KASPERSKY lab

Kaspersky Security for Virtualization 4.0 Light Agent

Manuel d'implantation

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 10
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 24
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
Concept de l'administration de l'application via le Kaspersky Security Center 39
Préparatifs pour l'installation de l'application 41
Préparatifs 41
Fichiers indispensables à l'installation de l'application 45
Configurations requises pour les composants de Kaspersky Security Center 49
Configuration des ports utilisés par l'application 50
Comptes utilisateur pour l'installation et l'utilisation de l'application 54
Définition des règles de déplacement des machines virtuelles dans les groupes d'administration 57
Installation de l'application 59
Ordre des étapes d'installation de l'application 60

Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration....61
Installation via l'Assistant....63
Etape 1. Sélection de la langue de localisation....64
Etape 2. Consultation du Contrat de Licence Utilisateur Final....64
Etape 3. Création du mot de passe du compte administrateur du Serveur d'intégration....65
Etape 4. Saisie ou modification du mot de passe du compte utilisateur svm....65
Etape 5. Saisie du numéro du port pour la connexion au Serveur d'intégration....66
Etape 6. Lancement de l'installation et mise à jour des composants....66
Etape 7. Installation et mise à jour des composants....66
Etape 8. Fin du travail de l'Assistant....67
Installation via la ligne de commande....67
Consultation de la liste des plug-ins d'administration de Kaspersky Security....69
Installation du composant Serveur de protection....69
Etape 1. Sélection de l'action....71
Etape 2. Choix des hyperviseurs pour le déploiement des SVM....71
Etape 3. Choix de l'image de la SVM....74
Etape 4. Saisie des paramètres de la SVM....76
Etape 5. Configuration des paramètres réseau de la SVM....77
Etape 6. Saisie des paramètres de connexion au Kaspersky Security Center....78
Etape 7. Création du mot de passe de configuration et du mot de passe du compte root....79
Etape 8. Lancement du déploiement des SVM....79
Etape 9. Déploiement des SVM....79
Etape 10. Achèvement du déploiement des SVM....80
Fin de l'installation du composant Serveur de protection....81
Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles....81
Installation du composant Light Agent for Windows....83
Installation du Light Agent for Windows via Kaspersky Security Center....85
Création du paquet d'installation du Light Agent for Windows....85
Configuration des paramètres du paquet d'installation du Light Agent for Windows....88
Installation du Light Agent for Windows à l'aide de l'assistant d'installation....89

Etape 1. Fenêtre d'accueil de l'Assistant d'installation 91
Etape 2. Consultation du Contrat de Licence Utilisateur Final 91
Etape 3. Sélection du type d'installation....92
Etape 4. Sélection des composants du Light Agent pour l'installation 93
Etape 5. Sélection du dossier d'installation....94
Etape 6. Configuration de la zone de confiance....94
Etape 7. Lancement de l'installation....96
Etape 8. Installation du composant Light Agent for Windows 97
Etape 9. Fin de l'installation 97
Installation du Light Agent for Windows via la ligne de commande....97
Installation du Light Agent for Windows via l'éditeur des stratégies de groupe du service de catalogues....100
Installation du Light Agent for Windows sur un modèle de machine virtuelle....102
Compatibilité avec la technologie Citrix Provisioning Services....104
Compatibilité avec la technologie Citrix Personal vDisk....104
Modification de la composition des composants installés du Light Agent for Windows....105
Installation du composant Light Agent for Linux....107
Installation du Light Agent for Linux via Kaspersky Security Center....108
Préparation de la distribution du Light Agent for Linux....109
Création du paquet d'installation du Light Agent for Linux 110
Installation du Light Agent for Linux via la ligne de commande....111
Configuration initiale du Light Agent for Linux en mode interactif 112
Configuration initiale du Light Agent for Linux en mode silencieux 113
Modifications dans le Kaspersky Security Center après l'installation de l'application....114
Activation de l'application....116
A propos de l'activation de l'application....116
Conditions pour activer l'application à l'aide d'un code d'activation....118
Particularités de l'activation de l'application avec plusieurs types de clés....119
Procédure d'activation de l'application....120
Ajout d'une clé dans le stockage des clés de Kaspersky Security Center....121
Création d'une tâche d'activation de l'application....123
Etape 1. Sélection de l'application et du type de tâche....124
Etape 2. Ajout d'une clé 124

Etape 3. Choix de la SVM 126
Etape 4. Définition des paramètres de programmation de la tâche 127
Etape 5. Définition du nom de la tâche 128
Etape 6. Fin de la création de la tâche 128
Lancement de la tâche d'activation de l'application 129
Mise à jour des bases antivirus 130
A propos de la mise à jour des bases antivirus 130
Création d'une tâche de mise à jour sur le Serveur de protection 132
Lancement et arrêt de la tâche de mise à jour sur le Serveur de protection 134
Lancement et arrêt de l'application 135
Etat de la protection de la machine virtuelle 137
Mise à jour de la version précédente de l'application 138
Séquence de mise à jour de la version précédente de l'application 138
A propos de la mise en jour des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration 140
Procédure de conversion des stratégies et des tâches de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 142
Etape 1. Sélection de l'application requérant la conversion des stratégies et des tâches 143
Etape 2. Conversion des stratégies 143
Etape 3. Conversion des tâches 144
Etape 4. Fin de l'Assistant de conversion des stratégies et des tâches 144
A propos de la mise à jour du composant Light Agent for Windows 145
Modification de la configuration des SVM 146
Sélection de l'action 148
Choix de la SVM pour la modification de la configuration 149
Saisie du mot de passe de configuration 151
Modifier les adresses des hyperviseurs ou des serveurs de gestion de l'infrastructure virtuelle indiquées sur les machines virtuelles de protection 152
Modification de la liste des réseaux virtuels pour les SVM 152
Modification des paramètres réseau des SVM 153
Modification des paramètres de connexion au Kaspersky Security Center 154
Modification du mot de passe de configuration et des paramètres du compte root 155
Modification des paramètres de connexion au serveur VMware vCenter 155

Modification des paramètres de connexion aux hyperviseurs Microsoft Windows Server (Hyper-V) 156
Modification des paramètres de connexion aux hyperviseurs Citrix XenServer 157
Modification des paramètres de connexion aux hyperviseurs KVM....158
Lancement de la modification de la configuration des SVM 159
Modification de la configuration des SVM....159
Fin de la modification de la configuration des SVM 160
Consultation et modification des paramètres du Serveur d'intégration 161
Lancement de la console de gestion du Serveur d'intégration 161
Modification des paramètres du Serveur d'intégration....163
Modification des mots de passe des comptes utilisateur du Serveur d'intégration ..164
Suppression de l'application 166
Ordre des étapes de suppression de l'application 167
Suppression du composant Serveur de protection 168
Suppression du composant Light Agent for Windows 168
Suppression du Light Agent for Windows à l'aide de l'assistant d'installation 169
Etape 1. Confirmation de la suppression du composant Light Agent for Windows 170
Etape 2. Suppression du composant Light Agent for Windows....170
Suppression du Light Agent for Windows via la ligne de commande 170
Suppression du Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues 171
Suppression du Light Agent for Windows dans le modèle de machines virtuelles 172
Suppression du composant Light Agent for Linux 173
Suppression de l'Agent d'administration de Kaspersky Security Center des machines virtuelles 174
Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration....175
Contacter le Support Technique 176
Modes d'obtention du Support Technique 176
Support Technique par téléphone 177
Support Technique via Kaspersky CompanyAccount....177

Application. Description du journal de l'Assistant.....179
Glossaire.....182
AO Kaspersky Lab.....187
Informations sur le code tiers.....189
Avis de marques déposées.....190
Index.....191

Présentation du manuel

Le manuel d'implantation Kaspersky Security for Virtualization 4.0 Light Agent (ensuite appelé aussi “ Kaspersky Security ”) est adressé aux spécialistes de l'installation et de l'administration de Kaspersky Security, et aux spécialistes de 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.

Les informations fournies dans le présent manuel vous permettront de réaliser les opérations suivantes :

- planification de l'installation de l'application (en tenant compte des principes de fonctionnement de l'application, de la configuration requise, des schémas typiques de déploiement et des particularités de la compatibilité avec d'autres applications) ;
- préparation de l'installation, installation et activation de Kaspersky Security ;
- configuration de l'application après l'installation ;
- mise à jour et la suppression de l'application.

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 10

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.

Configuration logicielle et matérielle (cf. page 24)

Cette section fournit les informations sur les configurations matérielle et logicielle requises pour Kaspersky Security.

Architecture de l'application (cf. page 29)

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

Préparation de l'installation de l'application (cf. page 41)

Cette section présente les étapes de préparation à réaliser avant d'installer l'application Kaspersky Security.

Installation de l'application (cf. page 59)

Cette section explique, étape par étape, comment installer l'application, et décrit les modifications apportées à Kaspersky Security Center après l'installation.

Activation de l'application (cf. page 116)

Cette section explique comme activer l'application.

Mise à jour des bases antivirus (cf. page 130)

Cette section explique la mise à jour des bases antivirus.

Lancement et arrêt de l'application (cf. page 135)

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

Etat de la protection de la machine virtuelle (cf. page 137)

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

Mise à jour de la version antérieure de l'application (cf. page 138)

Cette section explique comment réaliser la mise à jour depuis une version antérieure de l'application.

Modification de la configuration des SVM (cf. p. 146)

Cette section fournit des informations sur la modification de la configuration des SVM dotées du module Serveur de protection.

Consultation et modification des paramètres du Serveur d'intégration (cf. page 161)

Cette section explique comment consulter et modifier les paramètres du Serveur d'intégration.

Suppression de l'application (cf. page 166)

Cette section explique comment supprimer l'application Kaspersky Security de l'infrastructure virtuelle.

Contacter le Support Technique (cf. page 176)

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

Application. Description du journal de l'Assistant (cf. page 179)

Cette section décrit les informations inscrites dans le journal de l'assistant pendant le déploiement des SVM et la modification de la configuration de ces dernières.

Glossaire (cf. page 182)

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

AO Kaspersky Lab (cf. page 187)

Cette section contient des informations sur AO Kaspersky Lab.

Information sur le code tiers (cf. page 189)

Cette section contient des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page 190)

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".
La *mise à jour*, c'est... L'événement *Bases dépassées* survient.	Les éléments de texte suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.

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

Sources d'informations sur l'application

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

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

Dans cette section

Sources pour 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 176).

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

Page de Kaspersky Security sur le site de Kaspersky Lab

La page de l'application (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

NOUVEAUTES 22

Distribution 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.

Outre la *protection en temps réel* assurée par les composants de l'application, il est conseillé de réaliser une *analyse* périodique des machines virtuelles et de leurs modèles à la recherche d'éventuels virus et d'autres applications présentant une menace.

La *mise à jour* des bases de l'application utilisées pour détecter les menaces est requise pour maintenir l'application Kaspersky Security à jour.

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 la présence éventuelle de 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 ;

- via la ligne de commande pour Light Agent for Linux ;

- 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.

- Il est possible de désactiver le lancement de l'interface locale de Light Agent pour Windows sur la machine virtuelle protégée. La désactivation du lancement de l'interface permet de diminuer l'utilisation de la mémoire, y compris lors de l'utilisation sur des machines virtuelles dotées d'un système d'exploitation pour serveur 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 (cf. section "Fichiers indispensables à l'installation de l'application" à la page 45), y compris l'image de la SVM (machine virtuelle de protection) dotée du système d'exploitation 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, l'application Kaspersky Security Center d'une des versions suivantes doit être installée :

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

> Ce manuel décrit l'utilisation avec la version Kaspersky Security Center 10 Service Pack 2.

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'un 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 LTSB / RS1 (version 32 / 64 bits) ;
- Windows Server 2008 Service Pack 2 toutes éditions (en mode d'installation complète ou en mode Server Core) (version 32 / 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 pour l'installation et l'utilisation 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 d'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 ou 10.1.1-X représente le numéro de version. 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).

Le fonctionnement du Serveur d'intégration, de la Console de gestion du Serveur d'intégration et des plug-ins d'administration de Kaspersky Security requiert la plateforme Microsoft.NET Framework 4.6. La plateforme sera installée automatiquement 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

Concept de l'administration de l'application via le Kaspersky Security Center 39

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 présentant une menace, 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 ;
- via la ligne de commande pour Light Agent for Linux ;
- 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 administrer le fonctionnement du Light Agent installé sur les machines virtuelles protégées avec le Kaspersky Security Center, il est nécessaire d'installer l'Agent d'administration sur ces machines virtuelles (cf. section "Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles" à la page 81). 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 où la Console d'administration de Kaspersky Security Center est basée (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 61).

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.
- Recherche la présence de virus et autres applications malveillantes dans les fichiers de toutes les machines virtuelles sur lesquelles Light Agent est installé.
- 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. L'application utilise les services KSN si vous avez accepté les conditions de participation au programme Kaspersky Security Network pendant l'installation.
- 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 composants de l'application indispensables au bon fonctionnement du Light Agent se chargent à partir du dossier de la SVM vers la machine virtuelle protégée.
- Contrôle les clés et les restrictions de licence.

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. Déployez la SVM sur chaque hyperviseur qui appartient au cluster d'hyperviseurs (cf. section "Installation du composant Serveur de protection" à la page 69). Si vous souhaitez effectuer une migration à chaud de la SVM entre les noeuds du cluster, placez le dossier avec les fichiers de la SVM sur le volume partagé de cluster.

2. A 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. 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'utilisent les composants Light Agent for Windows pour la détection des SVM dans la stratégie de ces composants ou dans l'interface locale.

Vous pouvez choisir la méthode qu'utilisent les composants Light Agent for Linux pour la détection des SVM dans la stratégie de ces composants.

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.

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 la Console de gestion du Serveur d'intégration (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 61).

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 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 des composants Light Agent for Windows au Serveur d'intégration s'effectue dans la stratégie ou dans l'interface locale du composant Light Agent pour Windows.

   La configuration des paramètres de connexion des composants Light Agent for Linux au Serveur d'intégration s'effectue dans la stratégie du composant Light Agent pour Linux.

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 sa Console de gestion (cf. section "Consultation et modification des paramètres du Serveur d'intégration" à la page 161).

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* déterminent les paramètres de protection des machines virtuelles et les paramètres de fonctionnement des composants Light Agent et du Serveur de protection.
- Les *tâches* prennent en charge les fonctions de l'application telles que l'ajout d'une clé, l'analyse des machines virtuelles ou la mise à jour des bases de données et des composants de l'application.

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.

Les informations relatives à la configuration des stratégies et des tâches figurent dans le *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*.

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

Préparatifs pour l'installation de l'application

Cette section présente les étapes de préparation à réaliser avant d'installer l'application Kaspersky Security.

Dans cette section

Préparatifs 41

Fichiers indispensables à l'installation de l'application 45

Configurations requises pour les composants de Kaspersky Security Center 49

Configuration des ports utilisés par l'application 50

Comptes utilisateur pour l'installation et l'utilisation de l'application 54

Définition des règles de déplacement des machines virtuelles dans les groupes d'administration 57

Préparatifs

Avant de passer à l'installation des composants de Kaspersky Security, il est nécessaire de réaliser les opérations suivantes.

Actions générales

- Vérifiez la sélection de composants de Kaspersky Security Center (cf. section "Configuration requise pour les composants de Kaspersky Security Center" à la page 49), ainsi que l'adaptation des composants de Kaspersky Security Center et des composants de l'infrastructure virtuelle aux configurations matérielle et logicielle de Kaspersky Security (cf. section " Configurations logicielle et matérielle requises " à la page 24).
- Confirmez qu'aucun logiciel antivirus n'est installé sur les machines virtuelles que vous avez l'intention de protéger à l'aide de Kaspersky Security.

- Téléchargez les fichiers indispensables à l'installation de l'application depuis le site Internet de Kaspersky Lab (cf. section "Fichiers indispensables à l'installation de l'application" à la page 45).

- Vérifiez que l'image SVM n'est pas endommagée. Pour en savoir plus sur les procédés de vérification de l'image de la SVM, consultez la page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/ksv4). Vous pouvez aussi analyse l'intégrité de l'image de la SVM au cours de son déploiement. La vérification a lieu au moment de la sélection de l'image de la SVM dans l'Assistant d'installation (cf. section "Etape 3. Choix de l'image de la SVM" à la p. 74). Si le fichier de l'image est endommagé ou si la version de l'image n'est pas prise en charge, l'Assistant affiche un message d'erreur.

- Vérifier que la configuration du réseau ou des applications assurant le contrôle du trafic entre les machines virtuelles permet le trafic réseau entre les ports utilisés lors de l'installation et du fonctionnement de l'application (cf. section " Configuration des ports utilisés par l'application " à la page 50).

- Si l'adressage IP dynamique est utilisé sur le réseau, permettre le routage du trafic réseau depuis la SVM jusqu'à l'ordinateur sur lequel est installé le Serveur d'administration de Kaspersky Security Center.

- Si vous souhaitez que les machines virtuelles dotées de composants Kaspersky Security figurent automatiquement dans le groupe d'administration dès l'installation de l'application, il convient de créer des groupes d'administration dans la Console de gestion de Kaspersky Security Center et configurez les règles de placement automatique des machines virtuelles dans les groupes d'administration (cf. section "Configuration des règles de placement automatique des machines virtuelles dans les groupes d'administration" à la page 57).

Hyperviseur Microsoft Windows Server (Hyper-V)

Si l'infrastructure virtuelle compte la présence d'un hyperviseur Microsoft Windows Server (Hyper-V), il faudra également réaliser les opérations suivantes avant de passer à l'installation des composants de Kaspersky Security :

- Assurez-vous que le paquet de services d'intégration (Integration Services) est bien installé sur les machines virtuelles que vous souhaitez protéger.
- Assurez-vous que la ressource réseau commune ADMIN$ est active sur l'hyperviseur. Il est nécessaire de définir au préalable le rôle du serveur de fichiers (File Server) avec l'Assistant de configuration du serveur pour activer la ressource réseau ADMIN$ commune sur les hyperviseurs et Microsoft Windows Server 2012 R2 Hyper-V.
- Assurez-vous que le disque sur lequel se trouve la ressource réseau commune ADMIN$, dispose de suffisamment de place pour accueillir l'image de la SVM. Lors de l'installation du composant Serveur de protection, l'image de la SVM est copiée sur la ressource réseau commune ADMIN$, puis elle est transférée vers le dossier indiqué dans l'Assistant d'installation.
- Assurez-vous que les hyperviseurs qui n'appartiennent pas au domaine Active Directory sont dotés de l'application d'administration à distance Windows Remote Management (WinRM) version 3.0. Windows Remote Management (WinRM) version 3.0 figure dans le paquet d'installation de Windows Management Framework 3.0, que vous pouvez télécharger depuis le site de Microsoft via le lien http://www.microsoft.com/fr-fr/download/details.aspx?id=34595
- Si vous souhaitez utiliser un compte de domaine pour connecter la SVM à l'hyperviseur, assurez-vous que les conditions suivantes sont remplies :
  - La SVM doit pouvoir identifier l'adresse de l'hyperviseur à l'aide du serveur de nom de domaine (DNS) du domaine où se trouve l'hyperviseur sur lequel la SVM est déployée.
  - Le serveur DNS possède un enregistrement direct et inverse pour la SVM.
  - Les zones contenant les enregistrements concernant la SVM et l'hyperviseur sur lequel elle est déployée sont intégrées avec Active Directory.

- L'ordinateur sur lequel l'Assistant d'installation du composant Serveur de protection peut autoriser les noms des hyperviseurs sur lesquels la SVM est déployée.

- Si vous souhaitez que le nom d'utilisateur et le mot de passe du compte pour la connexion à l'hyperviseur qui ont été indiqués au moment du déploiement de la SVM soient transmis de façon chiffrée, vous pouvez configurer une connexion protégée à l'aide d'un certificat SSL entre l'hyperviseur sur lequel la SVM sera déployée et l'ordinateur où est installée la Console d'administration de Kaspersky Security Center.

Hyperviseur VMware ESXi

Si l'infrastructure virtuelle compte la présence d'un hyperviseur VMware ESXi, il faudra également réaliser les opérations suivantes avant de passer à l'installation des composants de Kaspersky Security :

- Assurez-vous que le paquet VMware Tools est bien installé sur les machines virtuelles que vous souhaitez protéger.

- Si l'ordinateur sur lequel est installée la Console d'administration de Kaspersky Security Center se connecte au serveur VMware vCenter via un serveur proxy, il faut s'assurer que les machines virtuelles sont accessibles via le serveur proxy.

Hyperviseur Citrix XenServer

Si l'infrastructure virtuelle compte la présence d'un hyperviseur Citrix XenServer, il faudra également réaliser les opérations suivantes avant de passer à l'installation des composants de Kaspersky Security :

- Assurez-vous que les machines virtuelles que vous souhaitez protéger sont équipées de l'application XenTools.

- Si vous utilisez un schéma de licence sur la base du nombre de noyaux dans les processeurs physiques sur les hyperviseurs, il faut s'assurer que le fichier de configuration /etc/ssh/sshd_config sur l'hyperviseur renferme la directive Ciphers avec les chiffres et les fonctions de hash suivants pris en charge par la SVM :

  - aes256-cbc ;

  - aes256-ecb ;

- aes256-cfb ;
- aes256-ofb ;
- aes256-ctr

Fichiers indispensables à l'installation de l'application

Avant d'installer l'application, vous devez télécharger depuis le site de Kaspersky Lab tous les fichiers indispensables à l'installation des composants de l'application Kaspersky Security.

Plug-in d'administration de Kaspersky Security et Serveur d'intégration

En vue d'installer les plug-ins d'administration de Kaspersky Security, le Serveur d'intégration et sa Console de gestion, vous devez télécharger le fichier SecurityCenterComponents_4.0.X.X_setup.exe depuis le site de Kaspersky Lab. Le chiffre 4.0.X.X désigne la version de l'application.

Ce fichier doit être placé sur l'ordinateur où l'application Kaspersky Security Center est installée.

Serveur de protection

Pour déployer ou la mise à jour de la SVM, il faut télécharger depuis le site de Kaspersky Lab une archive qui contient l'image de la SVM et le fichier de configuration au format XML (fichier de description de l'image).

La distribution de Kaspersky Security contient les archives suivantes en vue de l'installation du Serveur de protection sur les hyperviseurs de différents types :

- SVM.image_Hyper-V_4.0.X.X.vhdx.zip, où 4.0.X.X désigne la version de l'application. Les archives sont utilisées pour l'installation du Serveur de protection sur l'hyperviseur Microsoft Windows Server (Hyper-V) ; elles contiennent l'image de la SVM au format VHDX et le fichier de configuration SVM.image_manifest_4.0.X.X.xml, où 4.0.X.X désigne la version de l'application.
- SVM.image_XenServer_4.0.X.X.xva.zip, où 4.0.X.X désigne la version de l'application. Les archives sont utilisées pour l'installation du Serveur de protection sur l'hyperviseur Citrix XenServer ; elles contiennent l'image de la SVM au format XVA et le fichier de configuration SVM.image_manifest_4.0. X.X.xml.

- SVM.image_VMware_4.0.X.X.ova, où 4.0.X.X désigne la version de l'application. Les archives sont utilisées pour l'installation du Serveur de protection sur l'hyperviseur VMware ESXi ; elles contiennent l'image de la SVM au format OVA et le fichier de configuration SVM.image_manifest_4.0. X.X.xml.

- SVM.image_KVM_4.0.X.X.raw.gz, où 4.0.X.X désigne la version de l'application. Les archives sont utilisées pour l'installation du Serveur de protection sur l'hyperviseur KVM ; elles contiennent l'image SVM au format RAW et le fichier de configuration SVM.image_manifest_4.0. X.X.xml.

Le fichier de l'image de la SVM et le fichier de configuration au format XML doivent être placés dans le même dossier sur l'ordinateur accueillant la Console d'administration de Kaspersky Security Center ou dans le même dossier sur la ressource réseau auquel le compte de l'utilisateur effectuant l'installation dispose d'un accès en lecture. Si vous souhaitez installer le Serveur de protection sur des hyperviseurs de différents types, il faudra placer dans le même dossier les fichiers des images de la SVM pour chaque type d'hyperviseur ainsi que le fichier de configuration au format XML.

Light Agent for Windows

Pour l'installation du composant Light Agent for Windows, vous devez charger du site Internet de Kaspersky Lab l'archive autoextractible Agent_4.0. X.X_sfx_<identifiant de la langue>.exe, où 4.0.X.X. désigne la version de l'application ; <identifiant de la langue> désigne l'identifiant de la langue de Light Agent for Windows : ru, en, fr, de, etc.

Vous pouvez utiliser le fichier Agent_4.0. X.X_sfx_<identifiant de la langue>.exe comme distribution de l'application pour la création du package d'installation de Light Agent for Windows dans Kaspersky Security Center (cf. section "Création du paquet d'installation du Light Agent for Windows" à la p. 85).

Si vous souhaitez créer un paquet d'installation pour installer Light Agent for Windows sur des machines virtuelles qui utilisent la technologie Citrix Provisioning Services ou si vous souhaitez l'installer à l'aide de l'Assistant d'installation, vous devez décompacter au préalable l'archive Agent_4.0.X.X_sfx_<identifiant de la langue>.exe.

L'archive Agent_4.0. X.X_sfx_<identifiant de la langue>.exe contient les fichiers suivants :

- incompatible.txt : contient la liste des applications incompatibles avec Kaspersky Security. Il intervient lors de l'utilisation de Light Agent for Windows ;
- Ksvla.kud : fichier de description de l'application. Il intervient dans la création du paquet d'installation de Light Agent for Windows dans Kaspersky Security Center ;
- Ksvla_x64.msi : intervient dans l'installation de Light Agent for Windows sur un système d'exploitation 64 bits ;
- Ksvla_x86.msi : intervient dans l'installation de Light Agent for Windows sur un système d'exploitation 32 bits ;
- license.txt : contient le texte du Contrat de licence utilisateur final reprenant les conditions d'utilisation de l'application ;
- setup.exe : intervient dans l'installation de Light Agent for Windows à l'aide de l'Assistant d'installation.

Light Agent for Linux

Pour l'installation du composant Light Agent for Linux, vous devez charger du site Internet de Kaspersky Lab les fichiers suivants :

- paquet d'installation de Light Agent for Linux (en fonction du système d'exploitation de la machine virtuelle et du gestionnaire de paquets utilisé dans le système d'exploitation) :
  - lightagent_4.0.X-X_amd64.deb : paquet au format DEB pour système d'exploitation 64 bits ;
  - lightagent_4.0.X-X_i386.deb : paquet au format DEB pour système d'exploitation 32 bits ;
  - lightagent-4.0.X-X.x86_64.rpm : paquet au format RPM pour système d'exploitation 64 bits ;
  - lightagent-4.0.X-X.i686.rpm : paquet au format RPM pour système d'exploitation 32 bits ;

- archive d'installation de Light Agent for Linux dans le Kaspersky Security Center (en fonction du gestionnaire de paquets utilisé dans le système d'exploitation de la machine virtuelle) :
  - lightagent-4.0.X-X_deb-<identifiant de la langue>.tar.gz pour l'installation à partir du paquet au format DEB ;
  - lightagent-4.0.X-X_rpm-<identifiant de la langue>.tar.gz pour l'installation à partir du paquet au format RPM ;

où :

- 4.0.X : désigne la version de l'application ;
- <identifiant de la langue> désigne l'identifiant à deux lettres de la langue : ru, en, fr, de, etc.

Les archives lightagent-4.0.X-X_deb - <identifiant de la langue>.tar.gz et lightagent-4.0.X-X_rpm-<identifiant de la langue>.tar.gz contiennent les fichiers suivants nécessaires à l'installation du Light Agent par le Kaspersky Security Center (cf. section "Installation du Light Agent for Linux via Kaspersky Security Center" à la p. 108) :

- akinstall.sh : utilisé pour l'installation du Light Agent for Linux via Kaspersky Security Center ;
- license.txt : contient le texte du Contrat de licence utilisateur final reprenant les conditions d'utilisation de l'application ;
- lightagent.ini ; fichier de configuration initiale. Utilisé pour l'installation de Light Agent for Linux à partir de la ligne de commande ;
- lightagent.kud : fichier de description de l'application. Utilisé pour la création du paquet d'installation de Light Agent for Windows dans Kaspersky Security Center ;

Agent d'administration Kaspersky Security Center.

Si vous voulez gérer le fonctionnement du composant Light Agent for Linux à l'aide de Kaspersky Security Center, sur la machine virtuelle, où ce composant sera installé, il convient d'installer l'Agent d'administration de Kaspersky Security Center version 10.1.1-X ou 10.1.1-X représente le numéro de version.

Pour l'installation du composant Agent d'administration version 10.1.1-X, vous devez charger à partir du site Internet de Kaspersky Lab un des paquets suivants (en fonction du gestionnaire de paquets utilisé dans le système d'exploitation de la machine virtuelle) :

- klnagent-10.1.1-X.i386.rpm ;
- klnagent_10.1.1-X_i386.deb.

Sur la machine virtuelle avec le composant Light Agent for Windows, vous pouvez utiliser l'Agent d'administration qui fait partie de la distribution de Kaspersky Security Center 10 Service Pack 2 ou Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

Configurations requises pour les composants de Kaspersky Security Center

L'installation et le fonctionnement de l'application Kaspersky Security nécessitent les composants Kaspersky Security Center suivants :

- Serveur d'administration.

  Les services suivants doivent être configurés sur le Serveur d'administration :

  - Service Activation Proxy : utilisé lors de l'activation de l'application Kaspersky Security. La configuration du service Activation Proxy s'opère dans les propriétés du Serveur d'administration de Kaspersky Security Center. Il est impossible d'activer l'application avec un code d'activation si le service Activation Proxy est déconnecté.
  - Service KSN Proxy : assure l'échange de données entre l'application Kaspersky Security et Kaspersky Security Network. La configuration du service KSN Proxy s'opère dans les propriétés du Serveur d'administration de Kaspersky Security Center. Si le service KSN Proxy est désactivé, l'échange de données entre Kaspersky Security et Kaspersky Security Network n'a pas lieu.

    Vous pouvez consulter les informations détaillées sur les services Activation Proxy et KSN Proxy dans la documentation de Kaspersky Security Center.

- Console d'administration. La Console d'administration doit être installée sur le poste de travail de l'administrateur.
- Agent d'administration. L'Agent d'administration assure l'interaction entre le Serveur d'administration et les machines virtuelles dotées de l'application Kaspersky Security.

  Il est nécessaire d'installer l'Agent d'administration sur l'ensemble des machines virtuelles que vous souhaitez protéger (cf. section "Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles" à la page 81).

  > Sur la machine virtuelle, où Light Agent for Linux sera installé, vous devez installer le composant Agent d'administration version 10.1.1.-X ou 10.1.1-X représente le numéro de version.

  Sur la machine virtuelle où Light Agent for Windows sera installé, vous pouvez installer l'Agent d'administration qui fait partie de la distribution de Kaspersky Security Center 10 Service Pack 2 ou Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

  Il n'est pas nécessaire d'installer l'Agent d'administration sur les SVM de Kaspersky Security car ce composant est inclus dans leurs images.

Configuration des ports utilisés par l'application

Pour l'installation et le fonctionnement des composants de l'application dans les configurations réseau et les logiciels utilisés pour le contrôle du trafic entre les machines virtuelles, il est nécessaire d'ouvrir les ports décrits dans le tableau ci-dessous.

Tableau 2. Ports utilisés par l'application

Port et protocole	Direction	Définition et description
80 TCP 443 TCP	De l'Assistant de déploiement et de modification de la configuration dans Kaspersky Security Center vers le serveur VMware vCenter.	Pour le déploiement d'une SVM sur l'hyperviseur VMware ESXi via le serveur VMware vCenter.
135 TCP / UDP 445 TCP / UDP	De l'Assistant de déploiement et de modification de la configuration dans Kaspersky Security Center vers l'hyperviseur Microsoft Windows Server (Hyper-V).	Pour le déploiement d'une SVM sur un hyperviseur Microsoft Windows Server (Hyper-V).
80 TCP 443 TCP	De l'Assistant de déploiement et de modification de la configuration dans Kaspersky Security Center vers un hyperviseur Citrix XenServer.	Pour le déploiement de la SVM sur un hyperviseur Citrix XenServer.
22 TCP	De l'Assistant de déploiement et de modification de la configuration dans Kaspersky Security Center vers un hyperviseur KVM.	Pour le déploiement de la SVM sur un hyperviseur KVM.
22 TCP	De l'Assistant de déploiement et de modification de la configuration dans Kaspersky Security Center vers SVM.	Pour la modification de la configuration des SVM.
80 TCP 443 TCP	De la SVM vers VMware vCenter Server.	Pour la coopération entre SVM et un hyperviseur VMware ESXi avec l'aide de VMware vCenter Server.
135 TCP / UDP 445 TCP / UDP 5985 TCP 5986 TCP	De la SVM vers un hyperviseur Microsoft Windows Server (Hyper-V).	Pour l'interaction d'une SVM avec un hyperviseur Microsoft Windows Server (Hyper-V).

Port et protocole	Direction	Définition et description
22 TCP 80 TCP 443 TCP	De la SVM vers un hyperviseur Citrix XenServer.	Pour la coopération entre la SVM et un hyperviseur Citrix XenServer.
22 TCP	De la SVM vers un hyperviseur KVM.	Pour la coopération entre la SVM et un hyperviseur KVM.
9876 UDP	De Light Agent vers le groupe Multicast.	Pour la réception par Light Agent des informations sur toutes les SVM disponibles pour une connexion sur tous les hyperviseurs de l'infrastructure virtuelle à l'aide de la multidiffusion (Multicast).
9876 UDP	De la SVM vers le groupe Multicast ou vers Light Agent.	Pour le transfert d'information à Light Agent sur les SVM disponibles à l'aide de la multidiffusion (Multicast) ou d'une liste d'adresses de la SVM.
7271 TCP	De la SVM vers le Serveur d'intégration.	Pour la coopération entre SVM et le Serveur d'intégration.
7271 TCP	De Light Agent vers le Serveur d'intégration.	Pour la coopération entre Light Agent et le Serveur d'intégration.
8000 UDP	De Light Agent vers la SVM.	Pour que Light Agent puisse recevoir les informations relatives à l'état de la SVM.
11111 TCP	De Light Agent vers la SVM.	Pour la transmission des demandes de service (par exemple, pour obtenir des informations sur la licence) de Light Agent vers la SVM.
9876 TCP	De Light Agent vers la SVM.	Pour la transmission des demandes d'analyse des fichiers de Light Agent vers la SVM.

Port et protocole	Direction	Définition et description
80 TCP	De Light Agent vers la SVM.	Pour la mise à jour des bases et des modules de l'application sur Light Agent.
15000 UDP	De Kaspersky Security Center vers la SVM.	Pour l'administration de l'application via le Kaspersky Security Center sur la SVM.
15000 UDP	De Kaspersky Security Center vers Light Agent.	Pour l'administration de l'application via le Kaspersky Security Center sur les Light Agent.
13000 TCP	De la SVM vers Kaspersky Security Center.	Pour l'administration de l'application via le Kaspersky Security Center sur la SVM.
14000 TCP	De Light Agent vers Kaspersky Security Center.	Pour l'administration de l'application via le Kaspersky Security Center sur les Light Agent.

Si le Light Agent installé sur la machine virtuelle protégée reçoit les informations relatives aux SVM via une diffusion multiple (Multicast) (cf. section "Connexion de la machine virtuelle protégée à la SVM" à la page 34), la connexion du Light Agent au Serveur de protection installé sur la SVM requiert le routage des paquets selon le protocole IGMP version 3 pour le groupe 239.255.76.65:9876.

Suite à l'installation, le Light Agent configure le Pare-feu Microsoft Windows afin qu'il autorise le trafic entrant et sortant pour le processus avp.exe. Si une stratégie de domaine est utilisée pour le Pare-feu Microsoft Windows, il sera nécessaire d'y configurer une règle pour les connexions entrantes et sortantes du processus avp.exe. Si un autre Pare-feu est utilisé, il sera nécessaire de configurer une règle de connexion concernant le processus avp.exe pour ce Pare-feu.

Si vous utilisez un hyperviseur Citrix XenServer ou VMware ESXi et que le mode proximité est activé sur la carte réseau du système d'exploitation invité de la machine virtuelle, ce système reçoit toutes les trames Ethernet qui transitent via le commutateur virtuel si la stratégie VLAN l'autorise. Ce mode peut être utilisé pour la surveillance et l'analyse du trafic sur des segments du réseau où la SVM et la machine virtuelle protégée s'exécutent. Vu que le trafic entre la SVM et la machine virtuelle protégée n'est pas chiffré et circule ouvertement, les précautions de sécurité impliquent d'éviter d'utiliser le mode de promiscuité sur les segments du réseau présentant une SVM active. Si ce mode est indispensable, il est possible d'assurer la surveillance du trafic par les autres machines virtuelles en vue de détecter les tentatives d'accès non autorisé au réseau et de mettre en œuvre les débogages. Pour ce faire, il est nécessaire de configurer des restrictions adaptées, visant à protéger le trafic circulant entre la SVM et les machines virtuelles protégées contre tout accès non autorisé.

Comptes utilisateur pour l'installation et l'utilisation de l'application

L'installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration nécessite le compte utilisateur qui fait partie du groupe d'administrateurs locaux sur l'ordinateur où l'installation s'exécute (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la p. 61).

Si l'ordinateur sur lequel est installée la Console d'administration de Kaspersky Security Center appartient au domaine Microsoft Windows, pour le lancement de la Console de gestion du Serveur d'intégration, vous devez utiliser un compte utilisateur appartenant au groupe KLAdmins ou au groupe d'administrateurs locaux.

Hyperviseur VMware ESXi

Pour déployer et utiliser une SVM sur un hyperviseur VMware ESXi, il faut travailler avec les comptes utilisateur suivants :

- Pour déployer et modifier la configuration d'une SVM, il faut un compte administrateur doté des autorisations suivantes :
  - Datastore.Allocate space

- Datastore.Low level file operations
- Datastore.Remove file
- Global.Cancel task
- Global.Licenses
- Host.Config.Virtual machine autostart configuration
- Host.Inventory.Modify cluster
- Network.Assign network
- Tasks.Create task
- vApp.Import
- Virtual machine.Configuration.Add new disk
- Virtual machine.Configuration.Add or remove device
- Virtual machine.Interaction.Power Off
- Virtual machine.Interaction.Power On
- Virtual machine.Inventory.Create new
- Virtual machine.Inventory.Remove
- Virtual machine.Provisioning.Customize

- Afin d'utiliser les SVM, il est indispensable de disposer d'un compte auquel a été attribué le rôle système préinstallé ReadOnly.

> Les autorisations doivent être attribuées aux comptes du niveau supérieur de la hiérarchie des objets d'administration VMware – au niveau du serveur VMware vCenter.

Pour en savoir plus sur la création d'un compte utilisateur dans l'infrastructure VMware, consultez la documentation de VMware.

Hyperviseur Microsoft Windows Server (Hyper-V)

Le déploiement et le fonctionnement de la SVM sur l'hyperviseur Microsoft Windows Server (Hyper-V) nécessitent le compte utilisateur intégré de l'administrateur local ou le compte utilisateur de domaine qui fait partie du groupe Administrateurs Hyper-V. Dans le cas du compte utilisateur de domaine, vous devez aussi octroyer les droits de connexion et d'utilisation à distance des espaces suivants des noms WMI :

- root\cimv2 ;
- root\virtualization ;
- root\virtualization\v2 (pour les versions des systèmes d'exploitation serveur Microsoft Windows, à partir de la version Windows Server 2012 R2).

Hyperviseur Citrix XenServer

Pour déployer et utiliser une SVM sur un hyperviseur Citrix Xenserver, il faut utiliser un compte administrateur possédant les autorisations Pool Administrator.

Hyperviseur KVM

Pour déployer et utiliser une SVM sur un hyperviseur KVM, il faut utiliser un compte administrateur possédant les autorisations suivantes :

- création d'une session interactive à distance avec l'hyperviseur via SSH par le biais de la saisie du mot de passe d'authentification ;
- exécution de commandes via l'utilitaire virsh (utilitaire de ligne de commande Linux, prévu pour l'administration des machines virtuelles et des hyperviseurs KVM) ;
- modification du contenu du répertoire pool du stockage des images de machines virtuelles (l'emplacement exact est déterminé via le service libvirtd) ;
- modification du contenu du dossier des fichiers temporaires (/tmp) ;
- montage des images de machines virtuelles dans le dossier /mnt. En l'absence d'un tel dossier, il faudra disposer de l'autorisation de création de ce dossier dans le répertoire racine.

Pour utiliser une SVM, il faut disposer sur l'hyperviseur KVM d'un compte possédant les autorisations suivantes :

- création d'une session interactive à distance avec l'hyperviseur via SSH par le biais de la saisie du mot de passe d'authentification ;
- exécution des commandes prévues pour la récupération des informations sur l'infrastructure virtuelle à l'aide de l'utilitaire virsh (commandes read-only) ;
- modification du contenu du dossier des fichiers temporaires (/tmp).

Pour savoir comment créer un compte, consultez la documentation KVM.

Définition des règles de déplacement des machines virtuelles dans les groupes d'administration

Pour administrer les composants de l'application Kaspersky Security installés sur les machines virtuelles via le Kaspersky Security Center, il est nécessaire de placer les machines virtuelles de protection dans les groupes d'administration.

Le *Groupe d'administration* est un ensemble de machines virtuelles regroupées selon certaines caractéristiques pour être administrées en tant qu'entité unique.

Avant l'installation de l'application Kaspersky Security, vous pouvez créer les groupes d'administration dans la Console de gestion de Kaspersky Security Center en vue du placement des machines virtuelles dotées des composants de l'application. Vous pouvez également définir des règles de déplacement automatique des machines virtuelles dans les groupes d'administration.

Si les règles de déplacement des machines virtuelles dans les groupes d'administration ne sont pas définies, le Kaspersky Security Center place les machines virtuelles détectées sur le réseau dans le dossier **Périphériques non distribués** après l'installation. Dans ce cas, vous devrez déplacer manuellement les machines virtuelles dans le groupe d'administration.

► *Pour définir les règles de déplacement des machines virtuelles dans les groupes d'administration, procédez comme suit :*

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

2. Dans l'arborescence de la console choisissez le dossier **Périphériques non distribués**, ouvrez le menu contextuel et choisissez le point **Propriétés**.

   La fenêtre **Propriétés : Périphériques non distribués** s'ouvre.

3. Dans la section **Déplacement des ordinateurs**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouvelle règle** s'ouvre.

4. Définissez les règles de déplacement des machines virtuelles dans les groupes d'administration.

   Vous pouvez consulter les informations détaillées sur le déplacement des machines virtuelles dans les groupes dans la documentation de Kaspersky Security Center.

5. Cliquez sur le bouton **OK** pour fermer la fenêtre **Nouvelle règle**.

   La règle définie s'affiche dans la liste des règles de la section **Déplacement des ordinateurs**.

6. Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Périphériques non distribués**

Lors de la création des règles de déplacement des machines virtuelles dans les groupes d'administration, vous pouvez utiliser les balises (cf. section " Modifications dans Kaspersky Security Center après l'installation de l'application " à la page 114). Les SVM et les machines virtuelles protégées disposant de l'Agent d'administration de Kaspersky Security Center transmettent automatiquement les informations sur les balises à Kaspersky Security Center.

Installation de l'application

Cette section fournit les informations suivantes :

- description de l'ordre d'installation des modules de l'application ;
- instructions concernant l'installation des composants de l'application ;
- description des modifications dans Kaspersky Security Center après l'installation de l'application.

Dans cette section

Ordre des étapes d'installation de l'application 60

Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration 61

Installation du composant Serveur de protection 69

Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles 81

Installation du composant Light Agent for Windows 83

Installation du composant Light Agent for Linux 107

Modifications dans le Kaspersky Security Center après l'installation de l'application 114

Ordre des étapes d'installation de l'application

L'installation de l'application Kaspersky Security for Virtualization 4.0 Light Agent dans l'infrastructure virtuelle inclut les étapes suivantes :

1. Installation des plug-ins d'administration de Kaspersky Security, du Serveur d'intégration et de la Console de gestion du Serveur d'intégration (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 61).

   - Pour l'administration de l'application à l'aide de Kaspersky Security Center, les plug-ins d'administration suivants sont utilisés :

     - Kaspersky Security for Virtualization 4.0 Light Agent for Windows ;
     - Kaspersky Security for Virtualization 4.0 Light Agent for Linux ;
     - Kaspersky Security for Virtualization 4.0 Light Agent – Serveur de protection.

     Les plug-ins d'administration de Kaspersky Security doivent être installés sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center.

   - Le serveur d'intégration doit être installé sur l'ordinateur où est installé le Serveur d'administration de Kaspersky Security Center.

   - La console de gestion du Serveur d'intégration doit être installée sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center.

2. Installation du composant Serveur de protection de Kaspersky Security (cf. section "Installation du composant Serveur de protection" à la page 69). L'installation du composant Serveur de protection se déroule via le déploiement de SVM sur les hyperviseurs.

   Une fois le composant Serveur de protection installé, il convient de réaliser les opérations suivantes :

   - Activer l'application (cf. section "A propos de l'activation de l'application" à la page 116).
   - Mettre à jour les bases antivirus de l'application (cf. section "Mise à jour des bases antivirus" à la page 130).

3. Installation du composant Agent d'administration de Kaspersky Security Center. Si vous souhaitez administrer le fonctionnement du composant Light Agent à l'aide de Kaspersky Security Center, il faut installer l'Agent d'administration sur les machines virtuelles ainsi que les modèles de machines virtuelles (cf. section "Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles" à la page 81).

4. L'installation sur les machines virtuelles du composant Light Agent for Windows (cf. section "Installation du composant Light Agent for Windows" p. 83) et/ou Light Agent for Linux (cf. section "Installation du composant Light Agent for Linux" p. 107).

Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration

Vous pouvez installer les plug-ins d'administration de Kaspersky Security, le serveur d'intégration et la Console de gestion du serveur d'intégration d'une des méthodes suivantes :

- en mode interactif, à l'aide de l'Assistant (cf. section "Installation via l'Assistant" à la page 63) ;

- en mode silencieux à partir de la ligne de commande (cf. section "Installation via la ligne de commande" à la page 67).

L'installation des plug-ins d'administration de Kaspersky Security et des composants du Serveur d'intégration doit s'effectuer sous le compte utilisateur qui fait partie du groupe d'administrateurs locaux.

En fonction de la présence de composants de Kaspersky Security Center sur l'ordinateur, les actions suivantes peuvent avoir lieu après l'installation :

- Si seule la Console d'administration de Kaspersky Security Center est installée sur l'ordinateur, les plug-ins d'administration de Kaspersky Security et la Console de gestion du Serveur d'intégration sont installés.
- Si le Serveur d'administration de Kaspersky Security Center et la Console d'administration de Kaspersky Security Center sont installés sur l'ordinateur, les plug-ins d'administration de Kaspersky Security, le Serveur d'intégration et la Console de gestion du Serveur d'intégration sont installés.

Pour réussir l'installation du Serveur d'intégration, il est nécessaire d'autoriser les connexions via le port qui sera utilisé par les SVM et les Light Agents pour se connecter au Serveur d'intégration. Cette opération s'effectue dans les paramètres de la configuration réseau ou de l'application contrôlant le trafic. Le port utilisé par défaut est le 7271 via le protocole TCP.

L'interaction entre le Serveur d'intégration et la Console de gestion, les SVM, les Light Agents et le serveur VMware vCenter se déroule via une connexion sécurisée par SSL. Pour éliminer les vulnérabilités du système d'exploitation pour le protocole SSL lors de l'installation, le Serveur d'intégration introduit dans la base de registre système les modifications décrites par l'assistance technique de Microsoft (http://support.microsoft.com/kb/245030). Suite à ces modifications, les protocoles et codes cryptographiques suivants sont désactivés :

- SSL 3.0 ;
- SSL 2.0 ;
- AES 128 ;
- RC2 40/56/128 ;
- RC4 40/56/64/128/ ;
- 3DES 168.

Si un Serveur d'intégration a été préalablement installé dans votre infrastructure virtuelle et que, lors de sa suppression, vous avez enregistré les données utilisées lors du fonctionnement du Serveur d'intégration (cf. section " Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration " à la page 175), ces données sont automatiquement utilisées lors de la réinstallation d'un Serveur d'intégration.

Une fois que les plug-ins d'administration de Kaspersky Security ont été installés, ils apparaissent dans la liste des plug-ins d'administration dans les propriétés du Serveur d'administration de Kaspersky Security Center (cf. section "Consultation de la liste des plug-ins d'administration de Kaspersky Security installés" à la page 69).

Dans cette section

Installation via l'Assistant 63

Installation via la ligne de commande..... 67

Consultation de la liste des plug-ins d'administration de Kaspersky Security 69

Installation via l'Assistant

► *Pour installer les plug-ins d'administration de Kaspersky Security et les composants du Serveur d'intégration à l'aide de l'Assistant, procédez comme suit :*

1. Sur l'ordinateur où sont installés la Console d'administration et le Serveur d'administration de Kaspersky Security Center, exécutez le fichier SecurityCenterComponents_4.0.XX_setup.exe où 4.0.X.X désigne la version de l'application. Ce fichier fait partie de la distribution (cf. section "Fichiers, indispensables à l'installation de l'application" à la page 45).

   > Si le serveur d'administration de Kaspersky Security Center n'est pas installé sur l'ordinateur, il est impossible d'installer le serveur d'intégration sur cet ordinateur. Seuls les plug-ins d'administration de Kaspersky Security et la Console de gestion du Serveur d'intégration sont installés.

   Lancez l'Assistant d'installation.

2. Suivez les instructions de l'Assistant.

Dans cette section

Etape 1. Sélection de la langue de localisation 64

Etape 2. Consultation du Contrat de licence..... 64

Etape 3. Création du mot de passe du compte administrateur du Serveur d'intégration 65

Etape 4. Saisie ou modification du mot de passe du compte utilisateur svm 65

Etape 5. Saisie du numéro du port pour la connexion au Serveur d'intégration 66

Etape 6. Lancement de l'installation et mise à jour des composants 66

Etape 7. Installation et mise à jour des composants..... 66

Etape 8. Fin du travail de l'Assistant..... 67

Etape 1. Sélection de la langue de localisation

Cette fenêtre utilise la langue de localisation du système d'exploitation installé sur l'ordinateur où est installé l'Assistant.

Cette étape permet de sélectionner la langue de localisation de l'Assistant et des composants de Kaspersky Security.

Passez à l'étape suivante de l'Assistant.

Etape 2. Consultation du Contrat de Licence Utilisateur Final

A cette étape, vous devez prendre connaissance du Contrat de Licence Utilisateur Final conclu entre vous et Kaspersky Lab.

Lisez attentivement le Contrat de Licence Utilisateur Final et, si vous en acceptez tous les points, cochez la case **J'accepte les termes du contrat de licence**.

Passez à l'étape suivante de l'Assistant.

Etape 3. Création du mot de passe du compte administrateur du Serveur d'intégration.

Cette étape est proposée si l'ordinateur sur lequel est exécuté l'Assistant est doté du Serveur d'administration de Kaspersky Security Center et si l'ordinateur n'appartient pas au domaine Microsoft Windows.

L'administration du Serveur d'intégration s'opère sous le compte utilisateur de l'administrateur *admin* du Serveur d'intégration. Le nom du compte utilisateur ne peut pas être modifié.

Créez le mot de passe du compte administrateur du Serveur d'intégration. Pour ce faire, saisissez le mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.

Le mot de passe doit comporter entre 1 et 60 caractères. Vous pouvez utiliser l'alphabet latin, des chiffres et les symboles suivants : `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~.`

Passez à l'étape suivante de l'Assistant.

Etape 4. Saisie ou modification du mot de passe du compte utilisateur svm

Cette étape s'affiche si le Serveur d'intégration installé précédemment utilisé pour le fonctionnement de l'application Kaspersky Security for Virtualization 3.0 Service Pack 1 Agentless est détecté sur l'ordinateur où l'assistant est lancé.

Par souci de sécurité, vous devez indiquer le mot de passe du compte utilisateur svm qui était utilisé pour la connexion de la SVM au Serveur d'intégration.

Dans les champs **Mot de passe** et **Confirmation du mot de passe**, saisissez le mot de passe du compte utilisateur svm spécifié auparavant ou saisissez un nouveau mot de passe pour ce compte.

Passez à l'étape suivante de l'Assistant.

Etape 5. Saisie du numéro du port pour la connexion au Serveur d'intégration

Cette étape s'affiche si le Serveur d'administration de Kaspersky Security Center est installé sur l'ordinateur allumé et si le port utilisé par défaut pour la connexion au Serveur d'intégration est occupé. Le port utilisé par défaut pour la connexion au Serveur d'intégration est le port 7271.

Indiquez le numéro du port de connexion au Serveur d'intégration dans le champ **Port**.

Passez à l'étape suivante de l'Assistant.

Etape 6. Lancement de l'installation et mise à jour des composants

Cette étape de l'Assistant fournit les renseignements relatifs aux actions que l'Assistant exécute sur les plug-ins d'administration, le Serveur d'intégration et la Console de gestion du Serveur d'intégration.

L'Assistant réalise la mise à jour des composants de Kaspersky Security si des versions antérieures sont détectées sur l'ordinateur.

Cliquez sur le bouton **Suivant** pour lancer l'exécution des actions citées.

Etape 7. Installation et mise à jour des composants

Cette étape correspond à l'installation et/ou à la mise à jour des composants. Attendez la fin de l'Assistant

Si une erreur survient pendant le fonctionnement de l'Assistant, celui rétablira le système à l'état antérieur aux modifications.

Etape 8. Fin du travail de l'Assistant

Cette étape affiche les informations relatives aux résultats des opérations de l'Assistant.

Les informations sur le fonctionnement de l'Assistant sont consignées dans les journaux de l'Assistant. Les journaux de l'Assistant se présentent sous la forme de fichiers au format TXT et sont enregistrés dans le dossier %temp% sur l'ordinateur sur lequel a été exécuté l'Assistant. Si l'exécution de l'Assistant se solde par une erreur, vous pouvez utiliser ces journaux lorsque vous contactez le Support Technique.

Pour fermer la fenêtre de l'Assistant, cliquez sur **Terminer**.

Installation via la ligne de commande

► *Pour installer les plug-ins d'administration de Kaspersky Security et les composants du Serveur d'intégration via la ligne de commande, procédez comme suit :*

Saisissez une des commandes suivantes dans la ligne de commande :

- Si l'ordinateur sur lequel l'installation a lieu appartient au domaine Microsoft Windows :

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<identifiant de la langue> --accept-eula=<yes>
  ```

- Si l'ordinateur sur lequel l'installation a lieu n'appartient pas au domaine Microsoft Windows :

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<identifiant de la langue> --accept-eula=<yes> --viisPass=<mot de passe>
  ```

où :

- `4.0.X.X` désigne la version de l'application.
- `<identifiant de la langue>` : code de deux lettres qui identifie la langue des composants installés.

- `<mot de passe>` : mot de du compte administrateur du Serveur d'intégration.
  Le compte administrateur du Serveur d'intégration admin est utilisé pour administrer le Serveur d'intégration si l'ordinateur sur lequel est installé le Serveur d'intégration n'appartient pas au domaine Microsoft Windows.

- `accept-eula=<yes>` signifie que vous acceptez les conditions du Contrat de Licence Utilisateur Final. Le Contrat de Licence Utilisateur Final est repris dans la distribution de l'application (cf. section "Distribution" à la page. 23). L'accord avec les conditions du Contrat de licence utilisateur final est une condition sine qua non pour l'installation des plug-ins d'administration de Kaspersky Security et des composants du Serveur d'intégration.

  Vous pouvez prendre connaissance du texte du Contrat de licence utilisateur final avant l'installation de l'application. Pour cela, dans la ligne de commande, saisissez la commande suivante :

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe lang=<identifiant de la langue> --show-eula
  ```

  Le texte du Contrat de licence utilisateur final s'affiche dans le fichier license _ <identifiant de la langue>.txt dans le dossier tmp.

Le port utilisé par défaut pour la connexion au Serveur d'intégration est le port 7271. Si vous souhaitez utiliser un autre port de connexion au Serveur d'intégration, définissez le paramètre `--viisPort=<numéro de port>` sur la ligne de commande.

L'installation des plug-ins d'administration et des modules du serveur d'intégration prend un certain temps. Vous pouvez consulter les informations sur le résultat de l'installation dans le fichier

%temp%\Kaspersky_Security_for_Virtualization_4.0_Light_Agent_Silent_Mode_Result_{0}.log,

Où {0} est l'heure d'achèvement de l'installation indiquée au format jj_MM_aaaa_HH_mm_ss.

Consultation de la liste des plug-ins d'administration de Kaspersky Security

► *Pour consulter la liste des plug-ins d'administration de Kaspersky Security, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le dossier **Serveur d'administration**, puis choisissez l'une des options suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
   - Ouvrez la fenêtre des propriétés du Serveur d'administration en cliquant sur le lien **Propriétés du Serveur d'administration**. Le lien se trouve dans l'espace de travail dans le groupe **Serveur d'administration**.

   La fenêtre **Propriétés : Serveur d'administration** s'ouvre.
3. Dans la section **Avancé** de la liste située à gauche, sélectionnez la section **Informations sur les plug-ins d'administration des applications installés**.

   Les plug-ins d'administration de Kaspersky Security apparaissent dans la partie droite de la liste des plug-ins installés :
   - **Kaspersky Security for Virtualization 4.0 Light Agent for Windows** ;
   - **Kaspersky Security for Virtualization 4.0 Light Agent for Windows** ;
   - **Kaspersky Security for Virtualization 4.0 SP2 Light Agent – Serveur de protection**.

Installation du composant Serveur de protection

Le composant Serveur de protection est livré sous la forme d'une image de SVM. L'installation du composant Serveur de protection de Kaspersky Security s'effectue via le déploiement de la SVM sur l'hyperviseur.

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. Plusieurs SVM peuvent être déployées sur un seul hyperviseur.

Pendant l'installation du composant Serveur de protection, vous pouvez désigner plusieurs hyperviseurs sur lesquels les SVM seront installées.

► *Pour installer le composant Serveur de protection, 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.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization 4.0 Light Agent** pour lancer l'Assistant. Le lien se trouve dans l'espace de travail dans le groupe **Déploiement**.
4. Suivez les instructions de l'Assistant.

Lors de l'installation, l'Assistant d'installation enregistre les informations que vous avez renseignées à chaque étape de l'Assistant dans le journal de l'Assistant (cf. section Appendice. Description du journal de l'Assistant" à la page 179). Le journal de l'Assistant se trouve sur l'ordinateur où l'Assistant a été lancé, dans le fichier %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log.

> Les informations du fichier sont écrasées à chaque lancement de l'Assistant. Pour pouvoir utiliser les informations du journal de fonctionnement de l'Assistant ultérieurement, il faut enregistrer le fichier dans un emplacement permanent.

Vous pouvez utiliser le journal de l'Assistant lorsque vous contactez le Service de Support Technique si le déploiement d'une SVM s'est terminé sur une erreur.

Dans cette section

Etape 1. Sélection de l'action 71

Etape 2. Choix des hyperviseurs pour le déploiement des SVM 71

Etape 3. Choix de l'image de la SVM 74

Etape 4. Saisie des paramètres de la SVM 76

Etape 5. Configuration des paramètres réseau de la SVM 77

Etape 6. Saisie des paramètres de connexion au Kaspersky Security Center 78

Etape 7. Création du mot de passe de configuration et du mot de passe du compte root 79

Etape 8. Lancement du déploiement des SVM 79

Etape 9. Déploiement des SVM 79

Etape 10. Achèvement du déploiement des SVM 80

Fin de l'installation du composant Serveur de protection 81

Etape 1. Sélection de l'action

A cette étape, sélectionnez l'option **Déploiement des SVM**.

Passez à l'étape suivante de l'Assistant.

Etape 2. Choix des hyperviseurs pour le déploiement des SVM

A cette étape, sélectionnez les hyperviseurs sur lesquels vous souhaitez déployer la SVM.

S'il s'agit de la première exécution de l'Assistant, la liste des hyperviseurs est vide. Si des SVM ont déjà été déployées sur les hyperviseurs de votre infrastructure virtuelle, le tableau reprend la liste de ces hyperviseurs et des SVM déployées sur ces hyperviseurs. Vous pouvez ajouter à la liste les hyperviseurs sur lesquels vous souhaitez déployer les SVM.

Si pour l'administration de l'infrastructure virtuelle, vous utilisez Microsoft System Center Virtual Machine Manager (appelé ensuite "Microsoft SCVMM"), vous pouvez indiquer les paramètres de connexion à Microsoft SCVMM pour ajouter à la liste tous les hyperviseurs qui se trouvent sous son administration.

► *Pour ajouter une adresse IP au tableau, procédez comme suit :*

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

   La fenêtre **Paramètres de connexion à l'infrastructure virtuelle** s'ouvre.

2. Définissez les paramètres suivants de connexion aux hyperviseurs ou au serveur d'administration de l'infrastructure virtuelle administrant les hyperviseurs.

   - **Type**.

     Liste déroulante qui permet de sélectionner le type d'hyperviseur ou de serveur d'administration de l'infrastructure virtuelle.

   - **Adresses**.

     Adresses des hyperviseurs sur lesquels vous souhaitez déployer les SVM ou adresse du serveur d'administration de l'infrastructure virtuelle assurant l'administration des hyperviseurs.

     L'adresse de l'hyperviseur ou du serveur d'administration de l'infrastructure virtuelle peut être son adresse IP au format IPv4 ou son nom de domaine complet (FQDN). Vous pouvez indiquer plusieurs adresses IP ou noms de domaines complets d'hyperviseur en les séparant par un point-virgule ou des retours à la ligne.

     Le nombre d'adresses reconnues correctement s'affiche sous la liste.

   - **Nom d'utilisateur**.

     Nom du compte employé pour la connexion de l'Assistant à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle. Si vous utilisez un compte d'utilisateur de domaine pour vous connecter à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle, vous pouvez indiquer le nom du compte sous la forme `<domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<domaine>`.

- **Mot de passe**.

  Mot de passe du compte employé pour la connexion de l'Assistant à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle.

3. Cliquez sur le bouton **Se connecter**.

   La fenêtre **Paramètres de connexion à l'infrastructure virtuelle** se ferme et les hyperviseurs sélectionnés sont ajoutés à la liste des hyperviseurs. Si la connexion à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle n'a pas pu être établie, des informations sur les erreurs de connexion s'affichent dans le tableau.

Le tableau reprend les informations suivantes sur les hyperviseurs et les SVM précédemment déployées sur les hyperviseurs :

- **Nom**.

  Nom de l'hyperviseur, du serveur d'administration de l'infrastructure virtuelle ou de la SVM déployée sur l'hyperviseur.

  Si des restrictions concernant le déploiement de la SVM sur l'hyperviseur s'appliquent ou si la connexion avec l'hyperviseur ou avec le serveur d'administration de l'infrastructure virtuelle n'est pas établie, la colonne **Nom** affiche une icône d'avertissement. Le tableau et les info-bulles de l'icône reprenne la description des restrictions ou de l'erreur de connexion.

  Le bouton **Nom** du tableau permet de réaliser les opérations suivantes :

  - supprimer de la liste l'hyperviseur sélectionné ou tous les hyperviseurs administrés par le serveur d'administration de l'infrastructure virtuelle sélectionné ;
  - ouvrir la fenêtre **Paramètres de connexion à l'infrastructure virtuelle** pour modifier les paramètres du compte utilisateur employé pour établir la connexion à l'hyperviseur sélectionné ou au serveur d'administration de l'infrastructure virtuelle.

- **Condition**.

  L'état de l'hyperviseur ou du SVM.

  L'état de l'hyperviseur peut avoir une des valeurs suivantes : *Allumé*, *Eteint*, *Mode de maintenance*. En cas d'échec de la connexion à l'hyperviseur, la colonne affiche *La connexion n'a pas été établie*.

  L'état de la SVM peut avoir une des valeurs suivantes : *Lancée*, *Arrêtée*.

- **Protection**.

  Numéro de la version de l'image SVM.

Pour rafraîchir la liste des hyperviseurs dans le tableau, cliquez sur le bouton **Mettre à jour** qui se trouve au-dessus de la liste.

► *Pour sélectionner les hyperviseurs en vue du déploiement des SVM, procédez comme suit :*

1. Dans le tableau, cochez la case à gauche des hyperviseurs sur lesquels vous souhaitez déployer une SVM.

   Vous pouvez sélectionner les hyperviseurs qui ne sont soumis à aucune restriction pour le déploiement de la SVM.

2. Si vous souhaitez autoriser le déploiement parallèle de SVM sur plusieurs hyperviseurs, cochez la case **Autoriser le déploiement parallèle simultanément sur X hyperviseurs**.

Passez à l'étape suivante de l'Assistant.

Etape 3. Choix de l'image de la SVM

Lors de cette étape, indiquez le fichier de l'image de la SVM pour le déploiement sur l'hyperviseur. Le fichier de l'image de la SVM et le fichier de configuration au format XML doivent être placés dans le même dossier. Si vous installez le Serveur de protection sur des hyperviseurs de types différents, dans un seul dossier, vous devez installer les fichiers des images des SVM pour chaque type d'hyperviseurs et le fichier de configuration au format XML (cf. section "Fichiers indispensables à l'installation de l'application" à la p. 45).

Pour désigner l'image de la SVM, cliquez sur le bouton **Parcourir** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration au format XML.

Les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Nom de l'application**.

  Le nom de l'application qui est installée sur la SVM.

- **Version de la SVM**.

  Numéro de la version de l'image SVM.

- **Editeur**.

  Editeur de l'application qui est installée sur la SVM.

- **Éditeur**.

  L'éditeur qui a publié le fichier de l'image SVM. Pour déployer la SVM, utilisez les fichiers images édités par Kaspersky Lab.

- **Description**.

  Une brève description de l'image SVM.

- **Taille du disque virtuel**.

  Volume d'espace disque requis pour le déploiement de la SVM dans le référentiel de données.

- Informations sur les résultats de l'analyse du fichier image de la SVM pour chaque type d'hyperviseur. Il est conseillé de vérifier l'intégrité du fichier image de la SVM à l'aide du lien **Analyser**. Si le fichier de l'image a été modifié ou endommagé pendant son transfert entre l'éditeur et l'utilisateur final ou si le format de l'image n'est pas pris en charge, l'Assistant affiche un message d'erreur. Dans ce cas, téléchargez à nouveau l'archive contenant les fichiers indispensables au déploiement de la SVM depuis le site de Kaspersky Lab.

  Si l'analyse du fichier de l'image n'a pas eu lieu, la ligne affiche le texte **L'analyse n'a pas été effectuée**.

Passez à l'étape suivante de l'Assistant.

Etape 4. Saisie des paramètres de la SVM

A cette étape, indiquez les paramètres suivants de la SVM pour chaque hyperviseur :

- **Nom de la SVM**.

  Le nom de domaine complet (FQDN) de la SVM.

- **Stockage**.

  Le stockage des données de l'hyperviseur pour l'image de la SVM.

- **Nom du réseau**.

  Nom du réseau virtuel que la SVM doit utiliser pour communiquer avec les machines virtuelles et le Serveur d'administration de Kaspersky Security Center.

  Vous pouvez désigner un ou plusieurs réseaux virtuels accessibles aux hyperviseurs. Pour l'ajout ou la suppression d'un champ pour la sélection des réseaux virtuels, utilisez les boutons situés à côté du champ de sélection du réseau.

  Si l'infrastructure virtuelle utilise le module VMware Distributed Virtual Switch, vous pouvez désigner un groupe de ports virtuels distribués (Distributed Virtual Port Group) auquel la SVM se connectera.

  Si vous avez l'intention d'utiliser une attribution dynamique des adresses IP (DHCP) pour toutes les SVM, les paramètres réseau seront récupérés sur le serveur DHCP via le premier réseau virtuel de la liste des réseaux indiqués pour chacune des SVM. Assurez-vous que l'Assistant puisse se connecter à la SVM selon les paramètres réseau du premier réseau virtuel reçus du serveur DHCP.

- **Identifiant VLAN**.

  Identifiant du réseau local virtuel (VLAN) utilisé pour la communication entre la SVM d'un côté, et les machines virtuelles et le Serveur d'Administration de Kaspersky Security Center de l'autre.

  Si le réseau local virtuel n'est pas utilisé, la colonne affiche *N/A*.

  La colonne s'affiche seulement si l'hyperviseur Microsoft Windows Server (Hyper-V) est sélectionné pour le déploiement de la SVM.

Si vous souhaitez que l'Assistant utilise la libération dynamique d'espace sur le disque pour déployer les SVM sur les hyperviseurs VMware, cochez la case **Utiliser la libération dynamique d'espace dans le stockage de l'hyperviseur VMware ESXi**. Dans le stockage des données de l'hyperviseur, le volume minimal requis est réservé pour la SVM. Ce volume augmente en fonction des besoins. Si la case est décochée, la libération dynamique d'espace sur le disque n'est pas utilisée. Dans le stockage des données de l'hyperviseur, le volume requis est réservé immédiatement pour la SVM.

Passez à l'étape suivante de l'Assistant.

Etape 5. Configuration des paramètres réseau de la SVM

Lors de cette étape, configurez les paramètres de réseau de la SVM. Pour ce faire, exécutez une des actions suivantes :

- Si vous souhaitez utiliser les paramètres réseau reçu via le protocole DHCP pour l'ensemble des SVM, choisissez l'option **Adressage IP dynamique (DHCP)**. Si vous souhaitez indiquer les adresses IP du serveur DNS et du serveur DNS alternatif pour chaque SVM, décochez la case **Utiliser la liste des serveurs DNS obtenus par DHCP** et saisissez les adresses IP des serveurs DNS dans les colonnes **Serveur DNS** et **Serveur DNS alternatif** du tableau. Les adresses IP des serveurs DNS obtenus via le protocole DHCP sont utilisées par défaut.

  Si, à l'étape précédente, vous avez indiqué plusieurs réseaux virtuels pour la SVM, les paramètres réseau pour celle-ci seront, par défaut, obtenus auprès du serveur DHCP en fonction du premier réseau virtuel de la liste des réseaux indiqués.

- Si vous souhaitez désigner les paramètres réseau des SVM manuellement, choisissez l'option **Adressage IP statique** et définissez les paramètres suivants pour chaque SVM :

  - Adresse IP de la SVM ;
  - masque du sous-réseau ;
  - passerelle ;
  - serveur DNS ;
  - serveur DNS alternatif.

Si vous aviez indiqué à l'étape précédente plusieurs réseaux virtuels pour la SVM, renseignez les paramètres réseau pour chacun des réseaux virtuels.

Passez à l'étape suivante de l'Assistant.

Etape 6. Saisie des paramètres de connexion au Kaspersky Security Center

Cette étape se déroule si l'Assistant d'installation ne parvient pas à définir automatiquement les paramètres de connexion au Kaspersky Security Center.

A cette étape, indiquez les paramètres suivants pour la connexion de la SVM au Serveur d'administration de Kaspersky Security Center :

- **Adresse**.

  Adresse du poste sur lequel le Serveur d'Administration de Kaspersky Security Center est installé. Vous pouvez saisir l'adresse IP au format IPv4 ou le nom de domaine complet de l'ordinateur (FQDN).

- **Port**.

  Numéro du port pour la connexion de la SVM au Serveur d'administration de Kaspersky Security Center.

- **Port SSL**.

  Numéro du port pour la connexion de la SVM au Serveur d'administration de Kaspersky Security Center à l'aide d'un certificat SSL.

Passez à l'étape suivante de l'Assistant.

Etape 7. Création du mot de passe de configuration et du mot de passe du compte root

Cette étape permet de créer le mot de passe de la configuration et le mot de passe du compte root sur les SVM. Le mot de passe de la configuration est requis pour modifier la configuration des SVM. Le compte utilisateur root est utilisé pour la configuration des SVM.

> Il est recommandé d'utiliser pour les mots de passe les caractères de l'alphabet latin et les chiffres.

Si vous souhaitez configurer l'accès du compte root à la SVM via SSH, cochez la case **Autoriser l'accès à distance du compte root via SSH**.

Passez à l'étape suivante de l'Assistant.

Etape 8. Lancement du déploiement des SVM

A cette étape, la fenêtre de l'Assistant affiche tous les paramètres saisis plus tôt et nécessaires au déploiement d'une SVM sur l'hyperviseur.

Pour lancer le déploiement des SVM, passez à l'étape suivante de l'Assistant.

Etape 9. Déploiement des SVM

Cette étape consiste à déployer les SVM sur les hyperviseurs. Le processus dure un certain temps. Attendez la fin du processus de déploiement.

Les informations au processus et aux résultats du déploiement de chaque SVM sont reprises dans la fenêtre de l'Assistant.

Après l'achèvement du déploiement, la SVM s'active automatiquement.

Si une erreur survient lors du déploiement de la SVM sur un hyperviseur, l'Assistant annule les modifications apportées à cet hyperviseur. Le déploiement se poursuit sur les autres hyperviseurs.

Passez à l'étape suivante de l'Assistant.

Etape 10. Achèvement du déploiement des SVM

A cette étape, les informations relatives au résultat du déploiement des SVM sur les hyperviseurs s'affichent.

L'Assistant affiche des liens qui vous permettent d'ouvrir le journal de l'Assistant et un rapport abrégé.

Celui-ci contient des informations sur les résultats de l'exécution des étapes de déploiement de chaque SVM. Le rapport abrégé est enregistré dans un fichier temporaire. Pour pouvoir utiliser les informations du rapport ultérieurement, vous devez enregistrer le fichier dans un emplacement permanent.

Le journal de l'Assistant contient les informations indiquées par vos soins à chaque étape de l'Assistant. Si le déploiement d'une SVM s'est terminé sur une erreur, vous pouvez utiliser le journal de l'Assistant lors de vos communications avec le Support Technique.

Le journal de l'Assistant est enregistré sur l'ordinateur où l'Assistant a été lancé, dans le fichier %LocalAppData%\Kaspersky_Lab\SvmDeploymentWizard.log. Il ne contient aucune information relative aux comptes.

Fermez l'Assistant.

Une fois le travail de l'Assistant terminé dans l'infrastructure virtuelle, il est conseillé de réaliser les tâches de fin d'installation du composant Serveur de protection (cf. section "Fin de l'installation du composant Serveur de protection" à la page 81).

Si votre infrastructure virtuelle comporte un hyperviseur Microsoft Windows Server (Hyper-V), un message indiquant qu'il faut mettre à jour le paquet de services d'intégration (Integration Services) sur la SVM est susceptible d'apparaître dans le journal des événements une fois le déploiement de la SVM effectué. Vous pouvez ignorer ce message car la mise à jour du paquet de services d'intégration n'est pas nécessaire pour le bon fonctionnement de la SVM.

Fin de l'installation du composant Serveur de protection

Après l'installation du Serveur de protection, il est conseillé de réaliser les opérations suivantes :

- Analyser la date système sur les SVM par via l'hyperviseur utilisé. Si la date et l'heure du Serveur d'administration de Kaspersky Security Center et la date et l'heure de la SVM ne correspondent pas, une erreur est susceptible de survenir lors de la connexion de cette machine au Kaspersky Security Center ; le fonctionnement de l'application peut être entravé.
- Indiquer le compte que la SVM utilise pour établir la connexion avec l'hyperviseur ou le serveur d'administration de l'infrastructure virtuelle. Pour ce faire, il faut modifier la configuration des SVM (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Il est conseillé d'utiliser un compte créé pour le fonctionnement de l'application (cf. section "Comptes utilisateur pour l'installation et l'utilisation de l'application" à la page 54). Par défaut, le compte utilisé pour connecter la SVM à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle est le compte renseigné à la deuxième étape du déploiement des SVM.

Une fois la SVM déployée sur l'hyperviseur, vous pouvez modifier les ressources de l'hyperviseur qui lui sont attribuées, par exemple, en fonction des recommandations des experts de Kaspersky Lab (cf. section " Configurations logicielle et matérielle requises " à la page 24). Vous pouvez réguler les performances de la SVM à l'aide des ressources sélectionnées.

Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles

Si vous souhaitez administrer le composant Light Agent à l'aide de Kaspersky Security Center, il est nécessaire d'installer le composant Agent d'administration de Kaspersky Security Center sur les machines virtuelles et les modèles de machine virtuelle avant l'installation du composant Light Agent. L'Agent d'administration assure l'interaction entre le Serveur d'administration de Kaspersky Security Center et les machines virtuelles protégées. 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 se réalise seulement via l'interface locale (dans le cas du Light Agent for Windows) ou via la ligne de commande (dans le cas du Light Agent for Linux).

Vous pouvez installer l'Agent d'administration de l'une des manières suivantes :

- sur les machines virtuelles avec le système d'exploitation Windows ;
  - localement sur chaque machine virtuelle à l'aide de l'assistant d'installation. Il s'agit de l'approche conseillée pour installer l'Agent d'administration sur les modèles de machines virtuelles.
  - A distance dans Kaspersky Security Center à l'aide de l'assistant de déploiement de la protection ou de la tâche d'installation à distance de l'application. Le paquet d'installation à distance de l'Agent d'administration est créé automatiquement lors de l'installation de l'application Kaspersky Security Center et se trouve dans le dossier **Paquets d'installation**.

    Dans les propriétés du paquet d'installation de l'Agent d'administration, section **Avancé**, il est conseillé de cocher la case **Optimiser les paramètres pour VDI (Virtual Desktop Infrastructure)**. Pour en savoir plus sur l'installation à distance de l'application via le Kaspersky Security Center, consultez la documentation de Kaspersky Security Center.
- Sur les machines virtuelles avec le système d'exploitation Linux, via ce dernier.

  Sur la machine virtuelle, où Light Agent for Linux sera installé, vous devez installer le composant Agent d'administration version 10.1.1.-X ou 10.1.1-X représente le numéro de version. Les paquets nécessaires à l'installation de l'Agent d'administration version 10.1.1-X, font partie de la distribution de Kaspersky Security for Virtualization 4.0 Light Agent (cf. section "Fichiers indispensables à l'installation de l'application" à la p. 45).

► *Pour installer l'Agent d'administration localement sur la machine virtuelle ou sur le modèle de machines virtuelles avec le système d'exploitation Windows, procédez comme suit :*

1. Lancez le fichier exécutable setup.exe sur la machine virtuelle. Le fichier setup.exe fait partie de la distribution de l'application Kaspersky Security Center et se trouve dans le dossier Packages\NetAgent.

   Lancez l'Assistant d'installation.

2. Suivez les instructions de l'Assistant d'installation.

3. Si vous installez l'Agent d'administration sur la machine virtuelle, cochez la case **Optimiser les paramètres de l'Agent d'administration pour l'infrastructure virtuelle** lors de l'installation à l'étape "Paramètres avancés". Si la case est cochée, l'inventaire des applications et des équipements est désactivé, de même que la recherche de vulnérabilités dans les fichiers exécutables lors du lancement de l'Assistant.

   Si vous installez l'Agent d'administration sur un modèle de machine virtuelle, cochez les cases suivantes lors de l'installation à l'étape "Paramètres avancés" :

   - **Activer le mode dynamique pour VDI**. Si la case est cochée et qu'une machine virtuelle est désactivée, cette dernière n'apparaît pas dans la Console d'administration de Kaspersky Security Center.

   - **Optimiser les paramètres de l'Agent d'administration pour l'infrastructure virtuelle**. Si la case est cochée, l'inventaire des applications et des équipements est désactivé, de même que la recherche de vulnérabilités dans les fichiers exécutables lors du lancement de l'Assistant.

Pour en savoir plus sur l'installation du composant Agent d'administration de Kaspersky Security Center, consultez la documentation de Kaspersky Security Center.

Installation du composant Light Agent for Windows

Le composant Light Agent for Windows peut être installé sur la machine virtuelle de différentes manières :

- localement à l'aide de l'assistant d'installation (cf. section "Installation du Light Agent for Windows à l'aide de l'assistant d'installation" à la p. 89).

  Ce mode est conseillé pour l'installation du composant Light Agent for Windows sur les modèles de machines virtuelles (cf. section "Installation du Light Agent for Windows sur le modèle de machines virtuelles" à la page 102).

- Depuis la ligne de commande (cf. section "Installation du Light Agent for Windows depuis la ligne de commande" à la page 97).

- A distance depuis le poste de travail de l'administrateur à l'aide de l'application Kaspersky Security Center (cf. section "Installation du Light Agent for Windows via Kaspersky Security Center" à la page 85).
- A distance à partir du poste de travail de l'administrateur, via l'éditeur d'administration des stratégies de groupe du service de catalogues (Active Directory Group Policies) (cf. section "Installation du Light Agent for Windows via l'éditeur des stratégies de groupe du service de catalogues" à la page 100).

Vous pouvez installer le Light Agent for Windows sur les machines virtuelles qui font partie de l'infrastructure dans laquelle les solutions suivantes sont utilisées pour la virtualisation :

- Citrix XenDesktop (cf. la section "Compatibilité avec la technologie Citrix Personal vDisk" à la p. 104) ;
- Citrix Provisioning Services (cf. section "Compatibilité avec la technologie Citrix Provisioning Services" à la p. 104).

Avant le début de l'installation du composant Light Agent for Windows (y compris l'installation à distance), il est conseillé de fermer l'ensemble des applications fonctionnant avec le système d'exploitation de la machine virtuelle.

Dans cette section

Installation du Light Agent for Windows via Kaspersky Security Center 85

Installation du Light Agent for Windows à l'aide de l'assistant d'installation 89

Installation du Light Agent for Windows via la ligne de commande..... 97

Installation du Light Agent for Windows via l'éditeur des stratégies de groupe du service de catalogues 100

Installation du Light Agent for Windows sur un modèle de machine virtuelle 102

Compatibilité avec la technologie Citrix Provisioning Services 104

Compatibilité avec la technologie Citrix Personal vDisk 104

Modification de la composition des composants installés du Light Agent for Windows..... 105

Installation du Light Agent for Windows via Kaspersky Security Center

Il est possible d'installer le Light Agent for Windows à distance, à partir du poste de travail de l'administrateur, à l'aide de l'application Kaspersky Security Center. L'installation s'opère à l'aide du paquet d'installation qui contient la sélection de paramètres indispensables à l'installation de l'application (cf. section "Création du paquet d'installation Light Agent for Windows" à la page 85). L'installation s'effectue à l'aide de l'assistant de déploiement de la protection ou à l'aide de la tâche d'installation à distance de l'application.

Pour en savoir plus sur l'installation à distance de l'application via le Kaspersky Security Center, consultez la documentation de Kaspersky Security Center.

Dans cette section

Création du paquet d'installation du Light Agent for Windows 85

Configuration des paramètres du paquet d'installation du Light Agent for Windows 88

Création du paquet d'installation du Light Agent for Windows

Le paquet d'installation est requis pour l'installation à distance du composant Light Agent for Windows via Kaspersky Security Center.

► *Pour créer le paquet d'installation de Light Agent for Windows, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Avancé/Installation à distance**, puis le dossier **Paquets d'installation**.
3. Cliquez sur le bouton **Créer un paquet d'installation** pour lancer l'assistant de création d'un paquet d'installation.
4. Dans la fenêtre ouverte de l'assistant, cliquez sur le bouton **Créer un paquet d'installation pour l'application de Kaspersky Lab**.

5. Dans la fenêtre de l'assistant, saisissez le nom du nouveau paquet d'installation et passez à l'étape suivante.

6. Dans la fenêtre de l'assistant **Choix de la distribution de l'application pour l'installation**, choisissez la distribution de l'application Kaspersky Security. Pour ce faire, procédez comme suit :

   a. Cliquez sur le bouton **Sélectionner** et indiquez le chemin d'accès à la distribution dans la fenêtre standard Windows **Ouvrir**. En guise de distribution de l'application, vous pouvez sélectionner un des fichiers suivants dans le fichier d'installation de Kaspersky Security :

      - archive autoextractible Agent_4.0.X.X_sfx_<identifiant de la langue>.exe, où 4.0.X.X désigne la version de l'application ; <identifiant de la langue> désigne l'identifiant de deux lettres de la langue de Light Agent for Windows : ru, en, fr, de, etc ;
      - fichier Ksvla.kud qui se trouve dans l'archive autoextractible Agent_4.0.X.X_sfx_<identifiant de la langue>.exe. Si vous souhaitez utiliser le fichier Ksvla.kud, il faut d'abord décompacter l'archive.

      Si vous souhaitez créer un paquet d'installation pour l'installation du Light Agent sur les machines virtuelles qui utilisent la technologie Citrix Provisioning Services, vous devez utiliser le fichier Ksvla.kud. Il convient d'introduire les modifications préalables suivantes dans le fichier Ksvla.kud : dans la section `[Setup]` à la fin de la ligne`Params=/s /pAKINSTALL=1 /pEULA=1`, ajoutez le paramètre `/pINSTALLONPVS=1`.

   b. Cliquez sur le bouton **Ouvrir**.

      La fenêtre de l'assistant **Choix de la distribution de l'application pour l'installation** affiche le nom de l'application.

   Par défaut, dans la fenêtre de l'assistant **Choix de la distribution de l'application pour l'installation**, la case **Copier les mises à jour du stockage au paquet d'installation** est cochée. Kaspersky Security Center ajoute au paquet d'installation toutes les mises à jour des bases et des composants de Light Agent for Windows disponibles dans le stockage de Kaspersky Security Center. Une fois que le composant Light Agent for Windows a été installé sur la machine virtuelle, les bases et les composants de Light Agent for Windows sont automatiquement mis à jour.

   Passez à l'étape suivante de l'Assistant.

7. Dans la fenêtre de l'assistant **Contrat de licence**, prenez connaissance des conditions du Contrat de Licence Utilisateur Final conclu entre vous et Kaspersky Lab. Il faut accepter les termes du Contrat de Licence Utilisateur Final pour pouvoir poursuivre la création du paquet d'installation. Cochez la case **J'accepte les dispositions du Contrat de Licence Utilisateur Final** et passez à l'étape suivante de l'Assistant.

8. L'Assistant télécharge les fichiers indispensables à l'installation de l'application sur le Serveur d'administration de Kaspersky Security Center. Attendez la fin du téléchargement.

9. Dans la fenêtre de l'assistant **Paramètres d'installation à distance de l'application**, indiquez les paramètres d'installation suivants du Light Agent for Windows :

   - Sélectionnez le type d'installation :

     - **Installation des modules de protection**. Sélectionnez cette option si vous souhaitez installer les modules de la protection du Light Agent for Windows avec les paramètres recommandés par les experts de Kaspersky Lab sur la machine virtuelle.

     - **Installation des modules de protection et de contrôle**. Sélectionnez cette option si vous souhaitez installer les modules de la protection et les modules de contrôle du Light Agent for Windows avec les paramètres recommandés par les experts de Kaspersky Lab sur la machine virtuelle.

   - Indiquez en cas de nécessité le chemin d'accès au dossier d'installation.

   - Si vous voulez transférer les paramètres du Light Agent enregistrés dans le paquet d'installation, cliquez sur le bouton **Parcourir**, puis choisissez le fichier doté de l'extension cfg dans la fenêtre **Sélection du fichier de configuration** qui s'ouvre.

   Passez à l'étape suivante de l'Assistant.

10. Dans la fenêtre ouverte, l'assistant crée le paquet d'installation et envoie un message sur la fin de la procédure. Cliquez sur le bouton **Terminer** pour terminer le fonctionnement de l'assistant.

Le paquet d'installation créé est placé dans l'arborescence de la console d'administration de Kaspersky Security Center dans le dossier **Avancé/Installation à distance**, sous-dossier **Paquets d'installation**. Vous pouvez utiliser le même paquet d'installation plusieurs fois.

Après la création du paquet d'installation, vous pouvez modifier les paramètres d'installation du Light Agent for Windows ou réaliser une configuration plus détaillée des paramètres d'installation (par exemple, définir la liste des composants du Light Agent à installer) (cf. section "Configuration des paramètres du paquet d'installation du Light Agent" à la page 88).

Configuration des paramètres du paquet d'installation du Light Agent for Windows

► *Pour modifier les paramètres du paquet d'installation du Light Agent for Windows, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Avancé/Installation à distance**, puis le dossier **Paquets d'installation**.
3. Dans la liste des paquets d'installation, sélectionnez un paquet d'installation du Light Agent et ouvrez la fenêtre **Propriétés : <Nom du paquet d'installation>** de l'une des manières suivantes :
   - en double-cliquant ;
   - cliquez avec le bouton droit pour ouvrir le menu contextuel et sélectionnez l'option **Propriétés** ;
   - via le lien **Ouvrir la fenêtre des propriétés du paquet d'installation**, situé à droite de la liste des tâches dans le groupe avec les paramètres du paquet d'installation.

4. La section **Paramètres** permet de modifier les paramètres d'installation du Light Agent for Windows configurés lors de la création du paquet d'installation. Elle permet également d'indiquer les composants du Light Agent qui doivent être installés sur la machine virtuelle protégée :

   - Si la case en regard d'un composant est cochée, Kaspersky Security installe le composant sur la machine virtuelle. Si le composant est déjà installé, rien ne change.
   - Si la case en regard d'un composant n'est pas cochée, Kaspersky Security supprime le composant. Si le composant n'était pas installé, rien ne change.

   Toutes les sections de la fenêtre **Propriétés : <nom du paquet d'installation>**, sauf la section **Paramètres**, sont standard pour l'application Kaspersky Security Center. Pour plus d'informations sur les sections standards, consultez la documentation de Kaspersky Security Center.

5. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés <nom du paquet d'installation>**.

Installation du Light Agent for Windows à l'aide de l'assistant d'installation

Avant de commencer l'installation du composant Light Agent for Windows, il est conseillé de fermer l'ensemble des applications fonctionnant dans le système d'exploitation de la machine virtuelle.

► *Pour installer le composant Light Agent for Windows à l'aide de l'Assistant d'installation, procédez comme suit :*

1. Lancez l'archive autoextractible Agent_4.0.X.X_sfx_ru.exe, où 4.0.X.X désigne la version de l'application. Ce fichier fait partie de la distribution (cf. section "Fichiers, indispensables à l'installation de l'application" à la page 45).

   L'Assistant de décompactage démarre. Suivez ses instructions.

2. Lancez le fichier setup.exe dans le système d'exploitation de la machine virtuelle que vous souhaitez protéger.

   L'Assistant d'installation du Light Agent démarre.

3. Suivez les instructions de l'Assistant d'installation du Light Agent.

Avant l'installation du Light Agent for Windows sur la machine virtuelle que vous souhaitez protéger, l'Assistant d'installation vérifie si les conditions suivantes sont remplies :

- La conformité du système d'exploitation de la machine virtuelle à la configuration requise par Kaspersky Security (cf. section " Configurations matérielles et logicielles requises " à la page 24).

  Si l'une des conditions n'est pas remplie, un message apparaît.

- L'absence d'applications incompatibles sur la machine virtuelle. L'Assistant d'installation effectue une recherche sur la machine virtuelle afin de détecter les applications qui, lorsqu'elles fonctionnent simultanément avec Light Agent, peuvent entraîner des conflits. S'il détecte de telles applications, l'Assistant d'installation affiche leur liste et demande confirmation pour les supprimer. Lorsqu'il reçoit la confirmation, l'Assistant d'installation tente de supprimer l'application automatiquement. Si la suppression de ces applications demande un redémarrage, l'Assistant d'installation redémarre la machine virtuelle. La liste des applications incompatibles figure dans le fichier incompatible.txt, repris dans le paquet d'installation de Kaspersky Security.

  Si la machine virtuelle comporte des applications que l'Assistant d'installation ne peut pas supprimer automatiquement, il vous est proposé de les supprimer manuellement.

Pendant l'installation, la machine virtuelle est soumise à la recherche d'une infection active. En cas de la détection d'une menace et d'impossibilité de désinfection, l'installation s'arrête sur une erreur. Pour neutraliser la menace, il est conseillé d'utiliser les utilitaires KVRT et Rescue Disc. La description des utilitaires figure dans la Base des connaissances (http://support.kaspersky.com/fr/11102).

Dans cette section

Etape 1. Fenêtre d'accueil de l'Assistant d'installation 91

Etape 2. Consultation du Contrat de licence 91

Etape 3. Sélection du type d'installation 92

Etape 4. Sélection des composants du Light Agent pour l'installation 93

Etape 5. Sélection du dossier d'installation 94

Etape 6. Configuration de la zone de confiance 94

Etape 7. Lancement de l'installation 96

Etape 8. Installation du composant Light Agent for Windows 97

Etape 9. Fin de l'installation 97

Etape 1. Fenêtre d'accueil de l'Assistant d'installation

Si les conditions d'installation du composant Light Agent for Windows sont conformes à la configuration requise, la fenêtre de démarrage de l'Assistant d'installation s'affiche. La fenêtre de démarrage de l'Assistant d'installation contient des informations sur le lancement de l'installation du Light Agent for Windows sur la machine virtuelle que vous souhaitez protéger.

Passez à l'étape suivante de l'Assistant d'installation.

Etape 2. Consultation du Contrat de Licence Utilisateur Final

A cette étape, vous devez prendre connaissance du Contrat de Licence Utilisateur Final conclu entre vous et Kaspersky Lab.

Lisez attentivement le Contrat de Licence Utilisateur Final et, si vous en acceptez tous les points, cochez la case **J'accepte les termes du contrat de licence**.

Passez à l'étape suivante de l'Assistant.

Etape 3. Sélection du type d'installation

A cette étape, sélectionnez le type d'installation pour le composant Light Agent.

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.

Si vous installez Light Agent sur une machine virtuelle équipée d'un système d'exploitation Microsoft Windows pour poste de travail, vous avez le choix entre les paramètres suivants :

- **Installation des modules de protection**. Sélectionnez cette option si vous souhaitez installer les modules de la protection du Light Agent avec les paramètres recommandés par les experts de Kaspersky Lab sur la machine virtuelle.
- **Installation des modules de protection et de contrôle**. Sélectionnez cette option si vous souhaitez installer les modules de la protection et les modules de contrôle du Light Agent avec les paramètres recommandés par les experts de Kaspersky Lab sur la machine virtuelle.
- **Installation personnalisée**. Cochez cette case si vous souhaitez sélectionner le dossier où sera installée l'application (cf. section "Etape 5. Sélection d'un dossier pour l'installation" à la page 94), et les composants du Light Agent à installer (cf. section "Etape 4. Sélection des composants du Light Agent à installer" à la page 93).

Si vous installez le Light Agent sur une machine virtuelle équipée d'un système d'exploitation hôte Microsoft Windows pour serveur, vous avez le choix entre les options suivantes :

- **Installation complète**. Sélectionnez cette option si vous souhaitez installer les modules de la protection du Light Agent avec les paramètres recommandés par les experts de Kaspersky Lab sur la machine virtuelle.
- **Installation personnalisée**. Sélectionnez cette option si vous souhaitez sélectionner le dossier où sera installée l'application (cf. section "Etape 5. Sélection d'un dossier pour l'installation" à la page 94), et les modules de la protection du Light Agent à installer (cf. section "Etape 4. Sélection des composants du Light Agent à installer" à la page 93).

Passez à l'étape suivante de l'Assistant d'installation.

Etape 4. Sélection des composants du Light Agent pour l'installation

> Cette étape apparaît si vous avez coché la case **Installation personnalisée** ou si vous avez choisi l'option **Installation personnalisée** à l'étape "Sélection du type d'installation" (cf. section "Etape 3. Sélection du type d'installation" à la page 92).

A cette étape, vous pouvez choisir les composants du Light Agent que vous souhaitez installer.

Si vous installez Light Agent sur une machine virtuelle équipée d'un système d'exploitation Microsoft Windows pour poste de travail, les composants suivants sont installés par défaut :

- tous les modules de la protection si vous avez choisir l'option "Installation des composants de protection" ;
- tous les modules de la protection et tous les modules de contrôle si vous avez choisi l'option "Installation des modules de la protection et de contrôle".

Si vous installez le Light Agent sur une machine virtuelle équipée d'un système d'exploitation Microsoft Windows pour serveur, tous les composants de protection sont installés par défaut. Les modules de contrôle ne sont pas installés sur la machine virtuelle dotée d'un système d'exploitation Microsoft Windows pour serveur.

Pour sélectionner le composant Light Agent en vue du suivi de l'installation, ouvrez le menu contextuel en cliquant sur l'icône située en regard du nom du composant et sélectionnez l'option **Le composant sera installé sur** le disque dur local. Les informations concernant la nature des tâches exécutées par le composant sélectionné et l'espace nécessaire sur le disque dur pour l'installation de ce composant se trouvent dans la partie inférieure de la fenêtre de l'Assistant d'installation.

Pour en savoir plus sur l'espace disponible sur le disque dur de la machine virtuelle à protéger, cliquez sur le bouton **Disque**. Ces informations apparaissent dans la fenêtre contextuelle **Espace disque disponible**.

Pour renoncer à l'installation du composant Light Agent, ouvrez le menu contextuel en cliquant sur l'icône située en regard du nom du composant et sélectionnez l'option **Le composant ne sera pas disponible**.

Pour retourner à la liste des composants du Light Agent installés par défaut, cliquez sur le bouton **Effacer**.

Passez à l'étape suivante de l'Assistant d'installation.

Etape 5. Sélection du dossier d'installation

> Cette étape apparaît si vous avez coché la case **Installation personnalisée** ou si vous avez choisi l'option **Installation personnalisée** à l'étape "Sélection du type d'installation" (cf. section "Etape 3. Sélection du type d'installation" à la page 92).

A cette étape, indiquez le chemin vers le dossier où le Light Agent for Windows sera installé. Pour ce faire, cliquez sur le bouton **Parcourir** et, dans la fenêtre **Modification du dossier d'installation de l'application** qui s'ouvre, sélectionnez le dossier pour l'installation.

Pour prendre connaissance des informations concernant l'espace disponible sur le disque dur de la machine virtuelle à protéger, cliquez sur le bouton **Disque**. Ces informations apparaissent dans la fenêtre contextuelle **Espace disque disponible**.

Passez à l'étape suivante de l'Assistant d'installation.

Etape 6. Configuration de la zone de confiance

Lors de cette étape, vous pouvez créer une zone de confiance pour le composant Light Agent for Windows.

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.

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 d'installation.

Etape 7. Lancement de l’installation

Le système d'exploitation de la machine virtuelle à protéger étant susceptible de comporter des programmes malveillants pouvant entraver l'installation du Light Agent, il est conseillé de protéger l'installation.

Par défaut, la protection de l'installation est activée.

Il est recommandé de désactiver la protection de l'installation lorsqu'il est impossible de mener à bien l'installation du Light Agent. Par exemple, cette situation peut se produire lors de l'installation à distance via Windows Remote Desktop. La protection activée de l'installation du Light Agent peut en être la cause. Dans ce cas, interrompez l'installation et relancez l'Assistant d'installation. A cette étape, décochez la case **Protéger le processus d'installation**.

Si vous installez Light Agent sur une machine virtuelle qui utilise la technologie Citrix Provisionning Services, cochez la case **Garantir la compatibilité avec Citrix Provisioning Services**.

Si vous installez Light Agent sur le modèle de machines virtuelles temporaires, cochez la case **Installation sur un modèle pour les pools temporels VDI** (cf. section "**Installation du Light Agent for Windows sur le modèle de machines virtuelles**" à la page 102). Les mises à jour demandant le redémarrage de la machine virtuelle protégée ne s'installeront pas sur les machines virtuelles créées à partir de ce modèle. À la réception des mises à jour demandant le redémarrage de la machine virtuelle protégée, le Light Agent enverra à Kaspersky Security Center un message sur la nécessité de la mise à jour des bases et des modules de l'application sur le modèle des machines virtuelles protégées.

> Pour en savoir plus sur l'installation de Light Agent sur les modèles de machine virtuelle, consultez également la Base des connaissances (http://support.kaspersky.com/fr/13108).

La case **Ajouter le chemin d'accès au fichier avp.com à la variable système %PATH%** active / désactive la fonction qui ajoute le chemin vers le fichier avp.com dans la variable système %PATH%. Si la case est cochée, il n'est pas nécessaire de saisir le chemin vers le fichier utilisé pour le lancement du Light Agent ou de l'une de ses tâches à partir de la ligne de commande. Il suffit de saisir le nom du fichier utilisé et la commande pour le lancement de la tâche correspondante.

Pour lancer l'installation du Light Agent, cliquez sur le bouton **Installer**.

Les connexions réseau en cours risquent d'être interrompues lors de l'installation du Light Agent sur la machine virtuelle. La majorité des connexions interrompues seront rétablies automatiquement après quelques secondes.

Etape 8. Installation du composant Light Agent for Windows

Il s'agit de l'étape d'installation du composant Light Agent for Windows. L'installation nécessite un peu de temps, veuillez patienter jusqu'à la fin.

Etape 9. Fin de l'installation

A cette étape, quittez l'Assistant.

Le composant Light Agent for Windows se lance automatiquement sur la machine virtuelle après son installation.

Le Light Agent for Windows se connecte à la SVM. Le Serveur de protection transmet les informations sur la licence au Light Agent.

Le Light Agent for Windows vérifie si un paquet de mises à jour est disponible dans le dossier de la SVM à laquelle il est connecté. En cas de présence d'un paquet de mises à jour du Light Agent for Windows, l'application installe les mises à jour des bases et des composants de l'application nécessaires au fonctionnement de l'application sur la machine virtuelle protégée.

Installation du Light Agent for Windows via la ligne de commande

Les privilèges d’administrateur sont nécessaires pour lancer l’installation du Light Agent via la ligne de commande.

► *Pour installer le Light Agent for Windows à partir de la ligne de commande en mode interactif, procédez comme suit :*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `setup.exe`
- `msiexec /i <nom du paquet d'installation au format MSI>`.

Lancez l'Assistant d'installation de l'application. Suivez ses instructions.

Le fichier setup.exe et le paquet d'installation au format MSI font partie de la distribution de Kaspersky Security (cf. section "Fichiers indispensables à l'installation de l'application" à la page 45).

► *Pour installer le Light Agent for Windows à partir de la ligne de commande en mode discret (sans lancement de l'Assistant d'installation de l'application) :*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `setup.exe /s /pEULA=1 /pALLOWREBOOT=1|0`
- `msiexec /i <nom du paquet d'installation au format MSI> EULA=1 ALLOWREBOOT=1|0 /qn`,

où :

- `EULA=1` signifie que vous acceptez les conditions du Contrat de Licence Utilisateur Final. Le Contrat de Licence Utilisateur Final est repris dans la distribution de l'application (cf. section "Distribution" à la page. 23). L'acceptation des conditions du Contrat de Licence Utilisateur Final est indispensable à l'installation de l'application.
- `ALLOWREBOOT=1|0` indique l'autorisation ou l'interdiction concernant le redémarrage automatique de la machine virtuelle, si celui-ci est demandé après l'installation. Paramètre facultatif. Si la valeur du paramètre `ALLOWREBOOT` n'est pas indiquée dans la commande, il est considéré par défaut que vous interdisez le redémarrage de la machine virtuelle après l'installation de l'application. Le redémarrage automatique de la machine virtuelle peut avoir lieu uniquement en mode d'installation discrète (avec la clé `/qn`).

  Le redémarrage de la machine virtuelle peut être nécessaire si, lors de l'installation du Light Agent, une application antivirus tierce est détectée et supprimée.

► *Pour installer Light Agent sur une machine virtuelle qui utilise la technologie Citrix Provisionning Services,*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `setup.exe /pINSTALLONPVS=1`
- `msiexec /i <nom du paquet d'installation au format MSI> INSTALLONPVS=1`.

► *Pour installer le Light Agent sur un modèle de machines virtuelles temporaires,*

indiquez dans la commande le paramètre `USEPVMDETECTION=1`, par exemple : `setup.exe /pUSEPVMDETECTION=1`.

► *Pour installer le Light Agent avec un mot de passe pour la manipulation de l'application,*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `setup.exe /pKLLOGIN=<nom d'utilisateur> /pKLPASSWD=***** /pKLPASSWDAREA=<zone d'action du mot de passe>`
- `msiexec /i <nom du paquet d'installation au format MSI> KLLOGIN=<nom d'utilisateur> KLPASSWD=***** KLPASSWDAREA=<zone d'action du mot de passe>`.

Au lieu de `<zone d'action du mot de passe>`, vous pouvez indiquer l'une des valeurs du paramètre `KLPASSWDAREA` suivantes via ";" :

- `SET`. Définition d'un mot de passe pour la modification des paramètres de l'application.
- `EXIT`. Définition d'un mot de passe pour quitter l'application.
- `DISPROTECT`. Définition d'un mot de passe pour la désactivation des modules de la protection et l'arrêt des tâches d'analyse.
- `DISPOLICY`. Définition d'un mot de passe pour la désactivation des stratégies de Kaspersky Security Center.
- `UNINST`. Définition d'un mot de passe pour la suppression de l'application de la machine virtuelle.
- `DISCTRL`. Définition d'un mot de passe pour la désactivation des modules de contrôle (Contrôle du lancement des applications, Contrôle de l'activité des applications, Contrôle des périphériques, Contrôle Internet).

Les fichiers suivants peuvent être utilisés lors de l'installation de l'application via la ligne de commande :

- Fichier setup.ini. Ce fichier contient les paramètres généraux d'installation de l'application. Il est utilisé pour installer le composant Light Agent à partir de la ligne de commande ou via l'éditeur d'administration des stratégies de groupe du service des catalogues (cf. section "Installation du Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues" à la page 100). Le fichier setup.ini est créé manuellement. Une description du fichier setup.ini est disponible sur la page dédiée à l'application dans la base de connaissances (http://support.kaspersky.com/fr/131176).
- Fichier de configuration install.cfg. Le fichier contient les paramètres du composant Light Agent et sert à importer ces paramètres lors de l'installation du Light Agent et lors de la création d'une stratégie pour le Light Agent. Il permet également de transférer les paramètres configurés de l'application sur une autre machine virtuelle protégée. Le fichier de configuration est créé dans l'interface locale du Light Agent (informations détaillées dans le *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

Les fichiers setup.ini et install.cfg doivent être situés dans le même dossier que le paquet d'installation de Kaspersky Security for Virtualization 4.0 Light Agent.

Installation du Light Agent for Windows via l'éditeur des stratégies de groupe du service de catalogues

Grâce à l'éditeur d'administration des stratégies de groupe du service d'annuaire (Active Directory Group Policies), vous pouvez installer le composant Light Agent for Windows sur les machines virtuelles associées à l'objet de stratégie de groupe sélectionné sans utiliser le Kaspersky Security Center.

Pour en savoir plus sur l'éditeur d'administration des stratégies de groupe du service de catalogues, veuillez consulter l'*Aide de Microsoft Windows*.

Avant de commencer l'installation du composant Light Agent for Windows, il est conseillé de fermer l'ensemble des applications fonctionnant dans le système d'exploitation de la machine virtuelle.

► *Pour installer le Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues, procédez comme suit :*

1. Créez un dossier réseau partagé sur l'ordinateur où est installé le contrôleur de domaine.
2. Placez les fichiers suivants dans le dossier réseau partagé :
   - paquet d'installation de Kaspersky Security au format MSI ;
   - fichier setup.ini avec la valeur de paramètre `EULA` égale à 1. Une description du fichier setup.ini est disponible sur la page dédiée à l'application dans la base de connaissances (http://support.kaspersky.com/fr/13176).
3. Ouvrez la fenêtre de Microsoft Windows **Administration des stratégies de groupe**.
4. Dans l'arborescence de la fenêtre **Administration des stratégies de groupe**, sélectionnez l'objet de stratégie de groupe (Group Policy Object) auquel sont associées les machines virtuelles dédiées à l'installation du Light Agent for Windows.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet de stratégie de groupe, puis sélectionnez l'option **Modifier**.

   L'éditeur d'administration des stratégies de groupe du service de catalogues s'ouvre.
6. Créez un nouveau paquet d'installation pour l'éditeur d'administration des stratégies de groupe. Pour ce faire, procédez comme suit :
   a. Dans l'arborescence de la console, sélectionnez **Objet de la stratégie groupée \ Configuration de l'ordinateur \ Stratégies \ Configuration des applications \ Installation de l'application**.
   b. Cliquez-droit pour ouvrir le menu contextuel du poste **Installation de l'application**.
   c. Dans le menu contextuel, sélectionnez l'option **Créer** → **Paquet**.

      La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.
   d. Dans la fenêtre standard **Ouvrir** de Microsoft Windows, cochez l'option pour le paquet d'installation de Kaspersky Security au format MSI.

      La fenêtre **Déploiement de l'application** s'ouvre.

e. Dans la fenêtre de dialogue **Déploiement de l'application**, sélectionnez le paramètre **Attribué**.

f. Cliquez sur le bouton **OK**.

La stratégie de groupe s'applique sur chaque machine virtuelle associée à l'objet de stratégie de groupe lors du lancement des machines virtuelles suivant. Ainsi, le composant Light Agent for Windows sera installé sur l'ensemble des machines virtuelles associées à l'objet de stratégie de groupe sélectionné.

Installation du Light Agent for Windows sur un modèle de machine virtuelle

► *Pour installer le composant Light Agent for Windows sur le modèle de machine virtuelle, procédez comme suit :*

1. Sur l'hyperviseur, activez la machine virtuelle tenant lieu de modèle de machine virtuelle.
2. Installez le composant Light Agent for Windows sur le modèle de machine virtuelle. L'installation s'opère en mode interactif, à l'aide de l'Assistant d'installation (cf. section "Installation du Light Agent for Windows à l'aide de l'assistant d'installation" à la page 89).
3. Lors de l'étape 7 de l'assistant (cf. section "Etape 7. Lancement de l'installation" à la p. 96) cochez la case **Installation sur un modèle pour les pools temporels VDI** si une infrastructure VDI d'un des types suivants est créée à partir du modèle :
   - catalogue Citrix XenDesktop random ;
   - catalogue Citrix XenDesktop static à l'aide de Citrix Personal vDisk ;
   - catalogue Citrix XenDesktop static sans enregistrement des modifications de l'utilisateur ;
   - pool automated VMware Horizon View de type linked clone.

   Si la case est cochée, les mises à jour demandant le redémarrage de la machine virtuelle protégée ne s'installeront pas sur les machines virtuelles créées à partir de ce modèle. À la réception des mises à jour demandant le redémarrage de la machine virtuelle protégée, le Light Agent enverra à Kaspersky Security Center un message sur la nécessité de la mise à jour des bases et des modules de l'application sur le modèle des machines virtuelles protégées.

Il n'est pas recommandé de cocher la case **Installation sur un modèles pour les pools temporels VDI** si une infrastructure VDI d'un des types suivants est créée à partir des types suivants :

- catalogue Citrix XenDesktop static dedicated à l'aide des disques locaux ;
- pool automated VMware Horizon View de type full clone.

4. La configuration de la connexion de Light Agent à KVM s'effectue dans l'interface locale de Light Agent for Windows (cf. *Manuel* de *l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent for Windows*). Après la connexion de la SVM, le Serveur de protection transmet les informations sur la licence au Light Agent. Vous devez attendre les réceptions des informations sur la licence par Light Agent.

5. Le Light Agent vérifie si un paquet de mises à jour est disponible dans le dossier de la SVM à laquelle il est connecté. En cas de présence d'un paquet de mises à jour du Light Agent for Windows, l'application installe les mises à jour des bases et des composants de l'application nécessaires au fonctionnement de l'application sur la machine virtuelle protégée.

   Vous pouvez attendre les réceptions par le Light Agent de la mise à jour des bases et des modules de l'application ou lancer manuellement la tâche de mise à jour dans l'interface locale du Light Agent for Windows, puis analyser le modèle de machine virtuelle pour y détecter des logiciels malveillants (cf. *Manuel* de *l'utilisateur de Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

   Il est recommandé de redémarrer le modèle de machine virtuelle pour optimiser le processus de démarrage du système d'exploitation.

6. Recréez des machines virtuelles à partir du modèle mis à jour. Pour plus d'informations, consultez la documentation concernant l'infrastructure virtuelle.

Pour en savoir plus sur l'installation de Light Agent sur les modèles de machine virtuelle, consultez également la Base des connaissances (http://support.kaspersky.com/fr/13108).

Compatibilité avec la technologie Citrix Provisioning Services

Il est possible d'installer Light Agent sur une machine virtuelle qui utilise la technologie Citrix Provisionning Services,

> Si le logiciel Citrix Provisioning Services Target Device est installé sur la machine virtuelle, il doit être supprimé avant le lancement de l'installation du composant Light Agent.
> Citrix Provisioning Services Target Device doit être installé après l'installation du Light Agent.

Pour garantir la compatibilité entre Kaspersky Security et la technologie Citrix Provisioning Services, il faut installer le Light Agent d'une des manières suivantes :

- Via l'Assistant d'installation. A l'étape 7 de l'Assistant, cochez la case **Garantir la compatibilité avec Citrix Provisioning Services**.
- Depuis la ligne de commande avec le paramètre INSTALLONPVS=1 (cf. section " Installation du Light Agent for Windows depuis la ligne de commande " à la page 97).
- A distance via Kaspersky Security Center. Lors de la création d'un paquet d'installation, utilisez le fichier Ksvla.kud (cf. section " Création d'un paquet d'installation du Light Agent for Windows " à la page 85).

L'interface locale du Light Agent installé sur une machine virtuelle protégée reprend les informations relatives à la compatibilité avec la technologie Citrix Provisionning Services.
Les informations relatives à la prise en charge ou non de Citrix Provisioning Services, figurent dans la fenêtre **Support Technique** qui s'ouvre au départ de la fenêtre principale de l'application.

Compatibilité avec la technologie Citrix Personal vDisk

Vous pouvez installer le Light Agent sur une machine virtuelle qui utilise la technologie Citrix Personal vDisk via une des méthodes suivantes prévues pour cette tâche d'installation.

> L'application Citrix Personal vDisk doit être installée sur la machine virtuelle de protection avant l'installation du composant Light Agent.

Pour garantir la compatibilité avec la technologie Citrix Personal vDisk, Kaspersky Security ajoute automatiquement la section suivante au fichier custom_files_rules.txt :

```
[Rule-Begin]

Type=File-Catalog-Construction

Action=Catalog-Location-Guest-Modifiable

name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"

[Rule-End]
```

Modification de la composition des composants installés du Light Agent for Windows

Après l'installation de Light Agent for Windows sur la machine virtuelle, vous pouvez modifier la liste des composants installés du Light Agent d'une des manières suivantes :

- A l'aide d'une tâche de groupe de modification des modules de l'application. La tâche est créée dans Kaspersky Security Center. Lors de l'exécution de cette tâche, Kaspersky Security installe ou supprime les composants du Light Agent sur les machines virtuelles protégées conformément à la liste configurée des composants.
- Via une nouvelle installation à distance du Light Agent for Windows via Kaspersky Security Center à l'aide d'un paque d'installation dans lequel la liste des composants du Light Agent a été modifiée (cf. section "Configuration des paramètres u paquet d'installation du Light Agent for Windows" à la page 88).

► *Pour modifier la composition des composants installés du Light Agent for Windows à l'aide d'une tâche de groupe de modification des modules 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 pour l'ensemble des machines virtuelles protégées de ce groupe, 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 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 **Modification des modules de l'application**.

5. Sélectionnez le type d'installation du Light Agent, puis passez à l'étape suivante de l'Assistant.

6. Si vous créez une tâche pour une ou plusieurs machines virtuelles, indiquez le mode de sélection de celles-ci. En fonction du mode choisi pour la sélection des machines virtuelles, procédez comme suit dans la fenêtre qui s'ouvre :

   - Dans la liste des machines virtuelles détectées, désignez les machines virtuelles sur lesquelles vous souhaitez modifier la composition des composants du Light Agent installés. Pour ce faire, cochez la case à gauche, en regard du nom de la machine virtuelle.

   - Cliquez sur le bouton **Ajouter** ou **Ajouter un intervalle IP** et définissez manuellement les adresses des machines virtuelles.

   - Cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier au format TXT contenant la liste des adresses des machines virtuelles.

   - Appuyez sur le bouton **Sélectionner**, et dans la fenêtre qui s'ouvre, indiquez le nom de l'ensemble contenant les machines virtuelles sur lesquelles vous souhaitez modifier la composition des composants installés du Light Agent.

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

7. Configurez le mode de lancement de la tâche, puis passez à l'étape suivante de l'Assistant.

8. Indiquez le nom de la tâche créée et passez à l'étape suivante de l'Assistant.

9. Quittez l'Assistant de création d'une tâche. La tâche créée apparaît dans la liste des tâches pour le groupe sélectionné dans l'onglet **Tâches** ou dans le dossier **Tâches**.

10. Sélectionnez la tâche créée dans la liste des tâches et ouvrez la fenêtre **Propriétés : <nom de la tâche>** d'un double-clic de la souris ou à l'aide de l'option **Propriétés** du menu contextuel.

11. Dans la section **Paramètres**, désignez les composants du Light Agent qu'il faut installer sur la machine virtuelle protégée :

    - Si la case en regard d'un composant est cochée, Kaspersky Security installe le composant sur la machine virtuelle. Si le composant est déjà installé, rien ne change.

    - Si la case en regard d'un composant n'est pas cochée, Kaspersky Security supprime le composant. Si le composant n'était pas installé, rien ne change.

12. Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés :<nom de la tâche>**

13. Lancez la tâche de modification de la composition des composants ou attendez son lancement programmé.

Installation du composant Light Agent for Linux

Le Light Agent for Linux peut être installé sur la machine virtuelle par une des méthodes suivantes :

- Depuis la ligne de commande (cf. section "Installation du Light Agent for Linux depuis la ligne de commande" à la page 111).

- A distance depuis le poste de travail de l'administrateur à l'aide de l'application Kaspersky Security Center (cf. section "Installation du Light Agent for Linux via Kaspersky Security Center" à la page 108).

Avant l'installation du Light Agent for Linux, vous devez installer l'Agent d'administration de Kaspersky Security Center (cf. section "Installation de l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles" à la p. 81).

Dans cette section

Installation du Light Agent for Linux via Kaspersky Security Center 108

Installation du Light Agent for Linux via la ligne de commande 111

Installation du Light Agent for Linux via Kaspersky Security Center

Il est possible d'installer le Light Agent for Linux à distance, à partir du poste de travail de l'administrateur, à l'aide de l'application Kaspersky Security Center. L'installation s'effectue à l'aide de l'assistant de déploiement de la protection ou à l'aide de la tâche d'installation à distance de l'application. L'installation s'opère à l'aide du paquet d'installation qui contient la sélection de paramètres indispensables à l'installation de l'application (cf. section "Création du paquet d'installation Light Agent for Linux" à la page 110).

Avant la création d'un paquet d'installation, vous devez exécuter la préparation de la distribution du Light Agent for Linux (cf. section "Préparation de la distribution du Light Agent for Linux" à la p. 109).

L'installation de l'Agent d'administration sur la machine virtuelle avec le système d'exploitation Linux dans Kaspersky Security Center n'est pas prise en charge. Par conséquent, lors de l'installation du Light Agent for Linux à l'aide de la tâche de l'installation à distance de l'application, dans la fenêtre **Avancé**, ne cochez pas la case **Installer l'Agent d'administration avec l'application donnée**.

Pour en savoir plus sur l'installation à distance de l'application via le Kaspersky Security Center, consultez la documentation de Kaspersky Security Center.

Dans cette section

Préparation de la distribution du Light Agent for Linux 109

Création du paquet d'installation du Light Agent for Linux 110

Préparation de la distribution du Light Agent for Linux

► *Pour préparer la distribution du Light Agent for Linux à la création du paquet d'installation, procédez comme suit :*

1. Dans le dossier accessible au Serveur d'administration de Kaspersky Security Center, dépaquetez une des archives suivantes (en fonction du gestionnaire de paquets utilisé dans le système d'exploitation de la machine virtuelle) :

   - lightagent-4.0.X-X_rpm-<identifiant de la langue>.tar.gz (pour l'installation du paquet au format RPM) ;
   - lightagent-4.0.X-X_deb-<identifiant de la langue>.tar.gz (pour l'installation du paquet au format DEB) ;

   où :

   - 4.0.X : désigne la version de l'application.
   - <identifiant de la langue> désigne l'identifiant à deux lettres de la langue : ru, en, fr, de, etc.

2. Copiez dans le même dossier un des paquets suivants (en fonction du système d'exploitation de la machine virtuelle et du manager de paquets utilisé dans le système d'exploitation) :

   - lightagent-4.0.X-X.i686.rpm (paquet au format RPM pour le système d'exploitation 32 bits) ;
   - lightagent-4.0.X-X.x86_64.rpm (paquet au format RPM pour le système d'exploitation 64 bits) ;
   - lightagent_4.0.X-X_i386.deb (paquet au format DEB pour le système d'exploitation 32 bits) ;
   - lightagent_4.0.X-X_amd64.deb (paquet au format DEB pour le système d'exploitation 64 bits) ;

   où 4.0.X-X désigne la version de l'application.

Création du paquet d'installation du Light Agent for Linux

Le paquet d'installation est requis pour l'installation à distance du composant Light Agent for Linux via Kaspersky Security Center.

Avant la création d'un paquet d'installation, vous devez exécuter la préparation de la distribution du Light Agent for Linux (cf. section "Préparation de la distribution du Light Agent for Linux" à la p. 109).

► *Pour créer le paquet d'installation de Light Agent for Linux, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Avancé/Installation à distance**, puis le dossier **Paquets d'installation**.
3. Cliquez sur le bouton **Créer un paquet d'installation** pour lancer l'assistant de création d'un paquet d'installation.
4. Dans la fenêtre ouverte de l'assistant, cliquez sur le bouton **Créer un paquet d'installation pour l'application de Kaspersky Lab**.
5. Dans la fenêtre de l'assistant, saisissez le nom du nouveau paquet d'installation et passez à l'étape suivante.
6. Dans la fenêtre de l'assistant **Choix de la distribution de l'application pour l'installation**, choisissez la distribution de l'application Kaspersky Security. Cliquez pour cela sur le bouton **Sélectionner** et, dans la fenêtre Windows standard **Ouvrir**, indiquez le chemin d'accès au fichier lightagent.kud.

   La fenêtre de l'assistant **Choix de la distribution de l'application pour l'installation** affiche le nom de l'application.

   Passez à l'étape suivante de l'Assistant.

7. Dans la fenêtre de l'assistant **Contrat de licence**, prenez connaissance des conditions du Contrat de Licence Utilisateur Final conclu entre vous et Kaspersky Lab. Il faut accepter les termes du Contrat de Licence Utilisateur Final pour pouvoir poursuivre la création du paquet d'installation. Cochez la case **J'accepte les dispositions du Contrat de Licence Utilisateur Final** et passez à l'étape suivante de l'Assistant.

8. L'Assistant télécharge les fichiers indispensables à l'installation de l'application sur le Serveur d'administration de Kaspersky Security Center. Attendez la fin du téléchargement.

9. Fermez l'Assistant.

Le paquet d'installation créé est placé dans l'arborescence de la console d'administration de Kaspersky Security Center dans le dossier **Avancé/Installation à distance**, sous-dossier **Paquets d'installation**. Vous pouvez utiliser le même paquet d'installation plusieurs fois.

Installation du Light Agent for Linux via la ligne de commande

Le composant Light Agent for Linux se trouve dans les paquets aux formats DEB et RPM.

► *Pour installer le Light Agent for Linux via la ligne de commande, exécutez une des commandes suivantes (en fonction du système d'exploitation de la machine virtuelle et du gestionnaire de paquets utilisé dans le système d'exploitation) :*

- `# rpm -i lightagent-4.0.X-X.i686.rpm` – pour l'installation du paquet au format RPM sur le système d'exploitation de 32 bits ;
- `# rpm -i lightagent-4.0.X-X.x86_64.rpm` – pour l'installation du paquet au format RPM sur le système d'exploitation 64 bits ;
- `# dpkg-i lightagent_4.0.X-X_i386.deb` – pour l'installation du paquet au format DEB sur le système d'exploitation 32 bits ;
- `# dpkg-i lightagent_4.0.X-X_amd64.deb` – pour l'installation du package du format DEB sur le système d'exploitation 64 bits ;

où `4.0.X-X` désigne la version de l'application.

Après le lancement de la commande, l'installation est exécutée automatiquement.

Après l'achèvement de l'installation du Light Agent for Linux, vous exécuter sa configuration initiale par une des méthodes suivantes :

- en mode interactif (cf. section "Configuration initiale du Light Agent for Linux en mode interactif" à la p. 112) ;
- en mode silencieux (cf. la section "Configuration initiale du Light Agent for Linux en mode silencieux" à la p. 113).

Si vous n'exécutez pas la configuration initiale du Light Agent for Linux, la protection antivirus de la machine virtuelle ne sera pas opérationnelle.

Configuration initiale du Light Agent for Linux en mode interactif

► *Pour exécuter la configuration initiale du Light Agent for Linux en mode interactif, procédez comme suit :*

1. Exécutez la commande suivante :

   ```
   /opt/kaspersky/lightagent/bin/lightagent-setup.pl
   ```

   Le script de configuration initiale de l'application se lance.

2. Lisez le Contrat de Licence Utilisateur Final conclu entre vous et Kaspersky Lab.
   Pour ce faire, appuyez sur la touche **ENTREE**. Pour la fin de l'affichage utilisez la touche **Q**.
   Après la sortie du mode d'affichage, saisissez yes (ou y) si vous êtes d'accord avec les conditions du Contrat de licence utilisateur final.

   Pour la suite de la configuration initiale du Light Agent for Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

3. Indiquez l'identifiant de la langue des événements du Light Agent for Linux envoyés à Kaspersky Security Center : ru, en, fr ou autre.

   Par défaut, le script de configuration initiale de l'application propose d'utiliser l'identifiant de la langue en. Cliquez sur la touche **ENTREE** pour confirmer l'utilisation de l'anglais pour les événements ou indiquez un autre identifiant de langue.

4. Confirmez le chemin d'accès aux codes sources du noyau du système d'exploitation ou indiquez un autre chemin d'accès à ces codes sources.

   Si le script de configuration initiale de l'application détecte les codes sources du noyau du système d'exploitation dans le dossier par défaut, le chemin trouvé s'affiche sur l'écran. Pour confirmer le chemin d'accès aux codes sources du noyau du système d'exploitation, cliquez sur la touche **ENTREE**.

   Le script de configuration initiale de l'application lance la compilation du module du noyau du système d'exploitation Linux sur la machine virtuelle. Le module nécessaire à la tâche de protection en temps réel est compilé.

   Si la compilation du module du noyau ne s'est pas produite, la tâche de protection en temps réel ne traite pas l'opération sur les objets du système de fichiers de la machine virtuelle protégée.

5. La configuration du Light Agent for Linux s'exécute. Si, pendant la configuration, des erreurs apparaissent, des informations à leur sujet s'affichent à l'écran.

Configuration initiale du Light Agent for Linux en mode silencieux

► *Pour lancer la configuration initiale du Light Agent for Linux en mode silencieux,*

exécutez la commande suivante :

```
/opt/kaspersky/lightagent/bin/lightagent-setup.pl \

--auto-install=<chemin d'accès au fichier de configuration>
```

où :

<chemin d'accès au fichier de configuration> désigne le chemin complet d'accès au fichier de configuration initiale lightagent.ini (cf. section "Fichiers indispensables à l'installation de l'application" à la p. 45). L'application utilisera les paramètres indiqués dans ce fichier lors de l'exécution de la configuration initiale du Light Agent for Linux.

Le fichier de configuration initiale contient les paramètres suivants :

- EULA_AGREED : accord avec les conditions du Contrat de licence utilisateur final. Paramètre obligatoire. Valeur par défaut : yes.
- CONNECTOR_LOCALE : identifiant de la langue du Light Agent for Linux. Valeur par défaut : en.
- DEFAULT_KERNEL_SOURCES : utiliser le chemin d'accès aux codes sources du noyau du système d'exploitation, codes détectés par l'application dans le dossier par défaut. Valeur par défaut : yes.

Vous devez saisir les paramètres au format <nom du paramètre>=<valeur>. Les espaces entre le nom du paramètre et sa valeur ne sont pas traités.

Modifications dans le Kaspersky Security Center après l'installation de l'application

Après l'installation de Kaspersky Security dans l'infrastructure virtuelle, les SVM et les machines virtuelles protégées disposant de l'Agent d'administration transmettent les informations à leur sujet au Kaspersky Security Center. Par défaut, Kaspersky Security Center ajoute les machines virtuelles dotées de l'application Kaspersky Security au dossier **Périphériques non distribués**.

Dans la Console d'administration de Kaspersky Security Center, la SVM s'affiche sous le nom que vous avez indiqué pendant son déploiement. Le nom de la machine virtuelle protégée est identique à celui de la machine virtuelle sur le réseau (hostname). Si une machine virtuelle portant ce nom est déjà enregistrée sur le Serveur d'administration de Kaspersky Security Center, un chiffre est ajouté au nom de la nouvelle machine virtuelle, par exemple : <Nom>~1, <Nom>~2.

Vous pouvez déplacer manuellement les machines virtuelles dans le groupe d'administration **Ordinateurs administrés** ou dans les sous-groupes d'administration (pour des informations détaillées sur le déplacement des machines virtuelles dans les groupes d'administration, consultez la documentation de Kaspersky Security Center).

Si, avant l'installation, vous avez défini des règles de déplacement des machines virtuelles dans les groupes d'administration (cf. section "Définition des règles de déplacement des machines virtuelles dans les groupes d'administration" à la page 57), le Kaspersky Security Center déplace les machines virtuelles dotées de l'application Kaspersky Security dans les groupes d'administration indiqués en fonction de ces règles.

Une fois le déploiement sur l'hyperviseur effectué, la SVM transmet les balises suivantes à Kaspersky Security Center :

- %HvName%=<nom de l'hyperviseur> : nom de l'hyperviseur sur lequel s'exécute la SVM.
- %HvType%=<type de l'hyperviseur> : type de l'hyperviseur.

La machine virtuelle protégée disposant de l'Agent d'administration de Kaspersky Security Center transmet les balises suivantes à Kaspersky Security Center après connexion à la SVM exécutée sur ce même hyperviseur :

- %HvName%=<nom de l'hyperviseur> : nom de l'hyperviseur sur lequel s'exécute la machine virtuelle protégée.
- %HvType%=<type de l'hyperviseur> : type de l'hyperviseur.
- %VmType%=<Persistent / Nonpersistent> : symbole indiquant si la machine virtuelle est une machine virtuelle temporaire.

Vous pouvez utiliser les balises indiquées lors de la définition des règles de déplacement des SVM et des machines virtuelles protégées dans les groupes d'administration.

Activation de l'application

Cette section contient des informations sur l'activation de l'application.

Dans cette section

A propos de l'activation de l'application 116

Procédure d'activation de l'application..... 120

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 :

- 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 120).

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.

Vous pouvez regarder les informations sur les clés ajoutées sur les SVM dans la Console d'administration de Kaspersky Security Center.

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 (cf. section "Suppression du composant Serveur de protection" à la page 168).

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 118

Particularités de l'activation de l'application avec plusieurs types de clés..... 119

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 123).

   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 121) ou lorsque vous créez la tâche d'activation de l'application.

2. Lancez la tâche d'activation de l'application

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 121

Création d'une tâche d'activation de l'application 123

Lancement de la tâche d'activation de l'application 129

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 123).

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, sélectionnez l'onglet **Tâches**. Cliquez sur le bouton **Créer une tâche** pour lancer l'assistant de 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. Cliquez sur le bouton **Créer une tâche**.
     - Dans l'arborescence de la console, dans le dossier **Avancé**/**Administration des applications**, sélectionnez le sous-dossier **Licences pour une application Kaspersky Lab**. Cliquez sur le bouton **Diffuser 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 124

Etape 2. Ajout d'une clé 124

Etape 3. Choix de la SVM 126

Etape 4. Définition des paramètres de programmation de la tâche 127

Etape 5. Définition du nom de la tâche 128

Etape 6. Fin de la création de la tâche 128

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 121), 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. 121).
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, à n'importe quel moment, lancer manuellement la tâche de l'activation de l'application.

Lancement de la tâche d'activation de l'application

► *Pour lancer 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 :
   - 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 lancer une tâche d'activation de l'application. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
   - Choisissez le dossier **Tâches** à partir de l'arborescence de la console.
3. Dans la liste des tâches, sélectionnez la tâche d'activation de l'application que vous souhaitez lancer.
4. Exécutez 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.

Mise à jour des bases antivirus

Cette section contient des informations sur la procédure de mise à jour des bases antivirus de l'application.

Dans cette section

A propos de la mise à jour des bases antivirus 130

Tâches de mise à jour créées sur le Serveur de protection 132

Lancement et arrêt de la tâche de mise à jour sur le Serveur de protection 134

A propos de la mise à jour des bases antivirus

Après l'installation ou la mise à jour de Kaspersky Security, il faut mettre à jour les bases antivirus de l'application.

La mise à jour requiert une licence valide d'utilisation de l'application.

La source de mises à jour pour Kaspersky Security est un stockage du Serveur d'administration du Kaspersky Security Center.

La mise à jour des bases antivirus se déroule comme suit :

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 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. 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.

2. Les mises à jour des bases de données sont installées sur la SVM.

   - 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 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 cas de présence d'un paquet de mises à jour, l'application installe les mises à jour des bases nécessaires au fonctionnement du Light Agent sur la machine virtuelle protégée. La mise à jour des bases de données s'effectue via *les tâches de mise à jour* sur le Light Agent. Le lancement de la tâche de mise à jour sur le Light Agent est programmé. Par défaut, le mode de lancement des tâches est défini sur “ automatique ”. La tâche se lance toutes les deux heures.

Pour en savoir plus sur la mise à jour des bases de données et des composants de l'application, reportez-vous au *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*.

► *Pour actualiser les bases antivirus sur les SVM, 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. Lancez manuellement la tâche de téléchargement des mises à jour dans le stockage ou attendez le lancement planifié. Assurez-vous que la tâche de téléchargement des mises à jour dans le stockage a réussi (pour les détails, consultez la documentation de Kaspersky Security Center).

3. Créez une tâche de mise à jour sur le Serveur de protection (cf. section "Création d'une tâche de mise à jour sur le Serveur de protection" à la page 132).

4. Attendez l'exécution planifiée de la tâche de mise à jour ou lancez la tâche manuellement (cf. section " Lancement et arrêt de la tâche de mise à jour sur le Serveur de protection " à la page 134).

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 aussi à n'importe quel moment lancer ou arrêter manuellement la tâche.

Lancement et arrêt de la tâche de mise à jour sur le Serveur de protection

Quel que soit le mode de lancement choisi pour la tâche de mise à jour sur le Serveur de protection, vous pouvez lancer ou arrêter la tâche à tout moment.

► *Pour lancer ou arrêter la 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 lancer ou arrêter une tâche de mise à jour créée pour l'ensemble des SVM, 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, choisissez le dossier portant le nom du groupe d'administration comprenant les SVM pour lesquelles vous souhaitez lancer ou arrêter une tâche de mise à jour. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
   - Si vous souhaitez lancer ou arrêter une tâche de mise à jour créée pour une ou plusieurs SVM, 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.

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 "A propos de l'activation de l'application" à la page 116).

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 manuellement les tâches.

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*) ou à l'aide des commandes via la ligne de commande du Light Agent for Linux.

Mise à jour de la version précédente de l'application

Cette section explique comment réaliser la mise à jour depuis une version antérieure de l'application.

Dans cette section

Séquence de mise à jour de la version précédente de l'application 138

A propos de la mise en jour des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration 140

Procédure de conversion des stratégies et des tâches de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 142

A propos de la mise à jour du composant Light Agent for Windows 145

Séquence de mise à jour de la version précédente de l'application

Vous pouvez mettre à jour les versions suivantes de l'application jusqu'à Kaspersky Security for Virtualization 4.0 Light Agent :

- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent ;
- Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2

La mise à jour de l'application est composée des étapes suivantes :

1. Mise à jour du Kaspersky Security Center 10 vers le Kaspersky Security Center 10 Service Pack 2 ou Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (informations détaillées dans la documentation du Kaspersky Security Center).
2. Mise à jour des plug-ins d'administration de Kaspersky Security, du Serveur d'intégration et de la Console de gestion du Serveur d'intégration (cf. section "A propos de la mise à jour des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 140).

3. Mise à jour du composant Serveur de protection. La mise à jour est exécutée par déploiement de la SVM avec une nouvelle version du composant Serveur de protection sur les hyperviseurs. Le déploiement est exécuté à l'aide d'un Assistant d'installation (cf. section "Installation du composant Serveur de protection" à la page 69).

   Les SVM avec la version précédente du composant Serveur de protection continuent à fonctionner sur les hyperviseurs. Elles assurent la protection des machines virtuelles avec la version de l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 pendant la mise à jour de l'application. Vous pouvez supprimer les SVM avec la version précédente du composant Serveur de protection après la mise à jour du composant Light Agent sur toutes les machines virtuelles protégées (voir p. 5).

   Après le déploiement des SVM dotées d'une nouvelle version du Serveur de protection, il faut réaliser les opérations suivantes :

   - Activer l'application sur les SVM dotées de la nouvelle version du composant Serveur de protection (cf. section "A propos de l'activation de l'application" à la page 116).
   - Mettre à jour les bases antivirus de l'application sur les SVM dotées de la nouvelle version du composant Serveur de protection (cf. section "Mise à jour des bases antivirus" à la page 130).

   > Si vous utilisez un schéma de licence sur la base du nombre de noyaux utilisés dans les processeurs physiques sur les hyperviseurs, Kaspersky Security peut envoyer à Kaspersky Security Center un événement relatif au non-respect des restrictions de la licence après l'activation de l'application sur les SVM disposant de la nouvelle version du composant Serveur de protection. Vous pouvez ignorer cet événement.

4. Mise à jour du composant Light Agent sur les machines virtuelles protégées (cf. section "A propos de la mise à jour du composant Light Agent for Windows" à la page 145).

5. Suppression des SVM dotées de la version précédente du composant Serveur de protection. Après la mise à jour du composant Light Agent sur toutes les machines virtuelles protégées, il faut supprimer sur les hyperviseurs les SVM dotées de la version antérieure du composant Serveur de protection. La suppression des SVM s'effectue via la console de gestion de l'infrastructure virtuelle (informations détaillées dans la Documentation sur les hyperviseurs utilisés).

Les SVM supprimées apparaissent toujours dans la Console d'administration de Kaspersky Security Center. A l'issue du délai défini dans les paramètres de Kaspersky Security Center (pour les détails, consultez la documentation de Kaspersky Security Center), les SVM sont automatiquement supprimées de la Console d'administration.

Vous pouvez supprimer manuellement des SVM dotées de la version antérieure du composant Serveur de protection de la Console d'administration de Kaspersky Security Center directement après la fin de la procédure de mise à jour.

A propos de la mise en jour des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration

Mises à jour de l'application Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Si les composants d'administration Kaspersky Security version Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent (plug-ins d'administration Kaspersky Security, Serveur d'intégration, Console de gestion du Serveur d'intégration) sont installés sur l'ordinateur, vous devez les mettre à jour. La mise à jour s'effectue par l'installation de la nouvelle version des plug-ins d'administration de Kaspersky Security, du Serveur d'intégration et de la Console de gestion du Serveur d'intégration (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 61).

Il n'est pas nécessaire de supprimer les plug-ins d'administration de la version Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent.

Les plug-ins mis à jour permettent d'administrer la version de l'application Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, installée sur les SVM et les machines virtuelles protégées. Les stratégies et les tâches configurées à l'aide des plug-ins d'administration de la version Kaspersky Security for Virtualization 4.0 Light Agent, sont convertis automatiquement en stratégies et en tâches Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent après la première ouverture et le premier enregistrement des paramètres dans la stratégie et la tâche. De plus, les paramètres manquants dans les stratégies et les tâches de la version Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent acceptent les valeurs par défaut.

Si la Console d'administration Kaspersky Security Center est installée sur plusieurs ordinateurs, vous devez mettre à jour les plug-ins d'administration de Kaspersky Security sur tous les ordinateurs. Les paramètres de l'application dans les plug-ins d'administration de Kaspersky Security sont différents selon les versions. Pour cette raison, l'utilisation des plug-ins d'administration de versions différentes peut donner lieu à une désynchronisation entre les paramètres configurés et utilisés de l'application.

Si des erreurs apparaissent après la mise à jour des plug-ins d'administration de Kaspersky Security lors du fonctionnement de l'application, vous pouvez revenir à l'utilisation des plug-ins d'administration de la version précédente. Pour cela, vous devez supprimer les plug-ins d'administration de Kaspersky Security de la nouvelle version (cf. section "Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la p. 175), puis installer les plug-ins d'administration de la version précédente.

Mise à jour de l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2

Si les plug-ins d'administration Kaspersky Security de la version Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 sont installés sur l'ordinateur, la mise à jour des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration comprend les étapes suivantes :

1. Installation de la nouvelle version des plug-ins d'administration de Kaspersky Security, installation du Serveur d'intégration et de la Console de gestion du Serveur d'intégration (cf. section "Installation des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 61).

   Les plug-ins d'administration de la version Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 continuent à fonctionner. A l'aide de ces derniers, vous pouvez administrer la version de l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 installée sur les SVM et les machines virtuelles protégées.

2. Conversion des stratégies et des tâches de la version Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 L'Assistant de conversion des stratégies et tâches de Kaspersky Security Center permet de créer de nouvelles stratégies et tâches utilisant les paramètres de stratégies et de tâches provenant d'une version précédente de l'application Kaspersky Security (cf. section " Procédure de conversion des stratégies et tâches de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 " à la page 142).

Vous pouvez également créer des stratégies sur la base de stratégies existantes à l'aide de l'Assistant de création de stratégies. Pour ce faire, à l'étape "Sélection de l'application pour la création d'une stratégie de groupe", cochez la case **Utiliser les paramètres de la stratégie existante de la version antérieure de l'application**. Pour en savoir plus sur la création d'une stratégie, reportez-vous au *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*.

3. Suppression des plug-ins d'administration de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 Pour supprimer les plug-ins d'administration de Kaspersky Security, utilisez les méthodes standard de suppression des applications du système d'exploitation. Dans la liste des applications, vous devez sélectionner pour la suppression l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2.

Après l'achèvement de la mise à jour de l'application, vous pouvez supprimer les stratégies et tâches créées pour l'application de la version Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2.

Procédure de conversion des stratégies et des tâches de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2

► *Pour convertir les stratégies et les tâches de Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2, 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.
3. En cliquant sur le bouton droit de la souris, ouvrez le menu contextuel et sélectionnez l'option **Toutes les tâches → Assistant de conversion des stratégies et des tâches**.

   L'Assistant de conversion des stratégies et des tâches se lance.
4. Suivez les indications de l'Assistant de conversion des stratégies et des tâches.

Dans cette section

Etape 1. Sélection de l’application requérant la conversion des stratégies et des tâches 143

Etape 2. Conversion des stratégies 143

Etape 3. Conversion des tâches 144

Etape 4. Fin de l'Assistant de conversion des stratégies et des tâches 144

Etape 1. Sélection de l’application requérant la conversion des stratégies et des tâches

A cette étape, sélectionnez une des options suivantes dans la liste **Nom de l'application** :

- **Kaspersky Security for Virtualization 4.0 Light Agent – Serveur de protection** si vous souhaitez convertir des stratégies pour le Serveur de protection ou des tâches exécutées sur les SVM.
- **Kaspersky Security for Virtualization 4.0 Light Agent for Windows** si vous souhaitez convertir des stratégies pour le Light Agent et des tâches créées dans Kaspersky Security Center et exécutées sur les machines virtuelles protégées.

Passez à l'étape suivante de l'Assistant de conversion des stratégies et des tâches.

Etape 2. Conversion des stratégies

Cette étape permet de sélectionner les stratégies à convertir. Pour sélectionner la stratégie, cochez la case à gauche du nom de cette stratégie.

Passez à l'étape suivante de l'Assistant de conversion des stratégies et des tâches.

Si vous avez sélectionné pour la conversion une stratégie pour le Serveur de protection dans laquelle l'utilisation des services du Kaspersky Security Network est activée, la fenêtre **Kaspersky Security Network** s'ouvre. Cette fenêtre vous permet de prendre connaissance du Règlement du Kaspersky Security Network ou du Règlement du Kaspersky Private Security Network, en fonction du type de KSN utilisé par Kaspersky Security.

Pour poursuivre la procédure de conversion des stratégies et tâches, réalisez l'une des opérations suivantes :

- Cliquez sur le bouton **Accepter**, si vous souhaitez activer l'utilisation des services du Kaspersky Security Network.
- Cliquez sur le bouton **Refuser**, si vous souhaitez désactiver l'utilisation des services du Kaspersky Security Network.

Etape 3. Conversion des tâches

Cette étape permet de sélectionner les tâches à convertir. Pour sélectionner la tâche, cochez la case à gauche du nom de cette tâche.

Passez à l'étape suivante de l'Assistant de conversion des stratégies et des tâches.

Etape 4. Fin de l'Assistant de conversion des stratégies et des tâches

Cette étape correspond à la fin de l'Assistant de conversion des stratégies et des tâches.

Les stratégies converties s'afficheront dans la liste des stratégies sous l'onglet **Stratégies** du dossier comportant le nom du groupe d'administration. Les stratégies converties obtiennent le nom suivant : "<nom de la stratégie d'origine> (convertie)".

Les tâches converties apparaissent dans la liste des tâches sur l'onglet **Tâches** du dossier portant le nom du groupe d'administration ou dans le dossier **Tâches**. Les tâches converties obtiennent le nom suivant : "<nom de la tâche d'origine> (convertie)".

Les stratégies et les tâches converties utilisent les paramètres des stratégies et des tâches de la version antérieure de Kaspersky Security. Les paramètres non repris dans les stratégies et les tâches de la version antérieure de l'application prennent les valeurs par défaut dans les stratégies et tâches converties.

Vous pouvez supprimer les stratégies et les tâches d'origine après la fin de la mise à jour de l'application (cf. documentation de Kaspersky Security Center).

A propos de la mise à jour du composant Light Agent for Windows

La mise à jour du composant Light Agent for Windows s'opère via l'installation de la nouvelle version du composant Light Agent for Windows sur les machines virtuelles protégées. L'installation est exécutée localement sur la machine virtuelle ou à distance via Kaspersky Security Center ou via l'éditeur d'administration des stratégies de groupe du service de catalogues.

Le composant Light Agent for Windows mise à jour utilise les tâches et les paramètres de fonctionnement de l'application configuré pour la version antérieure du composant Light Agent for Windows.

Lors de la mise à jour du composant Light Agent for Windows sur une machine virtuelle protégée, les copies de sauvegarde des fichiers créées lors de la réparation ou de la suppression de fichiers sont conservées. Vous pouvez utiliser les fichiers de la sauvegarde via l'interface de l'application.

Une fois lancé sur la machine virtuelle, le composant Light Agent se connecte à la SVM dotée de la nouvelle version du composant Serveur de protection.

Si des erreurs surviennent dans l'application après la mise à jour du composant Light Agent for Windows, vous pouvez revenir à l'utilisation de la version antérieure du composant Light Agent for Windows. Pour cela, vous devez supprimer une nouvelle version du composant Light Agent for Windows sur la machine virtuelle, puis installer la version précédente du composant Light Agent for Windows.

Modification de la configuration des SVM

Vous pouvez modifier la configuration des SVM :

- mot de passe de la configuration et mot de passe du compte utilisateur root ;
- mode d'accès distant pour le compte utilisateur root ;
- paramètres de réseau de la SVM ;
- nombre de réseaux virtuels que la SVM utilise pour communiquer avec les machines virtuelles et le Serveur d'administration de Kaspersky Security Center ;
- adresses des hyperviseurs spécifiées sur les SVM ;
- paramètres de connexion de la SVM au Serveur d'administration de Kaspersky Security Center ;
- nom et mot de passe du compte utilisateur de connexion des SVM à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle.

► *Afin de modifier la configuration des SVM, 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.

3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization 4.0 Light Agent** pour lancer l'Assistant. Le lien se trouve dans l'espace de travail dans le groupe **Déploiement**.

   > Vous pouvez modifier la configuration des SVM avec la version installée de l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2. Pour ce faire, lancez l'assistant en cliquant sur le lien **Administrer Kaspersky Security for Virtualization 3.0 SP2 Light Agent**. Dans ce cas, les paramètres absents dans la version de l'application Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 ne s'affichent pas dans l'assistant. Par exemple, il est impossible de modifier la quantité de réseaux virtuels qu'utilise la SVM ou l'adresse de l'hyperviseur figurant sur la SVM.

4. Suivez les instructions de l'Assistant.

Pendant la modification de la configuration des SVM, l'Assistant d'installation consigne dans son journal de fonctionnement les informations que vous renseignez à chaque étape de l'Assistant (cf. section "Application.). Description du journal de l'Assistant" à la page 179).

Vous pouvez utiliser le journal de l'Assistant lorsque vous contactez le Service de Support Technique si la modification de la configuration des SVM s'est terminée sur une erreur.

Le journal de l'Assistant se trouve sur l'ordinateur où l'Assistant a été lancé, dans le fichier %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log.

> Les informations du fichier sont écrasées à chaque lancement de l'Assistant. Pour pouvoir utiliser les informations du journal de fonctionnement de l'Assistant ultérieurement, il faut enregistrer le fichier dans un emplacement permanent.

Dans cette section

Sélection de l'action 148

Choix de la SVM pour la modification de la configuration 149

Saisie du mot de passe de configuration 151

Modification des adresses des hyperviseurs ou des serveurs d'administration de l'architecture virtuelle 152

Modification de la liste des réseaux virtuels pour les SVM 152

Modification des paramètres réseau des SVM 153

Modification des paramètres de connexion au Kaspersky Security Center 154

Modification du mot de passe de configuration et des paramètres du compte root 155

Modification des paramètres de connexion au serveur VMware vCenter 155

Modification des paramètres de connexion aux hyperviseurs Microsoft Windows Server (Hyper-V) 156

Modification des paramètres de connexion aux hyperviseurs Citrix XenServer 157

Modification des paramètres de connexion aux hyperviseurs KVM 158

Lancement de la modification de la configuration des SVM 159

Modification de la configuration des SVM 159

Fin de la modification de la configuration des SVM 160

Sélection de l'action

A cette étape, sélectionnez l'option **Modification de la configuration des SVM**.

Passez à l'étape suivante de l'Assistant.

Choix de la SVM pour la modification de la configuration

A cette étape, désignez les SVM dont vous souhaitez modifier la configuration.

Le tableau affiche une liste des hyperviseurs et des SVM déployées sur les hyperviseurs. Vous pouvez ajouter à la liste les hyperviseurs sur lesquels vous souhaitez modifier la configuration des SVM.

► *Pour ajouter une adresse IP au tableau, procédez comme suit :*

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

   La fenêtre **Paramètres de connexion à l'infrastructure virtuelle** s'ouvre.

2. Définissez les paramètres suivants de connexion aux hyperviseurs sur lesquels vous souhaitez modifier la configuration de la SVM ou les paramètres de connexion au serveur d'administration de l'infrastructure virtuelle sous l'administration de laquelle les hyperviseurs fonctionnent.

   - **Type**.

     Liste déroulante qui permet de sélectionner le type d'hyperviseur ou de serveur d'administration de l'infrastructure virtuelle.

   - **Adresses**.

     Liste des adresses des hyperviseurs sur lesquels vous souhaitez modifier la configuration des SVM ou l'adresse du serveur d'administration de l'infrastructure virtuelle sous l'administration de laquelle fonctionnent les hyperviseurs.

     L'adresse de l'hyperviseur ou du serveur d'administration de l'infrastructure virtuelle peut être son adresse IP au format IPv4 ou son nom de domaine complet (FQDN). Vous pouvez indiquer des adresses IP ou noms de domaines complets en les séparant par un point-virgule ou des retours à la ligne.

     Le nombre d'adresses reconnues correctement s'affiche sous la liste.

- **Nom d'utilisateur**.

  Nom du compte employé pour la connexion de l'Assistant à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle. Si vous utilisez un compte d'utilisateur de domaine pour vous connecter à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle, vous pouvez indiquer le nom du compte sous la forme `<domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<domaine>`.

- **Mot de passe**.

  Mot de passe du compte employé pour la connexion de l'Assistant à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle.

3. Cliquez sur le bouton **Se connecter**.

   La fenêtre **Paramètres de connexion à l'infrastructure virtuelle** se ferme et les hyperviseurs sélectionnés sont ajoutés à la liste des hyperviseurs. Si la connexion à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle n'a pas pu être établie, des informations sur les erreurs de connexion s'affichent dans le tableau.

Le tableau reprend les informations suivantes sur les hyperviseurs et les SVM déployées sur les hyperviseurs :

- **Nom**.

  Le nom de l'hyperviseur ou le nom du SVM, déployé sur l'hyperviseur.

  Si des restrictions existent quant à la modification de la configuration de la SVM sur l'hyperviseur ou en l'absence de connexion avec l'hyperviseur ou le serveur d'administration de l'infrastructure virtuelle, des points d'exclamation apparaissent dans la colonne **Nom**. Le tableau et les info-bulles de l'icône reprenne la description des restrictions ou de l'erreur de connexion.

  Le bouton **Nom** du tableau permet de réaliser les opérations suivantes :

  - supprimer de la liste l'hyperviseur sélectionné ou tous les hyperviseurs administrés par le serveur d'administration de l'infrastructure virtuelle sélectionné ;

- ouvrir la fenêtre **Paramètres de connexion à l'infrastructure virtuelle** pour modifier les paramètres du compte utilisateur employé pour établir la connexion à l'hyperviseur sélectionné ou au serveur d'administration de l'infrastructure virtuelle.

- **Condition**.

  L'état de l'hyperviseur ou du SVM.

  L'état de l'hyperviseur peut avoir une des valeurs suivantes : *Allumé*, *Eteint*, *Mode de maintenance*. En cas d'échec de la connexion à l'hyperviseur, la colonne affiche *La connexion n'a pas été établie*.

  L'état de la SVM peut avoir une des valeurs suivantes : *Lancée*, *Arrêtée*.

- **Protection**.

  Numéro de la version de l'image SVM.

Pour rafraîchir la liste des hyperviseurs dans le tableau, cliquez sur le bouton **Mettre à jour** qui se trouve au-dessus de la liste.

► *Pour choisir les SVM dont vous souhaitez modifier la configuration,*

cochez dans le tableau les cases à gauche des noms des SVM.

Vous pouvez sélectionner les SVM pour lesquelles il n'existe pas de restriction sur la modification de la configuration.

Passez à l'étape suivante de l'Assistant.

Saisie du mot de passe de configuration

A cette étape, indiquez le mot de passe de la configuration qui a été défini lors de l'installation du module Serveur de protection.

Passez à l'étape suivante de l'Assistant.

Modifier les adresses des hyperviseurs ou des serveurs de gestion de l’infrastructure virtuelle indiquées sur les machines virtuelles de protection

Cette étape permet de modifier les adresses des hyperviseurs ou des serveurs d'administration de l’infrastructure virtuelle définis sur les SVM.

Pour cela, cochez la case **Modifier les adresses des hyperviseurs ou des serveurs d'administration de l’infrastructure virtuelle indiquées sur les SVM** et indiquez dans la colonne **Nouvelle adresse** une des valeurs suivantes :

- pour les SVM sur les hyperviseurs Microsoft Windows Server (Hyper-V), Citrix XenServer ou KVM : nouvelle adresse IP au format IPv4 ou nom de domaine complet (FQDN) de chaque hyperviseur dont l'adresse doit être modifiée ;
- pour les SVM sur les hyperviseurs VMware ESXi : nouvelle adresse IP au format IPv4 ou nom de domaine complet (FQDN) du serveur VMware vCenter qui gère les hyperviseurs.

Passez à l'étape suivante de l'Assistant.

Modification de la liste des réseaux virtuels pour les SVM

Lors de cette étape, vous pouvez modifier le nombre de réseaux virtuels que les SVM doivent utiliser pour communiquer avec les machines virtuelles et le Serveur d'administration de Kaspersky Security Center. Pour ce faire, cochez la case **Modifier la liste de réseaux virtuels**, puis modifiez la liste des réseaux utilisés dans la colonne **Nom du réseau** pour chaque SVM.

Vous pouvez désigner un ou plusieurs réseaux virtuels accessibles aux hyperviseurs. Pour ajouter ou supprimer un champ de sélection des réseaux virtuels, utilisez les boutons situés à droite du champ de sélection du réseau.

Si vous avez l'intention d'utiliser pour toutes les SVM une attribution dynamique des adresses IP (DHCP), les paramètres réseau seront récupérés sur le serveur DHCP via le premier réseau virtuel de la liste des réseaux indiqués pour chacune des SVM. Assurez-vous que l'Assistant puisse se connecter à la SVM selon les paramètres réseau du premier réseau virtuel reçus du serveur DHCP.

Si l'infrastructure virtuelle utilise le module VMware Distributed Virtual Switch, vous pouvez désigner un groupe de ports virtuels distribués (Distributed Virtual Port Group) auquel la SVM se connectera.

Passez à l'étape suivante de l'Assistant.

Modification des paramètres réseau des SVM

A cette étape, vous pouvez modifier les paramètres suivants des SVM : Pour cela, cochez la case **Modifier les paramètres réseau des SVM**.

> Si vous avez modifié le nombre de réseaux virtuels pour une ou plusieurs SVM, la case **Modifier les paramètres réseau des SVM** ne s'affiche pas. Vous devez configurer les paramètres réseau des SVM sélectionnées pour la modification de configuration.

► *Pour configurer les paramètres réseau des SVM, effectuez une des actions suivantes :*

- Si vous souhaitez utiliser les paramètres réseau reçu via le protocole DHCP pour l'ensemble des SVM, choisissez l'option **Adressage IP dynamique (DHCP)**.

  Si vous souhaitez indiquer les adresses IP du serveur DNS et du serveur DNS alternatif pour chaque SVM, décochez la case **Utiliser la liste des serveurs DNS obtenus par DHCP** et saisissez les adresses IP des serveurs DNS dans les colonnes **Serveur DNS** et **Serveur DNS alternatif** du tableau. Les adresses IP des serveurs DNS obtenus via le protocole DHCP sont utilisées par défaut.

  Si la SVM utiliser plusieurs réseaux virtuels, les paramètres réseau seront récupérés sur le serveur DHCP via le premier réseau virtuel de la liste de réseau créée lors du déploiement de la SVM. Assurez-vous que l'Assistant puisse se connecter à la SVM selon les paramètres réseau du premier réseau virtuel reçus du serveur DHCP.

- Si vous souhaitez désigner les paramètres réseau des SVM manuellement, choisissez l'option **Adressage IP statique** et définissez les paramètres suivants pour chaque SVM :
  - adresse IP de la SVM (par défaut son adresse actuelle est indiquée dans la colonne) ;
  - masque du sous-réseau ;
  - passerelle ;
  - serveur DNS ;
  - serveur DNS alternatif.

Passez à l'étape suivante de l'Assistant.

Modification des paramètres de connexion au Kaspersky Security Center

Cette étape permet de modifier les paramètres de connexion des SVM au Serveur d'administration de Kaspersky Security Center.

Pour ce faire, cochez la case **Modifier les paramètres de connexion au Kaspersky Security Center** et modifiez les paramètres suivants :

- **Adresse**.

  Adresse du poste sur lequel le Serveur d'Administration de Kaspersky Security Center est installé. Vous pouvez saisir l'adresse IP au format IPv4 ou le nom de domaine complet de l'ordinateur (FQDN).

- **Port**.

  Numéro du port pour la connexion de la SVM au Serveur d'administration de Kaspersky Security Center.

- **Port SSL**.

  Numéro du port pour la connexion de la SVM au Serveur d'administration de Kaspersky Security Center à l'aide d'un certificat SSL.

Passez à l'étape suivante de l'Assistant.

Modification du mot de passe de configuration et des paramètres du compte root

A cette étape, vous pouvez modifier les paramètres suivants :

- Mot de passe de la configuration : mot de passe nécessaire pour apporter des modifications à la configuration des SVM. Pour ce faire, cochez la case **Modifier le mot de passe de la configuration** et saisissez le nouveau mot de passe de configuration dans les champs **Mot de passe** et **Confirmation**.
- Mot de passe du compte utilisateur root. Pour ce faire, cochez la case **Modifier le mot de passe du compte root** et saisissez le nouveau mot de passe dans les champs **Mot de passe** et **Confirmation**.
- Mode d'accès à distance aux SVM pour le compte utilisateur root ; Pour ce faire, cochez la case **Modifier le mode d'accès à distance pour le compte root** puis réalisez une des opérations suivantes :
  - si vous souhaitez autoriser l'accès du compte root aux SVM via SSH, cochez la case **Autoriser l'accès à distance du compte root via SSH** ;
  - si vous souhaitez interdire l'accès du compte root aux SVM via SSH, décochez la case **Autoriser l'accès à distance du compte root via SSH**.

Passez à l'étape suivante de l'Assistant.

Modification des paramètres de connexion au serveur VMware vCenter

> Cette étape apparaît si des SVM déployées sur des hyperviseurs VMware ESXi ont été sélectionnées en vue d'une modification de leur configuration.

Cette étape permet de modifier le compte utilisateur que les SVM utilisent pour se connecter au serveur VMware vCenter.

Le compte utilisé par défaut pour la connexion des SVM à l'infrastructure virtuelle est celui que vous avez renseigné lors de l'installation du module Serveur de protection (cf. section "Etape 2.. Choix des hyperviseurs pour le déploiement des SVM" à la p. 71). Afin d'améliorer la sécurité, il est conseillé d'utiliser un compte utilisateur créé pour le fonctionnement des SVM. Pour en savoir plus sur ce compte, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*.

Si vous souhaitez modifier le compte utilisateur utilisé par les SVM pour la connexion au serveur VMware vCenter, cochez la case **Modifier le compte de connexion au serveur VMware vCenter** et saisissez les paramètres de ce compte dans les champs **Nom d'utilisateur** et **Mot de passe**.

Ces paramètres interviennent dans le fonctionnement des SVM en vue d'obtenir des informations sur l'infrastructure virtuelle.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. En cas d'échec de la connexion, un tableau contenant les informations relatives à l'échec s'affiche dans la fenêtre. L'erreur de connexion est décrite dans le tableau. Vérifiez les paramètres du compte utilisateur indiqué et le cas échéant, renseignez un autre nom d'utilisateur et un autre mot de passe pour la connexion des SVM au serveur VMware vCenter.

Modification des paramètres de connexion aux hyperviseurs Microsoft Windows Server (Hyper-V)

Cette étape apparaît si des SVM déployées sur des hyperviseurs Microsoft Windows Server (Hyper-V) ont été sélectionnées en vue d'une modification de leur configuration.

Cette étape permet de modifier le compte utilisateur que les SVM utilisent pour se connecter aux hyperviseurs Microsoft Windows Server (Hyper-V).

Le compte utilisé par défaut pour la connexion des SVM à l'infrastructure virtuelle est celui que vous avez renseigné lors de l'installation du module Serveur de protection (cf. section "Etape 2.. Choix des hyperviseurs pour le déploiement des SVM" à la p. 71). Afin d'améliorer la sécurité, il est conseillé d'utiliser un compte utilisateur créé pour le fonctionnement des SVM. Pour en savoir plus sur ce compte, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*.

Si vous souhaitez modifier le compte utilisateur utilisé par les SVM pour la connexion aux hyperviseurs Microsoft Windows Server (Hyper-V), cochez la case **Modifier le compte de connexion aux hyperviseurs Microsoft Windows Server (Hyper-V)** et saisissez les paramètres de ce compte dans les champs **Nom d'utilisateur** et **Mot de passe**.

Ces paramètres interviennent dans le fonctionnement des SVM en vue d'obtenir des informations sur l'infrastructure virtuelle.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifie s'il est possible de se connecter aux hyperviseurs Microsoft Windows Server (Hyper-V) sélectionnés en vue d'une modification de la configuration de la SVM à l'aide du nom d'utilisateur et du mot de passe du compte. En cas d'échec de la connexion avec au moins un des hyperviseurs, un tableau contenant les informations relatives à l'échec s'affiche dans la fenêtre. La description de l'erreur de connexion apparaît dans le tableau pour chaque hyperviseur. Cette étape permet de définir le nom et le mot de passe du compte utilisateur pour la connexion de la SVM à l'hyperviseur Microsoft Windows Server (Hyper-V).

Modification des paramètres de connexion aux hyperviseurs Citrix XenServer

> Cette étape apparaît si des SVM déployées sur des hyperviseurs Citrix XenServer ont été sélectionnées en vue d'une modification de leur configuration.

Cette étape permet de modifier le compte utilisateur que les SVM utilisent pour se connecter aux hyperviseurs Citrix XenServer.

Le compte utilisé par défaut pour la connexion des SVM à l'infrastructure virtuelle est celui que vous avez renseigné lors de l'installation du module Serveur de protection (cf. section "Etape 2..

Choix des hyperviseurs pour le déploiement des SVM" à la p. 71). Afin d'améliorer la sécurité, il est conseillé d'utiliser un compte utilisateur créé pour le fonctionnement des SVM. Pour en savoir plus sur ce compte, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*.

Si vous souhaitez modifier le compte utilisateur utilisé par les SVM pour la connexion aux hyperviseurs Citrix XenServer, cochez la case **Modifier le compte de connexion aux hyperviseurs Citrix XenServer** et saisissez les paramètres de ce compte dans les champs **Nom d'utilisateur** et **Mot de passe**.

Ces paramètres interviennent dans le fonctionnement des SVM en vue d'obtenir des informations sur l'infrastructure virtuelle.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifie s'il est possible de se connecter aux hyperviseurs Citrix XenServer sélectionnés en vue d'une modification de la configuration de la SVM à l'aide du nom d'utilisateur et du mot de passe du compte. En cas d'échec de la connexion avec au moins un des hyperviseurs, un tableau contenant les informations relatives à l'échec s'affiche dans la fenêtre. La description de l'erreur de connexion apparaît dans le tableau pour chaque hyperviseur. Vérifiez les paramètres du compte utilisateur indiqué et le cas échéant, renseignez un autre nom d'utilisateur et un autre mot de passe pour la connexion des SVM aux hyperviseurs Citrix XenServer.

Modification des paramètres de connexion aux hyperviseurs KVM

Cette étape apparaît si des SVM déployées sur des hyperviseurs KVM ont été sélectionnées en vue d'une modification de leur configuration.

Cette étape permet de modifier le compte utilisateur que les SVM utilisent pour se connecter aux hyperviseurs KVM.

Le compte utilisé par défaut pour la connexion des SVM à l'infrastructure virtuelle est celui que vous avez renseigné lors de l'installation du module Serveur de protection (cf. section "Etape 2. Choix des hyperviseurs pour le déploiement des SVM" à la p. 71). Afin d'améliorer la sécurité, il est conseillé d'utiliser un compte utilisateur créé pour le fonctionnement des SVM. Pour en savoir plus sur ce compte, reportez-vous au *Manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent*.

Si vous souhaitez modifier le compte utilisateur utilisé par les SVM pour la connexion aux hyperviseurs KVM, cochez la case **Modifier le compte de connexion aux hyperviseurs KVM** et saisissez les paramètres de ce compte dans les champs **Nom d'utilisateur** et **Mot de passe**.

Ces paramètres interviennent dans le fonctionnement des SVM en vue d'obtenir des informations sur l'infrastructure virtuelle.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifie s'il est possible de se connecter aux hyperviseurs KVM sélectionnés en vue d'une modification de la configuration de la SVM à l'aide du nom d'utilisateur et du mot de passe du compte utilisateur. En cas d'échec de la connexion avec au moins un des hyperviseurs, un tableau contenant les informations relatives à l'échec s'affiche dans la fenêtre. La description de l'erreur de connexion apparaît dans le tableau pour chaque hyperviseur. Vérifiez les paramètres du compte utilisateur indiqué et le cas échéant, renseignez un autre nom d'utilisateur et un autre mot de passe pour la connexion des SVM aux hyperviseurs KVM.

Lancement de la modification de la configuration des SVM

A cette étape, la fenêtre de l'Assistant affiche tous les paramètres saisis plus tôt et nécessaires à la modification de la configuration des SVM.

Pour lancer la modification de la configuration des SVM, passez à l'étape suivante de l'Assistant.

Modification de la configuration des SVM

Cette étape consiste à modifier la configuration des SVM.

Les informations relatives à la modification de la configuration de chaque SVM et aux résultats de celle-ci sont reprises dans la fenêtre de l'Assistant. Le processus dure un certain temps. Attendez la fin du processus de modification.

Passez à l'étape suivante de l'Assistant.

Fin de la modification de la configuration des SVM

Cette étape fournit des informations relatives aux résultats de la modification de la configuration des SVM.

L'Assistant affiche les liens qui donnent accès au rapport succinct et au journal de l'Assistant.

Celui-ci contient des informations sur les résultats de l'exécution des étapes de modification de la configuration sur toutes les SVM. Le rapport abrégé est enregistré dans un fichier temporaire. Pour pouvoir utiliser les informations du rapport ultérieurement, vous devez enregistrer le fichier dans un emplacement permanent.

Le journal de l'Assistant contient les informations indiquées par vos soins à chaque étape de l'Assistant. (cf. section "Appendice. Description du journal de l'Assistant" à la page 179).
Si des erreurs sont survenues lors de la modification de la configuration des SVM, vous pouvez utiliser le journal de l'Assistant pour vos communications avec le Support Technique.

Le journal de l'Assistant est enregistré sur l'ordinateur où l'Assistant a été lancé, dans le dossier C:\Users\%user%\AppData\Local\KasperskyDeploymentWizard.log. Il ne contient aucune information relative aux comptes utilisateur.

Fermez l'Assistant.

Consultation et modification des paramètres du Serveur d'intégration

La console de gestion du Serveur d'intégration permet de réaliser les opérations suivantes :

- consulter les paramètres du Serveur d'intégration et son journal de fonctionnement ;
- modifier les mots de passe des comptes utilisateur du Serveur d'intégration :
  - compte utilisateur d'administration du Serveur d'intégration ;
  - compte utilisateur de connexion des SVM au Serveur d'intégration ;
  - compte utilisateur de connexion des Light Agents au Serveur d'intégration.

> Les noms des comptes utilisateur ne peuvent pas être modifiés.

Dans cette section

Lancement de la console de gestion du Serveur d'intégration 161

Modification des paramètres du Serveur d'intégration 163

Modification des mots de passe des comptes utilisateur du Serveur d'intégration 164

Lancement de la console de gestion du Serveur d'intégration

> Si l'ordinateur hébergeant la Console de gestion du Serveur d'intégration fait partie du domaine Microsoft Windows, assurez-vous que votre compte utilisateur de domaine fait partie du groupe KLAdmins ou du groupe d'administrateurs locaux sur l'ordinateur où est installé le Serveur d'intégration.

► *Pour installer la Console de gestion du Serveur d'intégration, 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.
3. Lancez la console de gestion du Serveur d'intégration en cliquant sur le lien **Démarrer la console de gestion du serveur d'intégration** dans le groupe **Déploiement**.
4. Si une des conditions suivantes est remplie, une fenêtre permet de saisir les paramètres de connexion au Serveur d'intégration :

   - si l'ordinateur hébergeant la Console de gestion du Serveur d'intégration ne fait pas partie du domaine Microsoft Windows ;
   - si l'ordinateur hébergeant la Console de gestion du Serveur d'intégration fait partie du domaine Microsoft Windows mais qu'elle ne réussit pas à se connecter au Serveur d'intégration en utilisant l'adresse et le port de la connexion spécifiés dans les paramètres du Serveur d'intégration.

   Définissez les paramètres de connexion suivants :

   - Adresse du Serveur d'intégration avec lequel a été établie la connexion.
   - Compte utilisateur pour la connexion au Serveur d'intégration :
     - Si l'ordinateur hébergeant la Console de gestion du Serveur d'intégration n'appartient pas au domaine et si votre compte utilisateur de domaine appartient au groupe KLAdmin ou au groupe d'administrateurs locaux de l'ordinateur où se trouve le Serveur d'intégration, vous pouvez utiliser le compte utilisateur de domaine. Pour cela, cochez la case **Utiliser un compte de domaine**.

       Si vous voulez utiliser le compte utilisateur administrateur du Serveur d'intégration, saisissez le mot de passe de l'administrateur dans le champ **Mot de passe**.

- Si l'ordinateur hébergeant la Console de gestion du Serveur d'intégration n'appartient pas au domaine ou s'il lui appartient mais si votre compte utilisateur n'appartient pas au groupe KLAdmin ou au groupe d'administrateurs locaux de l'ordinateur où se trouve le Serveur d'intégration, vous pouvez utiliser uniquement le compte utilisateur d'administrateur du Serveur d'intégration. Saisissez le mot de passe de l'administrateur du Serveur d'intégration dans le champ **Mot de passe**.

Cliquez sur le bouton **Se connecter**.

5. La Console de gestion vérifie le certificat SSL obtenu du Serveur d'intégration. La fenêtre **Analyse du certificat** s'ouvre avec un message si le certificat reçu n'est pas un certificat de confiance ou s'il n'est pas compatible avec le certificat précédemment installé. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat obtenu.

   Pour maintenir la connexion au Serveur d'intégration, cliquez sur **Accepter le certificat** dans la fenêtre **Analyse du certificat**. Le certificat récupéré sera installé en tant que certificat de confiance. Une fois que vous avez cliqué sur le bouton Ignorer, le certificat est enregistré dans la base de registres du système d'exploitation de l'ordinateur sur lequel la Console de gestion du Serveur d'intégration est installée.

La console de gestion du Serveur d'intégration s'ouvre.

Modification des paramètres du Serveur d'intégration

► *Pour modifier les paramètres du Serveur d'intégration, procédez comme suit :*

1. Lancez la Console de gestion du Serveur d'administration (cf. section "Lancement de la console de gestion du Serveur d'intégration" à la page 161).

   Section **Paramètres du Serveur d'intégration**

   La section **Paramètres du Serveur d'intégration** affiche les paramètres suivants du Serveur d'intégration avec lequel la connexion est établie :

   - version du Serveur d'intégration ;

- nom du compte utilisateur sous lequel a été établie la connexion au Serveur d'intégration ;
- type d'authentification utilisé pour la connexion au Serveur d'intégration ;
- Adresse IP au format IPv4 ou nom de domaine complet (FQDN) et port du Serveur d'intégration.

Le lien **Consulter les enregistrements des travaux** permet d'ouvrir le journal de fonctionnement du Serveur d'intégration. Le journal de fonctionnement s'ouvre dans l'éditeur de texte Bloc-Notes. Pour plus de détails sur les journaux du Serveur d'intégration, cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*.

2. Pour fermer la Console de gestion, cliquez sur le bouton **Fermer**.

Modification des mots de passe des comptes utilisateur du Serveur d'intégration

► *Pour modifier les paramètres des comptes du Serveur d'intégration, procédez comme suit :*

1. Lancez la Console de gestion du Serveur d'administration (cf. section "Lancement de la console de gestion du Serveur d'intégration" à la page 161).
2. La section **Comptes du serveur d'intégration** contient un tableau qui permet de sélectionner le nom de compte dont vous souhaitez modifier le mot de passe.
3. Le lien **Modifier le mot de passe du compte** ouvre la fenêtre **Mot de passe du compte** dans laquelle vous pouvez saisir le nouveau mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.

   Les mots de passe doivent comporter entre 1 et 60 caractères. Vous pouvez utiliser l'alphabet latin, des chiffres et les symboles suivants : `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`.

4. Cliquez sur le bouton **OK** dans la fenêtre **Mot de passe du compte**.
5. Pour appliquer les modifications et fermer la Console de gestion, cliquez sur le bouton **Fermer**.

Si la stratégie pour le Serveur de protection prévoit la connexion de SVM au Serveur d'intégration et que vous avez modifié le mot de passe du compte utilisateur de connexion des SVM, vous configurer à nouveau la connexion des SVM au Serveur d'intégration dans la stratégie du Serveur de protection.

Si la stratégie pour le Light Agent prévoit la connexion de Light Agents au Serveur d'intégration et que vous avez modifié le mot de passe du compte utilisateur de connexion des Light Agents, vous devez configurer à nouveau la connexion des Light Agents au Serveur d'intégration dans la stratégie du Light Agent for Windows et dans celle du Light Agent for Linux.

Les nouveaux paramètres du compte de connexion au Serveur d'intégration sont transmis à la stratégie lors de l'enregistrement des paramètres de la stratégie.

Suppression de l'application

Cette section explique comment supprimer l'application Kaspersky Security de l'infrastructure virtuelle.

Une fois l'application Kaspersky Security supprimée, les machines virtuelles et les données de l'utilisateur ne sont plus protégées.

Dans cette section

Ordre des étapes de suppression de l'application 167

Suppression du composant Serveur de protection 168

Suppression du composant Light Agent for Windows..... 168

Suppression du composant Light Agent for Linux 173

Suppression de l'Agent d'administration de Kaspersky Security Center des machines virtuelles..... 174

Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration 175

Ordre des étapes de suppression de l'application

La suppression de l'application Kaspersky Security de l'infrastructure virtuelle comprend les étapes suivantes :

1. Suppression du composant Serveur de protection de Kaspersky Security.

   Vous pouvez supprimer le Serveur de protection sur certains ou sur tous les hyperviseurs de l'infrastructure virtuelle (cf. section "Suppression du composant Serveur de protection" à la page 168).

2. La suppression du composant Light Agent for Windows (cf. section "Suppression du composant Light Agent for Windows" à la p. 168) ou Light Agent for Linux (cf. section "Suppression du composant Light Agent for Linux" à la p. 173).

   Vous pouvez supprimer le composant Light Agent de l'ensemble des machines virtuelles ou uniquement de certaines d'entre elles.

3. Suppression du composant Light Agent for Windows des modèles de machines virtuelles (cf. section "Suppression du Light Agent for Windows du modèle de machines virtuelles" à la page 172).

4. Si l'Agent d'administration de Kaspersky Security Center a été installé sur les machines virtuelles protégées et les modèles de machines virtuelles, il faut supprimer le composant Agent d'administration de ces machines virtuelles protégées et de ces modèles de machines virtuelles (cf. section "Suppression de l'Agent d'administration de Kaspersky Security Center des machines virtuelles" à la page 174).

5. Suppression des plug-ins d'administration de Kaspersky Security, du Serveur d'intégration et de la Console de gestion du Serveur d'intégration (cf. section "Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration" à la page 175).

Après la suppression des composants Serveur de protection et Light Agent, les machines virtuelles sur lesquelles ceux-ci étaient installés apparaissent toujours dans la Console d'administration de Kaspersky Security Center. A l'issue du délai défini dans les paramètres de Kaspersky Security Center (cf. Documentation de Kaspersky Security Center), les machines virtuelles sont automatiquement supprimées de la Console d'administration. Vous pouvez supprimer manuellement des machines virtuelles de la Console d'administration de Kaspersky Security Center, ceci dès la fin de la procédure de suppression de l'application.

Suppression du composant Serveur de protection

Pour la suppression du composant Serveur de protection, vous devez supprimer des SVM sur les hyperviseurs.

Vous pouvez supprimer les SVM sur tous ou certains hyperviseurs de l'infrastructure virtuelle. Suite à la suppression de la SVM de l'hyperviseur, les machines virtuelles protégées de cet hyperviseur se connectent à une SVM fonctionnant sur un autre hyperviseur (cf. section "Connexion du Light Agent à la SVM" à la page 34).

La suppression des SVM s'effectue via la console de gestion de l'infrastructure virtuelle (informations détaillées dans la Documentation sur les hyperviseurs utilisés).

Suppression du composant Light Agent for Windows

Vous pouvez supprimer Light Agent for Windows de la machine virtuelle d'une des manières suivantes :

- en local, en mode interactif, à l'aide de l'Assistant d'installation (cf. section "Suppression du Light Agent for Windows à l'aide de l'assistant d'installation" à la page 169) ;
- depuis la ligne de commande (cf. section "Suppression du Light Agent for Windows via la ligne de commande" à la page 170) ;
- à distance via l'application Kaspersky Security Center (consultez la documentation de Kaspersky Security Center) ;
- à distance via l'éditeur d'administration des stratégies de groupe du service de catalogues (Active Directory Group Policies) (cf. section "Suppression du Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues" à la page 171).

Lors de la suppression du composant Light Agent for Windows sur la machine virtuelle, tous les fichiers créés pendant le fonctionnement de l'application sont supprimés.

Dans cette section

Suppression du Light Agent for Windows à l'aide de l'assistant d'installation 169

Suppression du Light Agent for Windows via la ligne de commande 170

Suppression du Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues 171

Suppression du Light Agent for Windows dans le modèle de machines virtuelles 172

Suppression du Light Agent for Windows à l'aide de l'assistant d'installation

► *Pour supprimer le composant Light Agent for Windows à l'aide de l'Assistant d'installation, procédez comme suit :*

1. Sur la machine virtuelle disposant du composant Light Agent for Windows, ouvrez la liste des programmes en utilisant les outils standards de suppression ou de modification des programmes dans le système d'exploitation.
2. Dans la liste des programmes, sélectionnez **Kaspersky Security for Virtualization 4.0 Light Agent** et lancez l'Assistant d'installation.
3. Dans la fenêtre **Modification, restauration ou suppression de l'application** de l'Assistant d'installation, cliquez sur le bouton **Suppression**.
4. Suivez les instructions de l'Assistant d'installation.

Dans cette section

Etape 1. Confirmation de la suppression du composant Light Agent for Windows 170

Etape 2. Suppression du composant Light Agent for Windows 170

Etape 1. Confirmation de la suppression du composant Light Agent for Windows

Vu que la suppression du composant Light Agent for Windows expose la machine virtuelle aux menaces, il vous est nécessaire de confirmer votre intention. Pour confirmer la suppression, cliquez sur le bouton **Supprimer**.

Vous pouvez annuler la suppression du composant Light Agent for Windows jusqu'au dernier moment du processus en cliquant sur **Annuler**.

Etape 2. Suppression du composant Light Agent for Windows

A cette étape, l'Assistant d'installation supprime le composant Light Agent for Windows de la machine virtuelle. Attendez la fin du processus de suppression.

Le processus de suppression peut nécessiter le redémarrage du système d'exploitation de la machine virtuelle. Si vous décidez de reporter le redémarrage, la fin de la procédure de suppression sera reportée jusqu'au moment où le système d'exploitation sera redémarré ou jusqu'à l'arrêt et au redémarrage de la machine virtuelle.

Suppression du Light Agent for Windows via la ligne de commande

► *Pour supprimer le Light Agent for Windows à partir de la ligne de commande en mode interactif, procédez comme suit :*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA}` ou `setup.exe /x` si un système d'exploitation invité 32 bits est installé sur la machine virtuelle.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463}` ou `setup.exe /x` si un système d'exploitation invité 64 bits est installé sur la machine virtuelle.

Lancez l'Assistant d'installation de l'application. Suivez ses instructions.

► *Pour supprimer le Light Agent for Windows à partir de la ligne de commande en mode discret (sans lancement de l'Assistant d'installation de l'application) :*

saisissez l'une des commandes suivantes dans la ligne de commande :

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA} /qn` ou `setup.exe /s /x` si un système d'exploitation invité 32 bits est installé sur la machine virtuelle.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463} /qn` ou `setup.exe /s /x` si un système d'exploitation invité 64 bits est installé sur la machine virtuelle.

Suppression du Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues

Grâce à l'éditeur d'administration des stratégies de groupe du service d'annuaire (Active Directory Group Policies), vous pouvez supprimer le composant Light Agent for Windows des machines virtuelles associées à l'objet de stratégie de groupe sélectionné sans utiliser le Kaspersky Security Center.

Pour en savoir plus sur l'éditeur d'administration des stratégies de groupe du service de catalogues, veuillez consulter l'*Aide de Microsoft Windows*.

► *Pour supprimer le Light Agent for Windows via l'éditeur d'administration des stratégies de groupe du service de catalogues, procédez comme suit :*

1. Ouvrez la fenêtre de Microsoft Windows **Administration des stratégies de groupe**.
2. Dans l'arborescence de la fenêtre **Administration des stratégies de groupe**, sélectionnez l'objet de stratégie de groupe (Group Policy Object) auquel sont associées les machines virtuelles dédiées à la suppression du Light Agent for Windows.
3. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'objet de stratégie de groupe, puis sélectionnez l'option **Modifier**.

   L'éditeur d'administration des stratégies de groupe du service de catalogues s'ouvre.

4. Dans l'arborescence de la console, sélectionnez **Objet de la stratégie groupée \ Configuration de l'ordinateur \ Stratégies \ Configuration des applications \ Installation de l'application**.

5. Dans la liste des paquets d'installation, sélectionnez le paquet d'installation de Kaspersky Security for Virtualization 4.0 Light Agent.

6. Cliquez-droit pour ouvrir le menu contextuel de l'installation, puis choisissez l'option **Toutes les tâches** → **Supprimer**.

   La fenêtre **Suppression des applications** s'ouvre.

7. Dans la fenêtre **Suppression des applications**, sélectionnez le paramètre **Suppression immédiate de cette application des ordinateurs de tous les utilisateurs**.

La stratégie de groupe s'applique sur chaque machine virtuelle protégée associée à l'objet de stratégie de groupe lors du lancement des machines virtuelles suivant. Ainsi, le composant Light Agent for Windows sera supprimé de l'ensemble des machines virtuelles protégées associées à l'objet de stratégie de groupe sélectionné.

Un redémarrage des machines virtuelles peut être requis une fois la suppression terminée.

Suppression du Light Agent for Windows dans le modèle de machines virtuelles

► *Pour supprimer le composant Light Agent for Windows du modèle de machine virtuelle, procédez comme suit :*

1. Sur l'hyperviseur, activez la machine virtuelle tenant lieu de modèle de machine virtuelle.

2. Supprimez le composant Light Agent for Windows en mode interactif à l'aide de l'assistant d'installation (cf. la section "Suppression de Light Agent for Windows à l'aide de l'assistant d'installation" à la p. 169).

3. Recréez des machines virtuelles à partir du modèle mis à jour. Pour plus d'informations, consultez la documentation concernant l'infrastructure virtuelle.

Suppression du composant Light Agent for Linux

Vous pouvez supprimer Light Agent for Linux de la machine virtuelle d'une des manières suivantes :

- en local via la ligne de commande ;
- à distance via l'application Kaspersky Security Center (consultez la documentation de Kaspersky Security Center).

► *Pour supprimer le Light Agent for Linux via la ligne de commande, exécutez une des commandes suivantes (en fonction du gestionnaire de paquets utilisé dans le système d'exploitation) :*

- `# rpm -e lightagent` si le Light Agent a été installé à partir d'un paquet au format RPM ;
- `# dpkg -P lightagent` si le Light Agent a été installé à partir d'un paquet au format DEB.

La procédure de suppression est exécutée automatiquement. Toutes les tâches qui étaient exécutées sur la machine virtuelle au moment de la suppression du Light Agent for Linux seront arrêtées.

Lors de la suppression de Light Agent for Linux, l'application propose de lancer le script qui supprimera sur la machine virtuelle protégée les fichiers créés pendant l'utilisation de l'application dans les dossiers suivants :

- /etc/opt/kaspersky/lightagent/ ;
- /opt/kaspersky/lightagent/ ;
- /var/opt/kaspersky/lightagent/ ;
- /var/log/kaspersky/lightagent/.

► *Pour supprimer, à l'aide d'un script, les fichiers créés pendant l'utilisation de l'application, procédez comme suit :*

1. Lancez le script via la commande suivante :

   ```
   # /tmp/cleanup.pl
   ```

2. Confirmez la suppression des fichiers en saisissant `yes`. Si vous souhaitez annuler la suppression des fichiers et arrêter le script, saisissez `no`.

Vous pouvez également supprimer manuellement les fichiers créés pendant le fonctionnement de l'application.

► *Pour supprimer manuellement les fichiers créés pendant le fonctionnement de l'application,*

exécutez la commande suivante :

```
rm -rf <chemin vers le dossier>
```

Après la suppression de Light Agent for Linux, il est conseillé de redémarrer la machine virtuelle.

Suppression de l'Agent d'administration de Kaspersky Security Center des machines virtuelles

Vous pouvez supprimer l'Agent d'administration de Kaspersky Security Center des machines virtuelles et des modèles de machines virtuelles de l'une des manières suivantes :

- depuis les machines virtuelles avec le système d'exploitation Windows :
  - En local, en mode interactif, via le système d'exploitation Windows. Il s'agit de l'approche conseillée pour la suppression de l'Agent d'administration des modèles de machines virtuelles.
  - A distance via Kaspersky Security Center à l'aide de la tâche de désinstallation à distance de l'application (cf. la documentation de Kaspersky Security Center).
- Depuis les machines virtuelles avec le système d'exploitation Linux – via le système d'exploitation Linux.

Suppression des plug-ins d'administration de Kaspersky Security et du Serveur d'intégration

Vous pouvez supprimer les plug-ins d'administration de Kaspersky Security, le Serveur d'intégration et la Console de gestion du Serveur d'intégration d'une des méthodes suivantes :

- En mode interactif à l'aide des outils standard de suppression des applications du système d'exploitation. Dans la liste des applications, il faut sélectionner pour la suppression **Kaspersky Security for Virtualization 4.0 Light Agent – modules de gestion**.
  La suppression s'opère à l'aide de l'Assistant.

- En mode silencieux via la ligne de commande. Vous devez saisir `SecurityCenterComponents_4.0.X.X_setup.exe –q –uninstall` dans la ligne de commande où `4.0.X.X` désigne le numéro de version de l'application.

Lors de la suppression du Serveur d'intégration via l'Assistant, vous pouvez enregistrer les données suivantes, utilisées au cours du fonctionnement du Serveur d'intégration :

- le certificat SSL utilisé pour l'établissement d'une connexion sécurisée avec le Serveur d'intégration ;

- les paramètres du Serveur d'intégration, y compris les mots de passe des comptes du Serveur d'intégration ;

- les données enregistrées par le Serveur d'intégration au cours de son fonctionnement (cf. section "A propos du Serveur d'intégration" à la p. 37) ;

- journaux du Serveur d'intégration.

Si vous souhaitez enregistrer les données indiquées, cliquez sur le bouton **Enregistrer les données du Serveur d'intégration** dans la fenêtre qui vous propose d'enregistrer les données. Les données et paramètres enregistrés sont automatiquement utilisés lors de la réinstallation d'un Serveur d'intégration.

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 176

Support Technique par téléphone 177

Support Technique via Kaspersky CompanyAccount 177

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).

Application. Description du journal de l'Assistant

Pendant le déploiement des SVM et pendant la modification de la configuration des SVM, l'Assistant consigne dans le journal de l'Assistant toutes les informations que vous avez saisies à chaque étape de l'Assistant.

Lors de l'installation des SVM, les informations suivantes sont consignées dans le journal de l'Assistant :

- action choisie (déploiement des SVM) ;
- type d'hyperviseur ou de serveur d'administration de l'infrastructure virtuelle ;
- adresse de l'hyperviseur ou du serveur d'administration de l'infrastructure virtuelle ;
- version de l'hyperviseur ou du serveur d'administration de l'infrastructure virtuelle ;
- nom de l'hyperviseur, version du système d'exploitation installé dessus, nombre de machines virtuelles sur l'hyperviseur ;
- nom du compte utilisateur employé pour connecter l'assistant d'installation à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle ;
- nom du compte utilisateur employé pour la connexion des SVM à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle ;
- numéro de la version de l'image de la SVM ;
- versions des SVM précédemment déployées ;
- état de l'éditeur de l'image de la SVM ;
- chemin vers le fichier de l'image de la SVM et informations sur cette image (éditeur, description, taille du disque virtuel) ;
- état de l'analyse de l'image de la SVM ;

- liste de l'ensemble des hyperviseurs VMware ESXi sous l'administration d'un serveur VMware vCenter, leur état, les états de la protection et les autorisations des comptes utilisés pour la connexion au serveur VMware vCenter (uniquement en cas d'installation sur un hyperviseur VMware ESXi) ;
- liste et version des hyperviseurs VMware ESXi, sélectionnés pour le déploiement des SVM (uniquement lors de l'installation sur un hyperviseur VMware ESXi) ;
- si le déploiement parallèle des SVM sur plusieurs hyperviseurs est autorisé et le nombre de sessions parallèles (uniquement lors de l'installation sur un hyperviseur VMware ESXi) ;
- paramètres des SVM sur chacun des hyperviseurs sélectionnés (nom, stockage, nom du réseau) ;
- identifiant VLAN (uniquement en cas d'installation sur un hyperviseur Microsoft Windows Server (Hyper-V)) ;
- méthode de mise à disposition d'espace sur le disque (uniquement lors de l'installation sur un hyperviseur VMware ESXi) ;
- paramètres de connexion de la SVM au Serveur d'administration de Kaspersky Security Center (adresse IP, port, port SSL) ;
- possibilité ou non pour le compte utilisateur root d'accéder à distance à la SVM via SSH ;
- type d'authentification de la SVM sur un hyperviseur Microsoft Windows Server (Hyper-V) – locale, domaine ;
- paramètres réseau de la SVM : adresse IP, adresse IP de la passerelle réseau principale, adresses IP des serveurs DNS principal et alternatif, masque de sous-réseau.

Lors de la modification de la configuration des SVM, les informations suivantes sont consignées dans le journal de l'Assistant :

- action choisie (modification de la configuration des SVM) ;
- adresse IP ou noms de domaines complets des hyperviseurs sur lesquels la configuration des SVM est modifiée ;

- adresse IP ou noms de domaine complet des SVM sur lesquelles la configuration est modifiée ;
- renseignements pour savoir si, suite au changement de configuration, les données suivantes seront modifiées :
  - paramètres des comptes pour la connexion à la SVM (mot de passe de configuration, mot de passe du compte root, possibilité de connexion à la SVM à l'aide du compte root via SSH) suite à la modification de la configuration ;
  - adresse de l'hyperviseur ou du serveur d'administration de l'infrastructure virtuelle auquel la SVM est connectée ;
  - paramètres du compte utilisateur employé pour la connexion de la SVM à l'hyperviseur ou au serveur d'administration de l'infrastructure virtuelle ;
  - liste des réseaux virtuels utilisés par la SVM ;
  - paramètres réseau de la SVM (adresse IP, adresse IP de la passerelle réseau principale, adresses IP des serveurs DNS principal et alternatif, masque de sous-réseau).

Le journal de l'Assistant est enregistré sur l'ordinateur où l'Assistant a été lancé, dans le fichier %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\KasperskyDeploymentWizard.log. Il ne contient aucune information relative aux comptes.

> Les informations du fichier sont écrasées à chaque lancement de l'Assistant. Pour pouvoir utiliser les informations du journal de fonctionnement de l'Assistant ultérieurement, il faut enregistrer le fichier dans un emplacement permanent.

Les informations contenues dans le journal de l'Assistant ne sont pas envoyées automatiquement à Kaspersky Lab. Vous pouvez utiliser le journal de l'Assistant lorsque vous contactez le Service de Support Technique si le déploiement ou la modification de la configuration des SVM s'est terminé(e) par une erreur.

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.

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 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.

Copie de sauvegarde du fichier

Copie de fichier de la machine virtuelle et créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde sont conservées dans la sauvegarde dans un format spécial et ne présentent aucun danger.

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.

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 Etats-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 Etats-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 Etats-Unis et dans d'autres pays.

SUSE est une marque déposée de SUSE LLC enregistrée aux Etats-Unis et dans d'autres pays.

VMware, VMware ESXi, VMware Horizon et VMware vCenter sont des marques commerciales de VMware, Inc. ou une marque commerciale de VMware, Inc. déposées aux Etats-Unis ou dans d'autres juridictions.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Index

A

Activation de l'application 116

Agent d'administration 49, 81

installation 81

Architecture de l'application 29

C

Configuration logicielle 24

Configurations logicielle et matérielle 24

Console d'administration 49

E

Etat de la protection 137

I

Image de la SVM 29, 74

Installation de l'application 59

M

Mise à jour 130

Mise à jour

tâche de mise à jour 134
Mise à jour de l'application 138
Mise à jour des bases 130
Modification de la configuration des SVM 146
Modules de l'application 17

P

Plug-in d'administration
installation 61
Plug-in d'administration
suppression 175
Plug-in d'administration : 29

S

Serveur d'administration 49
Serveur de protection 29
suppression 168
Serveur de protection
installation 69
Serveur d'intégration 37
suppression 175
Serveur d'intégration
installation 61

Suppression de l'application....166

SVM....29

T

Tâche

ajout d'une clé....116, 123