelle	201
Consultation des informations sur les SVM	201
Consultation des informations sur la licence	202
Lancement de la tâche d'analyse	203
Lancement et arrêt de la tâche de mise à jour.....	207
Sauvegarde.....	210

Affichage d'aide sur les commandes de Kaspersky Security

La commande help affiche des informations sur les commandes d'administration de l'application Kaspersky Security.

Syntaxe de la commande

```
/opt/kaspersky/lightagent/bin/avp-cli help [command]
```

où :

command est le nom de la commande d'administration sur laquelle vous voulez recevoir de l'aide.

Valeurs possibles :

- license est la commande qui affiche des informations sur la licence sur la SVM.
- list est la commande qui affiche la liste des fichiers de la sauvegarde.
- restore est la commande qui restaure le fichier de la sauvegarde.
- scan est la commande qui lance l'analyse antivirus de la machine virtuelle.
- statistics est la commande qui affiche les statistiques sur le fonctionnement de la tâche de mise à jour.
- status est la commande qui affiche les informations sur l'état en cours de la tâche de mise à jour.
- start est la commande qui lance la tâche de mise à jour des bases de données.
- stop est la commande qui arrête l'exécution de la tâche de mise à jour des bases de données.
- svminfo est la commande qui affiche les informations sur les SVM auxquelles la machine virtuelle protégée est connectée.
- trace est la commande qui active ou désactive la création de fichiers de trace sur la machine virtuelle protégée.
- update est la commande qui lance la tâche de mise à jour des bases de données avec des paramètres supplémentaires.

Avant l'exécution des commandes, assurez-vous que le service lightagent est lancé sur la machine virtuelle protégée.

Consultation des informations sur l'état de la protection de la machine virtuelle

Vous pouvez connaître l'état de la machine virtuelle protégée avec le composant installé Light Agent for Linux à l'aide des commandes suivantes :

- La commande `svminfo` (cf. section "Consultation des informations sur les SVM" à la p. [201](#)) permet de recevoir des informations sur les SVM auxquelles le Light Agent for Linux est connecté et sur les moyens de la réception des informations sur les SVM.
- La commande `license` (cf. section "Consultation des informations sur la licence" à la p. [202](#)) permet de recevoir des informations sur la licence par laquelle l'application est activée sur les SVM.
- La commande `status` (cf. section "Consultation de l'état de la tâche de mise à jour" à la p. [209](#)) permet de recevoir des informations sur l'état en cours de la tâche de mise à jour.
- La commande `statistics` (cf. la section "Consultation des statistiques du fonctionnement de la tâche de la mise à jour" à la p. [209](#)) permet de recevoir des statistiques du fonctionnement de la tâche de la mise à jour (pourcentage déjà exécuté, volume des mises à jour chargées et d'autres informations).
- La commande `update` (cf. section "Lancement de la tâche de la mise à jour avec des paramètres supplémentaires" à la p. [208](#)) permet de lancer la tâche de mise à jour des bases de données et enregistrer dans le fichier journal les informations sur les événements apparaissant pendant l'exécution de cette tâche (pourcentage déjà exécuté, résultat de l'exécution de la tâche et d'autres événements).

Consultation des informations sur les SVM

Par défaut, Light Agent détecte les SVM, travaillant en réseau à l'aide de la multidiffusion (Multicast). Vous pouvez configurer en cas de nécessité d'autres moyens de la détection des SVM (cf. section "A propos de la détection des SVM" à la p. [35](#)). L'administrateur configure le moyen qu'utilise le Light Agent pour la détection des SVM dans la stratégie pour le Light Agent for Linux (cf. section "le Pas 5. Configuration des paramètres de détection des SVM" à la p. [114](#)).

Vous pouvez recevoir des informations sur la SVM à laquelle le Light Agent est connecté à l'aide de la commande `svminfo`.

► *Pour afficher les informations sur SVM à laquelle le Light Agent est connecté, exécutez la commande suivante :*

```
lightagent svminfo
```

La commande affiche les informations suivantes :

- Current SVM : adresse IP de la SVM à laquelle le Light Agent est connecté ou nom complet de cette SVM au format FQDN.
- Discovery method : méthode de réception des informations sur la SVM. Valeurs possibles :
 - Multicast : par multidiffusion (Multicast) ;
 - VIIS : à l'aide du Serveur d'intégration ;
 - List : avec la liste d'adresses de SVM.
- List of known SVM : liste des SVM auxquelles les Light Agents peuvent se connecter. Ces informations s'affichent seulement si le moyen List est indiqué pour Discovery method.

Consultation des informations sur la licence

La commande `license` affiche des informations sur la licence d'activation de l'application.

► *Pour afficher des informations sur la licence d'activation de l'application, exécutez la commande suivante :*

```
lightagent license
```

La commande affiche les informations suivantes :

- License source : adresse IP de la SVM à laquelle le Light Agent for Linux est connecté ou nom de cette SVM au format FQDN ;
- Key : clé ajoutée sur la SVM ;

- License type : type de licence (commercial, d'essai, de test bêta, abonnement) pour la quantité <server (s)> ou <core (s)> ;
- Expiration date : la date de fin de la durée de validité de la licence (au format AAAA-MM-JJTHH:MM:SS) ;
- Days till expiration : quantité de jours avant la date de fin de validité de la licence ;

où :

server(s) : nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;

core(s) : quantité maximum de noyaux utilisés simultanément des processeurs physiques sur tous les hyperviseurs sur lesquels des SVM sont déployées.

Lancement de la tâche d'analyse

Vous pouvez lancer une tâche *d'analyse personnalisée* à partir de la machine virtuelle protégée après avoir indiqué la liste des fichiers à analyser, les noms de ces fichiers (ou les chemins d'accès) ou les modèles de leurs (ou les chemins d'accès) à l'aide des masques. Vous pouvez aussi lancer une *analyse complète* de tous les objets du système de fichiers de la machine virtuelle protégée.

Les objets du système de fichiers /dev, /sys et /proc sont exclus de l'analyse.

Vous pouvez lancer la tâche d'analyse avec des paramètres supplémentaires. Ces paramètres permettent d'enregistrer dans un fichier les événements apparaissant lors de l'exécution de la tâche ou d'utiliser les paramètres du fichier de configuration pour l'exécution de la tâche.

► **Pour lancer la tâche d'analyse, exécutez la commande suivante :**

```
lightagent scan [<chemin vers le fichier ou le dossier>] [<chemin vers le
fichier ou le dossier>...] [--@:<filelist.lst>] [--R[A]:<chemin vers le
fichier de rapport>]\

[--C:<chemin vers le fichier de configuration>]
```

où :

- <chemin vers le fichier ou le dossier> : chemin vers le fichier ou le dossier à analyser pour y détecter des virus et d'autres applications malveillantes. Vous pouvez utiliser des masques pour indiquer le chemin vers le fichier ou le dossier. Si vous n'indiquez pas de chemin vers les fichiers ou les dossiers, l'application analysera tous les objets du système de fichiers de la machine virtuelle protégée.
- @:<filelist.lst> : liste des fichiers à analyser. Dans un fichier de texte, indiquez à la ligne les fichiers et les dossiers que vous voulez analyser pour y détecter des virus et d'autres applications malveillantes.
- R:<chemin vers le fichier journal> : enregistrer dans le fichier journal seulement les événements importants apparaissant pendant l'exécution de la tâche d'analyse. Indiquez le chemin complet vers le fichier d'enregistrement des événements. L'application créera ce fichier et y consignera les événements.
- RA:<chemin vers le fichier journal> : enregistrer dans le fichier journal tous les événements apparaissant pendant l'exécution de la tâche d'analyse. Indiquez le chemin complet vers le fichier d'enregistrement des événements. L'application créera ce fichier et y consignera les événements.
- C:<chemin vers le fichier de configuration> : lors de l'analyse, utiliser les paramètres indiqués dans le fichier de configuration. Indiquez le chemin complet vers le fichier de configuration.

Prenez garde aux particularités de l'analyse des liens fixes et symboliques (cf. section "Particularité de l'analyse des liens symboliques et fixes" à la p. [81](#)).

Sélection des actions sur les fichiers infectés

Vous pouvez spécifier les actions suivantes que l'application Kaspersky Security exécutera à la détection des fichiers infectés :

- Informer (i0). Lors de la détection de fichiers infectés, Kaspersky Security vous informe.
- Réparer (i1). Kaspersky Security tente de désinfecter automatiquement tous les fichiers infectés détectés. Si la désinfection est impossible, l'application laisse les fichiers inchangés.

- Réparer. Supprimer si la désinfection est impossible. Ignorer les fichiers composés si la désinfection et la suppression sont impossibles (i2). Kaspersky Security tente de désinfecter automatiquement tous les fichiers infectés détectés. Si la désinfection est impossible, l'application les supprime. Si le fichier infecté fait partie d'un fichier composé et ne peut pas être supprimé, l'application laisse ce fichier inchangé.
- Réparer. Supprimer si la désinfection est impossible (i3). Kaspersky Security tente de désinfecter automatiquement tous les fichiers infectés détectés. Si la désinfection est impossible, l'application les supprime. Si le fichier infecté fait partie d'un fichier composé et ne peut pas être supprimé, l'application supprime tout le fichier composé. Cette action est exécutée par défaut.
- Supprimer (i4). Kaspersky Security supprime automatiquement le fichier infecté après avoir créé préalablement sa copie de sauvegarde. Si le fichier infecté faisant partie d'un fichier composé ne peut pas être supprimé, l'application supprime tout le fichier composé.

► *Pour indiquer les actions à exécuter sur les fichiers infectés, procédez comme suit :*

```
lightagent scan [<chemin vers le fichier ou le dossier>] [--i<0-4>]
```

où :

- <chemin vers le fichier ou le dossier> : chemin vers le fichier ou le dossier à analyser pour y détecter des virus et d'autres applications malveillantes. Si vous n'indiquez pas de chemin vers les fichiers ou les dossiers, l'application analysera tous les objets du système de fichiers de la machine virtuelle protégée.
- i0 : lors de la détection de fichiers infectés, exécuter l'action Informer.
- i1 : lors de la détection de fichiers infectés, exécuter l'action Réparer.
- i2 : lors de la détection de fichiers infectés, exécuter l'action Réparer.
Supprimer si la désinfection est impossible. Ignorer les fichiers composés si la désinfection et la suppression sont impossibles.
- i3 : lors de la détection de fichiers infectés, exécuter l'action Réparer.
Supprimer si la désinfection est impossible. Cette action est exécutée par défaut.
- i4 : lors la détection des fichiers infectés exécuter l'action Supprimer.

Analyse des fichiers composés

L'insertion de virus et d'autres applications malveillantes dans des fichiers composés tels que des archives ou les bases de données est une pratique de dissimulation très répandue.

Pour détecter les virus dissimulés et les autres applications malveillantes, vous devez décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse.

Vous pouvez limiter le cercle des fichiers composés analysés pour accélérer l'analyse.

En outre vous pouvez réduire le temps d'analyse des fichiers composés après avoir spécifié les restrictions suivantes :

- sur la durée d'analyse des fichiers composés : l'application cessera l'analyse du fichier composé à l'expiration du temps indiqué ;
- sur la taille maximale du fichier composé analysé : l'application ne décompressera pas et n'analysera pas les fichiers composés dont les tailles dépassent la valeur indiquée.

► *Pour configurer l'analyse des fichiers composés, exécuter la commande suivante :*

```
lightagent scan [--e:a] [--e:b] [--e:<seconds>] [--es:<size>]
```

où :

- --e:a : ne pas analyser les archives.
- --e:b : ne pas analyser les bases de messagerie et les fichiers aux formats de messagerie.
- --e:<seconds> : ne pas analyser les fichiers composés si leur analyse dure plus que le temps indiqué. Indiquez le temps maximal de l'analyse du fichier en secondes.
- --s:<size> : ne pas vérifier les fichiers composés si leur taille dépasse la valeur indiquée. Indiquez la taille maximale du fichier composé analysé en mégaoctets.

Utilisation de la technologie iChecker lors de l'analyse

Vous pouvez activer l'utilisation de la technologie iChecker lors de l'analyse de la machine virtuelle protégée. La technologie iChecker permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de l'application, de la dernière date d'analyse du fichier et des modifications des paramètres d'analyse. Par défaut, l'utilisation de la technologie iChecker lors de l'analyse de la machine virtuelle protégée est activée.

- *Pour désactiver l'utilisation de la technologie iChecker, exécutez la commande suivante :*

```
lightagent scan --iChecker:off
```

- *Pour activer l'utilisation de la technologie iChecker, exécutez la commande suivante :*

```
lightagent scan --iChecker:on
```

Lancement et arrêt de la tâche de mise à jour

- *Pour lancer la tâche de la mise à jour, exécutez la commande suivante :*

```
lightagent start Updater
```

Pour le lancement de la tâche de mise à jour des bases de données avec des paramètres supplémentaires, utilisez la commande `update` (cf. section "Lancement de la tâche de mise à jour avec des paramètres supplémentaires" à la p. [208](#)).

- *Pour arrêter la tâche de la mise à jour, exécutez la commande suivante :*

```
lightagent stop Updater
```

Lancement de la tâche de mise à jour avec des paramètres supplémentaires

Excepté la commande standard de lancement de la tâche de la mise à jour `start` (cf. section "Lancement et l'arrêt de la tâche de la mise à jour" à la p. [207](#)), vous pouvez utiliser la commande de lancement de la tâche de la mise à jour avec des paramètres supplémentaires. Ces paramètres permettent d'enregistrer dans un fichier les événements apparaissant lors de l'exécution de la tâche ou d'utiliser les paramètres du fichier de configuration pour l'exécution de la tâche.

► *Pour lancer la tâche de la mise à jour, exécutez la commande suivante :*

```
lightagent update [--R[A]:<chemin vers le fichier journal>] [--C:<chemin  
vers le fichier de configuration>]
```

où :

- `R:<chemin vers le fichier journal>` : enregistrer dans le fichier journal seulement les événements importants apparaissant pendant l'exécution de la tâche de mise à jour. Indiquez le chemin complet vers le fichier d'enregistrement des événements. L'application créera ce fichier et y consignera les événements.
- `RA:<chemin vers le fichier journal>` : enregistrer dans le fichier journal tous les événements apparaissant pendant l'exécution de la tâche de mise à jour. Indiquez le chemin complet vers le fichier d'enregistrement des événements. L'application créera ce fichier et y consignera les événements.
- `C:<chemin vers le fichier de configuration>` : lors de la mise à jour, utiliser les paramètres indiqués dans le fichier de configuration. Indiquez le chemin complet vers le fichier de configuration.

Exemple :

► *Lancer la tâche de la mise à jour et enregistrer les informations sur tous les événements qui sont apparus pendant l'exécution de la tâche dans le fichier `update.txt` :*

```
lightagent update --RA:/usr/local/update.txt
```


La commande enregistre dans un fichier journal les informations suivantes :

- Update source : adresse réseau du dossier sur la SVM où se trouvent les bases de l'application.
- Completion : pourcentage d'exécution de la tâche.
- Update status : résultat de l'exécution de la tâche. Valeurs possibles :
 - succeed : la tâche a été exécutée avec succès ;
 - failed : la tâche ne s'est pas exécutée suite à une erreur interne.

Consultation de l'état de la tâche de mise à jour

Vous pouvez consulter l'état en cours de la tâche de la mise à jour.

► *Pour consulter l'état de la tâche de la mise à jour, exécutez la commande suivante :*

```
lightagent status Updater
```

La commande consigne un des états suivants de la tâche de la mise à jour :

- Running : la tâche est en cours ;
- Starting : la tâche est lancée ;
- NeverStarted : la tâche n'a pas été lancée ;
- Stopped : la tâche est arrêtée ;
- Stopping la tâche s'arrête.

Consultation des statistiques du fonctionnement de la tâche de mise à jour

► *Pour consulter les statistiques du fonctionnement de la tâche de la mise à jour, exécutez la commande suivante :*

```
lightagent statistics Updater
```

La commande fournit les informations suivantes sur la tâche de la mise à jour :

- Current time : heure actuelle.
- Time Start : heure de lancement de la tâche.
- Time Finish : heure d'achèvement de la tâche.
- Completion : pourcentage d'exécution de la tâche.
- Reason : raison de l'achèvement de la tâche. Valeurs possibles :
 - Unknown : raison inconnue ;
 - NeverRun : la tâche n'a jamais été lancée ;
 - Completed : la tâche s'est exécutée avec succès ;
 - Canceled : l'utilisateur a arrêté la tâche ;
 - Failed : la tâche s'est arrêtée suite à une erreur interne.
- Total downloaded size : volume total des mises à jour chargées (en octets).
- Speed : vitesse de chargement des mises à jour (octets/sec).

Sauvegarde

Cette section contient les instructions sur l'utilisation de la sauvegarde.

Dans cette section

A propos de la sauvegarde	211
Consultation de la liste des fichiers dans la sauvegarde	211
Restauration des fichiers depuis la sauvegarde	212

A propos de la sauvegarde

La *sauvegarde* est une liste des copies de sauvegarde des fichiers infectés qui ont été supprimés ou modifiés pendant la désinfection. La *copie de sauvegarde* est une copie de fichier créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Si Kaspersky Security détecte un code malveillant dans un fichier, il bloque celui-ci, le supprime de son dossier d'origine et place une copie dans le dossier de sauvegarde avant de tenter de le réparer.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la réparation. Si le fichier désinfecté contenait des informations importantes, qui à la suite de la désinfection sont devenues entièrement ou partiellement inaccessibles, vous pouvez restaurer le fichier à partir de sa copie de sauvegarde (cf. section "Restauration des fichiers depuis la sauvegarde" à la p. [212](#)).

Consultation de la liste des fichiers dans la sauvegarde

► *Pour consulter la liste des fichiers dans la sauvegarde, exécutez la commande suivante :*

```
lightagent list backup
```

La commande affiche les informations suivantes sur les fichiers dans la sauvegarde :

- date et heure de placement du fichier dans la sauvegarde (au format AAAA-MM-JJTHH:MM:SS) ;
- identificateur du fichier ;
- chemin où le fichier est détecté et où il sera restauré (cf. section "Restauration des fichiers de la sauvegarde" à la p. [212](#)).

Restauration des fichiers depuis la sauvegarde

La restauration des fichiers infectés depuis la sauvegarde peut amener à l'infection de la machine virtuelle.

► *Pour restaurer un fichier depuis la sauvegarde, procédez comme suit :*

```
lightagent restore [--replace] <identificateur du fichier>
```

où :

- <identificateur du fichier> est l'identificateur numérique du fichier dans la sauvegarde ;
- replace signifie réenregistrer le fichier avec l'identificateur indiqué par le fichier restauré s'il se trouve dans le même dossier.

L'application restaurera le fichier dans le dossier du placement initial.

Contacter le Support Technique

Cette section explique comment bénéficier des services du Support Technique et des conditions à remplir.

Dans cette section

Modes d'obtention du Support Technique	213
Support Technique par téléphone	214
Support Technique via Kaspersky CompanyAccount	214
Obtention d'informations pour le Support Technique	215

Modes d'obtention du Support Technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans d'autres sources d'informations relatives à l'application (cf. section "Sources d'informations sur l'application" à la page [14](#)), contactez le Support Technique. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

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

Avant de contacter le service du Support Technique, veuillez lire les règles d'octroi du Support Technique (<http://support.kaspersky.com/fr/support/rules>).

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

- appeler le Support Technique par téléphone (<http://support.kaspersky.com/fr/b2b>) ;
- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Support Technique par téléphone

Dans la majorité des régions du monde, les experts du Support Technique sont joignables par téléphone. Vous pouvez trouver des informations sur les moyens de bénéficier de l'aide du Support Technique dans votre région ainsi que les coordonnées du Support Technique sur le site Internet du Support Technique de Kaspersky Lab (<http://support.kaspersky.com/fr/b2b>).

Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du support technique (<http://support.kaspersky.com/fr/support/rules>).

Support Technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) est un portail destiné aux organisations qui utilisent les applications de Kaspersky Lab. Le service en ligne Kaspersky CompanyAccount est destiné à l'interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le service en ligne Kaspersky CompanyAccount permet de suivre l'état du traitement des requêtes électroniques par les experts de Kaspersky Lab et de conserver un historique des requêtes électroniques.

Vous pouvez inscrire tous les collaborateurs de votre organisation au sein d'un seul compte 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, consultez le site du Support Technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

Obtention d'informations pour le Support Technique

Obtention des fichiers des données

Une fois que les experts du Support Technique de Kaspersky Lab sont au courant du problème survenu, ils peuvent vous demander d'envoyer les fichiers suivants :

- fichiers des statistiques système de la SVM ;
- fichiers de trace de la SVM et de la machine virtuelle protégée ;
- fichiers dump de la SVM et de la machine virtuelle protégée ;

Les fichiers dump sont enregistrés sur la machine virtuelle dans un format accessible pour la lecture. Il est recommandé de protéger les informations enregistrées sur la machine virtuelle contre l'accès non autorisé avant leur transmission à Kaspersky Lab. Pour de plus amples informations sur les méthodes de création et de configuration d'un fichier dump, vous pouvez vous adresser aux experts du Support Technique.

Modification des paramètres de l'application

De plus, les experts du Support Technique peuvent avoir besoin d'informations complémentaires sur le système d'exploitation, sur les processus lancés sur la machine virtuelle protégée, ainsi que des rapports détaillés sur le fonctionnement des composants de l'application.

Pendant le diagnostic, les experts du Support Technique peuvent vous demander de modifier les paramètres de l'application dans le cadre du débogage :

- activer la fonctionnalité d'obtention des informations diagnostiques élargies ;
- exécuter une configuration plus fine des modules séparés du Light Agent qui n'est pas disponibles via les outils standards de l'interface utilisateur ;
- modifier les paramètres de conservation des informations diagnostiques ;
- activer le mode de débogage pour le Serveur d'intégration ;
- configurer l'interception du trafic réseau et l'enregistrement du trafic réseau dans un fichier.

Les experts du Support Technique vous communiqueront toutes les informations nécessaires à l'exécution des étapes décrites : ordre des étapes, paramètres à modifier, fichiers de configuration, scripts, possibilités complémentaires de la ligne de commande, modules de débogage, utilitaires spécialisés ainsi que la liste des types de données transmises pour le débogage.

Les informations diagnostiques élargies collectées sont enregistrées sur votre machine virtuelle. L'envoi automatique des données à Kaspersky Lab n'est pas exécuté.

Il est fortement recommandé de n'effectuer les actions énumérées ci-avant que sous la supervision des experts du Support Technique et selon leurs instructions. La modification indépendante des paramètres d'utilisation de l'application par d'autres moyens que ceux décrits dans la documentation concernant l'application ou recommandés par les experts du Support Technique peut entraîner des ralentissements et des échecs du système d'exploitation, une baisse du niveau de protection de la machine virtuelle et des problèmes d'accessibilité et d'intégrité des informations traitées.

Obtention d'informations sur les SVM connectées au Serveur d'intégration

Les spécialistes du Support Technique peuvent vous demander de leur fournir des informations sur les SVM connectées au Serveur d'intégration.

► *Pour obtenir des informations relatives aux SVM connectées au Serveur d'intégration, procédez comme suit :*

1. Sur l'ordinateur sur lequel la Console d'administration de Kaspersky Security Center est installée, créez le paramètre de ligne SVMPlugin et attribuez-lui la valeur 1 dans la branche suivante du registre du système d'exploitation :
 - HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\VIIS\Console\Public\
(pour les systèmes d'exploitation 32 bits) ;
 - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\VIIS\Console\Public\
(pour les systèmes d'exploitation 64 bits).
2. Lancez la Console de gestion du Serveur d'intégration (cf. *Manuel d'implantation de Kaspersky Security for Virtualization 4.0 Light Agent*).
3. Ouvrez la section **Liste des SVM connectées**.

La partie droite de la fenêtre affiche les paramètres des SVM connectées au Serveur d'intégration.

A propos de la composition des fichiers de trace

Le *fichier de traçage* permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

Vous pouvez consulter les données enregistrées dans les fichiers de trace. Pour en savoir plus, vous devez vous adresser au Support Technique de Kaspersky Lab.

Tous les fichiers de trace contiennent les données communes suivantes :

- heure de l'événement ;
- numéro du flux d'exécution ;
- module de l'application à l'origine de l'événement ;

- degré de gravité de l'événement (information, avertissement, critique, erreur) ;
- description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande ;

Composition des fichiers de trace des SVM

Contenu du fichier de trace ScanServer.log

Vous pouvez inscrire les informations suivantes dans le fichier de trace ScanServer.log, en dehors des données générales (cf. section " A propos de la composition des fichiers de trace " à la p. [217](#)) :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur les machines virtuelles protégées.
- Nom du compte utilisateur d'accès au système d'exploitation si ce nom fait partie du nom du fichier.
- Votre adresse email ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.

Contenu du fichier de trace de l'agent d'administration

Le fichier de trace de l'agent d'administration contient, outre les données générales, des informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu du fichier de trace boot_config.log

Le fichier de trace boot_config.log, contient, outre les données générales, des informations sur le premier lancement après le déploiement ou la modification de la configuration des SVM.

Contenu du fichier de trace wdserver.log

Le fichier de trace wdserver.log, contient, outre les données générales, des informations sur les événements apparaissant pendant le fonctionnement du service watchdog.

Composition des fichiers de trace du Light Agent for Windows

Contenu des fichiers de trace SRV.log et GUI.log

Vous pouvez inscrire les informations suivantes dans les fichiers de traçage SRV.log et GUI.log, outre les données générales (cf. section " A propos de la composition des fichiers de trace " sur p. [217](#)) :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur la machine virtuelle protégée.
- Nom d'utilisateur et mot de passe s'ils sont transmis en clair. Ces données peuvent être consignées dans les fichiers de trace lors de l'analyse du trafic Internet. Le trafic est consigné dans les fichiers de trace seulement à partir du fichier exécutable du composant Surveillance du réseau trafmon2.ppl.
- Nom d'utilisateur et mot de passe s'ils figurent dans les en-têtes du protocole HTTP.
- Nom du compte utilisateur d'accès à Microsoft Windows, si celui-ci fait partie du nom du fichier.
- Votre adresse email ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.
- Les sites Internet que vous visitez ainsi que les liens de ces sites. Ces données sont consignées dans les fichiers de traçage lorsque l'application analyse les sites Internet.

Contenu des fichiers de trace Dumpwriter.log et AVPCon.dll.log

Le fichier de trace Dumpwriter.log contient, outre les données générales, les informations de service indispensables à la résolution des problèmes survenus pendant l'écriture du fichier de vidage.

Le fichier de trace AVPCon.dll.log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu du fichier de trace du plug-in de l'Antivirus Courrier

Outre les données générales, le fichier de trace du plug-in de l'Antivirus Courrier mcou.OUTLOOK.EXE peut contenir une partie des messages, y compris les adresses email.

Contenu du fichier de trace ALL.log

Le fichier de trace ALL.log contient, outre les données générales, des informations sur les événements de la ligne de commande.

Composition des fichiers de trace du Light Agent for Linux

Contenu du fichier de trace LightAgent.log

Vous pouvez inscrire les informations suivantes dans le fichier de trace LightAgent.log, en dehors des données générales (cf. section " A propos de la composition des fichiers de trace " à la p. [217](#)) :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur la machine virtuelle protégée.
- Nom du compte utilisateur d'accès au système d'exploitation si ce nom fait partie du nom du fichier.
- Votre adresse email ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.

Contenu du fichier de trace de l'agent d'administration

Le fichier de trace de l'agent d'administration contient, outre les données générales, des informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu du fichier de trace avp-cli.log

Le fichier de trace avp-cli.log contient, en dehors des données générales, des informations sur les événements de la ligne de commande.

Contenu du fichier de trace install.log

Le fichier de trace install.log contient, en dehors des données générales, la conclusion des résultats de l'exécution des commandes formant les paramètres nécessaires pour la préparation du lancement de Light Agent for Linux.

Contenu du fichier de trace wdserver.log

Le fichier de trace wdserver.log, contient, outre les données générales, des informations sur les événements apparaissant pendant le fonctionnement du service watchdog.

Utilisation des fichiers de trace des SVM

Vous pouvez créer un fichier de trace des SVM et configurer le niveau de détails des informations de débogage à l'aide du fichier de configuration de l'application ScanServer.conf situé sur la SVM. Pour de plus amples informations sur les méthodes de création et de configuration d'un fichier de trace, vous pouvez vous adresser aux experts du Support Technique.

Les fichiers de trace sont enregistrés sur les SVM dans un format accessible pour la lecture. L'utilisateur est responsable de la sécurité des informations, et plus exactement du contrôle et de la restriction de l'accès aux informations conservées sur la SVM avant leur envoi à Kaspersky Lab.

Il peut être nécessaire de désactiver la fonction d'annulation des modifications en vue de l'analyse des erreurs survenues au cours du déploiement ou de la modification de configuration de la SVM. Pour désactiver la fonction d'annulation des modifications, vous devez modifier le fichier KsvInstaller.exe.config. Ce fichier se trouve sur l'ordinateur où vous avez installé la Console d'administration Kaspersky Security Center.

► *Pour désactiver la fonction d'annulation, procédez comme suit :*

1. Sur l'ordinateur hébergeant la Console d'administration Kaspersky Security Center, ouvrez le fichier Kaspersky.Virtualization.Wizard.exe.config pour modification dans un éditeur de texte. Le dossier d'enregistrement du fichier du journal de fonctionnement de l'Assistant varie en fonction du système d'exploitation utilisé :
 - pour les systèmes d'exploitation 64 bits : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\ ;

- pour les systèmes d'exploitation 32 bits : %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\.

La modification du fichier doit être réalisée par un administrateur.

2. Dans la section `<appSettings></appSettings>`, modifiez la ligne `<add key="disableRollback" value="false" />` de la manière suivante :

```
<add key=" disableRollback" value="true" />
```

3. Enregistrez et fermez le fichier Kaspersky.Virtualization.Wizard.exe.config.

Utilisation des fichiers de trace sur le Light Agent for Windows

Vous pouvez créer un fichier de trace sur une machine virtuelle protégée avec le composant Light Agent for Windows à l'aide de l'application Kaspersky Security.

- *Pour créer des fichiers de trace sur une machine virtuelle protégée avec le composant Light Agent for Windows, procédez comme suit :*

1. Sur la machine virtuelle protégée, ouvrez la fenêtre principale de l'application Kaspersky Security (cf. document *Manuel de l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre **Support Technique**, cliquez sur le bouton **Suivi du système**.

La fenêtre **Informations pour le service d'assistance technique** s'ouvre.

4. Choisissez le niveau de traçage dans la liste déroulante **Niveau**.

Il est recommandé de demander au spécialiste du Support Technique le niveau du traçage requis. S'il n'existe aucune indication de l'expert du Support Technique, il est recommandé d'installer le niveau de traçage **Normal (500)**.

5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation où le problème apparaît.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

L'application créera les fichiers de trace avec le nom unique KSVLA.<numéro de version>_<date et heure de création_GMT>_<PID>.<type de fichier de trace>.log.enc1 dans le dossier %ProgramData %\Kaspersky Lab.

Les fichiers de trace sont conservés sous forme modifiée et inaccessible en lecture sur la machine virtuelle protégée avec le composant Light Agent for Windows pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application.

En outre, vous pouvez recevoir le fichier de trace de la machine virtuelle protégée avec le composant Light Agent for Windows à l'aide des clés du registre. Voir la description sur la page de l'application dans la Base de connaissances (<http://support.kaspersky.ru/13174>).

Utilisation des fichiers de trace sur le Light Agent for Linux

Sur la machine virtuelle protégée avec le composant Light Agent for Linux, vous pouvez créer, enregistrer et supprimer des fichiers de trace.

- *Pour créer un fichier de trace sur la machine virtuelle protégée avec le composant Light Agent for Linux, exécutez la commande suivante :*

```
lightagent trace on [<niveau de traçage>]
```

où :

<niveau de traçage> : niveau du détails des Informations de débogage. Vous avez le choix entre : 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000. Il est recommandé de demander au spécialiste du Support Technique le niveau du traçage requis. Ce paramètre n'est pas obligatoire. Si vous n'indiquez pas la valeur du niveau de traçage, l'application créera les fichiers de trace avec le niveau du détails par défaut à savoir 500.

L'application créera le fichier de trace avec le nom unique LightAgent.<date et heure de création>.log dans le dossier /var/log/kaspersky/lightagent. Vous pouvez enregistrer le fichier de trace créé dans un autre dossier sur la machine virtuelle protégée.

Les fichiers de trace se trouvent sur la machine virtuelle protégée avec le composant Light Agent for Linux dans un format accessible pour la lecture et sont supprimés définitivement lors de la suppression de l'application. L'utilisateur est responsable de la sécurité des informations, et plus exactement du contrôle et de la restriction de l'accès aux informations conservées sur la machine virtuelle protégée avant leur envoi à Kaspersky Lab.

- *Pour enregistrer le fichier de trace sur la machine virtuelle protégée avec le composant Light Agent for Linux, exécutez la commande suivante :*

```
lightagent trace --copyto <chemin vers le fichier de trace> [--overwrite]
```

où :

- copyto <chemin vers le fichier de trace> – enregistrer le fichier de trace dans le dossier indiqué. Indiquez le chemin complet vers le dossier dans lequel vous voulez enregistrer le fichier de trace.
- overwrite : si le dossier indiqué contient un fichier de trace avec ce nom, remplacer ce fichier par le fichier de trace enregistré.

- *Pour désactiver la création d'un fichier de trace sur la machine virtuelle protégée avec le composant Light Agent for Linux, exécutez la commande suivante :*

```
lightagent trace off
```

- *Pour supprimer les fichiers de trace de la machine virtuelle protégée avec le composant Light Agent for Linux, exécutez la commande suivante :*

```
lightagent trace --clear
```

L'application supprime les fichiers de trace du dossier /var/log/kaspersky/lightagent.

A propos des journaux du Serveur d'intégration

Les informations sur le fonctionnement du Serveur d'intégration et de la Console de gestion du Serveur d'intégration sont consignées dans les journaux suivants :

- %ProgramData%\Kaspersky Lab\VIIS\logs\service.log : journal de fonctionnement du Serveur d'intégration ;
- %ProgramData%\Kaspersky Lab\VIIS Console\logs\console.log : journal de fonctionnement de la Console de gestion du Serveur d'intégration.

Vous pouvez ouvrir le journal de fonctionnement du Serveur d'intégration via le lien **Consulter les enregistrements des travaux** dans la section **Paramètres du Serveur d'intégration** de la Console de gestion du Serveur d'intégration.

Les informations contenues dans le journal du Serveur d'intégration ne sont pas envoyées automatiquement à Kaspersky Lab. Vous pouvez utiliser les journaux lorsque vous contactez le Support Technique. Les informations consignées dans les fichiers des journaux peuvent être nécessaires à l'analyse et à l'éclaircissement des raisons de l'apparition d'erreurs dans le fonctionnement du Serveur d'intégration.

Les journaux ne sont pas chiffrés. Il est conseillé de protéger les informations contre l'accès non autorisé.

Vous pouvez modifier le niveau des détails des informations dans les journaux du Serveur d'intégration à l'aide du fichier de configuration. Pour les détails, vous pouvez contacter les experts du Support Technique.

Glossaire

A

Activation de l'application

Procédure d'activation de la licence permettant l'utilisation de l'ensemble des fonctions de la version de l'application tout au long de la durée de validité de la licence.

Analyse heuristique

Technologie de détection des menaces dont les données n'ont pas encore été ajoutées aux bases de l'application Kaspersky Lab. Permet de détecter des fichiers pouvant contenir un programme malveillant absent des bases ou une forme modifiée d'un virus connu.

Analyse sur la base de signatures

Technologie d'identification des menaces qui utilise les bases de l'application Kaspersky Lab contenant les descriptions des menaces connues et les méthodes de leur élimination.

La protection selon cette méthode offre le niveau minimum de sécurité. Conformément aux recommandations des experts de Kaspersky Lab, cette méthode d'analyse est toujours activée.

B

Base des adresses Internet de phishing

Liste des adresses Internet de ressources Web identifiées par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Bases de l'application

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les bases de l'application sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

C

Certificat de licence

Document qui vous est transmis avec le fichier clé ou le code d'activation de Kaspersky Lab.
Le document contient les informations sur la licence fournie.

Clé

Séquence unique de chiffres et de lettres. La clé permet l'utilisation de l'application conformément aux conditions du Contrat de Licence Utilisateur Final (au type de licence, à la durée de validité de la licence, aux restrictions imposées par celle-ci). L'application fonctionne uniquement lorsqu'elle dispose d'une clé.

Clé active

Clé utilisée lors du fonctionnement de l'application.

Clé additionnelle

Clé confirmant le droit d'utilisation de l'application mais qui ne s'utilise pas lors du fonctionnement.

Clé avec limitation en fonction du nombre de cœurs

Clé de l'application de protection des machines virtuelles, quel que soit le type de système d'exploitation installé. En fonction des restrictions imposées par la licence, l'application intervient dans la protection de toutes les machines virtuelles situées sur les hyperviseurs dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

Clé pour poste de travail

Clé de l'application en vue de protéger les machines virtuelles dotées d'un système d'exploitation pour postes de travail.

Clé pour serveur

Clé l'application en vue de protéger les machines virtuelles dotées d'un système d'exploitation pour serveurs.

Code d'activation

Code vous offrant un accès à Kaspersky Lab suite à l'activation d'une licence d'évaluation ou à l'acquisition de la licence commerciale pour l'utilisation de Kaspersky Security. Ce code est nécessaire pour l'activation de l'application.

Le code d'activation est une suite de vingt caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

Contrat de licence utilisateur final

Accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions selon lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

F

Fichier clé

Fichier de type xxxxxxxx.key vous offrant un accès à Kaspersky Lab suite à l'activation d'une licence d'évaluation ou à l'acquisition de la licence commerciale pour l'utilisation de Kaspersky Security. Le fichier clé est nécessaire pour l'activation de l'application.

K

Kaspersky CompanyAccount

Portail prévu pour l'envoi de demandes électroniques à Kaspersky Lab et le suivi de leur traitement par les experts du Support Technique.

Kaspersky Private Security Network

Solution permettant aux utilisateurs des applications antivirus de Kaspersky Lab d'accéder aux données de Kaspersky Security Network sans envoyer d'informations aux serveurs Kaspersky Security Network de Kaspersky Lab de leur côté.

Kaspersky Security Network (KSN)

Infrastructure des services de cloud qui offre l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Web et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

L

Licence

Droit d'utilisation de l'application, limité dans le temps et octroyé sur la base du Contrat de Licence Utilisateur Final.

M

Machine virtuelle protégée

Machine virtuelle sur laquelle le module Light Agent est installé.

O

Objets de démarrage

Ensemble d'applications indispensables au lancement et au fonctionnement du système d'exploitation et des applications installés sur votre machine virtuelle. Le système d'exploitation lance ces objets à chaque démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

Phishing

Type d'escroquerie sur Internet dont le but est d'obtenir un accès non autorisé aux données confidentielles des utilisateurs.

S

Sauvegarde

Dossier de sauvegarde spécifique pour les fichiers qui ont été supprimés ou modifiés durant la réparation.

Serveur d'administration

Composant de l'application Kaspersky Security Center qui remplit la fonction de sauvegarde centralisée des informations relatives aux applications Kaspersky Lab installées sur le réseau de l'organisation et qui gère ces informations.

Source des mises à jour

Ressource qui contient les mises à jour des bases et des composants des applications de Kaspersky Lab. La source de mises à jour pour Kaspersky Security est un stockage du Serveur d'administration du Kaspersky Security Center.

SVM

Secure virtual machine, SVM. Machine virtuelle sur l'hyperviseur où est installé le module Serveur de protection Kaspersky Security.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection des ordinateurs contre différents types de menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top quatre des leaders mondiaux du marché des solutions de sécurité informatique des utilisateurs finaux (classement “ IDC Worldwide Endpoint Security Revenue by Vendor ”). En Russie, d'après les données IDC, Kaspersky Lab est l'éditeur favori de systèmes de protection des ordinateurs pour les particuliers (“ IDC Endpoint Tracker 2014 ”).

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est un groupe international de sociétés avec 34 bureaux dans 31 pays du monde. 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 inclut des applications de protection des données pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des tablettes, des smartphones et d'autres appareils nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail et des appareils nomades, des machines virtuelles, des serveurs de fichiers et des serveurs Web, des passerelles de messagerie et des pare-feu. Le portefeuille de la société comprend également des produits spécialisés de protection contre les attaques DDoS, de protection des environnements grâce à un système automatisé de contrôle de processus et de prévention des escroqueries. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée des organisations de toutes tailles 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, développent les outils d'identification et de neutralisation de ces menaces et ajoutent les signatures de celles-ci 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 pas le fruit du hasard si le noyau logiciel de Kaspersky Antivirus est utilisé dans les produits de nombreux autres éditeurs de logiciels, tels que : 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 et 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. Par exemple, en 2014, selon les résultats des expériences et des recherches effectuées par le laboratoire antivirus autrichien qui fait autorité AV-Comparatives, Kaspersky Lab est devenu un des deux leaders pour la quantité de certificats Advanced+ reçus. Par conséquent, la société a été récompensée du certificat Top Rated. 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 plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab : <http://www.kaspersky.com/fr>

Encyclopédie Virus : <http://www.securelist.fr/>

Laboratoire antivirus : <http://newvirus.kaspersky.com/fr> (pour l'analyse des fichiers et sites suspects)

Forum de Kaspersky Lab : <http://forum.kaspersky.fr>

Informations sur le code tiers

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

Avis de marques déposées

Les marques et marques de service déposées appartiennent à leurs propriétaires respectifs.

CentOS est une marque déposée de la compagnie Red Hat, Inc.

Citrix, Citrix Provisioning Services XenApp, XenDesktop et XenServer sont des marques commerciales de Citrix Systems, Inc. et/ou de ses filiales enregistrées aux États-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc.

Linux est une marque de Linus Torvalds déposée aux États-Unis et dans d'autres pays.

Microsoft, Active Directory, Hyper-V, Windows et Windows Server sont des marques de Microsoft Corporation déposées aux États-Unis et dans d'autres pays.

Red Hat Enterprise Linux est une marque de Red Hat Inc. déposée aux États-Unis et dans d'autres pays.

SUSE est une marque déposée de SUSE LLC enregistrée aux États-Unis et dans d'autres pays.

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere et PowerCLI sont des marques commerciales de VMware, Inc. ou une marque commerciale de VMware, Inc. déposées aux États-Unis ou dans d'autres juridictions.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Index

A

Activation de l'application	46
Architecture de l'application	29

B

Bases de l'application	129
------------------------------	-----

C

Clé	42
Code d'activation	44
Configuration logicielle	23
Configurations logicielle et matérielle	23

E

Etat de la protection	77
-----------------------------	----

F

Fichier clé	44
Fichier de trace	217, 221, 222, 223

I

Image de la SVM	29
-----------------------	----

K

Kaspersky Security Network	192
----------------------------------	-----

L

Licence	40
code d'activation.....	44
Contrat de Licence Utilisateur Final	40
date d'expiration	40
Licence de l'application	40

M

Mise à jour	129
annulation de la dernière mise à jour	138
tâche de mise à jour	121
Modules de l'application	17

P

Plug-in d'administration	29
--------------------------------	----

R

Renouvellement de la licence	59
------------------------------------	----

Réparation de l'infection active	188
--	-----

S

Serveur de protection.....	29
Serveur d'intégration	37
Stratégie	83
configuration des paramètres	117
création	86, 94, 110
SVM.....	29

T

Tâche.....	121
ajout d'une clé	46, 53
restauration d'une mise à jour	138, 140