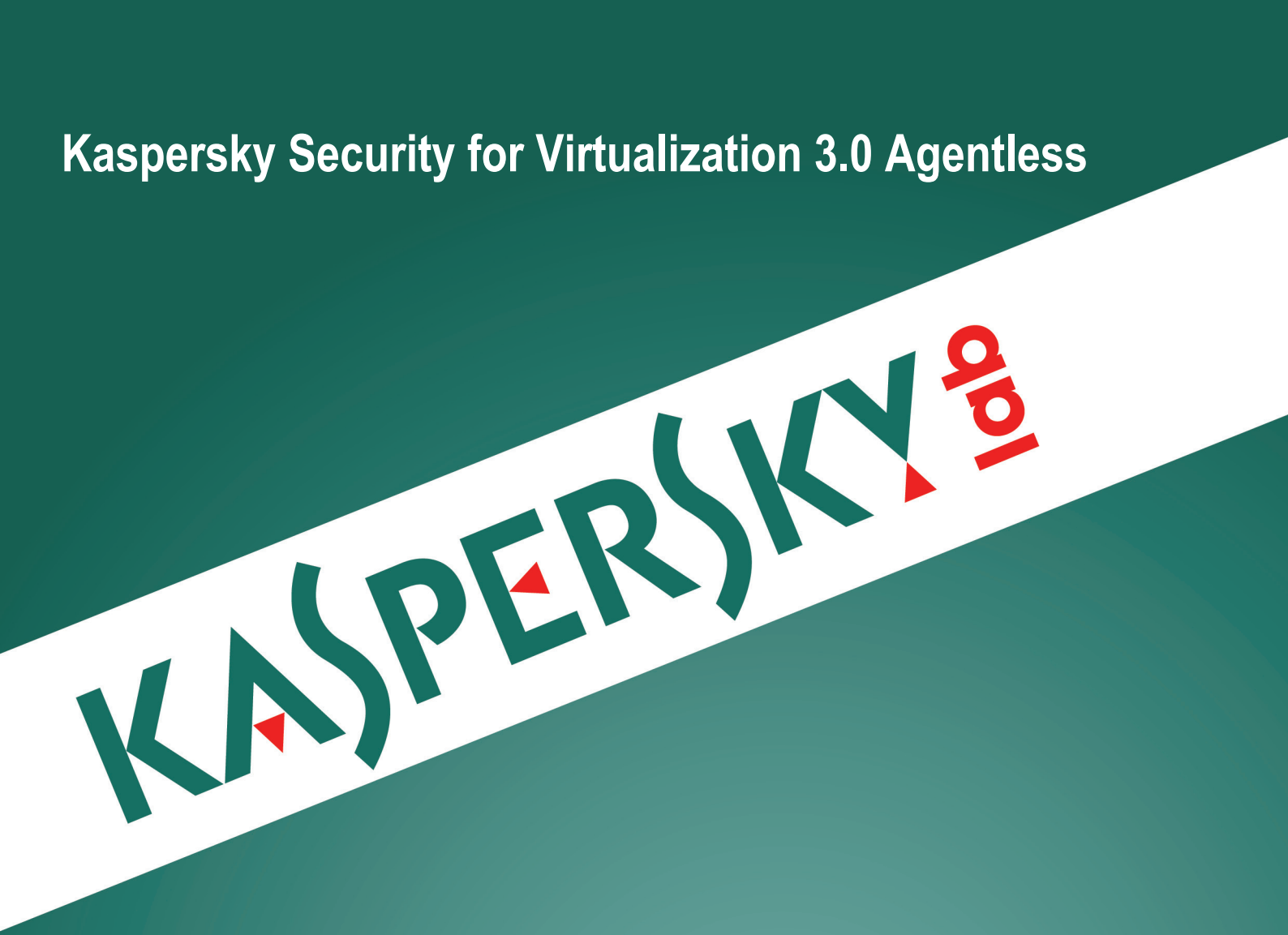
Kaspersky Security for Virtualization 3.0 Agentless



Manuel de l'administrateur

VERSION DE L'APPLICATION : 3.0 SERVICE PACK 1

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que ce document vous sera utile et qu'il répondra à la majorité des questions que vous pourrez vous poser.

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

Date d'édition : 21/05/2015

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

TABLE DES MATIERES

PRESENTATION DU MANUEL 6
Dans ce document 6
Conventions 8
SOURCES D'INFORMATIONS SUR L'APPLICATION 9
Sources pour des consultations indépendantes 9
Discussion sur les logiciels de Kaspersky Lab sur le forum 10
KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS 11
Nouveautés 12
Distribution 13
Configurations logicielle et matérielle 14
ARCHITECTURE DE L'APPLICATION 17
Présentation de l'architecture de l'application 17
Composition des images des machines virtuelles de protection Kaspersky Security 18
Intégration des modules de Kaspersky Security avec l'infrastructure virtuelle VMware 19
A propos du Serveur d'intégration 20
CONCEPT DE L'ADMINISTRATION DE L'APPLICATION VIA LE KASPERSKY SECURITY CENTER 22
A propos de la stratégie de Kaspersky Security et des profils de protection 23
Héritage des profils de protection 24
A propos du profil de protection racine 24
A propos des tâches de Kaspersky Security 25
LICENCE DE L'APPLICATION 26
A propos du Contrat de Licence Utilisateur Final 26
A propos de la licence 26
A propos du Certificat de licence 27
A propos de la clé 28
A propos du code d'activation 29
A propos du fichier clé 29
A propos de l'abonnement 29
Activation de l'application 30
Création d'une tâche d'ajout de clé 32
Lancement de la tâche d'ajout de clé 35
Renouvellement de la licence 36
Renouvellement de l'abonnement 36
Consultation des informations relatives aux clés ajoutées 37
Consultation des informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab 37
Consultation des informations relatives à la clé dans les propriétés de l'application 39
Consultation des informations relatives à la clé dans les propriétés de la tâche d'ajout de clé 41
Consultation du rapport sur l'utilisation des clés 42
LANCEMENT ET ARRET DE L'APPLICATION 45
ADMINISTRATION DE LA PROTECTION 46
Etat de la protection 46
Création d'une stratégie 46
Etape 1. Définition du nom de la stratégie de groupe pour l'application 47

Etape 2. Sélection de l'application pour la création de la stratégie de groupe 47
Etape 3. Configuration des paramètres du profil de protection racine 48
Etape 4. Accord de participation à Kaspersky Security Network 52
Etape 5. Création de la stratégie de groupe pour l'application 52
Consultation de l'infrastructure protégée du cluster KSC 53
Désactivation de la protection sur la machine virtuelle 54
Consultation de la liste des machines virtuelles et des machines virtuelles de protection du cluster KSC 55
ANTI-VIRUS FICHIERS 57
Protection des machines virtuelles 57
A propos de la protection des machines virtuelles 57
Utilisation des profils de protection 58
Analyse des machines virtuelles 65
A propos de l'analyse des machines virtuelles 65
Création d'une tâche d'analyse complète 67
Création d'une tâche d'analyse personnalisée 73
Lancement et arrêt de l'analyse complète et de l'analyse personnalisée 81
DETECTION DES INTRUSIONS 82
Concernant la protection des machines virtuelles contre les menaces réseau 82
Activation et désactivation de la détection des attaques réseau 83
Configuration des paramètres de blocage des adresses IP à l'origine d'une attaque réseau 83
Activation et désactivation de l'analyse des adresses Internet 84
Configuration des paramètres d'analyse des adresses Internet 85
Configuration du message de blocage de l'adresse Internet 86
SAUVEGARDE 87
A propos de la sauvegarde 87
Configuration des paramètres de la sauvegarde 88
Manipulation des copies de sauvegarde des fichiers 88
Consultation de la liste des copies de sauvegarde des fichiers 89
Enregistrement des fichiers de la sauvegarde sur le disque 89
Suppression des copies de sauvegarde des fichiers 90
MISE A JOUR DES BASES ANTIVIRUS 91
A propos de la mise à jour des bases antivirus 91
Récupération automatique des mises à jour des bases antivirus 91
Création de la tâche de diffusion des mises à jour 92
Consultation des résultats d'exécution de la tâche de diffusion des mises à jour 93
Lancement manuel de la tâche de diffusion des mises à jour 94
Remise à l'état antérieur à la dernière mise à jour 94
Création de la tâche de remise à l'état antérieur à la mise à jour 95
Lancement de la tâche de remise à l'état antérieur à la mise à jour 96
RAPPORTS ET NOTIFICATIONS 98
A propos des événements et des notifications 98
Types de rapports 99
Rapport sur les versions des applications de Kaspersky Lab 100
Rapport sur le déploiement de la protection 101
Rapport sur les ordinateurs les plus infectés 102
Rapport sur les virus 103
Rapport sur les erreurs 104

Rapport sur les bases utilisées 105
Rapport sur les attaques réseau 106
Rapport sur le fonctionnement du contrôle Web 107
Consultation des rapports 109
Configuration des paramètres de notification 110
Consultation des statistiques du fonctionnement de l'application 111
PARTICIPATION A KASPERSKY SECURITY NETWORK 113
A propos de la participation à Kaspersky Security Network 113
Présentation des données 114
Activation et désactivation de l'utilisation de Kaspersky Security Network 114
CONTACTER LE SUPPORT TECHNIQUE 116
Présentation du Support technique 116
Support Technique par téléphone 116
Support Technique via Kaspersky CompanyAccount 117
Collecte d'informations pour le Support Technique 117
Utilisation du fichier de traçage 118
Utilisation des fichiers de statistiques système 118
GLOSSAIRE 119
KASPERSKY LAB ZAO 123
INFORMATION SUR LE CODE TIERS 124
AVIS DE MARQUES COMMERCIALES 125
INDEX 126

PRESENTATION DU MANUEL

Le manuel de l'administrateur de Kaspersky Security for Virtualization 3.0 Agentless (ci-après également "Kaspersky Security") est destiné aux techniciens chargés de l'administration de Kaspersky Security et de l'assistance aux organisations qui utilisent Kaspersky Security. Le guide s'adresse aux experts techniques expérimentés dans l'utilisation de l'infrastructure virtuelle sous VMware vSphere™ et du système d'administration centralisée à distance des applications de Kaspersky Lab du Kaspersky Security Center.

Ce manuel poursuit les objectifs suivants :

- Décrire les principes de fonctionnement de Kaspersky Security, la configuration requise et les particularités de l'intégration à d'autres applications.
- Décrire l'utilisation de Kaspersky Security.
- Présenter les sources complémentaires d'informations sur l'application et les modes d'obtention du support technique.

DANS CETTE SECTION

Dans ce document.....6

Conventions.....8

DANS CE DOCUMENT

Ce manuel contient les sections suivantes :

Sources d'informations sur l'application (cf. page 9)

Cette section décrit les sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Security for Virtualization 3.0 Agentless (cf. page 11)

Cette section contient des informations sur la fonction, les principales possibilités et la composition de l'application.

Architecture de l'application (cf. page 17)

Cette section décrit les modules de l'application et leur logique de fonctionnement. Elle fournit également des informations sur l'intégration de l'application au système Kaspersky Security Center et à l'infrastructure virtuelle VMware™.

Concept de l'administration de l'application via le Kaspersky Security Center (cf. page. 22)

Cette section décrit le concept de l'administration de l'application via le Kaspersky Security Center.

Licence de l'application (cf. page 26)

Cette section présente les notions principales relatives à l'activation de l'application. Elle détaille le Contrat de licence et le Certificat de licence, les types de licences et l'activation de l'application.

Lancement et arrêt de l'application (cf. page 45)

Cette section explique comment lancer et arrêter l'application.

Administration de la protection (cf. page 46)

Cette section explique comment créer une stratégie, vérifier l'état de la protection des machines virtuelles et rechercher la présence éventuelle de problèmes dans la protection.

Antivirus Fichiers (cf. page 57)

Cette section contient des informations sur la configuration des paramètres du module Antivirus Fichiers.

Détection des intrusions (cf. page 82)

Cette section contient des informations sur la configuration des paramètres du module de Détection des intrusions.

Sauvegarde (cf. page 87)

Cette section présente la sauvegarde et explique comment la manipuler.

Mise à jour des bases antivirus (cf. page 91)

Cette section contient des informations sur la mise à jour des bases (ci-après mises à jour) et des instructions sur la configuration des paramètres de mise à jour.

Rapports et notifications (cf. page 98)

Cette section décrit les différents moyens d'obtenir des informations sur le fonctionnement de Kaspersky Security.

Participation au Kaspersky Security Network (cf. page 113)

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

Contacter le Support Technique (cf. page 116)

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Support Technique.

Glossaire (cf. page 119)

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

Kaspersky Lab ZAO (cf. page 123)

Cette section contient des informations sur Kaspersky Lab ZAO.

Information sur le code tiers (cf. page 124)

Cette section contient des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page 125)

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

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

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Ils contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Les bases sont dépassées* se produit.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application sont en caractères gras : par exemple, les champs de saisie, les options du menu et les boutons.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et sont accompagnées de 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 de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir à l'aide du clavier.
<Nom d'utilisateur>	Les variables se trouvent entre chevrons. La valeur correspondant à la variable remplace cette variable tandis que les chevrons sont omis.

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 9

Discussion sur les logiciels de Kaspersky Lab sur le forum 10

SOURCES POUR DES CONSULTATIONS INDEPENDANTES

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 la réponse à votre question, il est recommandé de contacter le Support Technique de Kaspersky Lab.

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

Page de Kaspersky Security sur le site de Kaspersky Lab

La page (http://www.kaspersky.com/fr/business-security/virtualization/agentless) fournit des informations générales sur l'application, ses possibilités et ses particularités.

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

Page de Kaspersky 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/ksv3nola) 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 reprend l'aide contextuelle. L'aide contextuelle contient des informations sur chacune des fenêtres du plug-in d'administration de Kaspersky Security : liste et description des paramètres.

Documentation

La distribution de l'application contient des documents qui vous aideront à installer et à activer l'application dans l'infrastructure virtuelle, à configurer ses paramètres de fonctionnement et à obtenir les informations sur ses principaux modes d'utilisation.

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 sur 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 3.0 AGENTLESS

Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 est une solution intégrée qui protège les machines virtuelles de l'hyperviseur VMware ESXi contre les virus, les autres programmes présentant une menace pour la sécurité de l'ordinateur (ci-après "contre les virus et autres programmes présentant une menace") et les intrusions réseau. Les composants de l'application sont intégrés à l'infrastructure virtuelle VMware à l'aide des technologies VMware vShield™ Endpoint et VMware Network Extensibility SDK 5.1. Ainsi, avec les technologies VMware vShield Endpoint et VMware Network Extensibility SDK 5.1, il est possible de protéger les machines virtuelles sans devoir installer un logiciel antivirus complémentaire sur les systèmes d'exploitation invités.

Kaspersky Security protège les machines virtuelles dotées d'un système d'exploitation invité Windows® ainsi que les versions serveur de ces systèmes (cf. section "Configuration logicielle et matérielle" à la page 14).

Kaspersky Security protège les machines virtuelles si elles sont activées (en ligne, c'est-à-dire non éteintes ou arrêtées) et si elles sont équipées du pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) activé.

Kaspersky Security permet de configurer la protection des machines virtuelles à n'importe quel niveau de la hiérarchie des objets d'administration de VMware : serveur VMware vCenter™, objet Datacenter, cluster VMware, hyperviseur VMware ESXi qui n'appartient pas au cluster VMware, pool de ressources, objet vApp et machine virtuelle. L'application prend en charge la protection des machines virtuelles lors de la migration dans le cadre d'un cluster DRS de VMware.

Kaspersky Security comprend les modules suivants :

- *Anti-Virus Fichiers* : module permettant d'éviter la contamination des objets du système de fichiers de la machine virtuelle. Le module est activé lors du lancement de Kaspersky Security. Il protège les machines virtuelles et analyse les objets de leur système de fichiers.

- *Détection des intrusions* : module analysant le trafic réseau des machines virtuelles et permettant de détecter et de bloquer l'activité caractéristique des attaques réseau. Ce module confronte également l'adresse Internet sollicitée par l'utilisateur à une base d'adresses Internet malveillantes et bloque l'accès aux adresses Internet nuisibles. Dans VMware vShield Manager, le module Détection des intrusions s'enregistre comme un service de Kaspersky Network Protection.

Kaspersky Security offre les possibilités suivantes :

- **Protection**. Elle analyse tous les fichiers que l'utilisateur ou une autre application ouvre, enregistre ou lance sur la machine virtuelle afin de déterminer s'ils contiennent d'éventuels virus ou d'autres programmes dangereux.

  - Si le fichier ne contient aucun virus ou programme dangereux, Kaspersky Security octroie l'accès à ce fichier.

  - Si le fichier contient des virus ou autres programmes dangereux, l'application Kaspersky Security exécute l'action définie dans les paramètres : par exemple, il répare ou bloque le fichier.

  Kaspersky Security transmet les informations sur tous les événements survenus dans le cadre de la protection des machines virtuelles au serveur d'administration du Kaspersky Security Center.

- **Analyse**. L'application peut rechercher la présence éventuelle de virus et autres programmes dangereux dans les fichiers de la machine virtuelle. Pour éviter la propagation d'objets malveillants, il est nécessaire d'analyser les fichiers de la machine virtuelle à l'aide des nouvelles bases antivirus. Vous pouvez réaliser une analyse à la demande ou la programmer. Kaspersky Security transmet les informations sur tous les événements survenus dans le cadre des tâches d'analyse au Serveur d'administration du Kaspersky Security Center.

- **Détection des attaques réseau**. L'application surveille le trafic réseau des machines virtuelles, à l'affût d'une activité caractéristique d'une attaque réseau. En cas de détection d'une tentative d'attaque réseau contre la machine virtuelle, Kaspersky Security peut bloquer l'adresse IP à partir de laquelle a été lancée l'attaque réseau. Kaspersky Security transmet les informations sur les événements survenus dans le cadre de la protection des machines virtuelles contre les attaques réseau au Serveur d'administration du Kaspersky Security Center.

- **Analyse des adresses Internet**. L'application confronte les adresses Internet ou les applications HTTP sollicitées par l'utilisateur à une base d'adresses Internet malveillantes. En cas de détection d'une adresse Internet dans la base des adresses Internet malveillantes, l'application peut bloquer l'accès à cette URL. Kaspersky Security transmet les informations sur tous les événements survenus dans le cadre de l'analyse des adresses Internet au Serveur d'administration du Kaspersky Security Center.

- **Conservation des copies de sauvegarde des fichiers**. L'application permet de conserver les copies de sauvegarde des fichiers qui ont été supprimés ou modifiés durant la réparation. Les copies de sauvegarde sont conservées dans la sauvegarde sous un format spécial et ne présentent aucun danger. Si les informations du fichier réparé sont devenues complètement ou partiellement inaccessibles suite à la réparation, vous pouvez conserver le fichier depuis sa copie de sauvegarde.

- **Mise à jour des bases antivirus**. L'application télécharge les mises à jour des bases anti-virus. Ceci garantit que la protection de la machine virtuelle est à jour contre les nouveaux virus et autres programmes dangereux. Vous pouvez réaliser manuellement la mise à jour des bases antivirus ou la programmer.

Le Kaspersky Security Center de Kaspersky Lab est le système d'administration à distance utilisé pour administrer Kaspersky Security.

Le Kaspersky Security Center permet de réaliser les opérations suivantes :

- installer l'application dans l'infrastructure virtuelle VMware ;
- configurer les paramètres de fonctionnement de l'application ;
- administrer 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 anti-virus de l'application ;
- utiliser les copies de sauvegarde des fichiers dans la sauvegarde ;
- créer des rapports sur les événements survenus pendant le fonctionnement de l'application ;
- supprimer l'application de l'infrastructure virtuelle VMware.

DANS CETTE SECTION

Nouveautés 12

Distribution 13

Configurations logicielle et matérielle 14

NOUVEAUTES

Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 présente les nouvelles fonctionnalités suivantes :

- Ajout de la compatibilité avec les composants de VMware vSphere 6.0.

- Nouveau module de l'application Kaspersky Security : Serveur d'intégration. Ce module est destiné aux infrastructures virtuelles comportant de nombreuses machines virtuelles de protection et vise à alléger la charge pesant sur le serveur VMware vCenter. Le serveur d'intégration se connecte au serveur VMware vCenter, obtient des informations sur l'infrastructure virtuelle VMware et transmet ces informations aux machines virtuelles de protection dès qu'elles en ont besoin. Cette opération permet de diminuer le nombre de requêtes que les machines virtuelles de protection envoient au serveur VMware vCenter.

- Possibilité d'utiliser l'application par abonnement. L'application peut être activée à l'aide du code d'activation fourni sur abonnement.
- La liste des exclusions du profil de protection racine comporte désormais des exclusions de la protection par défaut conseillées par Microsoft®. De même, il est désormais possible d'importer la liste des exclusions conseillées de Microsoft dans un profil de protection complémentaire et dans les exclusions des tâches d'analyse.
- Nouvelle possibilité d'exclure de l'analyse et de la protection les fichiers en fonction de leur nom, de leur chemin d'accès ou du masque indiqué (les caractères * et ? sont utilisés dans les noms de masque).
- Nouvelle fonction de vérification des certificats SSL reçus lors de l'établissement des connexions suivantes :
  - machine virtuelle de protection au serveur VMware vCenter ;
  - Serveur d'intégration au serveur VMware vCenter ;
  - machine virtuelle de protection au Serveur d'intégration ;
  - Console de gestion du Serveur d'intégration au Serveur d'intégration ;
  - plug-in d'administration de Kaspersky Security au serveur VMware vCenter ;
  - Assistant d'installation / de suppression / de mise à jour / de modification de la configuration des machines virtuelles de protection au Serveur d'intégration ;
  - Assistant d'installation / de suppression / de mise à jour / de modification de la configuration des machines virtuelles de protection au serveur VMware vCenter ;
  - Assistant d'installation / de suppression / de mise à jour / de modification de la configuration des machines virtuelles de protection à VMware vShield Manager.
- Nouvelle possibilité de définir un chemin vers les dossiers réseau sans tenir compte de la casse.
- Nouvelle possibilité de désactiver l'analyse des fichiers des disques réseau au cours de la protection.
- Nouvel affichage de l'état "désactivé ou suspendu" pour les machines virtuelles de la liste des machines virtuelles et des machines virtuelles de protection qui font partie du cluster KSC.
- Nouvelle possibilité d'importer/exporter la liste des exclusions de l'analyse et de la protection dans les tâches d'analyse et dans les profils de protection.
- Nouvelle possibilité de consulter les statistiques de fonctionnement de chaque machine virtuelle de protection dans la Console d'administration du Kaspersky Security Center (informations relatives à la durée de validité restante de la licence, au nombre d'objets analysés et aux bases antivirus).

DISTRIBUTION

Kaspersky Endpoint Security peut être acheté dans la boutique en ligne de Kaspersky Lab (par exemple http://www.kaspersky.com/fr, section **Boutique en ligne**) ou sur le site d'un partenaire.

La distribution contient les éléments suivants :

- les fichiers de l'application ;
- 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 courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et la distribution, écrivez au Service commercial à l'adresse sales@kaspersky.com.

CONFIGURATIONS LOGICIELLE ET MATERIELLE

Pour permettre le fonctionnement de Kaspersky Security sur le réseau local de l'organisation, l'application Kaspersky Security Center 10 Service Pack 1 doit être installée.

L'ordinateur sur lequel est installée la Console d'administration de Kaspersky Security Center doit être équipé de Microsoft .NET Framework 4.0 ou suivant.

Configuration requise pour le composant Anti-Virus Fichiers

Afin que le module Anti-Virus Fichiers fonctionne, l'infrastructure virtuelle VMware doit respecter les exigences de configuration suivantes :

- Hôte VMware ESXi 6.0, hôte VMware ESXi 5.5 patch 2 ou hôte VMware ESXi 5.1 patch 3.
- Serveur VMware vCenter 6.0.0a, serveur VMware vCenter 5.5 patch 2e ou serveur VMware vCenter 5.1 patch 3a.
- VMware vShield Endpoint du paquet VMware vCloud™ Networking and Security 5.5.4.1.
- VMware vShield Manager du paquet VMware vCloud Networking and Security 5.5.4.1.
- Pilote VMware Guest Introspection Thin Agent ou pilote VMware vShield Endpoint Thin Agent. Le pilote VMware Guest Introspection Thin Agent fait partie de la distribution VMware Tools livrée avec l'hyperviseur VMware ESXi 6.0 et l'hyperviseur VMware ESXi 5.5 patch 2. Le pilote VMware vShield Endpoint Thin Agent fait partie de la distribution VMware Tools livrée avec l'hyperviseur VMware ESXi 5.1 patch 3.

  Le pilote doit être installé sur la machine virtuelle protégée par Kaspersky Security.

  Lors de l'installation du paquet VMware Tools, le module VMware Devices Drivers / VMCI Driver / vShield Drivers doit être installé. Lors de l'installation du paquet VMware Tools avec les paramètres par défaut, le module VMware Devices Drivers / VMCI Driver / vShield Drivers ne sera pas installé.

Pour plus d'informations sur la mise à jour VMware Tools, consultez la documentation pour les produits VMware.

Configuration requise pour le module Détection des intrusions

Afin que le module Détection des intrusions fonctionne, l'infrastructure virtuelle VMware doit respecter les exigences de configuration suivantes :

- Hôte VMware ESXi 6.0, hôte VMware ESXi 5.5 patch 2 ou hôte VMware ESXi 5.1 patch 3.
- Serveur VMware vCenter 6.0.0a, serveur VMware vCenter 5.5 patch 2e ou serveur VMware vCenter 5.1 patch 3a.
- VMware vShield Manager du paquet VMware vCloud Networking and Security 5.5.4.1.
- VMware Distributed Virtual Switch 5.1.0 et suivante.

Pour utiliser le module Détection des intrusions, il faut avoir la licence valide pour vCloud Networking Security.

Configuration requise pour le module Serveur d'intégration

L'installation et la mise en service du module Serveur d'intégration sur l'ordinateur nécessitent la présence de l'un des systèmes d'exploitation suivants :

- Windows Server® 2008 R2.
- Windows Server 2008 R2, déployé en mode Server Core.
- Windows Server 2012.
- Windows Server 2012 déployé en mode Server Core.
- Windows 2012 R2.

L'installation du Serveur d'intégration et de la Console de gestion du Serveur d'intégration nécessite la plateforme Microsoft .NET Framework 4.0 ou une version ultérieure.

Configuration requise pour le système d'exploitation invité de la machine virtuelle protégée par Kaspersky Security

Le module Anti-Virus Fichiers garantit la protection des machines virtuelles sur lesquelles sont installés les systèmes d'exploitation invités suivants :

- Systèmes d'exploitation pour postes de travail :
  - Windows XP SP3 ou suivant (version 32 bits).
  - Windows 7 (version 32 ou 64 bits) ;
  - Windows 8 (version 32 ou 64 bits) ;
  - Windows 8.1 (32 / 64 bits) : lors de l'utilisation de VMware vSphere 5.5 patch 2 ou version ultérieure.
- Systèmes d'exploitation pour serveurs :
  - Windows Server 2003 SP2 ou suivant (versions 32 ou 64 bits) ;
  - Windows Server 2003 R2 (version 32 ou 64 bits) ;
  - Windows Server 2008 (versions 32 ou 64 bits) ;
  - Windows Server 2008 R2 (version 64 bits).
  - Windows Server 2012 sans prise en charge de ReFS (Resilient File System) (version 64 bits).
  - Windows Server 2012 R2 (64 bits) : lors de l'utilisation de VMware vSphere 5.5 patch 2d ou version ultérieure.

Les exigences du module Détection des intrusions envers le système d'exploitation invité de la machine virtuelle protégée correspondent aux exigences des hôtes VMware ESXi 6.0, VMware ESXi 5.5 patch 2 ou VMware ESXi 5.1 patch 3 vis-à-vis des systèmes d'exploitation invités.

Le module Détection des intrusions assure la protection des machines virtuelles utilisées avec l'adaptateur réseau E1000 ou VMXNET3.

Configuration matérielle requise

Il est nécessaire d'octroyer une quantité minimale de ressources système à la machine virtuelle de protection dotée du module Anti-Virus Fichiers :

- volume libre de mémoire vive: 2 Go ;
- nombre de processeurs 2 ;
- volume de l'espace libre : 30 Go ;

Il est nécessaire d'octroyer une quantité minimale de ressources système à la machine virtuelle de protection dotée du module Détection des intrusions :

- volume libre de mémoire vive: 1 Go ;
- nombre de processeurs 2 ;
- volume de l'espace libre : 8 Go ;

L'installation et la mise en service du module Serveur d'intégration impliquent que l'ordinateur satisfasse aux configurations matérielles minimales suivantes :

- volume de l'espace libre sur le disque : 40 Go ;
- volume de la mémoire vive :
  - 50 Mo pour la Console de gestion du Serveur d'intégration ;
  - 300 Mo pour un Serveur d'intégration ne desservant pas plus de 30 hyperviseurs et de 2 000 à 2 500 machines virtuelles protégées. Le volume de la mémoire vive peut varier en fonction de la taille de l'infrastructure virtuelle VMware.

Pour connaître la configuration requise pour le Kaspersky Security Center, consultez la documentation du Kaspersky Security Center.

Pour connaître la configuration requise pour l'infrastructure virtuelle VMware, consultez la documentation des produits VMware.

Pour connaître la configuration requise pour le système d'exploitation Windows, consultez la documentation des produits Windows.

ARCHITECTURE DE L'APPLICATION

Cette section décrit les modules de Kaspersky Security leur interaction.

DANS CETTE SECTION

Présentation de l'architecture de l'application.....17

Composition des images des machines virtuelles de protection Kaspersky Security.....18

Intégration des modules de Kaspersky Security avec l'infrastructure virtuelle VMware 19

A propos du Serveur d'intégration 20

PRESENTATION DE L'ARCHITECTURE DE L'APPLICATION

Kaspersky Security est une solution intégrée qui protège les machines virtuelles sur un hyperviseur VMware ESXi (cf. ill. ci-après).

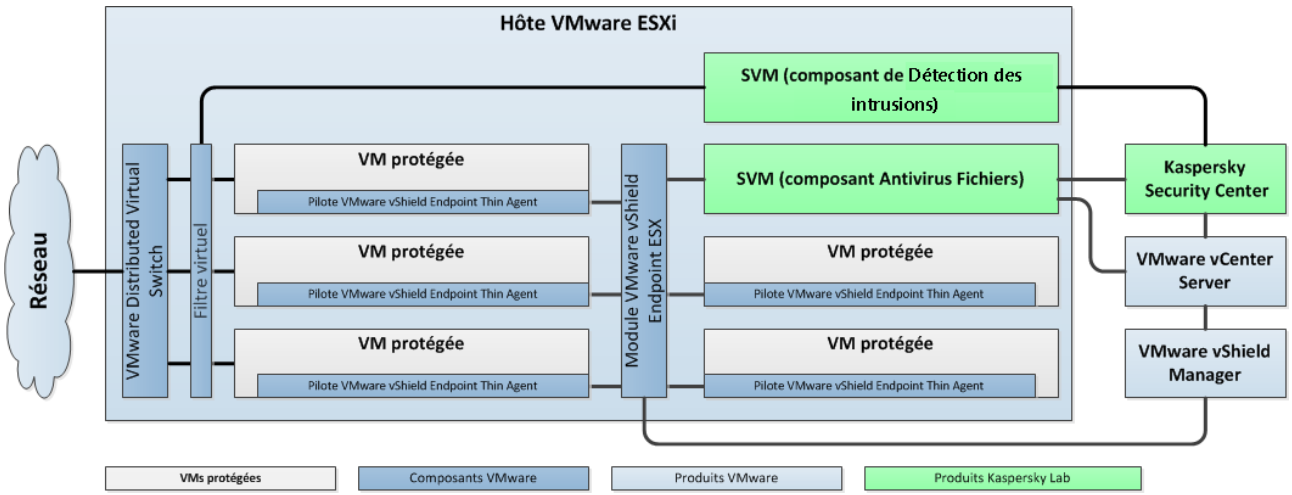


Illustration 1. Architecture de l'application

Kaspersky Security est installé sur un hyperviseur VMware ESXi et garantit la protection des machines virtuelles sur cet hyperviseur ESXi contre les virus et autres programmes dangereux.

Kaspersky Security se présente sous la forme de deux images de machines virtuelles de protection (voir la section "Composition des images des machines virtuelles de protection Kaspersky Security" page 18) :

- image de la machine virtuelle de protection assortie du module Anti-Virus Fichiers ;
- image de la machine virtuelle de protection sur laquelle le module Détection des intrusions est installé.

La machine virtuelle de protection est une machine virtuelle présente sur un hyperviseur VMware ESXi et sur laquelle un module de l'application Kaspersky Security est installé.

Installés sur un hyperviseur VMware ESXi, les composants de l'application Kaspersky Security garantissent la protection de toutes les machines virtuelles sur cet hyperviseur. Il n'est pas nécessaire d'installer l'application sur chaque machine virtuelle pour garantir leur protection.

L'infrastructure virtuelle de VMware peut contenir plusieurs hyperviseurs VMware ESXi. Il est nécessaire d'installer Kaspersky Security sur chaque hyperviseur dont il doit protéger les machines virtuelles.

L'installation de Kaspersky Security, ainsi que la configuration et l'administration de l'application, s'opèrent via le système d'administration centralisée à distance des applications du Kaspersky Security Center de Kaspersky Lab (cf. la documentation du Kaspersky Security Center).

L'interaction entre Kaspersky Security et l'application Kaspersky Security Center est assurée par l'agent d'administration, module du Kaspersky Security Center. L'agent d'administration figure dans l'image de la machine virtuelle de Kaspersky Security.

L'interface d'administration de l'application Kaspersky Security via le Kaspersky Security Center est assurée par le plug-in d'administration de Kaspersky Security. Le plug-in d'administration de Kaspersky Security fait partie de la distribution de Kaspersky Security. Le plug-in d'administration de Kaspersky Security doit être installé sur l'ordinateur hébergeant la Console d'administration du Kaspersky Security Center.

COMPOSITION DES IMAGES DES MACHINES VIRTUELLES DE PROTECTION KASPERSKY SECURITY

Dans la composition de l'image de la machine virtuelle de protection sur laquelle est installé le module Anti-Virus Fichiers entrent :

- Le système d'exploitation SUSE Linux® Enterprise Server 11 SP3.
- Le module Kaspersky Security Anti-Virus Fichiers.
- Bibliothèque EPSEC : module fourni par la société VMware. La bibliothèque EPSEC permet d'accéder aux fichiers des machines virtuelles protégées par Kaspersky Security.
- Agent d'administration : module du Kaspersky Security Center. L'Agent d'administration assure l'interaction avec le Serveur d'administration du Kaspersky Security Center et permet à ce dernier d'administrer Kaspersky Security.

Dans la composition de l'image de la machine virtuelle de protection sur laquelle est installé le module Détection des intrusions entrent :

- Le système d'exploitation SUSE Linux Enterprise Server 11 SP3.
- Module Détection des intrusions de Kaspersky Security.
- Bibliothèque VMware Network Extensibility SDK 5.1 : module de la société VMware. La bibliothèque VMware Network Extensibility SDK 5.1 offre la possibilité de surveiller le trafic réseau des machines virtuelles au niveau des paquets réseaux, ainsi que la possibilité de créer des filtres virtuels.
- Agent d'administration : module du Kaspersky Security Center. L'Agent d'administration assure l'interaction avec le Serveur d'administration du Kaspersky Security Center et permet à ce dernier d'administrer Kaspersky Security.

INTEGRATION DES MODULES DE KASPERSKY SECURITY AVEC L'INFRASTRUCTURE VIRTUELLE VMWARE

Composants VMware

L'intégration de l'Anti-Virus Fichiers à l'infrastructure virtuelle de VMware requiert les modules suivants :

- **VMware vShield Endpoint ESX™ Module**. Ce module est installé sur l'hyperviseur VMware ESXi. Il assure l'interaction du pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) installé sur la machine virtuelle et de la bibliothèque EPSEC installée sur la machine virtuelle de protection.

- **Serveur VMware vCenter**. Ce module intervient dans l'administration et l'automatisation des tâches d'exploitation au sein de l'infrastructure virtuelle VMware. Il participe au déploiement de Kaspersky Security. Les machines virtuelles de protection dotées du module Anti-Virus Fichiers et le plug-in d'administration Kaspersky Security reçoivent les informations relatives à l'infrastructure virtuelle VMware dont ils ont besoin pour exécuter leurs tâches depuis le serveur VMware vCenter.

  Les informations relatives à l'infrastructure virtuelle VMware sont enregistrées dans un fichier au format XML. Le fichier est situé sur l'ordinateur doté de la Console d'administration de Kaspersky Security Center, dans le dossier d'installation du plug-in d'administration de Kaspersky Security.

  Si un grand nombre de machines virtuelles échangent avec le serveur VMware vCenter, ce dernier peut subir une surcharge. Si votre infrastructure virtuelle comporte un grand nombre de machines virtuelles de protection, il est recommandé d'utiliser le module Serveur d'intégration de Kaspersky Security pour obtenir des informations relatives à l'infrastructure virtuelle VMware (cf. section "A propos du Serveur d'intégration" à la page 20).

- **VMware vShield Manager**. Ce module assure l'installation de VMware vShield Endpoint ESX Module sur les hyperviseurs VMware ESXi et l'enregistrement des machines virtuelles de protection.

Le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) collecte les informations sur les machines virtuelles et transmet les fichiers à analyser à l'application Kaspersky Security. Pour que Kaspersky Security puisse protéger les machines virtuelles, il est nécessaire d'installer et d'activer le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) sur ces machines virtuelles.

L'intégration du module Détection des intrusions à l'infrastructure virtuelle de VMware requiert les modules suivants :

- **VMware Distributed Virtual Switch**. Ce module permet de créer des réseaux virtuels et en assure la gestion.

- **Serveur VMware vCenter**. Ce module intervient dans l'administration et l'automatisation des tâches d'exploitation au sein de l'infrastructure virtuelle VMware. Il participe au déploiement de Kaspersky Security. Le module fournit des informations concernant les machines virtuelles installées sur les hyperviseurs VMware ESXi, les clusters VMware, les services installés et les paramètres de VMware Distributed Virtual Switches.

- **VMware vShield Manager**. Ce module assure l'enregistrement et le déploiement du module Détection des intrusions (service Kaspersky Network Protection) et le déploiement et l'enregistrement des machines virtuelles de protection sur les hyperviseurs VMware ESXi.

Les modules cités doivent être installés dans l'infrastructure virtuelle de VMware avant l'installation de Kaspersky Security.

Interaction des modules de Kaspersky Security avec l'infrastructure virtuelle VMware

Le module Anti-Virus Fichiers interagit avec l'infrastructure virtuelle VMware de la manière suivante :

1. L'utilisateur ou l'application ouvre, enregistre ou exécute des fichiers sur la machine virtuelle protégée par Kaspersky Security.

2. Le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) intercepte les informations relatives à ces événements et les transmet au module VMware vShield Endpoint ESX Module installé sur l'hyperviseur VMware ESXi.

3. Le module VMware vShield Endpoint ESX Module transmet les informations relatives aux événements reçus à la bibliothèque EPSEC installée sur la machine virtuelle de protection.

4. La bibliothèque EPSEC transmet les informations relatives aux événements reçus au module Anti-Virus Fichiers installé sur la machine virtuelle de protection et garantit l'accès aux fichiers sur la machine virtuelle.

5. Le module Anti-Virus Fichiers analyse les fichiers que l'utilisateur ouvre, enregistre et exécute sur la machine virtuelle afin de déterminer s'ils contiennent d'éventuels virus ou autres programmes dangereux.

    - Si le fichier ne contient aucun virus ou programme dangereux, Kaspersky Security octroie à l'utilisateur l'accès à ces fichiers.

    - Si des virus ou autres programmes dangereux sont détectés dans les fichiers, Kaspersky Security exécute l'action définie dans les paramètres du profil de protection attribué à cette machine virtuelle (cf. section "A propos de la stratégie de Kaspersky Security et des profils de protection" à la page 23). Par exemple, Kaspersky Security peut réparer ou bloquer le fichier.

Le module Détection des intrusions interagit avec l'infrastructure virtuelle VMware de la manière suivante :

1. Le filtre virtuel intercepte les paquets réseau dans le trafic entrant et sortant des machines virtuelles protégées et les envoie au module Détection des intrusions installé sur la machine virtuelle de protection.

2. Le module Détection des intrusions exécute les actions suivantes :

    - Il vérifie les paquets réseau sujets à des activités caractéristiques d'attaques réseau.

        - Si aucune attaque réseau n'est détectée, Kaspersky Security autorise le transfert du paquet réseau sur la machine virtuelle.

        - Si une activité caractéristique d'une attaque réseau est détectée, Kaspersky Security effectue l'action définie dans les paramètres du profil de protection (cf. section "A propos de la stratégie de Kaspersky Security et des profils de protection" à la page 23), attribué à cette machine virtuelle. Par exemple, Kaspersky Security bloque ou ignore les paquets réseau dont l'adresse IP est à l'origine d'une attaque réseau.

    - Il confronte l'ensemble des adresses Internet présentes dans les paquets réseaux à la base des adresses Internet malveillantes.

        - Si l'adresse Internet ne figure pas dans la base des URL malveillantes, Kaspersky Security autorise l'accès à cette adresse Internet.

        - Si une adresse Internet figure dans la base des adresses Internet malveillantes, Kaspersky Security exécute l'action définie dans les paramètres du profil de protection (cf. section "A propos de la stratégie de Kaspersky Security et des profils de protection" à la page 23), attribué à cette machine virtuelle. Par exemple, Kaspersky Security bloque ou autorise l'accès à cette URL.

A PROPOS DU SERVEUR D'INTEGRATION

Le Serveur d'intégration est un module de l'application Kaspersky Security qui assure l'interaction entre le serveur VMware vCenter et les machines virtuelles de protection dotées du module Anti-Virus Fichiers.

Lorsqu'elles sont actives, les machines virtuelles de protection se connectent au serveur VMware vCenter pour recevoir des informations concernant l'infrastructure VMware protégée (à propos des hyperviseurs et des machines virtuelles installées sur chaque hyperviseur). Si un grand nombre de machines virtuelles de protection sollicitent le serveur VMware vCenter, ce dernier peut subir une surcharge.

Si votre infrastructure virtuelle comporte un grand nombre de machines virtuelles de protection, il est conseillé d'utiliser le module de Kaspersky Security Serveur d'intégration pour obtenir des informations relatives à l'infrastructure virtuelle VMware. Le serveur d'intégration se connecte au serveur VMware vCenter, obtient des informations sur l'infrastructure virtuelle VMware et transmet ces informations aux machines virtuelles de protection dès qu'elles en ont besoin. Cette opération permet de diminuer le nombre de demandes que Kaspersky Security envoie au serveur VMware vCenter.

Vous pouvez installer le Serveur d'intégration sur n'importe quel ordinateur du réseau local de l'entreprise. La configuration des paramètres du Serveur d'intégration s'effectue dans la Console de gestion du Serveur d'intégration. Vous pouvez installer la Console de gestion sur l'ordinateur hébergeant le Serveur d'intégration, ou séparément.

Une fois que le Serveur d'intégration aura été installé et configuré, vous devrez configurer la connexion des machines virtuelles de protection dotées du module Anti-Virus Fichiers au Serveur d'intégration. Vous pouvez configurer la connexion lors de l'installation, de la mise à jour ou de la modification de la configuration des machines virtuelles de protection.

CONCEPT DE L'ADMINISTRATION DE L'APPLICATION VIA LE KASPERSKY SECURITY CENTER

L'administration de Kaspersky Security for Virtualization 3.0 Agentless s'opère via le système d'administration centralisée à distance du Kaspersky Security Center pour les applications de Kaspersky Lab. La machine virtuelle de protection est l'équivalent du poste client du Kaspersky Security Center pour l'application Kaspersky Security for Virtualization 3.0 Agentless. La synchronisation automatique des données entre les machines virtuelles de protection et le Serveur d'administration du Kaspersky Security Center se déroule de la même manière que la synchronisation des données entre les postes client et le Serveur d'administration (cf. documentation du Kaspersky Security Center).

Dans la Console d'administration du Kaspersky Security Center, le nom de la machine virtuelle peut refléter le nom de domaine ou le nom NetBIOS de cette machine, comme indiqué par ses propriétés répertoriées dans l'infrastructure virtuelle.

Les machines virtuelles de protection installées sur les hyperviseurs VMware ESXi sous l'administration d'un serveur VMware vCenter unique et les machines virtuelles qu'elles protègent sont réunies dans le Kaspersky Security Center en un *cluster KSC* (cluster Kaspersky Security Center) (cf. ill. ci-après). Le cluster KSC reçoit le nom du serveur VMware vCenter correspondant. Les objets d'administration VMware administrés par ce serveur VMware vCenter forment l'*infrastructure protégée* du cluster KSC.

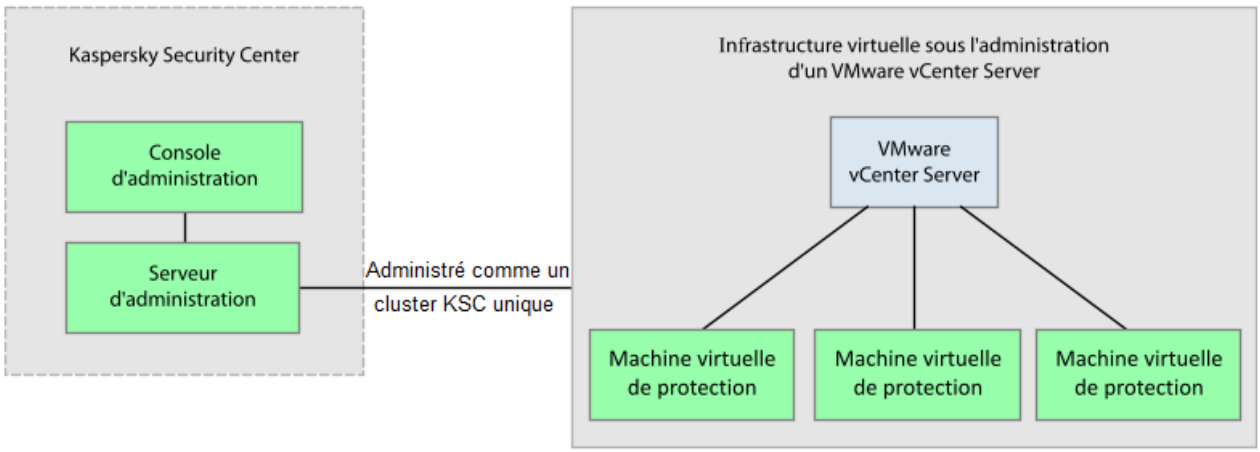


Illustration 2. Cluster KSC

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

- La *stratégie* définit les paramètres de protection des machines virtuelles contre les virus et les autres programmes présentant une menace, (cf. section "Création d'une stratégie" à la page 46), les paramètres de prévention des intrusions (cf. section "Détection des intrusions" à la page 82) et les paramètres des sauvegardes sur les machines virtuelles de protection (cf. section "A propos de la sauvegarde" à la page 87).

- Les *tâches d'analyse* déterminent les paramètres d'analyse des machines virtuelles (cf. section "Analyse des machines virtuelles" à la page 65).

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

DANS CETTE SECTION

A propos de la stratégie de Kaspersky Security et des profils de protection 23

A propos des tâches de Kaspersky Security 25

A PROPOS DE LA STRATEGIE DE KASPERSKY SECURITY ET DES PROFILS DE PROTECTION

Dans le cas de l'application Kaspersky Security for Virtualization 3.0 Agentless, la stratégie est appliquée au cluster KSC. Par conséquent, la stratégie s'applique à toutes les machines virtuelles de protection qui appartiennent au cluster KSC et définit les paramètres de protection de toutes les machines virtuelles figurant dans l'infrastructure protégée du cluster KSC.

Les paramètres de protection des machines virtuelles dans la stratégie sont définis par le *profil de protection* (cf. ill. ci-après). Une stratégie peut contenir plusieurs profils de protection. Un profil de protection est attribué aux objets d'administration de VMware appartenant à l'infrastructure protégée du cluster KSC. Un objet d'administration VMware ne peut se voir attribuer qu'un seul profil de protection.

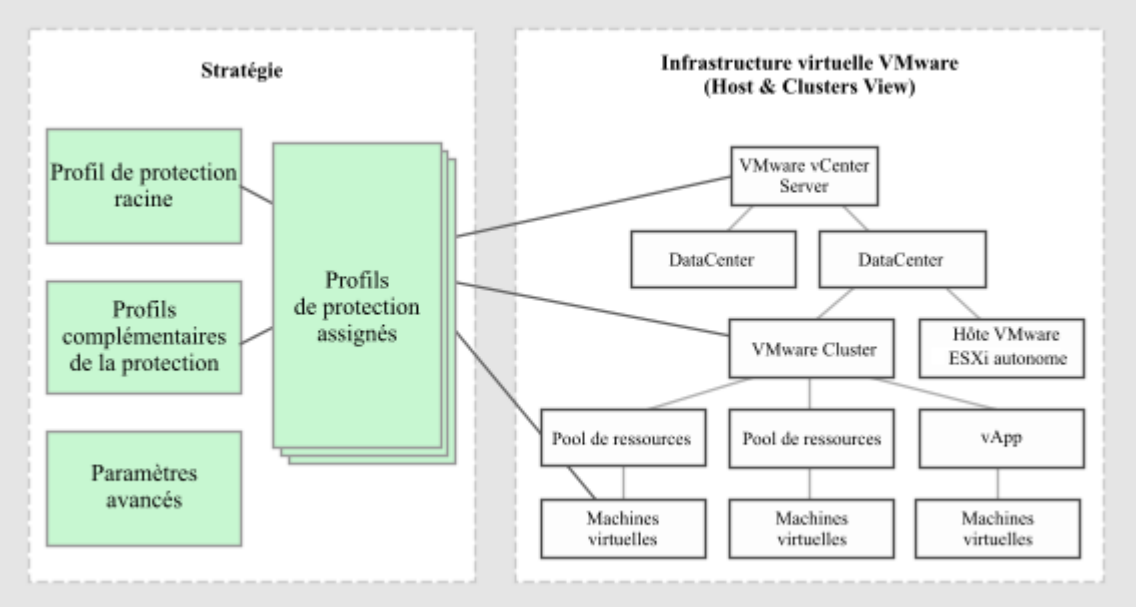


Illustration 3. Profils de protection

Kaspersky Security protège la machine virtuelle selon les paramètres définis dans le profil de protection qui lui a été attribué.

Le profil de protection permet de configurer les paramètres suivants :

- Niveau de sécurité. Vous pouvez sélectionner un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**) ou personnaliser vous-même le niveau de protection (**Utilisateur**). Le niveau de sécurité définit les paramètres d'analyse suivants :
  - analyse des archives, des archives autoextractibles, des objets OLE intégrés et des fichiers composés ;
  - limitation de la durée d'analyse des fichiers ;
  - liste des objets à détecter.

- Action exécutée par Kaspersky Security en cas de détection de fichiers infectés.
- Zone de protection (analyse des disques réseau au cours de la protection des machines virtuelles).
- Exclusions de la protection (en fonction du nom, de l'extension, du chemin d'accès au fichier, du masque de fichier ou du chemin d'accès au dossier dont les fichiers ne doivent pas être analysés).

Les profils de protection permettent de configurer en souplesse différents paramètres de protection pour diverses machines virtuelles.

Le Kaspersky Security Center permet de définir une hiérarchie complexe de groupes d'administration et de stratégies (pour en savoir plus, consultez la documentation du Kaspersky Security Center). Dans l'application Kaspersky Security, chaque stratégie utilise un ensemble de paramètres pour se connecter au serveur VMware vCenter. Si vous utilisez la hiérarchie complexe des groupes d'administration et des stratégies, la stratégie du niveau inférieur hérite des paramètres incorrects de connexion au serveur VMware vCenter, ce qui peut amener à une erreur de connexion. C'est pourquoi, pendant la configuration des paramètres de Kaspersky Security, il est conseillé de ne pas créer de hiérarchie complexe de groupes d'administration et de stratégies. Il est préférable de créer une stratégie distincte pour chaque cluster KSC.

DANS CETTE SECTION

Héritage des profils de protection 24

A propos du profil de protection racine 24

HERITAGE DES PROFILS DE PROTECTION

Kaspersky Security applique l'héritage des profils de protection selon la hiérarchie des objets d'administration de VMware.

Le profil de protection attribué à un objet d'administration de VMware est transmis à tous les objets enfants, y compris les machines virtuelles si l'objet enfant/la machine virtuelle ne possède pas son propre profil de protection (cf. section "Attribution d'un profil de protection à une machine virtuelle" à la page 64) ou, si l'objet enfant/la machine virtuelle ne sont pas exclus de la protection (cf. section "Désactivation de la protection sur la machine virtuelle" à la page 54). Ainsi, vous pouvez attribuer son propre profil de protection à une machine virtuelle ou créer pour celle-ci un profil hérité de l'objet parent.

L'objet d'administration de VMware peut être exclu de la protection. Si vous avez exclu un objet d'administration de VMware de la protection, alors tous les objets enfants, y compris les machines virtuelles, sont également exclus de la protection. Les objets enfants/machines virtuelles dotés de leur propre profil de protection sont toujours protégés par l'application.

L'héritage des profils de protection permet d'attribuer simultanément des paramètres identiques de protection à plusieurs machines virtuelles. Par exemple, vous pouvez attribuer des profils de protection identiques aux machines virtuelles qui appartiennent au cluster VMware ou au pool de ressources.

A PROPOS DU PROFIL DE PROTECTION RACINE

Le *profil de protection racine* est formé pendant la création de la stratégie. Le profil de protection racine est attribué à l'objet racine de la structure des objets d'administration de VMware, à savoir le serveur VMware vCenter. Conformément à l'ordre d'héritage des profils de protection, tous les objets d'administration de VMware, y compris les machines virtuelles appartenant à l'infrastructure protégée du cluster KSC, héritent du profil de protection racine si aucun profil de protection spécifique ne leur a été attribué. Ainsi, toutes les machines virtuelles appartenant à l'infrastructure protégée du cluster KSC se voient attribuer les mêmes paramètres de protection.

Après la création d'une stratégie, vous pouvez composer des profils de protection complémentaires et les utiliser pour une configuration plus souple de la protection des machines virtuelles.

Le profil de protection racine ne peut être supprimé, mais vous pouvez par contre en modifier les paramètres.

A PROPOS DES TACHES DE KASPERSKY SECURITY

Le Kaspersky Security Center gère le fonctionnement de l'application Kaspersky Security à l'aide de tâches. Les tâches remplissent les principales fonctions de l'application telles que l'analyse des machines virtuelles protégées ou la mise à jour des bases antivirus.

Pour utiliser Kaspersky Security via le Kaspersky Security Center, vous pouvez utiliser les *tâches de groupe*. Les tâches de groupe sont exécutées sur les postes clients du groupe d'administration sélectionné. Pour ce qui est de Kaspersky Security, les tâches de groupe (ci-après "les tâches") sont exécutées sur toutes les machines virtuelles de protection qui appartiennent au cluster KSC.

Pour administrer Kaspersky Security, vous pouvez utiliser les tâches suivantes :

- **Analyse complète**. Kaspersky Security recherche la présence éventuelle de virus et autres programmes dangereux sur toutes les machines virtuelles de tous les clusters KSC.
- **Analyse personnalisée**. Kaspersky Security recherche la présence éventuelle de virus et autres programmes dangereux sur les machines virtuelles sélectionnées dans le cluster KSC.
- **Diffusion des mises à jour**. Le Kaspersky Security Center diffuse et installe automatiquement les mises à jour des bases antivirus sur les machines virtuelles de protection.
- **Remise à l'état antérieur à la mise à jour**. Le Kaspersky Security Center revient à l'état antérieur à la dernière mise à jour des bases antivirus sur les machines virtuelles de protection.
- **Ajout d'une clé**. Le Kaspersky Security Center ajoute la clé d'activation de l'application ou de renouvellement de la licence sur les machines virtuelles de protection.

Vous pouvez réaliser les opérations suivantes sur les tâches :

- lancer et arrêter les tâches ;
- créer des tâches ;
- modifier les paramètres des tâches.

LICENCE DE L'APPLICATION

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

DANS CETTE SECTION

A propos du Contrat de Licence Utilisateur Final 26

A propos de la licence 26

A propos du Certificat de licence 27

A propos de la clé 28

A propos du code d'activation 29

A propos du fichier clé 29

A propos de l'abonnement 29

Activation de l'application 30

Renouvellement de la licence 36

Renouvellement de l'abonnement 36

Consultation des informations relatives aux clés ajoutées 37

A PROPOS DU CONTRAT DE LICENCE UTILISATEUR FINAL

Le *contrat de licence utilisateur final* est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement les conditions du Contrat de licence avant de commencer à utiliser l'application.

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

- Au cours de l'installation de l'application.
- En lisant le document license.txt. Ce document est repris dans la distribution de l'application (cf. section "Distribution" à la page. 13).

Vous acceptez les conditions du contrat de licence, en confirmant votre accord avec le texte du contrat de licence lors de l'installation de l'application.

Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application et ne pas l'utiliser.

A PROPOS DE LA LICENCE

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

La licence vous donne droit aux services suivants :

- Utilisation de l'application pour la protection des machines virtuelles sur les hyperviseurs VMware ESXi.

  Kaspersky Security protège uniquement les machines virtuelles de l'infrastructure virtuelle VMware sur lesquelles le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) est installé et activé et qui sont en ligne (c.-à-d. ni éteintes, ni suspendues).

- Contacter le Support Technique de Kaspersky Lab.

- Accès aux divers services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence.

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

Les types de licences suivants sont prévus :

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

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

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

  Une fois que la licence commerciale arrive à échéance, l'application continue à fonctionner mais ses fonctionnalités sont réduites. Vous pouvez continuer à protéger les machines virtuelles et à les analyser, mais uniquement à l'aide des bases antivirus installées avant l'expiration de la licence. Pour pouvoir profiter de toutes les fonctionnalités de Kaspersky Security, il est nécessaire de renouveler la licence commerciale. Il est conseillé de renouveler la licence commerciale avant son expiration afin de garantir la protection maximale contre les menaces informatiques.

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

- Licence selon le nombre de machines virtuelles protégées par l'application. Ce type de licence repose sur des clés pour serveur ou pour poste de travail (en fonction du système d'exploitation des machines virtuelles protégées). En fonction des restrictions imposées par la licence, l'application intervient dans la protection d'un nombre défini de machines virtuelles avec un système d'exploitation Windows invité.

- Licence selon le nombre de cœurs utilisés dans les processeurs physiques sur tous les hyperviseurs VMware ESXi hébergeant des machines virtuelles de protection. Ces licences reposent sur l'utilisation de clés avec des restrictions en fonction du nombre de cœurs (cf. section "A propos du fichier clé" à la page 29). En fonction des restrictions imposées par la licence, l'application intervient dans la protection de toutes les machines virtuelles avec des systèmes d'exploitation invités Windows installés sur les hyperviseurs VMware ESXi dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

Vous ne pouvez utiliser qu'un seul des deux modes de licence décrits sur un même serveur VMware vCenter.

A PROPOS DU CERTIFICAT DE LICENCE

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

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

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

- numéro de licence ;

- informations sur l'utilisateur titulaire de la licence ;

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

A PROPOS DE LA CLE

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

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

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

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

Kaspersky Security accepte les types de clés suivants :

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

La clé peut être active ou complémentaire.

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

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

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

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

A PROPOS DU CODE D'ACTIVATION

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

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

Si le code d'activation a été perdu après l'activation de l'application, vous pouvez le restaurer. Le code d'activation peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple. Pour restaurer le code d'activation, il est nécessaire de s'adresser au Support Technique de Kaspersky Lab (https://companyaccount.kaspersky.com).

A PROPOS DU FICHIER CLE

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

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

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

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

Pour restaurer le fichier clé, il est nécessaire de s'adresser au Support Technique.

A PROPOS DE L'ABONNEMENT

L'*abonnement à Kaspersky Security* constitue une commande pour l'utilisation de l'application selon des paramètres sélectionnés (date d'expiration, nombre de périphériques protégés). Il est possible de commander un abonnement à Kaspersky Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur Internet). Vous pouvez suspendre et reprendre l'abonnement, ainsi que le renouveler automatiquement ou l'arrêter.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour continuer à utiliser Kaspersky Security après la date d'expiration d'un abonnement limité, vous devez le renouveler (cf. section "Renouvellement de l'abonnement" à la page 36). L'abonnement illimité se renouvelle automatiquement selon les conditions en vigueur au moment du paiement au prestataire de services.

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

Le choix des possibilités de gestion de l'abonnement diffère selon les prestataires de services. De même, la période de grâce au cours de laquelle vous pouvez prolonger votre abonnement n'est pas toujours proposée.

A l'expiration de l'abonnement ou de la période de grâce (le cas échéant), Kaspersky Security continue à fonctionner mais ne met plus ses bases anti-virus à jour. De même, l'utilisation des services de Kaspersky Security Network n'est plus disponible.

Selon le fournisseur de services, une fois que l'abonnement et la période de grâce ont expiré, l'application peut être restreinte de la manière suivante : Kaspersky Security ne met plus à jour les bases anti-virus, n'utilise plus les services du Kaspersky Security Network et n'assure plus la protection et l'analyse des machines virtuelles. Pour en savoir plus sur les restrictions des fonctionnalités de l'application lors de l'expiration de l'abonnement, contactez le fournisseur de services auprès duquel vous avez acheté Kaspersky Security.

Pour utiliser Kaspersky Security sur abonnement, vous devez modifier le code d'activation fourni par le prestataire de services. Suite à l'enregistrement du code d'activation, une clé d'abonnement est ajoutée à l'application. Il s'agit d'une clé active correspondant à la licence d'utilisation de l'application par abonnement.

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

Lorsque vous utilisez l'application sur abonnement, vous pouvez l'activer par le biais d'un code d'activation fourni par le prestataire de service. Il est impossible d'appliquer un autre code d'activation (non fourni par un prestataire de service). Vous pouvez appliquer un autre code d'activation si l'abonnement a expiré ou que vous l'avez résilié. Pour résilier l'abonnement, vous devez contacter le prestataire de services auprès de qui vous avez acheté Kaspersky Security.

Il n'est pas conseillé d'utiliser les codes d'activation achetés par abonnement pour l'activation des versions précédentes de Kaspersky Security.

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.

Pour activer l'application, il est nécessaire d'ajouter la clé à toutes les machines virtuelles de protection.

Vous pouvez activer l'application par l'un des moyens suivants :

- fichier clé ;
- code d'activation.

Le recours à *la tâche d'ajout de clé* est incontournable pour ajouter une clé, quel que soit le mode que vous avez choisi pour activer l'application. Cette tâche ajoute la clé sur toutes les machines virtuelles de protection dans le cadre d'un cluster KSC, c'est à dire sur toutes les machines virtuelles installées sur les hyperviseurs VMware ESXi administrés par un serveur VMware vCenter.

Pour activer l'application avec un code d'activation, il convient de se connecter aux serveurs d'activation Kaspersky Lab. Pour se connecter aux serveurs d'activation Kaspersky Lab, il est nécessaire de remplir les conditions suivantes :

- Lors de la création de la tâche d'ajout de la clé, le serveur proxy assure l'interaction entre le plug-in d'administration Kaspersky Security et les serveurs d'activation Kaspersky Lab. Ses paramètres sont définis dans le système d'exploitation de l'ordinateur où est installée la Console d'administration du Kaspersky Security Center. Si le serveur proxy demande une authentification, vous devrez indiquer les paramètres d'authentification sur le serveur proxy lors de la création de la tâche d'ajout de clé.
- Lors de l'exécution de la tâche d'ajout de clé, l'interaction entre les serveurs d'activation et les machines virtuelles de protection gérées par le Kaspersky Security Center est garantie par le service Activation Proxy. La configuration du service Activation Proxy s'opère dans les propriétés du Serveur d'administration le Kaspersky Security Center. Il est impossible d'activer l'application avec un code d'activation si le service Activation Proxy est déconnecté. Vous pouvez consulter les informations détaillées sur le service Activation Proxy dans la documentation du Kaspersky Security Center.

Si vous utilisez un plan de licence en fonction du nombre de machines virtuelles protégées, le type de clé 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 machine virtuelle de protection une clé pour serveur ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour ordinateur de bureau, il faut ajouter à la machine virtuelle de protection une clé pour ordinateur de bureau ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour serveur et d'un système pour ordinateur de bureau, il faut ajouter à la machine virtuelle de protection une clé pour serveur et une clé pour ordinateur de bureau.

Si vous utilisez le mode de licence en fonction du nombre de cœurs de processeurs de l'hyperviseur VMware ESXi, vous aurez besoin d'une clé avec des restrictions en fonction du nombre de cœurs quel que soit le système d'exploitation des machines virtuelles.

Si vous ajoutez une clé avec des restrictions selon le nombre de cœurs et qu'une clé serveur et/ou poste de travail avait été ajoutée à la machine virtuelle de protection, les clés active et complémentaire (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 en fonction du nombre de cours avait été ajoutée à la machine virtuelle de protection, la clé active et complémentaire (le cas échéant) en fonction du 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 machine virtuelle de protection, la clé d'abonnement sera 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 machine virtuelle de protection, toutes les clés actives et, le cas échéant, les clés complémentaires, seront supprimées. La clé d'abonnement les remplacera.

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

Pour activer l'application, procédez comme suit :

1. Créez une tâche d'ajout de clé pour chaque cluster KSC reprenant les machines virtuelles de protection auxquelles vous souhaitez ajouter une clé (cf. section "Création d'une tâche d'ajout de clé" à la page 32).
2. Lancez la tâche d'ajout de clé (cf. section "Lancement de la tâche d'ajout de clé" à la page 35).

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

DANS CETTE SECTION

Création d'une tâche d'ajout de clé.....32

Lancement de la tâche d'ajout de clé.....35

CREATION D'UNE TACHE D'AJOUT DE CLE

Pour créer une tâche d'ajout de clé, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez créer une tâche d'ajout de clé.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Lancez l'Assistant de création d'une tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les instructions de l'Assistant de création d'une tâche.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 32

Etape 2. Sélection du type de tâche 32

Etape 3. Choix du mode d'activation 32

Etape 4. Ajout d'une clé 33

Etape 5. Définition des paramètres de programmation de la tâche 34

Etape 6. Fin de la création de la tâche 34

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche d'ajout de clé dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

A cette étape, sélectionnez le type de tâche **Ajout d'une clé** pour l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. CHOIX DU MODE D'ACTIVATION

A cette étape, choisissez un mode d'activation de l'application :

- **Désigner le fichier clé**. Sélectionnez cette option si vous souhaitez activer l'application via un fichier clé.
- **Saisir le code d'activation**. Sélectionnez cette option si vous souhaitez activer l'application via un code d'activation.

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

ETAPE 4. AJOUT D'UNE CLE

A cette étape, veuillez effectuer les actions suivantes (selon le mode d'activation que vous avez choisi à l'étape précédente) :

- Indiquez le chemin vers le fichier clé si vous souhaitez activer l'application via un fichier clé. Pour ce faire, cliquez sur le bouton **Parcourir** et dans la fenêtre **Sélection du fichier clé** qui s'ouvre, sélectionnez le fichier portant l'extension key.

- Entrez le code d'activation dans le champ **Code d'activation (20 caractères)**, si vous souhaitez activer l'application via un code d'activation.

  Si vous avez entré un code d'activation, Kaspersky Security transmet les données au serveur Kaspersky Lab pour vérification. Un serveur proxy est utilisé pour assurer l'interaction entre le plug-in d'administration Kaspersky Security et les serveurs d'activation Kaspersky Lab. Ses paramètres sont définis dans le système d'exploitation de l'ordinateur où est installée la Console d'administration du Kaspersky Security Center.

  Si le serveur proxy nécessite une authentification, la fenêtre **Authentification sur le serveur proxy** s'ouvre. Indiquez les paramètres d'authentification sur le serveur proxy :

  - **Nom d'utilisateur**. Nom du compte utilisateur sous lequel la connexion au serveur proxy s'opère.

  - **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion au serveur proxy.

    Si vous souhaitez enregistrer les paramètres d'authentification sur le serveur proxy, cochez la case **Enregistrer les paramètres de connexion**. Lors de la prochaine connexion au serveur proxy, l'authentification s'effectuera automatiquement à l'aide des paramètres indiqués.

Si vous souhaitez utiliser la clé ajoutée 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 une clé par abonnement en tant que clé complémentaire.

Après que vous avez sélectionné le fichier clé ou entré le code d'activation, 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.

- **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 de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;

  - pour une clé avec des restrictions selon le nombre de cœurs : la restriction correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.

- La **Durée de validité de la licence** est la durée d'utilisation de l'application indiquée dans le Certificat de licence (par exemple, 365 jours). Ce champ ne s'affiche pas si vous utilisez l'application par abonnement.

- **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle peut être utilisée uniquement jusqu'à l'échéance de ce délai de validité. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *Non définie*.

- La **Période de grâce** définit le nombre de jours suivant la fin 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 grâce.

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

ETAPE 5. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de la tâche d'ajout de clé :

- **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.

- **Lancement des tâches ignorées**. Cochez la case si vous voulez que l'application lance la tâche ignorée tout de suite après l'apparition de la machine virtuelle de protection dans le réseau.

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

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :

  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : 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**. La case est cochée par défaut.

- **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 6. FIN DE LA CREATION DE LA TACHE

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

Quittez l'Assistant de création d'une tâche. La tâche d'ajout de clé créée apparaît dans la liste des tâches sous l'onglet **Tâches**.

Si, dans la fenêtre **Programmation de l'exécution de la tâche**, vous avez défini une planification pour l'exécution de la tâche d'ajout de clé, cette tâche sera exécutée conformément à la programmation. Vous pouvez également lancer à n'importe quel moment la tâche d'ajout de clé manuellement (cf. section "Lancement de la tâche d'ajout de clé " à la page 35).

LANCEMENT DE LA TACHE D'AJOUT DE CLE

Pour lancer la tâche d'ajout de clé, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez lancer une tâche d'ajout de clé.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des tâches, sélectionnez la tâche d'ajout de clé que vous souhaitez lancer.
5. Pour lancer la tâche d'ajout d'une clé, cliquez sur le bouton **Lancer** dans le groupe **Exécution d'une tâche**.

Si vous ajoutez la clé active, la tâche d'ajout de la clé active l'application sur les machines virtuelles de protection du cluster KSC auxquelles il manque une clé active, et remplacera l'ancienne clé par la nouvelle sur les machines virtuelles de protection où l'application est déjà activée :

- Si vous ajoutez une clé avec des restrictions selon le nombre de cœurs et qu'une clé serveur et/ou poste de travail avait été ajoutée à la machine virtuelle de protection, les clés active et complémentaire (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 en fonction du nombre de cours avait été ajoutée à la machine virtuelle de protection, la clé active et complémentaire (le cas échéant) en fonction du 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 machine virtuelle de protection, 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 machine virtuelle de protection, l'exécution des tâches des clés actives et, le cas échéant, des clés complémentaires, sera annulée. La clé d'abonnement les remplacera.

Si vous ajoutez une clé complémentaire, la tâche ajoutera la clé complémentaire sur les machines virtuelles de protection qui font partie du cluster KSC sur lesquelles une clé active a déjà été installée.

La tâche de d'ajout d'une clé complémentaire sur la machine virtuelle de protection se solde par une erreur et la clé complémentaire n'est pas ajoutée si :

- il manque une clé active ;
- une clé par abonnement a été ajoutée en tant que clé active ;
- une clé d'évaluation est ajoutée en tant que clé complémentaire ;
- le type de la clé complémentaire ajoutée ne correspond pas au type de la clé active ajoutée antérieurement.

Il est impossible d'ajouter une clé de licence d'évaluation ou une clé d'abonnement en tant que clé complémentaire. Une clé de licence d'évaluation ne peut pas remplacer une clé commerciale active.

Vous pouvez consulter les informations sur le déroulement et les résultats de l'exécution des tâches dans la Console d'administration de Kaspersky Security Center d'une des manières suivantes :

- Dans la fenêtre **Résultats de l'exécution de la tâche**. Pour ouvrir la fenêtre, cliquez sur le bouton **Consulter les résultats** situé à droite de la liste des tâches, sous l'onglet **Tâches**.
- Dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les machines virtuelles de protection. La liste des événements apparaît dans le dossier **Rapports et notifications/Evénements** de l'arborescence de la Console d'administration du Kaspersky Security Center.

RENOUVELLEMENT DE LA LICENCE

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

Il est impossible d'ajouter une clé complémentaire si vous utilisez l'application par abonnement.

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

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

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

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

Pour renouveler la licence, procédez comme suit :

1. A l'aide de l'Assistant, créez une tâche d'ajout de clé pour chaque cluster KSC reprenant les machines virtuelles auxquelles vous souhaitez ajouter une clé complémentaire (cf. section "Création d'une tâche d'ajout de clé" à la page 32). A l'étape "Ajout de clé" de l'Assistant de création d'une tâche, cochez la case **Utiliser la clé en tant que clé complémentaire**.

2. Lancez la tâche d'ajout de clé (cf. section "Lancement de la tâche d'ajout de clé" à la page 35).

   La clé complémentaire s'ajoute suite à l'exécution des tâches sur les machines virtuelles de protection. Cette clé est utilisée automatiquement en tant que clé active à l'expiration de la licence de Kaspersky Security.

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

   Si le type de clé complémentaire ne correspond pas au type de clé active ajoutée antérieurement, la tâche d'ajout de la clé se solde sur une erreur et la clé complémentaire n'est pas ajoutée.

RENOUVELLEMENT DE L'ABONNEMENT

Si vous utilisez l'application par abonnement, Kaspersky Security se connecte automatiquement au serveur d'activation à des intervalles définis jusqu'à la fin de l'abonnement.

Si vous utilisez l'application avec un abonnement illimité, Kaspersky Security vérifie automatiquement et en arrière-plan la possibilité de renouveler la clé sur le serveur d'activation. Si cette opération est possible, il remplace la clé antérieure par la nouvelle. C'est ainsi que l'abonnement illimité à Kaspersky Security se renouvelle sans votre participation.

Si vous utilisez l'application avec un abonnement limité et que la date d'expiration de l'abonnement ou de la période de grâce permettant de renouveler l'abonnement est atteinte, Kaspersky Security en notifie le Serveur d'administration du Kaspersky Security Center et interrompt ses tentatives de renouvellement automatique. Kaspersky Security ne met plus à jour les bases anti-virus et n'utilise plus les services du Kaspersky Security Network.

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

Suite au renouvellement de l'abonnement, vous devrez relancer la tâche d'ajout de clé que vous avez créée pour l'ajout de la clé d'abonnement.

CONSULTATION DES INFORMATIONS RELATIVES AUX CLES AJOUTEES

Les informations relatives aux clés ajoutées sont accessibles :

- dans le dossier **Administration des applications** de l'arborescence de la console, dans le sous-dossier **Licence pour une application Kaspersky Lab** ;
- dans les propriétés de l'application installée sur la machine virtuelle de protection ;
- dans les propriétés de la tâche d'ajout de clé ;
- dans le rapport sur l'utilisation des clés.

DANS CETTE SECTION

Consultation des informations relatives à la clé dans le dossier Licence pour une application Kaspersky Lab 37

Consultation des informations relatives à la clé dans les propriétés de l'application.....39

Consultation des informations relatives à la clé dans les propriétés de la tâche d'ajout de clé.....41

Consultation du rapport sur l'utilisation des clés 42

CONSULTATION DES INFORMATIONS RELATIVES A LA CLE DANS LE DOSSIER LICENCE POUR UNE APPLICATION KASPERSKY LAB

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

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

   La liste des clés ajoutées aux machines virtuelles de protection apparaît dans la zone de travail.

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

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

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

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

   - La clé est une séquence unique de chiffres et de lettres.
   - **Type de licence** : évaluation, commerciale ou par abonnement.
   - **Application** : nom de l'application activée par l'ajout de cette clé et informations sur la licence.
   - **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé (par exemple, 365 jours).
   - **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle peut être utilisée uniquement jusqu'à l'échéance de sa durée de validité.
   - **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de la clé ajoutée.
   - **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 de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;
     - pour une clé avec des restrictions selon le nombre de cœurs : la restriction correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.
   - **Ordinateurs sur lesquels la clé est active** : nombre de machines virtuelles de protection sur lesquelles la clé a été ajoutée en tant que clé active.
   - **Ordinateurs sur lesquels la clé est complémentaire** : nombre de machines virtuelles de protection sur lesquelles la clé a été ajoutée en tant que clé complémentaire.
   - **Informations de service** : ce champ reprend les informations de service liées à la clé et à la licence.

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

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

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

   Kaspersky Security Center permet d'afficher, dans le dossier **Licence pour une application Kaspersky Lab**, les informations relatives à une seule clé ajoutée à chaque machine virtuelle de protection. Par conséquent, si votre machine virtuelle de protection possède une clé de type serveur et une clé de type poste de travail, les informations relatives à ces clés sont affichées de la manière suivante :

   - **Séquence unique de chiffres et de lettres** : combinaison de la clé pour serveur ou poste de travail. Vous pouvez utiliser la combinaison de la clé pour serveur ou poste de travail en vue de rechercher des informations concernant la machine virtuelle de protection sur laquelle ces types de clé ont été ajoutés (pour davantage de détails, reportez-vous à la Documentation du Kaspersky Security Center).

- **Durée de validité** : durée la plus longue entre les deux durées d'utilisation de l'application : durée d'utilisation de l'application avec la clé de type serveur ou durée d'utilisation de l'application avec la clé de type poste de travail.
- **Date de fin de validité** : date la plus éloignée entre les deux dates suivantes d'expiration de la validité de la clé : date d'expiration de la validité de la clé de type serveur ou date d'expiration de la validité de la clé de type poste de travail.
- **Date d'expiration de la validité de la licence** : date la plus éloignée entre les deux dates suivantes : la date de fin d'utilisation de l'application avec la clé de type serveur ou la date de fin d'utilisation de l'application avec la clé de type poste de travail.
- **Restriction** : somme des valeurs suivantes : nombre maximal de machines virtuelles avec système d'exploitation pour postes de travail et nombre maximal de machines virtuelles avec système d'exploitation pour serveurs que vous pouvez protéger à l'aide de l'application.
- **Période de grâce** : période de grâce la plus longue des deux entre celle correspondant à la clé pour serveur et celle correspondant à la clé pour poste de travail.
- **Etat de l'abonnement** : le champ indique l'état "actif" si l'abonnement correspondant à au moins l'une des clés (serveur ou poste de travail), se trouve "actif". Si les deux abonnements sont inactifs, le champ indique le meilleur état (par exemple, si un abonnement est "suspendu" et le deuxième "résilié", le champ indique l'état "suspendu").

CONSULTATION DES INFORMATIONS RELATIVES A LA CLE DANS LES PROPRIETES DE L'APPLICATION

Pour consulter les informations relatives à la clé dans les propriétés de l'application, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection dont vous souhaitez consulter les propriétés de l'application.
3. Dans la zone de travail, sélectionnez l'onglet **Ordinateurs**.
4. Dans la liste des machines virtuelles de protection, sélectionnez la machine virtuelle de protection pour laquelle vous souhaitez consulter les propriétés de l'application installée sur celle-ci.
5. Dans le menu contextuel de la machine virtuelle de protection, choisissez l'option **Propriétés**.

   La fenêtre **Propriétés : <nom de la machine virtuelle de protection>** s'ouvre.
6. Dans la fenêtre des propriétés de la machine virtuelle de protection, choisissez la section **Applications**.

   La liste des applications installées sur cette machine virtuelle de protection apparaît dans la partie droite de la fenêtre.
7. Sélectionnez l'application Kaspersky Security for Virtualization 3.0 Agentless.
8. Dans le menu contextuel de l'application, sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application Kaspersky Security for Virtualization 3.0 Agentless** s'ouvre.
9. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Clés**.

   La partie droite de la fenêtre affiche les informations relatives à la clé utilisée pour activer l'application. Le champ **Clé active** reprend les informations relatives à la clé active, tandis que le groupe **Clé complémentaire** reprend les informations relatives à la clé complémentaire. Si aucune clé complémentaire n'a été ajoutée, le groupe **Clé complémentaire** affiche la ligne *<Non ajoutée>*.

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

- La clé est une séquence unique de chiffres et de lettres.
- **Type de licence** : évaluation, commerciale ou par abonnement.
- **Date d'activation** : date d'activation de l'application via l'ajout de cette clé.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de cette clé.
- **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé (par exemple, 365 jours).
- **Restriction** : dépend du type de clé :
    - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
    - pour une clé de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;
    - pour une clé avec des restrictions selon le nombre de cœurs : la restriction correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.

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

- La clé est une séquence unique de chiffres et de lettres.
- **Type de licence** : type de licence : commerciale.
- **Durée de validité** : nombre de jours d'utilisation de l'application activée à l'aide de cette clé (par exemple, 365 jours).
- **Restriction** : dépend du type de clé :
    - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
    - pour une clé de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;
    - pour une clé avec des restrictions selon le nombre de cœurs : correspond au nombre maximal de cœurs de processeur physique sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.

Kaspersky Security Center permet d'afficher les informations relatives à une seule clé dans la fenêtre des propriétés de l'application. Par conséquent, si votre machine virtuelle de protection est dotée d'une clé de type serveur et d'une clé de type poste de travail, les informations relatives à ces clés sont affichées de la manière suivante :

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

- **Durée de validité** : durée la plus longue entre les deux durées d'utilisation de l'application : durée d'utilisation de l'application avec la clé de type serveur ou durée d'utilisation de l'application avec la clé de type poste de travail.

- **Restriction** : somme des valeurs suivantes : nombre maximal de machines virtuelles avec système d'exploitation pour postes de travail et nombre maximal de machines virtuelles avec système d'exploitation pour serveurs que vous pouvez protéger à l'aide de l'application.

CONSULTATION DES INFORMATIONS RELATIVES A LA CLE DANS LES PROPRIETES DE LA TACHE D'AJOUT DE CLE

Pour consulter les informations relatives à la clé dans les propriétés de la tâche d'ajout de clé, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection dont vous souhaitez consulter les propriétés de la tâche d'ajout de clé.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des tâches, sélectionnez la tâche d'ajout de clé dont vous souhaitez consulter les propriétés.
5. Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : <Nom de la tâche>** s'ouvre.
6. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Ajout d'une clé**.

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

   - La **clé** est une séquence unique de chiffres et de lettres.
   - **Type de licence** : évaluation, commerciale ou par abonnement.
   - **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 de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;
     - pour une clé avec des restrictions selon le nombre de cœurs : la restriction correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.
   - La **Durée de validité de la licence** est la durée d'utilisation de l'application indiquée dans le Certificat de licence (par exemple, 365 jours). Ce champ ne s'affiche pas si vous utilisez l'application par abonnement.
   - **Date de fin de validité** : date d'expiration de la validité de la clé. L'application est activée via l'ajout de cette clé ; elle ne peut être utilisée que jusqu'à l'échéance de sa durée de validité. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *Non définie*.
   - La **Période de grâce** définit le nombre de jours suivant la fin 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 grâce.

CONSULTATION DU RAPPORT SUR L'UTILISATION DES CLES

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

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Rapports et notifications**, sélectionnez le modèle du rapport "rapport sur l'utilisation des clés".

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

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

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

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

- le tableau des informations générales comporte les données sur les clés ajoutées aux machines virtuelles de protection ;
- le tableau des informations détaillées comporte des informations détaillées sur les clés et sur les machines virtuelles de protection qui les accueillent.

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

Le tableau des informations générales comporte les données suivantes sur les clés ajoutées aux machines virtuelles de protection :

- La **clé** est une séquence unique de chiffres et de lettres.
- **Utilisé en tant que clé active** : en fonction du type de clé :
  - pour une clé pour serveur ou poste de travail : nombre de machines virtuelles protégées pour lesquelles la clé est utilisée en tant que clé active ;
  - pour une clé avec des restrictions selon le nombre de cœurs : correspond au nombre de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.
- **Utilisée en tant que clé complémentaire** : nombre de machines virtuelles de protection sur lesquelles la clé a été ajoutée en tant que clé complémentaire.
- **Restriction** : dépend du type de clé :
  - pour une clé de serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant simultanément et pour lesquelles la protection est activée ;
  - pour une clé de poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant simultanément et pour lesquelles la protection est activée ;
  - pour une clé avec des restrictions selon le nombre de cœurs : la restriction correspond au nombre maximal de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.

- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application activée à l'aide de la clé ajoutée.
- **Date de fin de validité** : date d'expiration de la validité de la clé.
- **Utilisé en tant que clé active pour postes de travail** : nombre de machines virtuelles protégées avec système d'exploitation pour poste de travail et pour lesquelles la clé est utilisée en tant que clé active.
- **Utilisé en tant que clé active pour serveurs** : nombre de machines virtuelles protégées avec système d'exploitation pour serveur et pour lesquelles la clé est utilisée en tant que clé active.
- **Restriction pour postes de travail** : nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail lancées simultanément que vous pouvez protéger à l'aide de l'application.
- **Restriction pour serveurs** : nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs lancées simultanément que vous pouvez protéger à l'aide de l'application.
- **Autres informations** : informations de service liées à la clé et à la licence.

  La ligne en dessous reprend les informations de synthèse suivantes :

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

Le tableau des informations détaillées comporte les informations détaillées suivantes sur les clés et sur les machines virtuelles de protection qui les accueillent :

- **Groupe** : cluster KSC auquel appartiennent les machines virtuelles de protection avec la clé ajoutée.
- **Poste client** : nom de la machine virtuelle de protection avec la clé ajoutée.
- **Application** : application activée via l'ajout de cette clé.
- **Numéro de version** : numéro de la version de l'application.
- **Clé active** : clé ajoutée en tant que clé active sur cette machine virtuelle de protection.
- **Clé complémentaire** : clé ajoutée en tant que clé complémentaire sur cette machine virtuelle de protection.
- **Date d'expiration de la validité de la licence** : date de fin de l'utilisation de l'application à l'aide de cette clé.
- **Date de fin de validité** : date d'expiration de la validité de la clé.
- **Adresse IP** : adresse IP de la machine virtuelle de protection à laquelle la clé a été ajoutée.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle de protection est visible dans le réseau local de l'entreprise.

- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la machine virtuelle de protection au Serveur d'administration du Kaspersky Security Center.
- **Nom de domaine** : nom de la machine virtuelle de protection.
- **Nom NetBIOS** : nom de la machine virtuelle de protection.
- **Domaine DNS** : domaine DNS de la machine virtuelle de protection (indiqué uniquement si le nombre de la machine virtuelle de protection contient le nom du domaine DNS).
- **Utilisé** : dépend du type de clé :
  - pour une clé pour serveur ou poste de travail : nombre de machines virtuelles protégées avec système d'exploitation pour serveur ou poste de travail ;
  - pour une clé avec des restrictions selon le nombre de cœurs : correspond au nombre de cœurs de processeur physique utilisés sur tous les hyperviseurs VMware ESXi hébergeant les machines virtuelles de protection.
- **Utilisé pour postes de travail** : nombre de machines virtuelles dotées d'un système d'exploitation pour postes de travail.
- **Utilisé pour serveurs** : nombre de machines virtuelles dotées d'un système d'exploitation pour serveurs.

Kaspersky Security Center permet d'afficher, dans le rapport d'utilisation des clés, les informations relatives à une seule clé de chaque machine virtuelle de protection. Par conséquent, si vous avez ajouté à la machine virtuelle de protection une clé de type serveur et une autre de type poste de travail, les informations relatives à celles-ci sont présentées dans le rapport de la manière suivante :

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

LANCEMENT ET ARRET DE L'APPLICATION

Kaspersky Security est lancé automatiquement au démarrage du système d'exploitation sur la machine virtuelle de protection. Kaspersky Security gère les processus de protection des machines virtuelles, les tâches d'analyse, *la tâche de diffusion des mises à jour* et la *tâche de remise à l'état antérieur à la mise à jour*.

Si vous avez configuré les paramètres de Kaspersky Security à l'aide d'une stratégie (cf. section "Création d'une stratégie" à la page 46) et que vous avez activé l'application, la fonction de protection des machines virtuelles s'active automatiquement lors du lancement de l'application.

L'application ne protège pas les machines virtuelles si la machine virtuelle de protection n'est pas dotée de bases anti-virus.

L'analyse des machines virtuelles est lancée conformément à la programmation.

Kaspersky Security s'arrête automatiquement à l'arrêt du système d'exploitation de la machine virtuelle de protection.

ADMINISTRATION DE LA PROTECTION

Cette section contient des informations sur la détection des menaces de sécurité à l'encontre de l'ordinateur et sur la configuration de la protection contre ces menaces. Vous apprendrez également comment vérifier l'état de la protection des machines virtuelles et désactiver la protection pendant l'utilisation de l'application.

DANS CETTE SECTION

Etat de la protection 46

Création d'une stratégie 46

Consultation de l'infrastructure protégée du cluster KSC 53

Désactivation de la protection sur la machine virtuelle 54

Consultation de la liste des machines virtuelles et des machines virtuelles de protection du cluster KSC 55

ETAT DE LA PROTECTION

La machine virtuelle de protection Kaspersky Security dans le 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. L'application Kaspersky Security se distingue par le fait que l'état de la machine virtuelle de protection change en cas de détection de menaces sur les machines virtuelles qu'elle protège. Quand une machine virtuelle de protection détecte des menaces sur les machines virtuelles, son état devient *Critique* ou *Avertissement*. Pour en savoir plus sur les états du poste client, consultez la documentation du Kaspersky Security Center.

Les informations relatives aux menaces détectées par la machine virtuelle de protection sont consignées dans le rapport (cf. section "Types de rapports" à la page 99).

CREATION D'UNE STRATEGIE

Suite à l'installation de Kaspersky Security, il est nécessaire de configurer les paramètres d'utilisation de l'application à l'aide d'une stratégie (cf. section "A propos de la stratégie de Kaspersky Security et des profils de protection" à la page 23).

C'est seulement après la configuration des paramètres d'utilisation de l'application avec une stratégie et l'activation de l'application que Kaspersky Security commence à protéger les machines virtuelles. Si aucune clé n'est ajoutée sur la machine virtuelle de protection ou si elle ne présente aucune base anti-virus, l'application ne protège pas les machines virtuelles.

En cas de remplacement ou de réinstallation du serveur VMware vCenter, les stratégies créées antérieurement ne fonctionneront plus. Vous devrez supprimer les stratégies et en créer de nouvelles.

La création de la stratégie permet de générer un profil de protection racine (cf. section "A propos du profil de protection racine" à la page. 24). Les paramètres de protection indiqués dans le profil de protection racine sont appliqués à toutes les machines virtuelles de l'infrastructure protégée du cluster KSC.

Suite à la création de la stratégie, vous pouvez composer des profils de protection complémentaires et les affecter à certaines machines virtuelles ou à certains objets de l'infrastructure virtuelle VMware. Vous pouvez également configurer les paramètres suivants de l'application dans les propriétés de la stratégie :

- les paramètres de détection des attaques réseau et d'analyse des adresses Internet (cf. section "Détection des intrusions" à la page 82) ;
- les paramètres de la sauvegarde (cf. section "Configuration des paramètres de la sauvegarde" à la page 88) ;
- les paramètres d'utilisation des services KSN (cf. section "Participation au Kaspersky Security Network" à la page 113).

Pour créer une stratégie, procédez comme suit:

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC qui comprend les machines virtuelles de protection pour lesquelles vous souhaitez créer une stratégie.

   Sous l'onglet **Ordinateurs** du dossier portant le nom du cluster KSC, vous pouvez consulter la liste des machines virtuelles de protection qui appartiennent à ce cluster KSC.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Lancez l'Assistant de création d'une stratégie via le lien **Création d'une stratégie**.
5. Suivez les instructions de l'Assistant de création de stratégie.

DANS CETTE SECTION

Etape 1. Définition du nom de la stratégie de groupe pour l'application.....47

Etape 2. Sélection de l'application pour la création de la stratégie de groupe.....47

Etape 3. Configuration des paramètres du profil de protection racine.....48

Etape 4. Accord de participation à Kaspersky Security Network 52

Etape 5. Création de la stratégie de groupe pour l'application 52

ETAPE 1. DEFINITION DU NOM DE LA STRATEGIE DE GROUPE POUR L'APPLICATION

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

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

ETAPE 2. SELECTION DE L'APPLICATION POUR LA CREATION DE LA STRATEGIE DE GROUPE

Dans la liste **Nom de l'application**, sélectionnez le nom de l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. CONFIGURATION DES PARAMETRES DU PROFIL DE PROTECTION RACINE

Cette étape permet de modifier les paramètres par défaut du profil de protection racine. Une fois la stratégie créée, le profil de protection racine est attribué à toutes les machines virtuelles du cluster KSC.

Chaque groupe de paramètres du profil de protection racine est verrouillé  . Le "cadenas" indique s'il est interdit de modifier le groupe de paramètres dans les stratégies du niveau intégré de la hiérarchie (pour les groupes d'administration intégrés et les serveurs d'administration secondaires) et dans les paramètres des tâches. Si le "cadenas" d'un groupe de paramètres dans la stratégie est fermé, cela signifie qu'il est impossible de redéfinir ces paramètres (cf. Documentation du Kaspersky Security Center).

Pour modifier les paramètres du profil de protection racine, procédez comme suit :

1. Dans le groupe **Niveau de sécurité**, effectuez l'une des actions suivantes :

   - Si vous souhaitez utiliser l'un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.
   - Si vous souhaitez configurer vous-même le niveau de protection, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Paramètres du niveau de sécurité** :

   a. Dans le groupe **Analyse des archives et des fichiers composés**, définissez les paramètres suivants :

   - **Analyser les archives**.

     Activation ou désactivation de l'analyse des archives.

     La case est décochée par défaut.

   - **Supprimer les archives en cas d'échec de la réparation**.

     Suppression des archives dont la réparation est impossible.

     Si la case est cochée, Kaspersky Security supprime les archives dont la réparation a échoué.

     Si la case est décochée, l'application ne supprime pas les archives qui n'ont pu être réparées. Kaspersky Security signale au Serveur d'administration du Kaspersky Security Center que le fichier infecté n'a pas été supprimé.

     La case est accessible si la case **Analyser les archives** est cochée.

     La case est décochée par défaut.

   - **Analyser les archives autoextractibles**.

     Activation/désactivation de l'analyse des archives autoextractibles.

     Par défaut, la case pour les profils de protection est décochée et la case pour les tâches d'analyse est cochée.

   - **Analyser les objets OLE intégrés**.

     Activation ou désactivation de l'analyse des objets intégrés à un fichier.

     La case est cochée par défaut.

   - **Ne pas décompacter les fichiers composés de grande taille**.

     Quand la case est cochée, Kaspersky Security n'analyse pas les fichiers composés dont la taille dépasse la valeur du champ **Taille maximale du fichier composé à analyser**.

     Si la case est décochée, Kaspersky Security analyse les fichiers composés de toutes les tailles.

     Kaspersky Security analyse les fichiers de grande taille extraits des archives, quel que soit l'état de la case **Ne pas décompacter les fichiers composés de grande taille**.

     La case est cochée par défaut.

- **Taille maximale du fichier composé à analyser X Mo**.

  Taille maximale des fichiers composés pouvant être analysés (en mégaoctets). Kaspersky Security ne décompacte pas et n'analyse pas les objets dont la taille est supérieure à la valeur indiquée.

  Le paramètre ne peut être modifié si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

  La valeur par défaut est de 8 Mo.

b. Dans le groupe **Productivité**, définissez les paramètres suivants :

- **Limiter la durée d'analyse des fichiers**.

  Si la case est cochée, Kaspersky Security interrompt l'analyse si la durée de celle-ci atteint la valeur définie dans le champ **Ne pas analyser les fichiers pendant plus de X seconde(s)** et ignore ce fichier.

  Si la case est décochée, Kaspersky Security ne limite pas la durée de l'analyse des fichiers.

  Par défaut, la case pour les profils de protection est cochée et la case pour les tâches d'analyse est décochée.

- **Ne pas analyser les fichiers pendant plus de X seconde(s)**.

  Durée maximale de l'analyse du fichier (en secondes). Kaspersky Security interrompt l'analyse du fichier quand sa durée atteint la valeur définie pour ce paramètre.

  Le paramètre ne peut être modifié si la case **Limiter la durée d'analyse des fichiers** est cochée.

  La valeur par défaut est de 60 secondes.

c. Dans le groupe **Objets à détecter**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à détecter** qui apparaît :

- **Utilitaires malveillants**.

  Activation/désactivation de la protection contre les utilitaires malveillants.

  Les *utilitaires malveillants* n'exécutent pas d'actions malveillantes dès le lancement et peuvent être conservés et exécutés sur l'ordinateur de l'utilisateur sans présenter de risque. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants ou exécuter d'autres actions malveillantes.

  Si la case est cochée, la protection contre les utilitaires malveillants est activée.

  Si la case est décochée, la protection contre les utilitaires malveillants est désactivée.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation/désactivation de la protection contre les programmes publicitaires.

  Les *programmes publicitaires* permettent de montrer des publicités aux utilisateurs. Par exemple, ils affichent des bandeaux publicitaires dans l'interface d'autres programmes ou réorientent les demandes de recherche vers des pages publicitaires. Certains d'entre eux recueillent également des informations marketing sur l'utilisateur qu'ils renvoient à l'auteur : catégories de sites Internet visités, mots-clés utilisés dans les recherches, etc. A la différence des chevaux de Troie espions, ils transmettent ces informations avec l'autorisation de l'utilisateur.

  Si la case est cochée, la protection contre les logiciels publicitaires est activée.

  Si la case est décochée, la protection contre les logiciels publicitaires est désactivée.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation/désactivation de la protection contre les programmes numéroteurs.

  Si la case est cochée, la protection contre les programmes numéroteurs est activée.

  Si la case est décochée, la protection contre les programmes numéroteurs est désactivée.

  La case est cochée par défaut.

- **Autres**.

  Activation/désactivation de la protection d'autres applications légitimes qui peuvent être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

  La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi elles figurent les clients IRC, les programmes pour le chargement des fichiers, les applications d'administration à distance, les dispositifs de suivi de l'activité de l'utilisateur, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet. Toutefois, si des individus malintentionnés obtiennent l'accès à ces applications ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leurs fonctions pour nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  Si la case est décochée, la protection contre ces programmes est désactivée.

  La case est décochée par défaut.

- **Fichiers compactés plusieurs fois**.

  Exclusion ou inclusion de l'analyse des fichiers compactés à trois reprises au moins par un ou plusieurs compacteurs.

  Si le fichier a été compacté plus de trois fois par un ou plusieurs compacteurs, il s'agit vraisemblablement d'un fichier qui contient une application malveillante ou un programme permettant à des individus malintentionnés de nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les fichiers compactés à plusieurs reprises est activée et l'analyse de ce type de fichier est autorisée.

  Si la case est décochée, la protection contre les fichiers compressés à plusieurs reprises est désactivée.

  La case est cochée par défaut.

Kaspersky Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans les fichiers des machines virtuelles. C'est pourquoi les paramètres **Virus et vers** et **Chevaux de Troie** du groupe **Applications malveillantes** ne peuvent pas être modifiés.

d. Cliquez sur le bouton **OK** dans la fenêtre **Objets à détecter**.

e. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du niveau de sécurité**.

Si vous avez modifié les paramètres du niveau de protection, l'application créera un niveau utilisateur de protection. Le nom du niveau de protection dans le groupe **Niveau de sécurité** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action exécutée en cas de détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection de fichiers infectés :

- **Sélectionner l'action automatiquement**.

  Kaspersky Security exécute l'action définie par défaut par les experts de Kaspersky Lab. Il s'agit de **Réparer. Supprimer si la réparation est impossible**.

  Cette option est sélectionnée par défaut.

- **Réparer. Supprimer si la réparation est impossible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, l'application supprime ces fichiers. Kaspersky Security supprime les archives infectées qui n'ont pas pu être réparées uniquement si la case **Supprimer les archives en cas d'échec de la réparation** est cochée dans les paramètres du niveau de protection.

- **Réparer. Bloquer si la réparation n'est pas possible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, Kaspersky Security bloque ces fichiers.

- **Supprimer. Bloquer si la suppression n'est pas possible**.

  Kaspersky Security supprime automatiquement les fichiers infectés, sans tenter de les réparer. Si la suppression est impossible, Kaspersky Security bloque ces fichiers.

- **Bloquer**.

  Kaspersky Security bloque automatiquement les fichiers infectés, sans tenter de les réparer.

3. Si vous souhaitez exclure les disques réseau de la protection, décochez la case **Analyser les disques réseau** dans le groupe **Zone de protection**. Si la case est cochée, Kaspersky Security analyse tous les fichiers des disques réseau n'étant pas exclus de la protection. La case est cochée par défaut.

Kaspersky Security analyse toujours les fichiers des disques durs et amovibles. C'est la raison pour laquelle le paramètre **Analyser les disques amovibles et les disques durs** du groupe **Zone de protection** n'est pas modifiable.

4. Si vous souhaitez exclure n'importe quel fichier des machines virtuelles de protection, cliquez sur le bouton **Configuration** dans le groupe **Exclusions de la protection**.

   Dans la fenêtre **Exclusions de la protection** qui s'ouvre, définissez les paramètres suivants :

   a. Dans la fenêtre **Extensions des fichiers**, sélectionnez l'une des options suivantes :

      - **Analyser tout, sauf les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à ne pas analyser dans le cadre de la protection de la machine virtuelle.

      - **Analyser uniquement les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à analyser dans le cadre de la protection de la machine virtuelle.

      Vous pouvez séparer les extensions de fichier par un espace ou un saut de ligne. Lorsque vous indiquez les extensions de fichiers, vous pouvez utiliser n'importe quel caractère sauf `* | \ : " < > ? /`. Si le caractère "espace" est utilisé dans l'extension, il est nécessaire d'indiquer cette extension entre guillemets, par exemple : `"doc x"`.

      Si vous aviez choisi l'option **Analyser uniquement les fichiers avec les extensions suivantes** dans la liste déroulante, sans renseigner les extensions de fichier à analyser, Kaspersky Security analyse tous les fichiers.

   b. Composez la liste des objets à exclure de la protection dans le tableau **Dossiers et fichiers**, à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

      Par défaut, la liste des exclusions contient les objets recommandés par Microsoft (liste des exclusions recommandées par Microsoft accessible sur le site de Microsoft). Kaspersky Security exclut ces objets de la protection sur toutes les machines virtuelles auxquelles le profil de protection racine a été attribué. Vous pouvez consulter et modifier la liste de ces objets dans le tableau **Dossiers et fichiers**.

      Vous pouvez exclure de la protection les objets des types suivants :

      - Dossiers. Les fichiers des dossiers situés aux emplacements indiqués sont exclus de la protection. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure les sous-répertoires de la protection.

      - Les fichiers selon un masque. Sont exclus de la protection : les fichiers possédant le nom indiqué, les fichiers situés à l'emplacement indiqué ou les fichiers correspondant au masque indiqué.

        Les caractères `*` et `?` peuvent être utilisés dans la création d'un masque de fichier.

      Vous pouvez conserver la liste d'objets à exclure dans un fichier à l'aide du bouton **Exportation** et télécharger la liste des objets à exclure précédemment enregistrée à l'aide du bouton **Importation**.

L'utilisation de variables d'environnement n'est pas prise en charge dans la liste des exclusions. L'objet du système de fichiers défini via des variables d'environnement ne sera pas exclu de la protection.

Kaspersky Security ignore la casse dans les chemins d'accès aux dossiers des disques durs et amovibles pour lesquels aucun accès réseau n'est configuré.

La casse est prise en compte dans les chemins d'accès aux dossiers réseau exclus de la protection. Si vous souhaitez définir un chemin d'accès à des dossiers réseau sans que la casse ne soit prise en compte, décochez la case **Respecter la casse dans les chemins d'accès aux dossiers réseau**.

Décocher la case **Respecter la casse dans les chemins d'accès aux dossiers réseau** peut entraîner une diminution des performances de l'application Kaspersky Security.

5. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de la protection**.

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

ETAPE 4. ACCORD DE PARTICIPATION A KASPERSKY SECURITY NETWORK

Cette étape vous invite à participer à Kaspersky Security Network (cf. section "Participation à Kaspersky Security Network" à la page 113).

Kaspersky Security Network (KSN) est une infrastructure de services et de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network permet d'accélérer le temps de réaction de Kaspersky Security aux nouvelles menaces, d'améliorer l'efficacité de plusieurs modules de protection et de diminuer les risques de faux positifs.

Lisez attentivement les Conditions de participation à Kaspersky Security Network, puis choisissez l'une des options suivantes :

- Si vous acceptez toutes les dispositions spécifiées, cochez la case **J'accepte les conditions de participation au programme Kaspersky Security Network**.
- Si vous n'acceptez pas les conditions de participation, cochez la case **Je n'accepte pas les conditions de participation au programme Kaspersky Security Network**.

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

ETAPE 5. CREATION DE LA STRATEGIE DE GROUPE POUR L'APPLICATION

Choisissez l'option **Stratégie active**. Quittez l'Assistant de création de stratégie.

L'Assistant de création de stratégie s'arrête. La stratégie créée apparaît dans la liste des stratégies sous l'onglet **Stratégies**.

Après que le Kaspersky Security Center a transmis les informations à Kaspersky Security, la stratégie se propage aux machines virtuelles de protection. Kaspersky Security commence à protéger les machines virtuelles sur les hyperviseurs VMware ESXi conformément au profil de protection racine qui leur a été attribué.

Si aucune clé n'est ajoutée sur la machine virtuelle de protection ou si elle ne présente aucune base anti-virus, l'application ne protège pas les machines virtuelles.

CONSULTATION DE L'INFRASTRUCTURE PROTEGEE DU CLUSTER KSC

Pour consulter l'infrastructure protégée du cluster KSC, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez la section **Infrastructure protégée**.
6. Dans la partie droite de la fenêtre, cliquez sur le bouton **Connecter**.

   La fenêtre **Paramètres de connexion à VMware vCenter Server** s'ouvre.
7. Saisissez les paramètres de connexion du Kaspersky Security Center au serveur VMware vCenter :
   - **Adresse de VMware vCenter Server**.

     Adresse IP au format IPv4 ou nom de domaine complet du serveur VMware vCenter auquel la connexion est établie.
   - **Nom d'utilisateur**.

     Nom du compte utilisateur sous lequel la connexion au serveur VMware vCenter est établie. Il est recommandé d'indiquer le nom d'un compte utilisateur créé pour utiliser l'application et modifier la configuration des machines virtuelles de protection. Il faut que le rôle système préinstallé ReadOnly soit attribué à ce compte utilisateur.
   - **Mot de passe**.

     Mot de passe du compte utilisateur sous lequel la connexion au serveur VMware vCenter est établie.
8. Si nécessaire, définissez la valeur du paramètre **Enregistrer les paramètres de connexion**.

   Activation ou désactivation de l'enregistrement des paramètres de connexion au serveur VMware vCenter.

   Si la case est cochée, Kaspersky Security enregistre les derniers paramètres saisis pour la connexion au serveur VMware vCenter indiqué dans le champ **Adresse de VMware vCenter Server** : adresse du serveur VMware vCenter, nom et mot de passe du compte utilisateur. Lors des connexions ultérieures au serveur VMware vCenter, les paramètres enregistrés s'afficheront dans la fenêtre de saisie des paramètres de connexion. Le mot de passe du compte utilisateur est enregistré sous forme chiffrée sur l'ordinateur sur lequel est installée la Console d'administration Kaspersky Security Center.

   Si la case est décochée, les paramètres de connexion au serveur VMware vCenter ne sont pas enregistrés.

   Si vous décochez la case cochée lors de la connexion précédente au serveur VMware vCenter, les paramètres de connexion précédemment enregistrés sont supprimés par Kaspersky Security.

   La case est décochée par défaut.
9. Cliquez sur le bouton **OK**.

Le plug-in d'administration de Kaspersky Security vérifie le certificat SSL reçu du serveur VMware vCenter. La fenêtre **Vérification du certificat** s'ouvre avec un message d'erreur si le certificat reçu contient une erreur ou s'il n'est pas compatible avec le certificat précédemment installé. Vous pouvez consulter les informations sur le certificat reçu. Pour ce faire, cliquez sur le bouton **Afficher le certificat reçu** dans la fenêtre du message d'erreur.

Vous pouvez installer le certificat reçu en tant que certificat de confiance afin que VMware vCenter ne reçoive pas de message relatif à une erreur de certificat lors de la prochaine connexion à ce serveur VMware. Pour ce faire, cochez la case **Installer le certificat reçu et ne plus afficher les avertissements relatifs au serveur <adresse du serveur VMware vCenter>**. Après que vous avez cliqué sur le bouton **Ignorer**, le certificat est enregistré dans le répertoire du système d'exploitation de l'ordinateur hébergeant la Console d'administration du Kaspersky Security Center, dans la section HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<adresse du serveur>\, où <adresse du serveur> est l'adresse du serveur d'origine du certificat.

Pour maintenir la connexion au serveur VMware vCenter, cliquez sur **Ignorer** dans la fenêtre **Vérification du certificat**.

Le plug-in d'administration de Kaspersky Security établit la connexion au serveur VMware vCenter. Si la connexion n'est pas établie, vérifiez que le serveur VMware vCenter est accessible via le réseau et retentez la connexion.

Dans la partie droite de la fenêtre, l'infrastructure protégée du cluster KSC s'affiche : serveur VMware vCenter, objets Datacenter, clusters VMware, hyperviseurs VMware ESXi qui ne font pas partie du cluster VMware, pools de ressources, objets vApp et machines virtuelles. Kaspersky Security utilise la représentation de l'infrastructure protégée du cluster KSC sous la forme d'une arborescence d'hyperviseurs VMware ESXi et de clusters VMware (Hosts and Clusters view) (pour en savoir plus, consultez la documentation des produits VMware).

Si l'infrastructure virtuelle VMware contient deux machines virtuelles ou plus avec un même identifiant (vm-ID), l'arborescence des objets affiche une seule machine virtuelle. Si cette machine virtuelle possède un profil de protection, les paramètres de celui-ci sont appliqués à toutes les machines virtuelles qui possèdent un identificateur identique (vm-ID).

La colonne **Profil de protection** affiche le nom du profil de protection dont les paramètres sont appliqués à la protection des machines virtuelles par Kaspersky Security.

Les informations relatives aux profils de protection sont affichées de la manière suivante :

- Le nom du profil de protection clairement attribué apparaît en noir.
- Le nom du profil de protection hérité de l'objet parent apparaît en gris. Le nom se forme de la manière suivante : "hérité : <N>" où N représente le nom du profil de protection hérité de l'objet parent.

Si la machine virtuelle est exclue de la protection, la colonne **Profil de protection** affiche *(Pas de protection)*.

DESACTIVATION DE LA PROTECTION SUR LA MACHINE VIRTUELLE

Pour désactiver la protection sur la machine virtuelle, procédez comme suit :

1. Pour la visualiser, ouvrez l'infrastructure protégée du cluster KSC auquel est reliée la machine virtuelle dont vous avez besoin (cf. section "Consultation de l'infrastructure protégée du cluster KSC" à la page 53).

2. Exécutez une des actions suivantes :

   - Si vous souhaitez désactiver la protection sur une machine virtuelle, sélectionnez-la dans le tableau.
   - Si vous souhaitez désactiver la protection sur plusieurs machines virtuelles qui sont des objets enfant d'un objet d'administration VMware, sélectionnez cet objet d'administration dans le tableau.

     Vous pouvez sélectionner plusieurs objets d'administration VMware en même temps en maintenant la touche **CTRL** enfoncée.

3. Cliquez sur le bouton **Annuler la protection**.

   La protection de l'objet parent et de ses objets enfant dont la protection est héritée de l'objet parent est annulée. S'agissant des objets exclus de la protection, la colonne **Profil de protection** affiche le message *(Pas de protection)*.

CONSULTATION DE LA LISTE DES MACHINES VIRTUELLES ET DES MACHINES VIRTUELLES DE PROTECTION DU CLUSTER KSC

Pour consulter la liste des machines virtuelles et des machines virtuelles de protection qui font partie du cluster KSC, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier **Clusters et tableaux de serveurs**, situé dans le dossier au nom du cluster KSC.

3. Dans la zone de travail, sélectionnez un cluster KSC et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom du cluster>**.

4. Dans la fenêtre des propriétés du cluster KSC, choisissez la section **Liste des machines virtuelles**.

   Le tableau qui apparaît sur le côté droit de la fenêtre comporte la liste de toutes les machines virtuelles de protection et des machines virtuelles entrant dans la composition du cluster KSC sélectionné.

   L'ajout d'une nouvelle machine virtuelle, un changement de nom ou la modification d'un chemin d'accès n'entraîne pas la mise à jour automatique du tableau des machines virtuelles. Pour recevoir les informations actualisées sur les machines virtuelles intégrées au cluster KSC, cliquez sur le bouton **Actualiser la liste**.

Les colonnes du tableau affichent les informations suivantes à propos de chaque machine virtuelle :

- **Etat de la protection**.

  Etat de la protection de la machine virtuelle. Les symboles suivants sont utilisés pour désigner l'état :

  -  – la machine virtuelle est protégée. Kaspersky Security protège la machine virtuelle si les conditions suivantes sont remplies :
    - la machine virtuelle est en ligne (elle n'est pas déconnectée, ni arrêtée) ;
    - le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) est installé et activé sur la machine virtuelle ;
    - la protection est activée dans les propriétés de la stratégie appliquée à cette machine virtuelle.
  -  – la machine virtuelle n'est pas protégée. Kaspersky Security ne protège pas la machine virtuelle si l'une des conditions suivantes est remplie :
    - le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) n'est pas installé ou n'est pas activé sur la machine virtuelle ;
    - la protection est désactivée dans les propriétés de la stratégie appliquée à cette machine virtuelle.
  -  : la machine virtuelle est désactivée ou suspendue.

- **Nom de la machine virtuelle**.

  Nom de la machine virtuelle ou de la machine virtuelle de protection appartenant au cluster KSC.

- **Chemin d'accès à la machine virtuelle**.

  Chemin d'accès à la machine virtuelle ou à la machine virtuelle de protection dans l'infrastructure virtuelle VMware.

Le bouton **Exporter la liste des machines virtuelles** vous permet d'exporter les informations relatives à toutes les machines virtuelles de protection du cluster KSC dans un fichier XML.

Vous pouvez trier la liste en fonction des noms des machines virtuelles, filtrer la liste en fonction des états de protection et y rechercher le nom d'une machine virtuelle.

- *Pour trier la liste en fonction du nom des machines virtuelles,*

  cliquez sur le bouton gauche de la souris en haut de la colonne **Nom de la machine virtuelle**.

  La liste est classée dans l'ordre alphabétique des noms des machines virtuelles. En cliquant de nouveau sur l'en-tête de la colonne, la liste est classée dans l'ordre alphabétique inversé des noms des machines virtuelles.

- *Pour filtrer la liste en fonction de l'état de la protection des machines virtuelles,*

  cliquez sur l'un des boutons suivants :

  -  : indiquer les machines virtuelles protégées.
  -  : indiquer les machines virtuelles de protection et les machines virtuelles non protégées.
  -  : afficher les machines virtuelles désactivées ou suspendues.

  Pour supprimer le filtre appliqué à la liste selon le statut de la protection des machines virtuelles, cliquez sur le bouton  .

- *Pour effectuer une recherche dans la liste en fonction du nom de la machine virtuelle,*

  saisissez le nom de la machine virtuelle dans la ligne de recherche.

ANTI-VIRUS FICHIERS

Cette section contient des informations sur la configuration des paramètres du module Antivirus Fichiers.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Anti-Virus Fichiers.

DANS CETTE SECTION

Protection des machines virtuelles 57

Analyse des machines virtuelles..... 65

PROTECTION DES MACHINES VIRTUELLES

Cette section présente le mécanisme employé par Kaspersky Security pour protéger les machines virtuelles situées sur les hyperviseurs VMware ESXi contre les virus et autres programmes dangereux. Elle explique également comment configurer les paramètres de protection des machines virtuelles.

DANS CETTE SECTION

A propos de la protection des machines virtuelles..... 57

Utilisation des profils de protection 58

A PROPOS DE LA PROTECTION DES MACHINES VIRTUELLES

La machine virtuelle de protection dotée du module Anti-Virus Fichiers protège les machines virtuelles sur l'hyperviseur VMware ESXi. Kaspersky Security protège les machines virtuelles selon les paramètres définis dans les profils de protection qui leur ont été attribués (cf. section "Concept de l'administration de l'application via le Kaspersky Security Center" à la page 22).

Quand l'utilisateur ou l'application sollicite un fichier sur la machine virtuelle, Kaspersky Security analyse le fichier en question.

- Si le fichier ne contient aucun virus ou programme dangereux, Kaspersky Security octroie l'accès à ce fichier.
- Si Kaspersky Security détecte un virus ou autre programme dangereux dans un fichier, l'application attribue à ce dernier le statut *Infecté*. Si le résultat de l'analyse ne détermine pas clairement si le fichier est infecté (le fichier contient peut-être une séquence de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.), Kaspersky Security lui attribue également le statut *Infecté*.

  Ensuite, Kaspersky Security exécute sur le fichier l'action définie dans le profil de protection de cette machine virtuelle, par exemple répare ou bloque le fichier.

L'analyse selon les signatures et l'analyse heuristique sont utilisées tout au long de la protection des machines virtuelles. L'*analyse selon les signatures* repose sur les bases de Kaspersky Security qui contiennent des informations sur les menaces connues et sur les moyens de les neutraliser. La protection sur la base des signatures garantit le niveau minimum de protection. Conformément aux recommandations des experts de Kaspersky Lab, cette méthode d'analyse est toujours activée.

L'*analyse heuristique* est une technologie d'identification des menaces impossibles à définir reposant sur les bases des applications de Kaspersky Lab. Elle permet de détecter les fichiers qui pourraient contenir un virus inconnu, une application dangereuse ou une nouvelle modification d'un virus connu. Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état *Infecté*.

Le niveau de l'analyse heuristique dépend du niveau de sécurité sélectionné :

- Si le niveau de sécurité **Faible** est sélectionné, l'analyse heuristique est superficielle. L'Analyseur heuristique ne suit pas toutes les instructions des fichiers exécutables pendant la recherche du code malveillant dans les fichiers exécutables. A ce niveau de l'analyse heuristique, la possibilité de détecter une menace est faible par rapport au niveau Moyen. L'analyse requiert moins de ressources de la machine virtuelle et s'exécute plus rapidement.

- Si le niveau de sécurité **Recommandé**, **Elevé** ou **Utilisateur** est sélectionné, le niveau d'analyse heuristique est moyen. Lors de la recherche du code malveillant dans les fichiers, l'analyseur heuristique exécute le nombre d'instructions dans les fichiers exécutables qui est recommandé par les experts de Kaspersky Lab.

Les informations relatives à tous les événements survenus au cours de la protection des machines virtuelles sont consignées dans un rapport (cf. section "Types de rapports" à la page 99).

Il est conseillé de consulter périodiquement la liste des fichiers bloqués dans le cadre de la protection des machines virtuelles et de réaliser des actions sur ceux-ci. Par exemple, vous pouvez enregistrer une copie des fichiers auxquels l'utilisateur n'a pas accès sur la machine virtuelle et les supprimer. Les informations relatives aux fichiers bloqués figurent dans le rapport sur les virus ou dans la sélection d'événements des catégories *Fichier bloqué* (cf. Documentation du Kaspersky Security Center).

Pour pouvoir accéder aux fichiers bloqués par la protection des machines virtuelles, il est nécessaire de désactiver temporairement la protection de ces machines virtuelles (cf. section "Désactivation de la protection sur la machine virtuelle" à la page 54).

UTILISATION DES PROFILS DE PROTECTION

Vous pouvez exécuter les actions suivantes sur les profils de protection :

- créer un profil de protection ;
- modifier les paramètres des profils de protection ;
- attribuer des profils de protection aux machines virtuelles ;
- supprimer des profils de protection.

DANS CETTE SECTION

Création d'un profil de protection 58

Modification des paramètres du profil de protection 63

Attribution d'un profil de protection à une machine virtuelle 64

Suppression d'un profil de protection 65

CREATION D'UN PROFIL DE PROTECTION

Pour créer un profil de protection, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie pour laquelle vous souhaitez créer un profil de protection.

3. Dans la zone de travail, choisissez l'onglet **Stratégies**.

4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.

5. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Profils de protection**.

   La liste des profils de protection apparaît dans la partie droite de la fenêtre. Si vous créez le premier profil de protection de cette stratégie, la liste est vide.

6. Cliquez sur le bouton **Ajouter**.

7. Dans la fenêtre qui s'ouvre, saisissez le nom du profil de protection, puis cliquez sur **OK**.

   La fenêtre **Paramètres de protection** s'ouvre. Les paramètres du profil de protection sont similaires aux paramètres du profil de protection racine.

8. Dans le groupe **Niveau de sécurité**, effectuez l'une des actions suivantes :

   - Si vous souhaitez utiliser l'un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.

   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.

   - Si vous souhaitez configurer vous-même le niveau de protection, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Paramètres du niveau de sécurité** :

   a. Dans le groupe **Analyse des archives et des fichiers composés**, définissez les paramètres suivants :

      - **Analyser les archives**.

        Activation ou désactivation de l'analyse des archives.

        La case est décochée par défaut.

      - **Supprimer les archives en cas d'échec de la réparation**.

        Suppression des archives dont la réparation est impossible.

        Si la case est cochée, Kaspersky Security supprime les archives dont la réparation a échoué.

        Si la case est décochée, l'application ne supprime pas les archives qui n'ont pu être réparées. Kaspersky Security signale au Serveur d'administration du Kaspersky Security Center que le fichier infecté n'a pas été supprimé.

        La case est accessible si la case **Analyser les archives** est cochée.

        La case est décochée par défaut.

      - **Analyser les archives autoextractibles**.

        Activation/désactivation de l'analyse des archives autoextractibles.

        Par défaut, la case pour les profils de protection est décochée et la case pour les tâches d'analyse est cochée.

      - **Analyser les objets OLE intégrés**.

        Activation ou désactivation de l'analyse des objets intégrés à un fichier.

        La case est cochée par défaut.

      - **Ne pas décompacter les fichiers composés de grande taille**.

        Quand la case est cochée, Kaspersky Security n'analyse pas les fichiers composés dont la taille dépasse la valeur du champ **Taille maximale du fichier composé à analyser**.

        Si la case est décochée, Kaspersky Security analyse les fichiers composés de toutes les tailles.

Kaspersky Security analyse les fichiers de grande taille extraits des archives, quel que soit l'état de la case **Ne pas décompacter les fichiers composés de grande taille**.

La case est cochée par défaut.

- **Taille maximale du fichier composé à analyser X Mo**.

  Taille maximale des fichiers composés pouvant être analysés (en mégaoctets). Kaspersky Security ne décompacte pas et n'analyse pas les objets dont la taille est supérieure à la valeur indiquée.

  Le paramètre ne peut être modifié si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

  La valeur par défaut est de 8 Mo.

b. Dans le groupe **Productivité**, définissez les paramètres suivants :

- **Limiter la durée d'analyse des fichiers**.

  Si la case est cochée, Kaspersky Security interrompt l'analyse si la durée de celle-ci atteint la valeur définie dans le champ **Ne pas analyser les fichiers pendant plus de X seconde(s)** et ignore ce fichier.

  Si la case est décochée, Kaspersky Security ne limite pas la durée de l'analyse des fichiers.

  Par défaut, la case pour les profils de protection est cochée et la case pour les tâches d'analyse est décochée.

- **Ne pas analyser les fichiers pendant plus de X seconde(s)**.

  Durée maximale de l'analyse du fichier (en secondes). Kaspersky Security interrompt l'analyse du fichier quand sa durée atteint la valeur définie pour ce paramètre.

  Le paramètre ne peut être modifié si la case **Limiter la durée d'analyse des fichiers** est cochée.

  La valeur par défaut est de 60 secondes.

c. Dans le groupe **Objets à détecter**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à détecter** qui apparaît :

- **Utilitaires malveillants**.

  Activation/désactivation de la protection contre les utilitaires malveillants.

  Les *utilitaires malveillants* n'exécutent pas d'actions malveillantes dès le lancement et peuvent être conservés et exécutés sur l'ordinateur de l'utilisateur sans présenter de risque. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants ou exécuter d'autres actions malveillantes.

  Si la case est cochée, la protection contre les utilitaires malveillants est activée.

  Si la case est décochée, la protection contre les utilitaires malveillants est désactivée.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation/désactivation de la protection contre les programmes publicitaires.

  Les *programmes publicitaires* permettent de montrer des publicités aux utilisateurs. Par exemple, ils affichent des bandeaux publicitaires dans l'interface d'autres programmes ou réorientent les demandes de recherche vers des pages publicitaires. Certains d'entre eux recueillent également des informations marketing sur l'utilisateur qu'ils renvoient à l'auteur : catégories de sites Internet visités, mots-clés utilisés dans les recherches, etc. A la différence des chevaux de Troie espions, ils transmettent ces informations avec l'autorisation de l'utilisateur.

  Si la case est cochée, la protection contre les logiciels publicitaires est activée.

  Si la case est décochée, la protection contre les logiciels publicitaires est désactivée.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation/désactivation de la protection contre les programmes numéroteurs.

  Si la case est cochée, la protection contre les programmes numéroteurs est activée.

  Si la case est décochée, la protection contre les programmes numéroteurs est désactivée.

  La case est cochée par défaut.

- **Autres**.

  Activation/désactivation de la protection d'autres applications légitimes qui peuvent être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

  La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi elles figurent les clients IRC, les programmes pour le chargement des fichiers, les applications d'administration à distance, les dispositifs de suivi de l'activité de l'utilisateur, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet. Toutefois, si des individus malintentionnés obtiennent l'accès à ces applications ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leurs fonctions pour nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  Si la case est décochée, la protection contre ces programmes est désactivée.

  La case est décochée par défaut.

- **Fichiers compactés plusieurs fois**.

  Exclusion ou inclusion de l'analyse des fichiers compactés à trois reprises au moins par un ou plusieurs compacteurs.

  Si le fichier a été compacté plus de trois fois par un ou plusieurs compacteurs, il s'agit vraisemblablement d'un fichier qui contient une application malveillante ou un programme permettant à des individus malintentionnés de nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les fichiers compactés à plusieurs reprises est activée et l'analyse de ce type de fichier est autorisée.

  Si la case est décochée, la protection contre les fichiers compressés à plusieurs reprises est désactivée.

  La case est cochée par défaut.

Kaspersky Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans les fichiers des machines virtuelles. C'est pourquoi les paramètres **Virus et vers** et **Chevaux de Troie** du groupe **Applications malveillantes** ne peuvent pas être modifiés.

d. Cliquez sur le bouton **OK** dans la fenêtre **Objets à détecter**.

e. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du niveau de sécurité**.

Si vous avez modifié les paramètres du niveau de protection, l'application créera un niveau utilisateur de protection. Le nom du niveau de protection dans le groupe **Niveau de sécurité** sera remplacé par **Utilisateur**.

9. Dans le groupe **Action exécutée en cas de détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection de fichiers infectés :

- **Sélectionner l'action automatiquement**.

  Kaspersky Security exécute l'action définie par défaut par les experts de Kaspersky Lab. Il s'agit de **Réparer. Supprimer si la réparation est impossible**.

  Cette option est sélectionnée par défaut.

- **Réparer. Supprimer si la réparation est impossible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, l'application supprime ces fichiers. Kaspersky Security supprime les archives infectées qui n'ont pas pu être réparées uniquement si la case **Supprimer les archives en cas d'échec de la réparation** est cochée dans les paramètres du niveau de protection.

- **Réparer. Bloquer si la réparation n'est pas possible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, Kaspersky Security bloque ces fichiers.

- **Supprimer. Bloquer si la suppression n'est pas possible**.

  Kaspersky Security supprime automatiquement les fichiers infectés, sans tenter de les réparer. Si la suppression est impossible, Kaspersky Security bloque ces fichiers.

- **Bloquer**.

  Kaspersky Security bloque automatiquement les fichiers infectés, sans tenter de les réparer.

10. Si vous souhaitez exclure les disques réseau de la protection, décochez la case **Analyser les disques réseau** dans le groupe **Zone de protection**.

    Si la case est cochée, Kaspersky Security analyse tous les fichiers des disques réseau n'étant pas exclus de la protection. La case est cochée par défaut.

    Kaspersky Security analyse toujours les fichiers des disques durs et amovibles. C'est la raison pour laquelle le paramètre **Analyser les disques amovibles et les disques durs** du groupe **Zone de protection** n'est pas modifiable.

11. Si vous souhaitez exclure n'importe quel fichier des machines virtuelles de protection, cliquez sur le bouton **Configuration** dans le groupe **Exclusions de la protection**.

    Dans la fenêtre **Exclusions de la protection** qui s'ouvre, définissez les paramètres suivants :

    a. Dans la fenêtre **Extensions des fichiers**, sélectionnez l'une des options suivantes :

       - **Analyser tout, sauf les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à ne pas analyser dans le cadre de la protection de la machine virtuelle.

       - **Analyser uniquement les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à analyser dans le cadre de la protection de la machine virtuelle.

       Vous pouvez séparer les extensions de fichier par un espace ou un saut de ligne. Lorsque vous indiquez les extensions de fichiers, vous pouvez utiliser n'importe quel caractère sauf `* | \ : " < > ? /`. Si le caractère "espace" est utilisé dans l'extension, il est nécessaire d'indiquer cette extension entre guillemets, par exemple : `"doc x"`.

       Si vous aviez choisi l'option **Analyser uniquement les fichiers avec les extensions suivantes** dans la liste déroulante, sans renseigner les extensions de fichier à analyser, Kaspersky Security analyse tous les fichiers.

    b. Composez la liste des objets à exclure de la protection dans le tableau **Dossiers et fichiers**, à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Vous pouvez exclure de la protection les objets des types suivants :

       - Dossiers. Les fichiers des dossiers situés aux emplacements indiqués sont exclus de la protection. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure les sous-répertoires de la protection.

- Les fichiers selon un masque. Sont exclus de la protection : les fichiers possédant le nom indiqué, les fichiers situés à l'emplacement indiqué ou les fichiers correspondant au masque indiqué.

  Les caractères * et ? peuvent être utilisés dans la création d'un masque de fichier.

Vous pouvez conserver la liste d'objets à exclure dans un fichier à l'aide du bouton **Exportation** et télécharger la liste des objets à exclure précédemment enregistrée à l'aide du bouton **Importation**.

La distribution de l'application comprend le fichier microsoft_file_exclusions.xml. Ce fichier reprend la liste des objets dont l'exclusion a été conseillée par Microsoft (la liste des exclusions conseillées par Microsoft se trouve sur le site de Microsoft). Le fichier microsoft_file_exclusions.xml se trouve dans le dossier d'installation du plug-in d'administration de Kaspersky Security, sur l'ordinateur où est installée la Console d'administration du Kaspersky Security Center. Vous pouvez importer ce fichier dans les exclusions du profil de protection. Ainsi, Kaspersky Security exclut de la protection les objets conseillés par Microsoft sur toutes les machines virtuelles auxquelles ce profil de protection a été attribué. A l'issue de l'importation, vous pouvez consulter et modifier la liste de ces objets dans le tableau **Dossiers et fichiers**.

L'utilisation de variables d'environnement n'est pas prise en charge dans la liste des exclusions. L'objet du système de fichiers défini via des variables d'environnement ne sera pas exclu de la protection.

Kaspersky Security ignore la casse dans les chemins d'accès aux dossiers des disques durs et amovibles pour lesquels aucun accès réseau n'est configuré. La casse est prise en compte dans les chemins d'accès aux dossiers réseau exclus de la protection. Si vous souhaitez définir un chemin d'accès à des dossiers réseau sans que la casse ne soit prise en compte, décochez la case **Respecter la casse dans les chemins d'accès aux dossiers réseau**.

Décocher la case **Respecter la casse dans les chemins d'accès aux dossiers réseau** peut entraîner une diminution des performances de l'application Kaspersky Security.

12. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de la protection**.
13. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de protection**.

    Dans la fenêtre **Propriétés : <Nom de la stratégie>**, le nouveau profil apparaît dans la liste des profils de protection.

Après avoir créé un profil de protection, vous pouvez l'attribuer aux machines virtuelles (cf. section "Attribution d'un paramètre de protection aux machines virtuelles" à la page 64).

MODIFICATION DES PARAMETRES DU PROFIL DE PROTECTION

Vous pouvez modifier les paramètres du profil de protection et les paramètres du profil de protection racine.

Pour modifier les paramètres d'un profil de protection, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie dont vous souhaitez modifier le profil de protection racine.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Procédez comme suit :

   - Si vous voulez modifier les paramètres du profil de protection racine, procédez comme suit :

     a. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez la section **Profil de protection racine**.

     b. Dans la partie droite de la fenêtre, modifiez les paramètres du profil de protection racine (cf. section "Etape 3. Configuration des paramètres du profil de protection racine" à la page 48).

c. Cliquez sur le bouton **OK**.

- Si vous voulez modifier les paramètres du profil de protection, procédez comme suit :

  a. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez la section **Profils de protection**.

     La liste des profils de protection apparaît dans la partie droite de la fenêtre.

  b. Dans la liste des profils de protection, sélectionnez le profil que vous souhaitez modifier, puis cliquez sur le bouton **Modifier**.

     La fenêtre **Paramètres de protection** s'ouvre.

  c. Modifiez les paramètres du profil de protection (cf. section "Création d'un profil de protection" à la page 58).

  d. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de protection**.

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

Les modifications des paramètres du profil de protection entrent en vigueur après la synchronisation des données entre l'application du Kaspersky Security Center et les machines virtuelles de protection.

ATTRIBUTION D'UN PROFIL DE PROTECTION A UNE MACHINE VIRTUELLE

Après la création de la stratégie, tous les objets d'administration VMware reçoivent le profil de protection racine (cf. section "A propos du profil de protection racine" à la page. 24). Vous pouvez attribuer aux machines virtuelles leur propre profil de protection.

Pour attribuer un profil de protection à une machine virtuelle, procédez comme suit :

1. Pour la visualiser, ouvrez l'infrastructure protégée du cluster KSC de la machine virtuelle à laquelle vous souhaitez attribuer un profil de protection (cf. section "Consultation de l'infrastructure protégée du cluster KSC" à la page 53).

2. Exécutez une des actions suivantes :

   - Si vous souhaitez attribuer un profil de protection à une machine virtuelle, sélectionnez-la dans le tableau.

   - Si vous souhaitez attribuer un profil de protection identique à plusieurs machines virtuelles constituant des objets enfant d'un objet d'administration de VMware, sélectionnez cet objet d'administration dans le tableau. Vous pouvez sélectionner plusieurs objets d'administration VMware en même temps en maintenant la touche **CTRL** enfoncée.

3. Cliquez sur le bouton **Attribuer un profil de protection**.

   La fenêtre **Profil de protection attribué** s'ouvre.

4. Dans la fenêtre **Profil de protection attribué**, sélectionnez l'une des options suivantes :

   - **Parent "N"**, où N représente le nom du profil de protection attribué à l'objet parent. Le profil de protection de l'objet parent est attribué à la machine virtuelle.

   - **Indiqué**. La machine virtuelle reçoit l'un des profils de protection de la stratégie.

5. Cliquez sur le bouton **OK**.

   Le profil de protection sélectionné sera attribué à l'objet d'administration VMware et à ses objets enfants qui ne possèdent pas de profil de protection clairement attribué et qui ne sont pas exclus de la protection. Le profil de protection attribué apparaît dans la colonne **Profil de protection** du tableau.

SUPPRESSION D'UN PROFIL DE PROTECTION

Pour supprimer un profil de protection, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie dont vous souhaitez supprimer le profil de protection.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez la section **Profils de protection**.

   La liste des profils de protection apparaît dans la partie droite de la fenêtre.
6. Dans la liste des profils de protection, sélectionnez le profil que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.
7. Si ce profil de protection est attribué aux machines virtuelles, une fenêtre s'ouvre pour confirmer la suppression. Cliquez sur le bouton **Oui**.
8. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés:<Nom de la stratégie>**.

Le profil de protection est supprimé. L'application protège désormais les machines virtuelles soumises antérieurement à ce profil de protection selon les paramètres du profil de protection de leur objet parent dans l'infrastructure virtuelle VMware. Si l'objet parent est exclu de la protection, l'application ne protègera pas ces machines virtuelles.

ANALYSE DES MACHINES VIRTUELLES

Cette section présente comment Kaspersky Security analyse les fichiers des machines virtuelles sur les hyperviseurs VMware ESXi et explique comme configurer les paramètres de l'analyse.

DANS CETTE SECTION

A propos de l'analyse des machines virtuelles 65

Création d'une tâche d'analyse complète 67

Création d'une tâche d'analyse personnalisée 73

Lancement et arrêt de l'analyse complète et de l'analyse personnalisée 81

A PROPOS DE L'ANALYSE DES MACHINES VIRTUELLES

Kaspersky Security peut rechercher la présence éventuelle de virus et d'autres programmes dangereux dans les fichiers des machines virtuelles. Pour éviter la propagation d'objets malveillants, il est nécessaire d'analyser les fichiers des machines virtuelles à l'aide de nouvelles bases antivirus.

L'analyse selon les signatures et l'analyse heuristique sont utilisées tout au long de l'analyse des machines virtuelles. L'*analyse selon les signatures* repose sur les bases de Kaspersky Security qui contiennent des informations sur les menaces connues et sur les moyens de les neutraliser. La protection sur la base des signatures garantit le niveau minimum de protection. Conformément aux recommandations des experts de Kaspersky Lab, cette méthode d'analyse est toujours activée.

L'*analyse heuristique* est une technologie d'identification des menaces impossibles à définir reposant sur les bases des applications de Kaspersky Lab. Elle permet de détecter les fichiers qui pourraient contenir un virus inconnu, une application dangereuse ou une nouvelle modification d'un virus connu. Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état *Infecté*.

L'analyse des machines virtuelles utilise toujours un niveau approfondi d'analyse heuristique, quel que soit le niveau de sécurité sélectionné. L'analyseur heuristique exécute un nombre maximal d'instructions dans le fichier exécutable, ce qui permet d'augmenter la probabilité de détecter des menaces.

Kaspersky Security utilise les tâches d'analyse suivantes :

- **Analyse complète**. Au cours de tâche, les machines virtuelles de protection recherchent la présence éventuelle de virus et d'autres programmes dangereux sur toutes les machines virtuelles de tous les clusters KSC.

- **Analyse personnalisée**. Au cours de cette tâche, les machines virtuelles de protection recherchent la présence éventuelle de virus et d'autres programmes dangereux sur les machines virtuelles sélectionnées dans le cluster KSC indiqué.

Pendant l'exécution de l'analyse, Kaspersky Security analyse les fichiers des machines virtuelles repris dans les paramètres de l'analyse. Pendant l'exécution de l'analyse, une machine virtuelle de protection dotée du module Antivirus Fichiers analyse simultanément les fichiers de quatre machines virtuelles au maximum.

Kaspersky Security n'analyse pas la machine virtuelle si :

- Vous avez ajouté la machine virtuelle à la liste des objets de l'infrastructure virtuelle (Inventory) de la console VMware vSphere Client ou que vous avez créé la machine virtuelle sur l'hyperviseur VMware ESXi après le lancement de la tâche d'analyse.

- Vous avez désactivé ou arrêté la machine virtuelle avant le début de l'analyse de cette machine virtuelle et vous l'avez réactivée avant la fin de la tâche d'analyse.

- Vous avez supprimé la machine virtuelle de la liste des objets de l'infrastructure virtuelle (Inventory) dans la console VMware vSphere Client avant le début de l'analyse de cette machine virtuelle.

- La machine virtuelle incluse dans la zone d'action de la tâche d'analyse lancée migre sur l'hyperviseur VMware ESXi où la tâche d'analyse n'est pas lancée.

- Le système d'exploitation hôte installé sur la machine virtuelle ne correspond pas aux configurations requises de Kaspersky Security.

- Le pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) n'est pas installé ou n'est pas activé sur la machine virtuelle.

Vous pouvez lancer la tâche d'analyse manuellement ou programmer l'exécution de l'analyse.

La progression de l'analyse s'affiche sous l'onglet **Tâches** de la zone de travail du dossier au nom du cluster KSC contenant les machines virtuelles pour lesquelles vous avez lancé la tâche d'analyse (cf. section "Lancement et arrêt de l'analyse complète et de l'analyse personnalisée" à la page 81).

Les informations sur les résultats de l'analyse et tous les événements survenus pendant l'exécution des tâches d'analyse sont consignées dans le rapport (cf. section "Types de rapports" à la page 99).

A l'issue de l'analyse, il est conseillé de consulter la liste des fichiers bloqués suite à l'exécution de la tâche et d'exécuter manuellement sur ceux-ci les actions recommandées. Par exemple, enregistrer une copie des fichiers auxquels l'utilisateur n'a pas accès sur la machine virtuelle et les supprimer. Il est nécessaire, au préalable, d'exclure de la protection les machines virtuelles sur lesquelles ces fichiers ont été bloqués. Les informations relatives aux fichiers bloqués figurent dans le rapport sur les virus ou dans la sélection d'événements des catégories *Fichier bloqué* (cf. Documentation du Kaspersky Security Center).

CREATION D'UNE TACHE D'ANALYSE COMPLETE

En cas de remplacement ou de réinstallation de la plateforme du serveur VMware vCenter, les tâches d'analyse complètes créées antérieurement ne fonctionneront pas. Il est nécessaire de les supprimer et d'en créer d'autres.

Pour créer une tâche d'analyse complète, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Exécutez une des actions suivantes :
   - Si vous souhaitez créer une tâche d'analyse complète pour les machines virtuelles de protection de tous les clusters KSC, choisissez le dossier **Ordinateurs administrés** dans l'arborescence de la console.
   - Si vous souhaitez créer une tâche d'analyse complète pour les machines virtuelles de protection d'un seul cluster KSC, sélectionnez le dossier portant le nom de ce cluster KSC dans le dossier **Ordinateurs administrés** de l'arborescence de la console.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Lancez l'Assistant de création d'une tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les instructions de l'Assistant de création d'une tâche.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 67

Etape 2. Sélection du type de tâche 67

Etape 3. Configuration des paramètres de l'analyse 67

Etape 4. Sélection de la zone d'analyse 71

Etape 5. Définition des paramètres de programmation de la tâche 72

Etape 6. Fin de la création de la tâche 73

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche d'analyse complète dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

A cette étape, sélectionnez le type de tâche **Analyse complète** pour l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. CONFIGURATION DES PARAMETRES DE L'ANALYSE

A cette étape, définissez les paramètres d'analyse des machines virtuelles.

Pour définir les paramètres d'analyse des machines virtuelles, procédez comme suit :

1. Dans le groupe **Niveau de sécurité**, effectuez l'une des actions suivantes :

   - Si vous souhaitez utiliser l'un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.
   - Si vous souhaitez configurer vous-même le niveau de protection, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Paramètres du niveau de sécurité** :

   a. Dans le groupe **Analyse des archives et des fichiers composés**, définissez les paramètres suivants :

      - **Analyser les archives**.

        Activation ou désactivation de l'analyse des archives.

        La case est décochée par défaut.

      - **Supprimer les archives en cas d'échec de la réparation**.

        Suppression des archives dont la réparation est impossible.

        Si la case est cochée, Kaspersky Security supprime les archives dont la réparation a échoué.

        Si la case est décochée, l'application ne supprime pas les archives qui n'ont pu être réparées. Kaspersky Security signale au Serveur d'administration du Kaspersky Security Center que le fichier infecté n'a pas été supprimé.

        La case est accessible si la case **Analyser les archives** est cochée.

        La case est décochée par défaut.

      - **Analyser les archives autoextractibles**.

        Activation/désactivation de l'analyse des archives autoextractibles.

        Par défaut, la case pour les profils de protection est décochée et la case pour les tâches d'analyse est cochée.

      - **Analyser les objets OLE intégrés**.

        Activation ou désactivation de l'analyse des objets intégrés à un fichier.

        La case est cochée par défaut.

      - **Ne pas décompacter les fichiers composés de grande taille**.

        Quand la case est cochée, Kaspersky Security n'analyse pas les fichiers composés dont la taille dépasse la valeur du champ **Taille maximale du fichier composé à analyser**.

        Si la case est décochée, Kaspersky Security analyse les fichiers composés de toutes les tailles.

        Kaspersky Security analyse les fichiers de grande taille extraits des archives, quel que soit l'état de la case **Ne pas décompacter les fichiers composés de grande taille**.

        La case est cochée par défaut.

      - **Taille maximale du fichier composé à analyser X Mo**.

        Taille maximale des fichiers composés pouvant être analysés (en mégaoctets). Kaspersky Security ne décompacte pas et n'analyse pas les objets dont la taille est supérieure à la valeur indiquée.

        Le paramètre ne peut être modifié si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

        La valeur par défaut est de 8 Mo.

   b. Dans le groupe **Productivité**, définissez les paramètres suivants :

      - **Limiter la durée d'analyse des fichiers**.

        Si la case est cochée, Kaspersky Security interrompt l'analyse si la durée de celle-ci atteint la valeur définie dans le champ **Ne pas analyser les fichiers pendant plus de X seconde(s)** et ignore ce fichier.

Si la case est décochée, Kaspersky Security ne limite pas la durée de l'analyse des fichiers.

Par défaut, la case pour les profils de protection est cochée et la case pour les tâches d'analyse est décochée.

- **Ne pas analyser les fichiers pendant plus de X seconde(s)**.

  Durée maximale de l'analyse du fichier (en secondes). Kaspersky Security interrompt l'analyse du fichier quand sa durée atteint la valeur définie pour ce paramètre.

  Le paramètre ne peut être modifié si la case **Limiter la durée d'analyse des fichiers** est cochée.

  La valeur par défaut est de 60 secondes.

c. Dans le groupe **Objets à détecter**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à détecter** qui apparaît :

- **Utilitaires malveillants**.

  Activation/désactivation de la protection contre les utilitaires malveillants.

  Les *utilitaires malveillants* n'exécutent pas d'actions malveillantes dès le lancement et peuvent être conservés et exécutés sur l'ordinateur de l'utilisateur sans présenter de risque. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants ou exécuter d'autres actions malveillantes.

  Si la case est cochée, la protection contre les utilitaires malveillants est activée.

  Si la case est décochée, la protection contre les utilitaires malveillants est désactivée.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation/désactivation de la protection contre les programmes publicitaires.

  Les *programmes publicitaires* permettent de montrer des publicités aux utilisateurs. Par exemple, ils affichent des bandeaux publicitaires dans l'interface d'autres programmes ou réorientent les demandes de recherche vers des pages publicitaires. Certains d'entre eux recueillent également des informations marketing sur l'utilisateur qu'ils renvoient à l'auteur : catégories de sites Internet visités, mots-clés utilisés dans les recherches, etc. A la différence des chevaux de Troie espions, ils transmettent ces informations avec l'autorisation de l'utilisateur.

  Si la case est cochée, la protection contre les logiciels publicitaires est activée.

  Si la case est décochée, la protection contre les logiciels publicitaires est désactivée.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation/désactivation de la protection contre les programmes numéroteurs.

  Si la case est cochée, la protection contre les programmes numéroteurs est activée.

  Si la case est décochée, la protection contre les programmes numéroteurs est désactivée.

  La case est cochée par défaut.

- **Autres**.

  Activation/désactivation de la protection d'autres applications légitimes qui peuvent être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

  La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi elles figurent les clients IRC, les programmes pour le chargement des fichiers, les applications d'administration à distance, les dispositifs de suivi de l'activité de l'utilisateur, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet. Toutefois, si des individus malintentionnés obtiennent l'accès à ces applications ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leurs fonctions pour nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

Si la case est décochée, la protection contre ces programmes est désactivée.

La case est décochée par défaut.

- **Fichiers compactés plusieurs fois**.

  Exclusion ou inclusion de l'analyse des fichiers compactés à trois reprises au moins par un ou plusieurs compacteurs.

  Si le fichier a été compacté plus de trois fois par un ou plusieurs compacteurs, il s'agit vraisemblablement d'un fichier qui contient une application malveillante ou un programme permettant à des individus malintentionnés de nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les fichiers compactés à plusieurs reprises est activée et l'analyse de ce type de fichier est autorisée.

  Si la case est décochée, la protection contre les fichiers compressés à plusieurs reprises est désactivée.

  La case est cochée par défaut.

Kaspersky Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans les fichiers des machines virtuelles. C'est pourquoi les paramètres **Virus et vers** et **Chevaux de Troie** du groupe **Applications malveillantes** ne peuvent pas être modifiés.

d. Cliquez sur le bouton **OK** dans la fenêtre **Objets à détecter**.

e. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du niveau de sécurité**.

Si vous avez modifié les paramètres du niveau de protection, l'application créera un niveau utilisateur de protection. Le nom du niveau de protection dans le groupe **Niveau de sécurité** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action exécutée en cas de détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection de fichiers infectés :

- **Sélectionner l'action automatiquement**.

  Kaspersky Security exécute l'action définie par défaut par les experts de Kaspersky Lab. Il s'agit de **Réparer. Supprimer si la réparation est impossible**.

  Cette option est sélectionnée par défaut.

- **Réparer. Supprimer si la réparation est impossible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, l'application supprime ces fichiers. Kaspersky Security supprime les archives infectées qui n'ont pas pu être réparées uniquement si la case **Supprimer les archives en cas d'échec de la réparation** est cochée dans les paramètres du niveau de protection.

- **Réparer. Bloquer si la réparation n'est pas possible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, Kaspersky Security bloque ces fichiers.

- **Supprimer. Bloquer si la suppression n'est pas possible**.

  Kaspersky Security supprime automatiquement les fichiers infectés, sans tenter de les réparer. Si la suppression est impossible, Kaspersky Security bloque ces fichiers.

- **Bloquer**.

  Kaspersky Security bloque automatiquement les fichiers infectés, sans tenter de les réparer.

3. Si vous souhaitez que Kaspersky Security analyse les fichiers sur les disques amovibles, cochez la case **Analyser les disques amovibles** dans le groupe **Disques amovibles**.

Si la case **Analyser les disques amovibles** est cochée mais qu'aucun chemin d'accès à un disque amovible n'est inclus dans la zone d'analyse de la tâche, Kaspersky Security n'analyse aucun disque amovible.

4. Dans la fenêtre **Arrêter l'analyse**, sélectionnez une des options suivantes :

   - **Au bout de X minutes après le lancement de l'analyse**.

     Durée maximale d'exécution de la tâche d'analyse (en minutes). A l'issue de ce délai, l'exécution de la tâche d'analyse est interrompue même si l'analyse n'est pas terminée.

     Cette option est sélectionnée par défaut, avec la valeur 120 minutes.

   - **A la fin de l'analyse des fichiers sur toutes les machines virtuelles protégées allumées au moment du lancement de la tâche**.

     La tâche d'analyse complète est exécutée jusqu'à ce que les fichiers de toutes les machines virtuelles protégées qui étaient actives au moment du lancement de la tâche aient été analysés.

     La tâche d'analyse personnalisée est exécutée jusqu'à ce que les fichiers de toutes les machines virtuelles protégées de la zone d'action de la tâche qui étaient actives au moment du lancement de la tâche aient été analysés.

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

ETAPE 4. SELECTION DE LA ZONE D'ANALYSE

Définissez la zone d'analyse au cours de cette étape. La zone d'analyse désigne l'emplacement et l'extension des fichiers des machines virtuelles (par exemple, tous les disques durs, les objets de démarrage, les bases de messagerie) analysés par Kaspersky Security pendant l'exécution de la tâche de vérification.

Choisissez l'une des options suivantes :

- **Analyser tous les dossiers et fichiers, sauf ceux indiqués**. Composez la liste des objets à exclure de la zone d'analyse à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Vous pouvez exclure de la zone d'analyse les objets des types suivants :

  - Dossiers. Les fichiers des dossiers situés aux emplacements indiqués sont exclus de la zone d'analyse. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure ses sous-répertoires de la zone d'analyse.

  - Les fichiers selon un masque. Sont exclus de la zone d'analyse : les fichiers possédant le nom indiqué, les fichiers situés à l'emplacement indiqué ou les fichiers correspondant au masque indiqué.

    Les caractères * et ? peuvent être utilisés dans la création d'un masque de fichier.

  Vous pouvez conserver la liste d'objets à exclure dans un fichier à l'aide du bouton **Exportation** et télécharger la liste des objets à exclure précédemment enregistrée à l'aide du bouton **Importation**.

  La distribution de l'application comprend le fichier microsoft_file_exclusions.xml. Ce fichier reprend la liste des objets dont l'exclusion a été conseillée par Microsoft (la liste des exclusions conseillées par Microsoft se trouve sur le site de Microsoft). Le fichier microsoft_file_exclusions.xml se trouve dans le dossier d'installation du plug-in d'administration de Kaspersky Security, sur l'ordinateur où est installée la Console d'administration du Kaspersky Security Center. Vous pouvez importer ce fichier dans les exclusions de la tâche d'analyse. Ainsi, Kaspersky Security n'analysera pas les objets conseillés par Microsoft lors de l'exécution de la tâche d'analyse. A l'issue de l'importation, vous pouvez consulter et modifier la liste de ces objets dans le tableau **Dossiers et fichiers**.

  L'utilisation de variables d'environnement n'est pas prise en charge dans la liste des exclusions. L'objet du système de fichiers défini via des variables d'environnement ne sera pas exclu de la zone d'analyse.

  Dans le groupe **Extensions des fichiers**, indiquez les extensions de fichiers que vous souhaitez inclure dans la zone d'analyse ou exclure de celle-ci. Pour ce faire, sélectionner une des options suivantes :

  - **Analyser tout, sauf les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à ne pas analyser dans le cadre de l'exécution de la tâche d'analyse.

- **Analyser uniquement les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à analyser dans le cadre de l'exécution de la tâche d'analyse.

  Vous pouvez séparer les extensions de fichier par un espace ou un saut de ligne. Lorsque vous indiquez les extensions de fichiers, vous pouvez utiliser n'importe quel caractère sauf `* | \ : " < > ? /`. Si le caractère "espace" est utilisé dans l'extension, il est nécessaire d'indiquer cette extension entre guillemets, par exemple : `"doc x"`.

  Si vous aviez choisi l'option **Analyser uniquement les fichiers avec les extensions suivantes** dans la liste déroulante, sans renseigner les extensions de fichier à analyser, Kaspersky Security analyse tous les fichiers.

Les dossiers exclus de l'analyse présentent une priorité supérieure à celle des extensions de fichiers incluses dans la zone d'analyse. Si un fichier figure dans un dossier exclu de l'analyse, il ne sera pas analysé, même si son extension fait partie des extensions à analyser.

- **Analyser uniquement les dossiers et fichiers indiqués**. Les boutons **Ajouter**, **Modifier** et **Supprimer** permettent de composer la liste des dossiers et des fichiers de la machine virtuelle qu'il est nécessaire d'analyser.

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

ETAPE 5. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de l'analyse complète :

- **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.

- **Lancement des tâches ignorées**. Cochez la case si une tentative de lancement des tâches doit avoir lieu lors du prochain démarrage de l'application sur la machine virtuelle de protection. Pour les modes **Manuel** et **Une fois**, la tâche est lancée directement après l'apparition de la machine virtuelle de protection sur le réseau.

  Si la case est décochée, le lancement de la tâche sur la machine virtuelle de protection aura lieu uniquement selon une programmation et pour les modes **Manuel** et **Une fois**, uniquement sur les machines virtuelles de protection visibles sur le réseau.

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :

  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : 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**. La case est cochée par défaut.

- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment du lancement supposé de la tâche, 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 sera lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment supposé de lancement. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

  L'option de lancement décalé de la tâche permet d'éviter qu'un trop grand nombre de machines virtuelles de protection contacte directement le Serveur d'administration du Kaspersky Security Center.

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

ETAPE 6. FIN DE LA CREATION DE LA TACHE

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

Quittez l'Assistant de création d'une tâche. La tâche d'analyse complète créée apparaît dans la liste des tâches sous l'onglet **Tâches**.

Si vous avez planifié l'exécution d'une tâche d'analyse complète dans la fenêtre **Programmation de l'exécution de la tâche**, cette tâche sera exécutée conformément à la programmation. Vous pouvez également lancer la tâche à n'importe quel moment ou l'arrêter manuellement (cf. section "Lancement et arrêt de l'analyse complète et de l'analyse personnalisée" à la plage 81).

CREATION D'UNE TACHE D'ANALYSE PERSONNALISEE

En cas de remplacement ou de réinstallation de la plateforme du serveur VMware vCenter, aucune tâche d'analyse personnalisée créée antérieurement ne fonctionnera. Il est nécessaire de les supprimer et d'en créer d'autres.

Pour créer une tâche d'analyse personnalisée, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez créer une tâche d'analyse personnalisée.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Lancez l'Assistant de création d'une tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les instructions de l'Assistant de création d'une tâche.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 74

Etape 2. Sélection du type de tâche 74

Etape 3. Connexion au serveur VMware vCenter 74

Etape 4. Sélection de la zone d'action de la tâche 75

Etape 5. Configuration des paramètres de l'analyse....75

Etape 6. Sélection de la zone d'analyse....79

Etape 7. Définition des paramètres de programmation de la tâche....80

Etape 8. Fin de la création de la tâche....80

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche d'analyse personnalisée dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

A cette étape, sélectionnez le type de tâche **Analyse personnalisée** pour l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. CONNEXION AU SERVEUR VMWARE VCENTER

A cette étape, définissez les paramètres de connexion de Kaspersky Security au serveur VMware vCenter :

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet du serveur VMware vCenter auquel la connexion est établie.

- **Nom d'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion au serveur VMware vCenter est établie. Il est recommandé d'indiquer le nom d'un compte utilisateur créé pour utiliser l'application et modifier la configuration des machines virtuelles de protection. Il faut que le rôle système préinstallé ReadOnly soit attribué à ce compte utilisateur.

- **Mot de passe**.

  Mot de passe du compte utilisateur sous lequel la connexion au serveur VMware vCenter est établie.

Si nécessaire, définissez la valeur du paramètre **Enregistrer les paramètres de connexion**.

Activation ou désactivation de l'enregistrement des paramètres de connexion au serveur VMware vCenter.

Si la case est cochée, Kaspersky Security enregistre les derniers paramètres saisis pour la connexion au serveur VMware vCenter indiqué dans le champ **Adresse de VMware vCenter Server** : adresse du serveur VMware vCenter, nom et mot de passe du compte utilisateur. Lors des connexions ultérieures au serveur VMware vCenter, les paramètres enregistrés s'afficheront dans la fenêtre de saisie des paramètres de connexion. Le mot de passe du compte utilisateur est enregistré sous forme chiffrée sur l'ordinateur sur lequel est installée la Console d'administration Kaspersky Security Center.

Si la case est décochée, les paramètres de connexion au serveur VMware vCenter ne sont pas enregistrés.

Si vous décochez la case cochée lors de la connexion précédente au serveur VMware vCenter, les paramètres de connexion précédemment enregistrés sont supprimés par Kaspersky Security.

La case est décochée par défaut.

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

L'Assistant de création d'une tâche vérifiera la possibilité de connexion au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant de création de la tâche le signalera et restera à l'étape actuelle.

L'Assistant de création d'une tâche vérifie le certificat SSL reçu du serveur VMware vCenter. La fenêtre **Vérification du certificat** s'ouvre avec un message d'erreur si le certificat reçu contient une erreur ou s'il n'est pas compatible avec le certificat précédemment installé. Vous pouvez consulter les informations sur le certificat reçu. Pour ce faire, cliquez sur le bouton **Afficher le certificat reçu** dans la fenêtre du message d'erreur.

Vous pouvez installer le certificat reçu en tant que certificat de confiance afin que VMware vCenter ne reçoive pas de message relatif à une erreur de certificat lors de la prochaine connexion à ce serveur VMware. Pour ce faire, cochez la case **Installer le certificat reçu et ne plus afficher les avertissements relatifs au serveur <adresse du serveur VMware vCenter>**. Après que vous avez cliqué sur le bouton **Ignorer**, le certificat est enregistré dans le répertoire du système d'exploitation de l'ordinateur hébergeant la Console d'administration du Kaspersky Security Center, dans la section HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<adresse du serveur>\, où <adresse du serveur> est l'adresse du serveur d'origine du certificat.

Pour maintenir la connexion au serveur VMware vCenter, cliquez sur **Ignorer** dans la fenêtre **Vérification du certificat**.

Si la connexion n'a pas été établie, quittez l'Assistant de création d'une tâche, vérifiez que le serveur VMware vCenter est accessible sur le réseau et recommencez la création de la tâche d'analyse personnalisée.

ETAPE 4. SELECTION DE LA ZONE D'ACTION DE LA TACHE

A cette étape, désignez les machines virtuelles dont vous souhaitez analyser les fichiers.

L'infrastructure virtuelle VMware administrée par un serveur VMware vCenter s'affiche dans le tableau sous la forme d'une arborescence d'objets : serveur VMware vCenter, objets Datacenter, clusters VMware, hyperviseurs VMware ESXi qui ne font pas partie du cluster VMware, pools de ressources, objets vApp et machines virtuelles.

Cochez les cases en regard des machines virtuelles que vous souhaitez analyser pendant l'exécution de la tâche créée.

Si l'infrastructure virtuelle VMware contient deux machines virtuelles ou plus avec un même identifiant (vm-ID), l'arborescence des objets affiche une seule machine virtuelle. Si cette machine virtuelle a été sélectionnée pour l'analyse à l'aide d'une tâche personnalisée, la tâche sera exécutée pour toutes les machines virtuelles qui possèdent le même identifiant (vm-ID).

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

ETAPE 5. CONFIGURATION DES PARAMETRES DE L'ANALYSE

A cette étape, définissez les paramètres d'analyse des machines virtuelles.

Pour définir les paramètres d'analyse des machines virtuelles, procédez comme suit :

1. Dans le groupe **Niveau de sécurité**, effectuez l'une des actions suivantes :

   - Si vous souhaitez utiliser l'un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.

   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.

   - Si vous souhaitez configurer vous-même le niveau de protection, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Paramètres du niveau de sécurité** :

   a. Dans le groupe **Analyse des archives et des fichiers composés**, définissez les paramètres suivants :

      - **Analyser les archives**.

        Activation ou désactivation de l'analyse des archives.

        La case est décochée par défaut.

- **Supprimer les archives en cas d'échec de la réparation**.

  Suppression des archives dont la réparation est impossible.

  Si la case est cochée, Kaspersky Security supprime les archives dont la réparation a échoué.

  Si la case est décochée, l'application ne supprime pas les archives qui n'ont pu être réparées. Kaspersky Security signale au Serveur d'administration du Kaspersky Security Center que le fichier infecté n'a pas été supprimé.

  La case est accessible si la case **Analyser les archives** est cochée.

  La case est décochée par défaut.

- **Analyser les archives autoextractibles**.

  Activation/désactivation de l'analyse des archives autoextractibles.

  Par défaut, la case pour les profils de protection est décochée et la case pour les tâches d'analyse est cochée.

- **Analyser les objets OLE intégrés**.

  Activation ou désactivation de l'analyse des objets intégrés à un fichier.

  La case est cochée par défaut.

- **Ne pas décompacter les fichiers composés de grande taille**.

  Quand la case est cochée, Kaspersky Security n'analyse pas les fichiers composés dont la taille dépasse la valeur du champ **Taille maximale du fichier composé à analyser**.

  Si la case est décochée, Kaspersky Security analyse les fichiers composés de toutes les tailles.

  Kaspersky Security analyse les fichiers de grande taille extraits des archives, quel que soit l'état de la case **Ne pas décompacter les fichiers composés de grande taille**.

  La case est cochée par défaut.

- **Taille maximale du fichier composé à analyser X Mo**.

  Taille maximale des fichiers composés pouvant être analysés (en mégaoctets). Kaspersky Security ne décompacte pas et n'analyse pas les objets dont la taille est supérieure à la valeur indiquée.

  Le paramètre ne peut être modifié si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

  La valeur par défaut est de 8 Mo.

b. Dans le groupe **Productivité**, définissez les paramètres suivants :

- **Limiter la durée d'analyse des fichiers**.

  Si la case est cochée, Kaspersky Security interrompt l'analyse si la durée de celle-ci atteint la valeur définie dans le champ **Ne pas analyser les fichiers pendant plus de X seconde(s)** et ignore ce fichier.

  Si la case est décochée, Kaspersky Security ne limite pas la durée de l'analyse des fichiers.

  Par défaut, la case pour les profils de protection est cochée et la case pour les tâches d'analyse est décochée.

- **Ne pas analyser les fichiers pendant plus de X seconde(s)**.

  Durée maximale de l'analyse du fichier (en secondes). Kaspersky Security interrompt l'analyse du fichier quand sa durée atteint la valeur définie pour ce paramètre.

  Le paramètre ne peut être modifié si la case **Limiter la durée d'analyse des fichiers** est cochée.

  La valeur par défaut est de 60 secondes.

c. Dans le groupe **Objets à détecter**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à détecter** qui apparaît :

- **Utilitaires malveillants**.

  Activation/désactivation de la protection contre les utilitaires malveillants.

Les *utilitaires malveillants* n'exécutent pas d'actions malveillantes dès le lancement et peuvent être conservés et exécutés sur l'ordinateur de l'utilisateur sans présenter de risque. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants ou exécuter d'autres actions malveillantes.

Si la case est cochée, la protection contre les utilitaires malveillants est activée.

Si la case est décochée, la protection contre les utilitaires malveillants est désactivée.

La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation/désactivation de la protection contre les programmes publicitaires.

  Les *programmes publicitaires* permettent de montrer des publicités aux utilisateurs. Par exemple, ils affichent des bandeaux publicitaires dans l'interface d'autres programmes ou réorientent les demandes de recherche vers des pages publicitaires. Certains d'entre eux recueillent également des informations marketing sur l'utilisateur qu'ils renvoient à l'auteur : catégories de sites Internet visités, mots-clés utilisés dans les recherches, etc. A la différence des chevaux de Troie espions, ils transmettent ces informations avec l'autorisation de l'utilisateur.

  Si la case est cochée, la protection contre les logiciels publicitaires est activée.

  Si la case est décochée, la protection contre les logiciels publicitaires est désactivée.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation/désactivation de la protection contre les programmes numéroteurs.

  Si la case est cochée, la protection contre les programmes numéroteurs est activée.

  Si la case est décochée, la protection contre les programmes numéroteurs est désactivée.

  La case est cochée par défaut.

- **Autres**.

  Activation/désactivation de la protection d'autres applications légitimes qui peuvent être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

  La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi elles figurent les clients IRC, les programmes pour le chargement des fichiers, les applications d'administration à distance, les dispositifs de suivi de l'activité de l'utilisateur, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet. Toutefois, si des individus malintentionnés obtiennent l'accès à ces applications ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leurs fonctions pour nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  Si la case est décochée, la protection contre ces programmes est désactivée.

  La case est décochée par défaut.

- **Fichiers compactés plusieurs fois**.

  Exclusion ou inclusion de l'analyse des fichiers compactés à trois reprises au moins par un ou plusieurs compacteurs.

  Si le fichier a été compacté plus de trois fois par un ou plusieurs compacteurs, il s'agit vraisemblablement d'un fichier qui contient une application malveillante ou un programme permettant à des individus malintentionnés de nuire à l'ordinateur ou aux données de l'utilisateur.

  Si la case est cochée, la protection contre les fichiers compactés à plusieurs reprises est activée et l'analyse de ce type de fichier est autorisée.

  Si la case est décochée, la protection contre les fichiers compressés à plusieurs reprises est désactivée.

  La case est cochée par défaut.

Kaspersky Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans les fichiers des machines virtuelles. C'est pourquoi les paramètres **Virus et vers** et **Chevaux de Troie** du groupe **Applications malveillantes** ne peuvent pas être modifiés.

d. Cliquez sur le bouton **OK** dans la fenêtre **Objets à détecter**.

e. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du niveau de sécurité**.

Si vous avez modifié les paramètres du niveau de protection, l'application créera un niveau utilisateur de protection. Le nom du niveau de protection dans le groupe **Niveau de sécurité** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action exécutée en cas de détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection de fichiers infectés :

- **Sélectionner l'action automatiquement**.

  Kaspersky Security exécute l'action définie par défaut par les experts de Kaspersky Lab. Il s'agit de **Réparer. Supprimer si la réparation est impossible**.

  Cette option est sélectionnée par défaut.

- **Réparer. Supprimer si la réparation est impossible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, l'application supprime ces fichiers. Kaspersky Security supprime les archives infectées qui n'ont pas pu être réparées uniquement si la case **Supprimer les archives en cas d'échec de la réparation** est cochée dans les paramètres du niveau de protection.

- **Réparer. Bloquer si la réparation n'est pas possible**.

  Kaspersky Security tente automatiquement de réparer les fichiers infectés. Si la réparation est impossible, Kaspersky Security bloque ces fichiers.

- **Supprimer. Bloquer si la suppression n'est pas possible**.

  Kaspersky Security supprime automatiquement les fichiers infectés, sans tenter de les réparer. Si la suppression est impossible, Kaspersky Security bloque ces fichiers.

- **Bloquer**.

  Kaspersky Security bloque automatiquement les fichiers infectés, sans tenter de les réparer.

3. Si vous souhaitez que Kaspersky Security analyse les fichiers sur les disques amovibles, cochez la case **Analyser les disques amovibles** dans le groupe **Disques amovibles**.

Si la case **Analyser les disques amovibles** est cochée mais qu'aucun chemin d'accès à un disque amovible n'est inclus dans la zone d'analyse de la tâche, Kaspersky Security n'analyse aucun disque amovible.

4. Dans la fenêtre **Arrêter l'analyse**, sélectionnez une des options suivantes :

- **Au bout de X minutes après le lancement de l'analyse**.

  Durée maximale d'exécution de la tâche d'analyse (en minutes). A l'issue de ce délai, l'exécution de la tâche d'analyse est interrompue même si l'analyse n'est pas terminée.

  Cette option est sélectionnée par défaut, avec la valeur 120 minutes.

- **A la fin de l'analyse des fichiers sur toutes les machines virtuelles protégées allumées au moment du lancement de la tâche**.

  La tâche d'analyse complète est exécutée jusqu'à ce que les fichiers de toutes les machines virtuelles protégées qui étaient actives au moment du lancement de la tâche aient été analysés.

  La tâche d'analyse personnalisée est exécutée jusqu'à ce que les fichiers de toutes les machines virtuelles protégées de la zone d'action de la tâche qui étaient actives au moment du lancement de la tâche aient été analysés.

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

ETAPE 6. SELECTION DE LA ZONE D'ANALYSE

Définissez la zone d'analyse au cours de cette étape. La zone d'analyse désigne l'emplacement et l'extension des fichiers des machines virtuelles (par exemple, tous les disques durs, les objets de démarrage, les bases de messagerie) analysés par Kaspersky Security pendant l'exécution de la tâche de vérification.

Choisissez l'une des options suivantes :

- **Analyser tous les dossiers et fichiers, sauf ceux indiqués**. Composez la liste des objets à exclure de la zone d'analyse à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Vous pouvez exclure de la zone d'analyse les objets des types suivants :

  - Dossiers. Les fichiers des dossiers situés aux emplacements indiqués sont exclus de la zone d'analyse. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure ses sous-répertoires de la zone d'analyse.

  - Les fichiers selon un masque. Sont exclus de la zone d'analyse : les fichiers possédant le nom indiqué, les fichiers situés à l'emplacement indiqué ou les fichiers correspondant au masque indiqué.

    Les caractères `*` et `?` peuvent être utilisés dans la création d'un masque de fichier.

  Vous pouvez conserver la liste d'objets à exclure dans un fichier à l'aide du bouton **Exportation** et télécharger la liste des objets à exclure précédemment enregistrée à l'aide du bouton **Importation**.

  La distribution de l'application comprend le fichier microsoft_file_exclusions.xml. Ce fichier reprend la liste des objets dont l'exclusion a été conseillée par Microsoft (la liste des exclusions conseillées par Microsoft se trouve sur le site de Microsoft). Le fichier microsoft_file_exclusions.xml se trouve dans le dossier d'installation du plug-in d'administration de Kaspersky Security, sur l'ordinateur où est installée la Console d'administration du Kaspersky Security Center. Vous pouvez importer ce fichier dans les exclusions de la tâche d'analyse. Ainsi, Kaspersky Security n'analysera pas les objets conseillés par Microsoft lors de l'exécution de la tâche d'analyse. A l'issue de l'importation, vous pouvez consulter et modifier la liste de ces objets dans le tableau **Dossiers et fichiers**.

  L'utilisation de variables d'environnement n'est pas prise en charge dans la liste des exclusions. L'objet du système de fichiers défini via des variables d'environnement ne sera pas exclu de la zone d'analyse.

  Dans le groupe **Extensions des fichiers**, indiquez les extensions de fichiers que vous souhaitez inclure dans la zone d'analyse ou exclure de celle-ci. Pour ce faire, sélectionner une des options suivantes :

  - **Analyser tout, sauf les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à ne pas analyser dans le cadre de l'exécution de la tâche d'analyse.

  - **Analyser uniquement les fichiers avec les extensions suivantes**. Dans le champ de saisie, indiquez la liste des extensions de fichiers à analyser dans le cadre de l'exécution de la tâche d'analyse.

    Vous pouvez séparer les extensions de fichier par un espace ou un saut de ligne. Lorsque vous indiquez les extensions de fichiers, vous pouvez utiliser n'importe quel caractère sauf `* | \ : " < > ? /`. Si le caractère "espace" est utilisé dans l'extension, il est nécessaire d'indiquer cette extension entre guillemets, par exemple : `"doc x"`.

    Si vous aviez choisi l'option **Analyser uniquement les fichiers avec les extensions suivantes** dans la liste déroulante, sans renseigner les extensions de fichier à analyser, Kaspersky Security analyse tous les fichiers.

  Les dossiers exclus de l'analyse présentent une priorité supérieure à celle des extensions de fichiers incluses dans la zone d'analyse. Si un fichier figure dans un dossier exclu de l'analyse, il ne sera pas analysé, même si son extension fait partie des extensions à analyser.

- **Analyser uniquement les dossiers et fichiers indiqués**. Les boutons **Ajouter**, **Modifier** et **Supprimer** permettent de composer la liste des dossiers et des fichiers de la machine virtuelle qu'il est nécessaire d'analyser.

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

ETAPE 7. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de la tâche d'analyse personnalisée :

- **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.

- **Lancement des tâches ignorées**. Cochez la case si une tentative de lancement de la tâche ignorée doit avoir lieu lors du prochain démarrage de l'application sur la machine virtuelle de protection. Pour les modes **Manuel** et **Une fois**, la tâche est lancée directement après l'apparition de la machine virtuelle de protection sur le réseau.

  Si la case est décochée, le lancement de la tâche sur la machine virtuelle de protection aura lieu uniquement selon une programmation et pour les modes **Manuel** et **Une fois**, uniquement sur les machines virtuelles de protection visibles sur le réseau.

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :

  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : 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**. La case est cochée par défaut.

- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment du lancement supposé de la tâche, 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 sera lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment supposé de lancement. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

  L'option de lancement décalé de la tâche permet d'éviter qu'un trop grand nombre de machines virtuelles de protection contacte directement le Serveur d'administration du Kaspersky Security Center.

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

ETAPE 8. FIN DE LA CREATION DE LA TACHE

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

Quittez l'Assistant de création d'une tâche. La tâche d'analyse créée apparaît dans la liste des tâches sous l'onglet **Tâches**.

Si vous avez défini dans la fenêtre **Programmation de l'exécution de la tâche** une planification pour l'exécution de la tâche d'analyse personnalisée, cette tâche sera exécutée conformément à la programmation. Vous pouvez également lancer la tâche à n'importe quel moment ou l'arrêter manuellement (cf. section " Lancement et arrêt de l'analyse complète et de l'analyse personnalisée " à la plage 81).

LANCEMENT ET ARRET DE L'ANALYSE COMPLETE ET DE L'ANALYSE PERSONNALISEE

Quel que soit le mode de lancement choisi pour l'analyse complète ou personnalisée, vous pouvez lancer ou arrêter les tâches à tout moment.

Pour lancer ou arrêter l'analyse complète ou personnalisée, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Exécutez une des actions suivantes :
   - Si vous souhaitez lancer ou arrêter une tâche d'analyse créée pour les machines virtuelles de protection de tous les clusters KSC, sélectionnez le dossier **Ordinateurs administrés** dans l'arborescence de la console.
   - Si vous souhaitez lancer ou arrêter une tâche d'analyse créée pour les machines virtuelles de protection d'un seul cluster KSC, dans le dossier **Ordinateurs administrés**, sélectionnez le dossier au nom de ce cluster.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des tâches, sélectionnez la tâche que vous souhaitez lancer ou arrêter.
5. Lancez ou arrêtez l'exécution de la tâche à l'aide du bouton **Lancer** ou **Arrêter** dans le groupe **Exécution d'une tâche**.

Vous pouvez consulter les informations sur le déroulement et les résultats de l'exécution des tâches dans la Console d'administration de Kaspersky Security Center d'une des manières suivantes :

- Dans la fenêtre **Résultats de l'exécution de la tâche**. Pour ouvrir la fenêtre, cliquez sur le bouton **Consulter les résultats** situé à droite de la liste des tâches, sous l'onglet **Tâches**.
- Dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les machines virtuelles de protection. La liste des événements apparaît dans le dossier **Rapports et notifications/Evénements** de l'arborescence de la Console d'administration du Kaspersky Security Center.

DETECTION DES INTRUSIONS

Cette section contient des informations sur la configuration des paramètres du module de Détection des intrusions.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des intrusions.

DANS CETTE SECTION

Concernant la protection des machines virtuelles contre les menaces réseau 82

Activation et désactivation de la détection des attaques réseau 83

Configuration des paramètres de blocage des adresses IP à l'origine d'une attaque réseau 83

Activation et désactivation de l'analyse des adresses Internet 84

Configuration des paramètres d'analyse des adresses Internet 85

Configuration du message de blocage de l'adresse Internet 86

CONCERNANT LA PROTECTION DES MACHINES VIRTUELLES CONTRE LES MENACES RESEAU

Le module Détection des intrusions de Kaspersky Security permet de suivre, dans le trafic réseau, les machines virtuelles dont l'activité est caractéristique des attaques réseau. Il confronte également l'adresse Internet sollicitée par l'utilisateur à une base d'adresses Internet malveillantes.

La machine virtuelle de protection dotée du module Détection des intrusions et installée sur un hyperviseur VMware ESXi protège toutes les machines virtuelles présentes sur cet hyperviseur.

Si vous souhaitez protéger les machines virtuelles contre les intrusions : après l'installation du module Détection des intrusions, il convient d'activer la détection des attaques réseau (cf. section "Activation et désactivation de la détection des attaques réseau" page 83) et l'analyse des adresses Internet (cf. section "Activation et désactivation de l'analyse des adresses Internet" page 84) dans les paramètres de la stratégie. Par défaut, Kaspersky Security ne détecte pas les intrusions et n'analyse pas les adresses Internet.

Si la détection des attaques réseau est activée, à savoir celle qui détecte les attaques réseau contre la machine virtuelle, Kaspersky Security peut bloquer l'adresse IP à l'origine de l'attaque pendant la durée indiquée afin de protéger automatiquement la machine virtuelle de futures attaques réseau éventuelles en provenance de cette adresse. Vous pouvez modifier les paramètres de blocage de l'adresse IP à l'origine de l'attaque réseau (cf. section "Configuration des paramètres de blocage des adresses IP à l'origine d'une attaque réseau" à la page 83).

Vous pouvez composer une liste des adresses IP que Kaspersky Security ne doit pas bloquer en cas de détection d'une activité caractéristique d'une attaque réseau.

Si l'analyse des adresses Internet est activée, Kaspersky Security confronte chaque adresse Internet ou certaines applications HTTP sollicitées par l'utilisateur à une base d'adresses Internet malveillantes :

- Si l'adresse Internet ne figure pas dans la base des URL malveillantes, Kaspersky Security autorise l'accès à cette adresse Internet.
- Si l'adresse Internet figure dans la base des adresses Internet malveillantes, l'application exécute l'action définie dans les paramètres Kaspersky Security (cf. section "Configuration des paramètres d'analyse des adresses Internet" à la page 85). Par exemple, elle bloque ou autorise l'accès à cette URL.

Si l'application Kaspersky Security bloque l'adresse Internet sollicitée par l'utilisateur ou une application, le navigateur de la machine virtuelle protégée affiche un message de blocage (cf. section "Configuration du message de blocage de l'adresse Internet" à la page 86).

Vous pouvez composer une liste des adresses Internet auxquelles l'accès ne doit pas être bloqué par Kaspersky Security si elles apparaissent dans la base des adresses Internet malveillantes, quelles que soient les actions paramétrées.

Les informations relatives aux événements survenus pendant la protection des machines virtuelles sont transmises au Serveur d'administration du Kaspersky Security Center et consignées dans un rapport (cf. section "Types de rapports" à la page 99).

La description des types connus d'intrusions, des méthodes de lutte contre ces attaques et de la base des adresses Internet malveillantes figurent dans les bases antivirus. La liste des intrusions détectées par le module Détection des intrusions et la base des adresses Internet malveillantes s'enrichissent au cours de la procédure de mise à jour des bases antivirus (cf. section "A propos de la mise à jour des bases", à la page 91).

ACTIVATION ET DESACTIVATION DE LA DETECTION DES ATTAQUES RESEAU

Pour activer ou désactiver la fonction de détection des attaques réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Détection des attaques réseau**.
6. Exécutez une des actions suivantes :
   - Cochez la case **Détecter les attaques réseau**, si vous souhaitez que Kaspersky Security détecte, dans le trafic des machines virtuelles protégées, les activités caractéristiques des attaques réseau.
   - Décochez la case **Détecter les attaques réseau**, si vous souhaitez que Kaspersky Security ne contrôle pas le trafic des machines virtuelles protégées dans le but de repérer les activités caractéristiques des attaques réseau.
7. Cliquez sur le bouton **OK**.

CONFIGURATION DES PARAMETRES DE BLOCAGE DES ADRESSES IP A L'ORIGINE D'UNE ATTAQUE RESEAU

Si la détection des attaques réseau est activée, par défaut, lors de la détection d'une attaque réseau, Kaspersky Security bloque l'adresse IP à l'origine de l'attaque réseau pendant 60 minutes. Vous pouvez désactiver le blocage des adresses IP, modifier la durée du blocage ou composer une liste des adresses IP que Kaspersky Security ne doit pas bloquer en cas de détection d'une attaque réseau via ces adresses IP.

Pour configurer les paramètres de blocage des adresses IP à l'origine de l'attaque réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.

3. Dans la zone de travail, choisissez l'onglet **Stratégies**.

4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.

5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Détection des attaques réseau**.

6. Définissez le paramètre **En cas d'attaque réseau, bloquer l'adresse IP pendant X minutes**.

   Activation ou désactivation du blocage de l'adresse IP à l'origine d'une attaque réseau.

   Si cette case est cochée, en cas de tentative d'attaque réseau, Kaspersky Security bloque l'adresse IP à l'origine de l'attaque pendant la durée indiquée afin de protéger automatiquement la machine virtuelle contre d'éventuelles attaques réseau en provenance de cette adresse IP.

   Si cette case n'est pas cochée, en cas de tentative d'attaque réseau, l'application ne déclenche pas automatiquement la protection contre d'éventuelles futures attaques réseau en provenance de cette adresse IP.

   La case est accessible si la case **Détecter les attaques réseau** est cochée.

   La valeur par défaut est de 60 minutes.

7. Si la case **En cas de détection d'une attaque réseau, bloquer l'adresse IP pendant X minutes** est cochée, indiquez la durée du blocage de l'adresse IP dans le champ situé à droite de la case.

8. Dans le tableau **Ne pas bloquer les adresses IP suivantes**, indiquez les adresses IP qui ne doivent pas être bloquées en cas de détection d'une attaque réseau via ces adresses IP. Pour ajouter une adresse IP au tableau, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter** ou pressez la touche **INSERT**.

   b. Entrez l'adresse IP au format IPv4 dans la colonne **Adresse IP**.

   c. Le cas échéant, entrez la description de l'adresse IP dans la colonne **Commentaires**.

   Après la saisie de l'adresse IP dans le tableau **Ne pas bloquer les adresses IP suivantes**, Kaspersky Security annule le blocage de l'adresse IP si cette dernière avait déjà été bloquée.

9. Cliquez sur le bouton **OK**.

ACTIVATION ET DESACTIVATION DE L'ANALYSE DES ADRESSES INTERNET

Pour activer ou désactiver l'analyse des adresses Internet, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.

3. Dans la zone de travail, choisissez l'onglet **Stratégies**.

4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.

5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Analyse des adresses Internet**.

6. Exécutez une des actions suivantes :

   - Cochez la case **Analyser l'adresse Internet sur la base des adresses Internet malveillantes**, si vous souhaitez que Kaspersky Security confronte une adresse Internet à la base des adresses Internet malveillantes.

- Décochez la case **Analyser l'adresse Internet sur la base des adresses Internet malveillantes**, si vous souhaitez que Kaspersky Security ne confronte pas les adresses Internet à la base des adresses Internet malveillantes.

7. Cliquez sur le bouton **OK**.

CONFIGURATION DES PARAMETRES D'ANALYSE DES ADRESSES INTERNET

Si l'analyse des adresses Internet est activée et qu'une adresse Internet ou une application sollicitée par l'utilisateur est détectée dans la base des adresses Internet malveillantes, Kaspersky Security bloque par défaut l'accès à cette URL. Vous pouvez modifier l'action par défaut ou composer une liste des adresses Internet auxquelles l'accès ne sera pas bloqué par Kaspersky Security si elles apparaissent dans la base des adresses Internet malveillantes.

Pour modifier les paramètres d'analyse des adresses Internet, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.

3. Dans la zone de travail, choisissez l'onglet **Stratégies**.

4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.

5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Analyse des adresses Internet**.

6. Dans le groupe **Action exécutée en cas de détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection d'une adresse Internet dans la base des adresses Internet malveillantes :

   - **Sélectionner l'action automatiquement**.

     Si Kaspersky Security détecte une adresse Internet qui figure dans la base des adresses Internet malveillantes, il exécute l'action définie par défaut par les spécialistes de Kaspersky Lab. Il s'agit de **Bloquer**.

     Cette option est sélectionnée par défaut.

   - **Bloquer**.

     Kaspersky Security bloque l'accès à toute URL reprise dans la base des adresses Internet malveillantes.

   - **Ignorer**.

     Kaspersky Security autorise l'accès à toute URL reprise dans la base des adresses Internet malveillantes.

7. Dans le tableau **Ne pas bloquer les adresses Internet suivantes** indiquez les adresses Internet auxquelles l'accès ne doit pas être bloqué si ces dernières apparaissent dans la base des adresses Internet malveillantes. Pour ajouter une adresse Internet au tableau, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter** ou pressez la touche **INSERT**.

   b. Entrez l'adresse Internet dans la colonne **Adresse Internet**.

8. Cliquez sur le bouton **OK**.

CONFIGURATION DU MESSAGE DE BLOCAGE DE L'ADRESSE INTERNET

En cas de blocage de l'adresse Internet sollicitée par l'utilisateur ou une application, Kaspersky Security affiche un message de blocage dans le navigateur de la machine virtuelle protégée. Vous pouvez consulter un exemple de message de blocage d'adresses Internet et en sélectionner la langue.

Pour sélectionner la langue du message de blocage de l'adresse Internet et consulter un exemple de message, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Etc.**
6. Cliquez sur le lien **Consulter un exemple de message** pour ouvrir un exemple de message de blocage de l'adresse Internet qui s'affiche dans le navigateur de la machine virtuelle protégée.

   L'exemple de message s'ouvre dans une nouvelle fenêtre.
7. Dans le groupe **Configuration de la géolocalisation**, cliquez sur la liste déroulante **Langue du message relatif au blocage de l'adresse Internet** pour sélectionner la langue du message de blocage de l'adresse Internet.

   Par défaut, la langue sélectionnée est celle qui correspond à la géolocalisation du plug-in d'administration de Kaspersky Security.
8. Cliquez sur le bouton **OK**.

SAUVEGARDE

Cette section présente la sauvegarde et explique comment la manipuler.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Anti-Virus Fichiers.

DANS CETTE SECTION

A propos de la sauvegarde 87

Configuration des paramètres de la sauvegarde 88

Manipulation des copies de sauvegarde des fichiers 88

A PROPOS DE LA SAUVEGARDE

La *sauvegarde* est un emplacement spécial qui héberge une copie de sauvegarde de tous les fichiers qui ont été supprimés ou modifiés durant la réparation.

La *copie de sauvegarde d'un fichier* est la copie d'un fichier de la machine virtuelle qui a été créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde sont conservées dans la sauvegarde sous un format spécial et ne présentent aucun danger.

Lorsque l'application Kaspersky Security détecte un fichier infecté, elle bloque l'accès de l'utilisateur de la machine virtuelle, puis place la copie du fichier dans la sauvegarde. Ensuite, l'application exécute sur le fichier l'action définie dans le profil de protection de cette machine virtuelle, par exemple le répare ou le supprime.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la réparation. Si le fichier réparé contenait des informations qui sont devenues entièrement ou partiellement inaccessibles après la réparation, vous pouvez conserver le fichier de la copie de sauvegarde sur le disque dur de l'ordinateur où la Console d'administration du Kaspersky Security Center est installée.

La sauvegarde est située sur la machine virtuelle de protection dotée du module Antivirus Fichiers. L'utilisation de la sauvegarde est activée par défaut sur chaque machine virtuelle de protection.

Le volume réservé à la sauvegarde sur la machine virtuelle de protection est de 1 Go. Si le volume total des copies de fichiers de la sauvegarde dépasse cette valeur, l'application Kaspersky Security supprime les copies de sauvegarde des fichiers les plus anciennes afin de maintenir un volume de données égal à 1 Go.

Par défaut, les copies de sauvegarde des fichiers sont conservées 30 jours maximum. A l'issue de ce délai, Kaspersky Security supprime automatiquement les copies de sauvegarde des fichiers de la sauvegarde.

Vous pouvez modifier la durée maximale de conservation des copies de sauvegarde des fichiers. Les paramètres de la sauvegarde sont repris dans les paramètres de la stratégie pour toutes les machines virtuelles de protection d'un cluster KSC (cf. section "Configuration des paramètres de la sauvegarde" page 88).

Vous pouvez manipuler les copies de sauvegarde des fichiers qui se trouvent dans les sauvegardes des machines virtuelles de protection, dans la Console d'administration du Kaspersky Security Center. La Console d'administration du Kaspersky Security Center propose la liste complète des copies de sauvegarde des fichiers placés par Kaspersky Security dans la sauvegarde pour chacune des machines virtuelles de protection dotées du module Antivirus Fichiers.

CONFIGURATION DES PARAMETRES DE LA SAUVEGARDE

Pour modifier les paramètres de la sauvegarde, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Sauvegarde**.
6. Dans la partie droite de la fenêtre, définissez les paramètres suivants :
   - **Placer les fichiers dans la sauvegarde**.

     Utilisation de la sauvegarde sur les machines virtuelles de protection équipées du module Antivirus Fichiers dans un cluster KSC.

     Si la case est cochée, Kaspersky Security place la copie de sauvegarde du fichier dans la sauvegarde avant de le réparer ou de le supprimer.

     Si la case est décochée, Kaspersky Security ne place pas la copie de sauvegarde du fichier dans la sauvegarde avant de le réparer ou de le supprimer.

     La case est cochée par défaut.

     Si vous avez utilisé la sauvegarde, puis décoché cette case, les copies de sauvegarde qui se trouvaient déjà dans la sauvegarde y restent. Ces copies de sauvegarde seront supprimées en fonction de la valeur du paramètre **Ne pas conserver les fichiers plus de X jours**.

   - **Ne pas conserver les fichiers plus de X jours**.

     Durée de conservation des copies de sauvegarde dans la sauvegarde. A l'issue de ce délai, Kaspersky Security supprime automatiquement les copies de sauvegarde des fichiers de la sauvegarde.

     Le paramètre peut être modifié si la case **Placer les fichiers dans la sauvegarde** est cochée.

     La valeur par défaut est de 30 jours.

     Si vous réduisez la durée de conservation des copies de sauvegarde des fichiers, Kaspersky Security supprime pendant un jour les copies qui se trouvent dans la sauvegarde depuis plus longtemps que la nouvelle valeur.
7. Cliquez sur le bouton **OK**.

MANIPULATION DES COPIES DE SAUVEGARDE DES FICHIERS

Vous pouvez exécuter les actions suivantes sur les copies de sauvegarde des fichiers :

- consulter la liste des copies de sauvegarde des fichiers ;
- enregistrer les fichiers depuis les copies de sauvegarde vers le disque dur de l'ordinateur sur lequel est installée la Console d'administration du Kaspersky Security Center ;
- supprimer les copies de sauvegarde des fichiers de la sauvegarde.

DANS CETTE SECTION

Consultation de la liste des copies de sauvegarde des fichiers 89

Enregistrement des fichiers de la sauvegarde sur le disque 89

Suppression des copies de sauvegarde des fichiers 90

CONSULTATION DE LA LISTE DES COPIES DE SAUVEGARDE DES FICHIERS

Pour consulter la liste des copies de sauvegarde des fichiers, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Stockages**, puis le dossier **Sauvegarde**.

   La zone de travail affiche la liste des copies de sauvegarde placées dans la sauvegarde sur toutes les machines virtuelles de protection.

   La liste des copies de sauvegarde des fichiers se présente sous la forme d'un tableau. Chaque ligne du tableau contient l'événement survenu avec le fichier infecté et des informations relatives à l'objet détecté dans le fichier.

   Les colonnes du tableau reprennent les informations suivantes :

   - **Ordinateur** : nom de la machine virtuelle de protection sur laquelle se trouve la sauvegarde.
   - **Nom** : nom du fichier.
   - **Etat** : indique l'état attribué par Kaspersky Security au fichier détecté : *Infecté*.
   - **Action exécutable** : action que l'application exécute actuellement sur la copie de sauvegarde du fichier dans la sauvegarde. Par exemple, si vous avez commandé de supprimer la copie de sauvegarde du fichier, cette colonne affiche *En cours de suppression*. Si l'application n'exécute pas d'actions sur cette copie de sauvegarde du fichier, ce champ est vide.
   - **Date de placement** : date et heure de placement de la copie de sauvegarde du fichier dans la sauvegarde.
   - **Objet** : nom de l'objet détecté dans le fichier. Si plusieurs objets sont détectés dans le fichier, la liste des copies de sauvegarde des fichiers consacre une ligne à chaque objet.
   - **Taille** : taille du fichier en octets.
   - **Dossier de restauration** : chemin complet vers le fichier d'origine sur la machine virtuelle.
   - **Description** : nom de la machine virtuelle et chemin complet vers le fichier d'origine dont la copie de sauvegarde est placée dans la sauvegarde.

ENREGISTREMENT DES FICHIERS DE LA SAUVEGARDE SUR LE DISQUE

Vous pouvez enregistrer les fichiers depuis la sauvegarde vers le disque dur de l'ordinateur sur lequel est installée la Console d'administration du Kaspersky Security Center.

Pour enregistrer les fichiers depuis la sauvegarde sur le disque, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Stockages**, puis le dossier **Sauvegarde**.

   La zone de travail affiche la liste des copies de sauvegarde placées dans la sauvegarde sur toutes les machines virtuelles de protection.
3. Dans la liste des copies de sauvegarde des fichiers, sélectionnez les fichiers que vous souhaitez enregistrer sur le disque. Utilisez les touches **CTRL** et **SHIFT** pour sélectionner plusieurs fichiers.
4. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Enregistrer sur le disque**.
   - Enregistrez les fichiers à l'aide du lien **Enregistrer sur le disque**. Le lien se trouve dans le groupe de manipulation des fichiers sélectionnés, à droite de la liste des copies de sauvegarde des fichiers.

     La fenêtre de sélection du dossier sur le disque dur s'ouvre. Les fichiers à conserver doivent être placés dans ce dossier.
5. Sélectionnez le dossier sur le disque dur de l'ordinateur dans lequel vous souhaitez enregistrer les fichiers.
6. Cliquez sur le bouton **OK**.

Kaspersky Security enregistre les fichiers que vous avez indiqués sur le disque dur de l'ordinateur sur lequel est installée la Console d'administration du Kaspersky Security Center.

Les fichiers sont conservés en mode non chiffré sur le disque dur de l'ordinateur où la Console d'administration du Kaspersky Security Center est installée.

SUPPRESSION DES COPIES DE SAUVEGARDE DES FICHIERS

Pour supprimer les copies de sauvegarde des fichiers, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez le dossier **Stockages**, puis le dossier **Sauvegarde**.

   La zone de travail affiche la liste des copies de sauvegarde placées dans la sauvegarde sur toutes les machines virtuelles de protection.
3. Dans la liste des copies de sauvegarde des fichiers, sélectionnez les fichiers que vous souhaitez supprimer. Utilisez les touches **CTRL** et **SHIFT** pour sélectionner plusieurs fichiers.
4. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer**.
   - Supprimez les fichiers à l'aide du lien **Supprimer les objets**. Le lien se trouve dans le groupe de manipulation des fichiers sélectionnés, à droite de la liste des copies de sauvegarde des fichiers.

Kaspersky Security supprime les copies de sauvegarde des fichiers des sauvegardes se trouvant sur les machines virtuelles de protection. A l'aide du lien **Actualiser**, vous pouvez mettre à jour la liste des copies de sauvegarde des fichiers pour voir les modifications dans la liste.

La mise à jour de la liste des copies de sauvegarde des fichiers peut prendre quelques minutes. Veuillez patienter jusqu'à la fin de l'opération.

MISE A JOUR DES BASES ANTIVIRUS

Cette section contient des informations sur la mise à jour des bases (ci-après mises à jour) et des instructions sur la configuration des paramètres de mise à jour.

DANS CETTE SECTION

A propos de la mise à jour des bases antivirus 91

Récupération automatique des mises à jour des bases antivirus 91

Remise à l'état antérieur à la dernière mise à jour.....94

A PROPOS DE LA MISE A JOUR DES BASES ANTIVIRUS

La mise à jour des bases antivirus garantit l'actualité de la protection des machines virtuelles. Chaque jour, de nouveaux virus et autres applications dangereuses apparaissent dans le monde. Les bases contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour que Kaspersky Security puisse détecter à temps les nouvelles menaces, il est nécessaire de mettre à jour les bases anti-virus à intervalle régulier.

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

La *source de mises à jour* est une ressource qui contient les mises à jour des bases et des modules 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.

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

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

RECUPERATION AUTOMATIQUE DES MISES A JOUR DES BASES ANTIVIRUS

Le Kaspersky Security Center permet de diffuser et d'installer automatiquement les mises à jour des bases antivirus sur les machines virtuelles de protection. Pour ce faire, il est nécessaire d'utiliser les tâches suivantes :

- **Tâche de téléchargement des mises à jour dans le stockage**. La tâche permet de télécharger le paquet de mises à jour depuis la source de mises à jour pour le Kaspersky Security Center, dans le stockage du Serveur d'administration. La tâche de téléchargement des mises à jour dans le stockage est créée automatiquement lors de l'utilisation de l'Assistant de configuration initiale du Kaspersky Security Center. La tâche de téléchargement des mises à jour dans le stockage peut être créée en un exemplaire unique. Par conséquent, vous pouvez créer une tâche de téléchargement des mises à jour dans le stockage uniquement si elle a été supprimée de la liste des tâches du Serveur d'administration. Pour plus d'informations, consultez la documentation du Kaspersky Security Center.

- **Tâche de diffusion des mises à jour**. La tâche permet de diffuser et d'installer les mises à jour des bases antivirus sur les machines virtuelles de protection directement après le téléchargement des mises à jour dans le stockage du Serveur d'administration.

Pour configurer la récupération automatique des mises à jour des bases antivirus, 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 du Kaspersky Security Center).

2. Créez une tâche de diffusion des mises à jour pour chaque cluster KSC reprenant les machines virtuelles sur lesquelles vous souhaitez mettre à jour les bases anti-virus (cf. section "Création de la tâche de diffusion des mises à jour" à la page 92).

CREATION DE LA TACHE DE DIFFUSION DES MISES A JOUR

Pour créer une tâche de diffusion des mises à jour, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC qui comprend les machines virtuelles de protection pour lesquelles vous souhaitez mettre à jour les bases anti-virus.

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

4. Lancez l'Assistant de création d'une tâche en cliquant sur le lien **Créer une tâche**.

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

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 92

Etape 2. Sélection du type de tâche 92

Etape 3. Définition des paramètres de programmation de la tâche 92

Etape 4. Fin de la création de la tâche..... 93

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche de diffusion des mises à jour dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

A cette étape, sélectionnez le type de tâche **Mise à jour** pour l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de la tâche de diffusion des mises à jour :

- **Lancement programmé**. Dans la liste déroulante, sélectionnez **Lors du téléchargement des mises à jour dans le stockage**.

- **Lancement des tâches ignorées**. Cochez la case si une tentative de lancement des tâches doit avoir lieu lors du prochain démarrage de l'application sur la machine virtuelle de protection.

  Si la case est cochée, la tâche sur la machine virtuelle de protection sera lancée uniquement selon la programmation.

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :

  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : 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**. La case est cochée par défaut.

- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment du lancement supposé de la tâche, 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 sera lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment supposé de lancement. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

  L'option de lancement décalé de la tâche permet d'éviter qu'un trop grand nombre de machines virtuelles de protection contacte directement le Serveur d'administration du Kaspersky Security Center.

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

ETAPE 4. FIN DE LA CREATION DE LA TACHE

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

Quittez l'Assistant de création d'une tâche. La tâche de diffusion des mises à jour créée apparaît dans la liste des tâches sous l'onglet **Tâches**.

La tâche sera exécutée chaque fois lors du téléchargement du paquet de mises à jour dans le stockage du Serveur d'administration et la mise à jour sera diffusée et installée sur les machines virtuelles de protection.

CONSULTATION DES RESULTATS D'EXECUTION DE LA TACHE DE DIFFUSION DES MISES A JOUR

Pour consulter les résultats de l'exécution de la tâche de diffusion des mises à jour, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC qui comprend les machines virtuelles de protection pour lesquelles la tâche de mise à jour a été configurée.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

4. Dans la liste des tâches, sélectionnez la tâche de diffusion des mises à jour dont vous souhaitez consulter les résultats d'exécution.

5. Cliquez sur le bouton **Consulter les résultats** situé à droite de la liste des tâches.

La fenêtre **Résultats de l'exécution de la tâche** s'ouvre.

Si la tâche de diffusion de la mise à jour s'est terminée sur une erreur, vous pouvez attendre le prochain lancement de la tâche selon la programmation ou lancer la tâche manuellement (cf. section "Lancement manuel de la tâche de diffusion des mises à jour" à la page 94).

Les résultats de l'exécution de la tâche peuvent également être consultés dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les machines virtuelles de protection. La liste des événements apparaît dans le dossier **Rapports et notifications/Evénements** de l'arborescence de la Console d'administration du Kaspersky Security Center.

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

LANCEMENT MANUEL DE LA TACHE DE DIFFUSION DES MISES A JOUR

Si la tâche de diffusion des mises à jour lancée selon la programmation s'est terminée sur une erreur, vous pouvez la lancer manuellement.

Pour lancer manuellement une tâche de diffusion des mises à jour, procédez comme suit :

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

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC sur les machines virtuelles de protection pour lesquelles vous souhaitez lancer une tâche de diffusion des mises à jour.

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

4. Dans la liste des tâches, sélectionnez la tâche de diffusion des mises à jour que vous souhaitez lancer.

5. Pour lancer la tâche, cliquez sur le bouton **Lancer** dans le groupe **Exécution d'une tâche**.

REMISE A L'ETAT ANTERIEUR A LA DERNIERE MISE A JOUR

Après la première mise à jour des bases antivirus, la fonction de remise à l'état antérieur à la dernière mise à jour est accessible.

Chaque fois que la mise à jour est lancée sur la machine virtuelle de protection, Kaspersky Security crée une copie de sauvegarde des bases antivirus utilisées, puis l'application procède à la mise à jour. Cela permet de revenir, le cas échéant, aux bases antivirus antérieures. La possibilité de revenir à l'état antérieur à la mise à jour est utile, par exemple, si la nouvelle version des bases antivirus contient une signature incorrecte qui fait que Kaspersky Security bloque une application sans danger.

Pour revenir à l'état antérieur à la dernière mise à jour, procédez comme suit :

1. Créez une tâche de remise à l'état antérieur à la mise à jour pour chaque cluster KSC reprenant les machines virtuelles sur lesquelles vous souhaitez effectuer une remise à l'état antérieur à la mise à jour (cf. section "Création d'une tâche de remise à l'état antérieur à la mise à jour" à la page 95).

2. Lancez la tâche de remise à l'état antérieur à la dernière mise à jour (cf. section "Lancement de la tâche de remise à l'état antérieur à la dernière mise à jour", page 96).

CREATION DE LA TACHE DE REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR

Pour créer une tâche de remise à l'état antérieur à la dernière mise jour, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez lancer la remise à l'état antérieur à la dernière mise à jour.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Lancez l'Assistant de création d'une tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les instructions de l'Assistant de création d'une tâche.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 95

Etape 2. Sélection du type de tâche 95

Etape 3. Définition des paramètres de programmation de la tâche 95

Etape 4. Fin de la création de la tâche 96

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche de remise à l'état antérieur à la dernière mise à jour dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

A cette étape, sélectionnez le type de tâche **Remise à l'état antérieur à la mise à jour** pour l'application Kaspersky Security for Virtualization 3.0 Agentless.

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

ETAPE 3. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de la tâche de remise à l'état antérieur à la dernière mise à jour :

- **Lancement programmé**. Dans la liste déroulante, sélectionnez le mode de lancement de la tâche **Manuel**.
- **Lancement des tâches ignorées**. Cochez la case si vous voulez que l'application lance la tâche ignorée tout de suite après l'apparition de la machine virtuelle de protection dans le réseau.

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

- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :

  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : 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**. La case est cochée par défaut.

- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment du lancement supposé de la tâche, 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 sera lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment supposé de lancement. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

  L'option de lancement décalé de la tâche permet d'éviter qu'un trop grand nombre de machines virtuelles de protection contacte directement le Serveur d'administration du Kaspersky Security Center.

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

ETAPE 4. FIN DE LA CREATION DE LA TACHE

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

Quittez l'Assistant de création d'une tâche. La tâche de remise à l'état antérieur à la dernière mise à jour créée apparaît dans la liste des tâches sous l'onglet **Tâches**.

LANCEMENT DE LA TACHE DE REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR

Pour lancer une tâche de remise à l'état antérieur à la dernière mise à jour, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez lancer la remise à l'état antérieur à la dernière mise à jour.

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

4. Dans la liste des tâches, sélectionnez la tâche de remise à l'état antérieur à la dernière mise à jour que vous souhaitez lancer.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Lancer**.

   - Cliquez sur le bouton **Lancer**. Le bouton se trouve à droite de la liste des tâches dans le groupe **Exécution de la tâche**.

RAPPORTS ET NOTIFICATIONS

Cette section décrit les différents moyens d'obtenir des informations sur le fonctionnement de Kaspersky Security.

DANS CETTE SECTION

A propos des événements et des notifications 98

Types de rapports..... 99

Consultation des rapports 109

Configuration des paramètres de notification 110

Consultation des statistiques du fonctionnement de l'application 111

A PROPOS DES EVENEMENTS ET DES NOTIFICATIONS

Les machines virtuelles de protection envoient des messages de service au Serveur d'administration du Kaspersky Security Center. Ces *événements* contiennent des informations relatives au fonctionnement de Kaspersky Security. Le Kaspersky Security Center génère différents types de rapport sur la base de ces notifications. Ces rapports fournissent, par exemple, des informations sur les fichiers infectés, sur les modifications des paramètres de protection et sur l'utilisation des clés et des bases antivirus. La Console d'administration du Kaspersky Security Center permet de consulter les rapports.

Kaspersky Security transmet au Serveur d'administration du Kaspersky Security Center les informations suivantes sur les machines virtuelles : nom de la machine virtuelle, nom et chemin d'accès aux fichiers considérés comme infectés par l'application. Kaspersky Security ne collecte et ne transmet via les réseaux aucune autre information sur les machines virtuelles protégées.

Les événements sont organisés selon les degrés d'importance suivants :

- **Messages d'information**. Evénements d'aide.
- **Avertissement**. Evénements qui doivent être examinés car ils désignent des situations importantes dans le fonctionnement de Kaspersky Security.
- **Refus de fonctionnement**. Evénements liés à un refus de fonctionnement de l'application.
- **Evénements critiques**. Evénements critiques, notamment ceux qui signalent des problèmes de fonctionnement de Kaspersky Security ou la présence de vulnérabilités dans la sécurité des machines virtuelles.

Une *notification* est un message contenant des informations relatives à un événement qui s'est produit sur une machine virtuelle de protection. Elle vous permet d'obtenir à temps des informations sur les événements survenus pendant le fonctionnement de l'application.

Vous pouvez configurer les paramètres de notifications relatives aux événements se produisant sur les machines virtuelles de protection.

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

TYPES DE RAPPORTS

Les rapports permettent d'obtenir des informations sur le fonctionnement de Kaspersky Security, notamment des renseignements sur le déploiement de la protection, l'état de la protection, l'exécution des tâches ou les menaces détectées.

Le Kaspersky Security Center propose un ensemble de rapports contenant des informations sur le fonctionnement de Kaspersky Security :

- **Rapport sur les versions des applications de Kaspersky Lab**. Contient des informations sur les versions des applications installées sur les postes client (machines virtuelles de protection et ordinateur sur lequel le Serveur d'administration et la Console d'administration du Kaspersky Security Center sont installés).
- **Rapport sur le déploiement de la protection**. Ce rapport contient les renseignements relatifs au déploiement de l'application.
- **Rapport sur les ordinateurs les plus infectés**. Ce rapport contient des informations concernant les machines virtuelles sur lesquelles l'analyse a détecté le plus grand nombre de fichiers infectés.
- **Rapport sur les virus**. Contient des informations sur les virus et autres programmes dangereux détectés sur les machines virtuelles.
- **Rapport sur l'utilisation des clés**. Contient des informations sur les clé ajoutées à l'application (cf. section "Consultation du rapport sur l'utilisation des clés" à la page 42).
- **Rapport sur les erreurs**. Ce rapport contient les informations relatives aux erreurs de fonctionnement de l'application.
- **Rapport sur les bases utilisées**. Ce rapport contient les informations relatives aux versions des bases antivirus utilisées sur les machines virtuelles de protection.
- **Rapport sur les attaques réseau**. Comprend des informations sur les attaques réseau enregistrées sur les machines virtuelles protégées.
- **Rapport sur le fonctionnement du contrôle Web**. Comporte des informations sur les connexions des utilisateurs ou des applications à des adresses Internet malveillantes consignées par le module Détection des intrusions de l'application Kaspersky Security.

Chaque rapport est présenté sous la forme d'un tableau des informations générales et d'un tableau des informations détaillées. Vous pouvez configurer le contenu des champs de chaque tableau. Pour en savoir plus sur les informations fournies dans les rapports, consultez la documentation du Kaspersky Security Center.

Le Rapport sur le registre du matériel n'est pas utilisé pour l'application Kaspersky Security. Vous pouvez consulter les informations sur les machines virtuelles de protection dans la console de gestion du serveur VMware vCenter.

DANS CETTE SECTION

Rapport sur les versions des applications de Kaspersky Lab 100

Rapport sur le déploiement de la protection 101

Rapport sur les ordinateurs les plus infectés 102

Rapport sur les virus 103

Rapport sur les erreurs 104

Rapport sur les bases utilisées 105

Rapport sur les attaques réseau.....106

Rapport sur le fonctionnement du contrôle Web.....107

RAPPORT SUR LES VERSIONS DES APPLICATIONS DE KASPERSKY LAB

Le rapport sur les versions des applications de Kaspersky Lab contient des informations sur les versions des modules de Kaspersky Security présents sur les machines virtuelles de protection et sur les modules du Kaspersky Security Center installés sur les postes client (machines virtuelles de protection et ordinateur sur lequel le Serveur d'administration et la Console d'administration du Kaspersky Security Center sont installés).

Il propose les informations de synthèse suivantes :

- **Application** : nom du module installé de Kaspersky Security ou du Kaspersky Security Center. Pour les deux modules de Kaspersky Security, ce champ indique le nom de l'application Kaspersky Security for Virtualization 3.0 Agentless.
- **Numéro de version** : numéro de la version du module installé de Kaspersky Security ou du Kaspersky Security Center.
- **Nombre d'ordinateurs** : pour les modules de l'application Kaspersky Security, ce champ affiche le nombre de machines virtuelles de protection présentant des modules Kaspersky Security ; pour le Kaspersky Security Center, ce champ reprend le nom des ordinateurs sur lesquels sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.
- **Nombre de groupes** : pour les modules de l'application Kaspersky Security, ce champ affiche le nombre de clusters KSC ; pour le Kaspersky Security Center, le nombre de groupes d'administration auxquels appartiennent les ordinateurs dotés du Serveur d'administration et de la Console d'administration du Kaspersky Security Center. Pour en savoir plus sur les groupes d'administration, consultez la documentation du Kaspersky Security Center.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Nombre de versions** : nombre total de versions différentes des modules de Kaspersky Security et du Kaspersky Security Center installés sur les postes clients.
  - **Nombre d'installations** : nombre total d'installations de ces modules sur les postes client (machines virtuelles de protection et ordinateur sur lequel le Serveur d'administration et la Console d'administration du Kaspersky Security Center sont installés).
  - **Nombre de postes** : nombre total de postes clients dotés des modules de Kaspersky Security et du Kaspersky Security Center.
  - **Nombre de groupes** : nombre total de groupes d'administration auxquels appartiennent ces postes client.

Le rapport propose les informations détaillées suivantes :

- **Application** : nom du module installé de Kaspersky Security ou du Kaspersky Security Center. Pour les deux modules de Kaspersky Security, ce champ indique le nom de l'application Kaspersky Security for Virtualization 3.0 Agentless.
- **Numéro de version** : numéro de la version du module installé de Kaspersky Security ou du Kaspersky Security Center.
- **Groupe** : pour les modules de l'application Kaspersky Security, ce champ reprend le cluster KSC qui contient les machines virtuelles de protection dotées de modules Kaspersky Security ; pour le Kaspersky Security Center, le groupe d'administration auquel appartient l'ordinateur doté du Serveur d'administration et de la Console d'administration du Kaspersky Security Center.

- **Poste client** : pour les modules de l'application Kaspersky Security, ce champ affiche le nom de la machine virtuelle de protection dotée du module ; pour le Kaspersky Security Center, ce champ reprend le nom de l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Installation** : date et heure de l'installation du module de Kaspersky Security ou du Kaspersky Security Center sur le poste client.

- **Visible dans le réseau** : date et heure à partir desquelles le poste client est visible dans le réseau local de l'entreprise.

- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion du poste client au Serveur d'administration du Kaspersky Security Center.

- **Adresse IP** : pour les modules de l'application Kaspersky Security, ce champ affiche l'adresse IP de la machine virtuelle de protection dotée du module ; pour le Kaspersky Security Center, ce champ reprend l'adresse IP de l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Nom de domaine** : pour les modules de l'application Kaspersky Security, ce champ affiche le nom de la machine virtuelle de protection dotée du module ; pour le Kaspersky Security Center, ce champ reprend le nom de l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Nom NetBIOS** : pour les modules de l'application Kaspersky Security, ce champ affiche le nom de la machine virtuelle de protection dotée du module ; pour le Kaspersky Security Center, ce champ reprend le nom de l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Domaine DNS** : domaine DNS de la machine virtuelle de protection ou du poste (indiqué uniquement si le nom de la machine virtuelle de protection ou du poste contient le nom du domaine DNS).

RAPPORT SUR LE DEPLOIEMENT DE LA PROTECTION

Le rapport sur le déploiement de la protection contient des informations concernant le déploiement de l'application sur les postes client (les machines virtuelles de protection et l'ordinateur sur lequel la Console d'administration du Kaspersky Security Center est installée).

Il propose les informations de synthèse suivantes :

- **Modules de protection** : modules et applications de Kaspersky Lab installés sur les postes client :
  - **L'agent d'administration et de protection antivirus est installé**.
  - **Seul l'agent d'administration est installé**.
  - **L'agent d'administration et la protection antivirus ne sont pas installés**.
- **Nombre d'ordinateurs** : nombre de postes client sur lesquels sont installés les modules et les applications.

  La ligne sous le champ **Nombre d'ordinateurs** affiche le nombre de postes client sur lesquels les modules et les applications indiqués sont installés.

Le rapport propose les informations détaillées suivantes :

- **Groupe** : pour Kaspersky Security, ce champ affiche le cluster KSC qui contient les machines virtuelles de protection ; pour le Kaspersky Security Center, le groupe d'administration auquel appartient l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Poste client** : pour Kaspersky Security, ce champ affiche le nom de la machine virtuelle de protection ; pour le Kaspersky Security Center, ce champ correspond au nom de l'ordinateur sur lequel sont installés le Serveur d'administration et la Console d'administration du Kaspersky Security Center.

- **Version de l'agent d'administration** : version de l'agent d'administration installé sur le poste client.
- **Nom de l'application antivirus** : nom de l'application de Kaspersky Lab installée sur le poste client.
- **Version de l'application antivirus** : version de l'application de Kaspersky Lab installée sur le poste client.

RAPPORT SUR LES ORDINATEURS LES PLUS INFECTES

Le rapport sur les ordinateurs les plus infectés contient des informations concernant les machines virtuelles sur lesquelles l'analyse a détecté le plus grand nombre de fichiers infectés.

Le champ **Période** indique la période couverte par le rapport. Par défaut, la période du rapport est égale à 30 jours à partir de la date de création du rapport.

Le rapport contient les informations suivantes concernant les machines virtuelles sur lesquelles l'analyse a détecté le plus grand nombre de fichiers infectés :

- **Poste client** : nom de la machine virtuelle sur laquelle un virus ou un autre programme dangereux a été détecté.
- **Groupe** : cluster KSC auquel appartient la machine virtuelle.
- **Nombre détecté** : nombre de fichiers infectés détectés sur cette machine virtuelle.
- **Objets différents** : nombre de virus et autres programmes dangereux différents détectés sur cette machine virtuelle.
- **Première détection** : date et heure de la première détection d'un virus ou d'un autre programme dangereux sur la machine virtuelle.
- **Dernière détection** : date et heure de la dernière détection d'un virus ou d'un autre programme dangereux sur la machine virtuelle.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle comportant le virus ou tout autre programme présentant une menace détecté est visible dans le réseau local de l'entreprise.
- **Nom NetBIOS** : nom de la machine virtuelle sur laquelle un virus ou un autre programme dangereux a été détecté.
- **Nom de domaine** : nom de la machine virtuelle de protection sur laquelle un virus ou un autre programme dangereux a été détecté.
- **Domaine DNS** : domaine DNS de la machine virtuelle (indiqué uniquement si le nom de la machine virtuelle contient le nom du domaine DNS).

  Dans la ligne ci-dessous, le champ **Ordinateurs dangereux** indique le nombre de machines virtuelles sur lesquelles l'analyse a détecté le plus grand nombre de fichiers infectés. Le champ **Groupes dangereux** indique le nombre de clusters KSC auxquels appartiennent ces machines virtuelles.

Le rapport propose les détails suivants pour chaque élément détecté :

- **Poste client** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Groupe** : cluster KSC auquel appartient la machine virtuelle.
- **Objet détecté** : nom de l'objet qui a été détecté sur la machine virtuelle.
- **Moment de détection** : date et heure de la détection de l'objet sur la machine virtuelle.
- **Chemin d'accès au fichier** : chemin d'accès au fichier figurant sur la machine virtuelle où l'objet a été détecté.
- **Type d'objet** : type de l'objet détecté.

- **Action** : résultat de l'action exécutée par l'application Kaspersky Security sur cet objet.
- **Application** : application qui a détecté l'objet.
- **Numéro de version** : numéro de la version de l'application.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle comportant l'objet détecté est visible dans le réseau local de l'entreprise.
- **Nom NetBIOS** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Nom de domaine** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Domaine DNS** : domaine DNS de la machine virtuelle (indiqué uniquement si le nom de la machine virtuelle contient le nom du domaine DNS).

RAPPORT SUR LES VIRUS

Le rapport sur les virus contient des informations sur les virus et autres programmes dangereux découverts sur les machines virtuelles lors de l'exécution de l'analyse des machines virtuelles, ainsi que des informations sur les fichiers bloqués par la protection des machines virtuelles.

Le champ **Période** indique la période couverte par le rapport. Par défaut, le rapport couvre une période de 30 jours, date de création du rapport comprise.

Le rapport propose les informations de synthèse suivantes sur les objets détectés :

- **Objet détecté** : nom de l'objet qui a été détecté sur les machines virtuelles.
- **Type d'objet** : type de l'objet détecté.
- **Nombre de détections** : nombre total de fichiers contenant l'objet détecté.
- **Nombre de fichiers différents** : nombre de fichiers différents contenant l'objet détecté.
- **Ordinateurs dangereux** : nombre de machines virtuelles sur lesquelles l'objet indiqué a été détecté.
- **Groupes infectés** : nombre de clusters KSC auxquels appartiennent ces machines virtuelles.
- **Première détection** : date et heure de la première détection de l'objet sur une machine virtuelle.
- **Dernière détection** : date et heure de la dernière détection de l'objet sur une machine virtuelle.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Divers objets** : nombre d'objets détectés sur l'ensemble des machines virtuelles au cours de la période couverte par le rapport.
  - **Divers fichiers** : nombre de fichiers détectés sur l'ensemble des machines virtuelles au cours de la période couverte par le rapport.
  - **Ordinateurs dangereux** : nombre total de machines virtuelles sur lesquelles des objets ont été détectés.
  - **Groupes infectés** : nombre total de clusters KSC auxquels appartiennent ces machines virtuelles.

Le rapport propose les détails suivants pour chaque détection d'objet :

- **Poste client** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Groupe** : cluster KSC auquel appartient la machine virtuelle.
- **Objet détecté** : nom de l'objet qui a été détecté sur la machine virtuelle.

- **Moment de détection** : date et heure de la détection de l'objet sur la machine virtuelle.
- **Chemin d'accès au fichier** : chemin d'accès au fichier figurant sur la machine virtuelle où l'objet a été détecté.
- **Type d'objet** : type de l'objet détecté.
- **Action** : action exécutée par l'application Kaspersky Security sur cet objet.
- **Application** : application qui a détecté l'objet.
- **Numéro de version** : numéro de la version de l'application.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle comportant l'objet détecté est visible dans le réseau local de l'entreprise.
- **Nom NetBIOS** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Nom de domaine** : nom de la machine virtuelle sur laquelle l'objet a été détecté.
- **Domaine DNS** : domaine DNS de la machine virtuelle (indiqué uniquement si le nom de la machine virtuelle contient le nom du domaine DNS).

RAPPORT SUR LES ERREURS

Le rapport sur les erreurs reprend les informations relatives aux refus de fonctionnement de l'application.

Le champ **Période** indique la période couverte par le rapport. Par défaut, le rapport couvre une période de 30 jours, date de création du rapport comprise.

Le rapport propose les informations de synthèse suivantes :

- **Type d'erreur** : type d'erreur détecté dans le fonctionnement de l'application. Par exemple, *La tâche s'est soldée sur une erreur*.
- **Nombre d'erreurs** : nombre d'erreurs du type indiqué.
- **Nombre d'applications** : nombre d'applications dans lesquelles l'erreur du type indiqué a été détectée.
- **Nombre d'ordinateurs** : nombre de machines virtuelles de protection sur lesquelles l'erreur du type indiqué a été détectée.
- **Nombre de groupes** : nombre de clusters KSC auxquels appartiennent les machines virtuelles de protection.
- **Heure de première erreur** : date et heure de la première détection de l'erreur.
- **Heure de dernière erreur** : date et heure de la dernière détection de l'erreur.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Total des erreurs** : nombre total d'erreurs consignées pour la période couverte par le rapport.
  - **Types d'erreur** : nombre total de types d'erreurs consignés pour la période couverte par le rapport.
  - **Nombre d'ordinateurs** : nombre total de machines virtuelles de protection sur lesquelles les erreurs du type indiqué ont été détectées.
  - **Nombre de groupes** : nombre total de clusters KSC auxquels appartiennent les machines virtuelles de protection.

Le rapport propose les détails suivants pour chaque erreur :

- **Groupe** : cluster KSC auquel appartient la machine virtuelle de protection sur laquelle l'erreur a été détectée.
- **Poste client** : nom de la machine virtuelle de protection qui a détecté l'erreur.
- **Application** : application dans laquelle l'erreur a été détectée.
- **Type d'erreur** : type d'erreur. Par exemple, *La tâche s'est soldée sur une erreur*.
- **Description d'erreur** : description détaillée de l'erreur.
- **Date de détection** : date et heure de détection de l'erreur.
- **Tâche** : tâche au cours de laquelle l'erreur a été détectée.
- **Adresse IP** : adresse IP de la machine virtuelle de protection.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle de protection est visible dans le réseau local de l'entreprise.
- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la machine virtuelle de protection au Serveur d'administration du Kaspersky Security Center.
- **Nom NetBIOS** : nom de la machine virtuelle de protection qui a détecté l'erreur.
- **Nom de domaine** : nom de la machine virtuelle de protection qui a détecté l'erreur.
- **Domaine DNS** : domaine DNS de la machine virtuelle de protection (indiqué uniquement si le nombre de la machine virtuelle de protection contient le nom du domaine DNS).

RAPPORT SUR LES BASES UTILISEES

Le rapport sur les bases utilisées contient les informations relatives aux versions des bases antivirus utilisées sur les machines virtuelles de protection.

Il propose les informations de synthèse suivantes :

- **Créées** : date et heure de création des bases antivirus utilisées sur les machines virtuelles de protection.
- **Nombre d'enregistrements** : nombre d'enregistrements dans ces bases antivirus.
- **Nombre d'ordinateurs** : nombre de machines virtuelles de protection sur lesquelles ces bases anti-virus sont utilisées.
- **Nombre de groupes** : nombre de clusters KSC auxquels appartiennent les machines virtuelles de protection utilisant ces bases antivirus.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Nombre de sélections de bases** : nombre total de sélections de bases antivirus utilisées sur les machines virtuelles de protection.
  - **A jour** : nombre total de bases antivirus à jour.
  - **Mise à jour dans les dernières 24 heures** : nombre total de bases antivirus mises à jour sur les machines virtuelles de protection au cours des dernières 24 heures.
  - **Mise à jour dans les 3 derniers jours** : nombre total de bases antivirus mises à jour sur les machines virtuelles de protection au cours des trois derniers jours.

- **Mise à jour dans les 7 derniers jours** : nombre total de bases antivirus mises à jour sur les machines virtuelles de protection au cours des sept derniers jours.
- **Mise à jour il y a plus de 7 jours** : nombre total de bases antivirus mises à jour sur les machines virtuelles de protection il y a plus de sept jours.

Le rapport propose les informations détaillées suivantes :

- **Groupe** : cluster KSC auquel appartiennent les machines virtuelles de protection utilisant ces bases antivirus.
- **Poste client** : nom de la machine virtuelle de protection.
- **Application** : nom de l'application installée sur la machine virtuelle de protection.
- **Numéro de version** : numéro de version de l'application installée sur la machine virtuelle de protection.
- **Créées** : date et heure de création des bases antivirus utilisées sur les machines virtuelles de protection.
- **Nombre d'enregistrements** : nombre d'enregistrements dans ces bases antivirus.
- **Adresse IP** : adresse IP de la machine virtuelle de protection.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle de protection est visible dans le réseau local de l'entreprise.
- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la machine virtuelle de protection au Serveur d'administration du Kaspersky Security Center.
- **Nom NetBIOS** : nom de la machine virtuelle de protection utilisant les bases antivirus.
- **Nom de domaine** : nom de la machine virtuelle de protection utilisant les bases antivirus.
- **Domaine DNS** : domaine DNS de la machine virtuelle de protection (indiqué uniquement si le nombre de la machine virtuelle de protection contient le nom du domaine DNS).

RAPPORT SUR LES ATTAQUES RESEAU

Le rapport sur les attaques réseau reprend les informations sur les attaques réseau enregistrées sur les machines virtuelles protégées.

Il propose les informations de synthèse suivantes :

- **Attaque** : type d'attaque réseau.
- **Nombre d'attaques** : nombre d'attaques réseau de ce type.
- **Adresses de provenance** : nombre d'adresses IP ayant lancé des attaques réseau.
- **Postes clients attaqués** : nombre de machines virtuelles de protection ayant détecté les attaques réseau.
- **Groupes attaqués** : nombre de clusters KSC auxquels appartiennent les machines virtuelles de protection ayant détecté l'attaque réseau.
- **Première attaque** : date et heure de la première attaque enregistrée.
- **Dernière attaque** : date et heure de la dernière attaque enregistrée.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Nombre d'attaques** : nombre d'attaques réseau de tous types.
  - **Types d'attaque** : nombre de types d'attaques réseau enregistrés.
  - **Adresses de provenance** : nombre d'adresses IP ayant lancé des attaques réseau.

- **Postes clients attaqués** : nombre de machines virtuelles de protection ayant détecté les attaques réseau.
- **Groupes attaqués** : nombre de clusters KSC auxquels appartiennent les machines virtuelles de protection ayant détecté l'attaque réseau.
- **Première attaque** : date et heure de la première attaque enregistrée.
- **Dernière attaque** : date et heure de la dernière attaque enregistrée.

Le rapport propose les informations détaillées suivantes :

- **Groupe** : cluster KSC auquel appartient la machine virtuelle de protection ayant détecté l'attaque réseau.
- **Poste client** : nom de la machine virtuelle de protection ayant détecté l'attaque réseau.
- **Adresses de provenance** : adresse IP ayant lancé l'attaque réseau.
- **Circonstances de l'attaque** : date et heure de l'attaque enregistrée.
- **Attaque** : type d'attaque réseau.
- **Protocole** : protocole ayant servi à lancer l'attaque réseau.
- **Port** : numéro de port ayant servi à lancer l'attaque réseau.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle de protection ayant détecté l'attaque réseau est visible dans le réseau local de l'entreprise.
- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la machine virtuelle de protection ayant détecté l'attaque réseau au Serveur d'administration du Kaspersky Security Center.
- **Adresse IP** : adresse IP de la machine virtuelle de protection ayant détecté l'attaque réseau.
- **Nom de domaine** : nom de la machine virtuelle de protection ayant détecté l'attaque réseau.
- **Nom NetBIOS** : nom de la machine virtuelle de protection ayant détecté l'attaque réseau.
- **Domaine DNS** : domaine DNS de la machine virtuelle de protection (indiqué uniquement si le nombre de la machine virtuelle de protection contient le nom du domaine DNS).
- **Application** : application ayant détecté l'attaque réseau.
- **Numéro de version** : numéro de la version du module Détection des intrusions de Kaspersky Security.

RAPPORT SUR LE FONCTIONNEMENT DU CONTROLE WEB

Le rapport sur le fonctionnement du contrôle Internet contient des renseignements sur les connexions des utilisateurs ou des applications installées sur les machines virtuelles protégées à des adresses Internet malveillantes reprises dans la base des adresses Internet malveillantes.

Il propose les informations de synthèse suivantes :

- **Résultat** : action que Kaspersky Security a exécuté en cas de détection d'une tentative de connexion à une adresse Internet malveillante.
- **Règle** : règle réseau régissant l'action de l'application lors de la détection d'une tentative de connexion à une adresse Internet malveillante. Pour Kaspersky Security, ce champ indique : *Kaspersky Security for Virtualization 3.0 Agentless : toute activité réseau via le protocole HTTP*.
- **Tentatives** : nombre de tentatives de connexion à une adresse Internet malveillante.

- **Comptes utilisateurs** : nombre de machines virtuelles à partir desquelles les tentatives de connexion à l'adresse Internet malveillante ont été lancées.
- **Adresse Internet** : nombre de tentatives de sollicitation des adresses Internet apparaissant dans la base des adresses Internet malveillantes.
- **Postes** : nombre de machines virtuelles de protection ayant détecté les tentatives de connexion à l'adresse Internet malveillante.
- **Groupe d'administration** : nombre de clusters KSC auxquels appartiennent les machines virtuelles de protection.
- **Première tentative** : date et heure de la première tentative de connexion à l'adresse Internet malveillante.
- **Dernière tentative** : date et heure de la dernière tentative de connexion à l'adresse Internet malveillante.

  La ligne en dessous reprend les informations de synthèse suivantes :

  - **Règles** : nombre de règles réseau régissant l'action de l'application lors de la détection d'une tentative de connexion à une adresse Internet malveillante. Pour Kaspersky Security ce champ indique : *1*.
  - **Blocages** : nombre de connexions aux adresses Internet malveillantes ayant été bloquées par Kaspersky Security.
  - **Avertissements** : nombre de connexions aux adresses Internet malveillantes ayant été autorisées conformément aux paramètres de l'application.
  - **Adresses Internet bloquées** : nombre d'adresses Internet malveillantes ayant été bloquées par Kaspersky Security.
  - **Avertissements sur les adresses Internet** : nombre d'adresses Internet malveillantes ayant été autorisées conformément aux paramètres de l'application.
  - **Utilisateurs bloqués** : nombre de machines virtuelles à partir desquelles les tentatives de connexion aux adresses Internet bloquées ont été lancées.
  - **Avertissements sur les utilisateurs** : nombre de machines virtuelles ayant été autorisées par Kaspersky Security à accéder aux adresses Internet malveillantes, conformément aux paramètres de l'application.
  - **Premier blocage** : date et heure du premier blocage de la tentative de connexion à l'adresse Internet malveillante.
  - **Dernier blocage** : date et heure du dernier blocage de la tentative de connexion à l'adresse Internet malveillante.
  - **Premier avertissement** : date et heure de la première connexion à l'adresse Internet malveillante ayant été autorisée conformément aux paramètres de l'application.
  - **Dernier avertissement** : date et heure de la dernière connexion à l'adresse Internet malveillante ayant été autorisée conformément aux paramètres de l'application.

Le rapport propose les informations détaillées suivantes :

- **Résultat** : action que Kaspersky Security a exécuté en cas de détection d'une tentative de connexion à une adresse Internet malveillante.
- **Règle** : règle réseau régissant l'action de l'application lors de la détection d'une tentative de connexion à une adresse Internet malveillante. Pour Kaspersky Security, ce champ indique : *Kaspersky Security for Virtualization 3.0 Agentless : toute activité réseau via le protocole HTTP*.
- **Compte utilisateur** : adresse IP de la machine virtuelle à partir de laquelle les tentatives de connexion à l'adresse Internet malveillante ont été lancées.

- **Adresse Internet** : adresse Internet reprise dans la base des adresses Internet malveillantes.
- **Circonstances** : date et heure de la détection de la tentative de connexion à l'adresse Internet malveillante.
- **Groupe** : cluster KSC auquel appartient la machine virtuelle de protection ayant détecté la tentative de connexion à une adresse Internet malveillante.
- **Poste client** : nom de la machine virtuelle de protection ayant détecté la tentative de connexion à l'adresse Internet malveillante.
- **Application** : nom de l'application ayant détecté la tentative de connexion à l'adresse Internet malveillante.
- **Numéro de version** : numéro de la version du module Détection des intrusions de Kaspersky Security.
- **Visible dans le réseau** : date et heure à partir desquelles la machine virtuelle de protection ayant détecté la tentative de connexion à l'adresse Internet malveillante est visible dans le réseau local de l'entreprise.
- **Dernière date de connexion au Serveur d'administration** : date et heure de la dernière connexion de la machine virtuelle de protection au Serveur d'administration du Kaspersky Security Center.
- **Adresse IP** : adresse IP de la machine virtuelle de protection ayant détecté la tentative de connexion à l'adresse Internet malveillante.
- **Nom de domaine** : nom de la machine virtuelle de protection.
- **Nom NetBIOS** : nom de la machine virtuelle de protection.
- **Domaine DNS** : domaine DNS de la machine virtuelle de protection (indiqué uniquement si le nombre de la machine virtuelle de protection contient le nom du domaine DNS).

CONSULTATION DES RAPPORTS

Pour consulter un rapport, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Rapports et notifications** de l'arborescence de la console, sélectionnez le modèle du rapport que vous souhaitez consulter.

   Le rapport créé selon le modèle sélectionné apparaît dans la zone de travail.

Le modèle du rapport relatif aux attaques réseau n'est, par défaut, pas compris dans la liste des modèles de rapport du dossier **Rapports et notifications**. Pour ajouter le modèle de rapport relatif aux attaques réseau dans la liste des modèles, utilisez l'Assistant de création d'un modèle de rapport (cf. documentation du Kaspersky Security Center). Une fois l'Assistant terminé, le modèle de rapport constitué sera ajouté au dossier **Rapports et notifications** de l'arborescence de la console.

Le rapport reprend les informations suivantes :

- type et nom du rapport, brève description et période couverte ainsi que les informations relatives au groupe pour lequel le rapport a été créé ;
- diagramme illustrant les données caractéristiques du rapport ;
- synthèse des indices du rapport ;
- tableau reprenant les détails du rapport.

Pour en savoir plus sur l'utilisation des rapports, consultez la Documentation du Kaspersky Security Center.

CONFIGURATION DES PARAMETRES DE NOTIFICATION

Pour configurer les paramètres de notification, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC dont vous souhaitez modifier les paramètres de notifications dans la stratégie.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Evénements**.
6. Dans la liste déroulante, sélectionnez le niveau d'importance des événements pour lesquels vous souhaitez être prévenu :
   - **Evénement critique**.
   - **Refus de fonctionnement**.
   - **Avertissement**.
   - **Information**.

   Le tableau en-dessous affiche les types d'événements du niveau d'importance sélectionné.
7. Sélectionnez les types d'événements pour lesquels vous souhaitez être prévenu :
   - Vous pouvez sélectionner plusieurs types à l'aide des touches **SHIFT** et **CTRL**.
   - Pour sélectionner tous les types, cliquez sur le bouton **Tout sélectionner**.
8. Cliquez sur le bouton **Propriétés**.
9. La fenêtre **Propriété<N événements>** (où N représente le nombre de types d'événement sélectionnés) s'ouvre.
10. Dans le groupe **Enregistrement d'événements**, cochez la case **Sur le Serveur d'administration pendant (jours)**. Kaspersky Security enverra au Serveur d'administration du Kaspersky Security Center les événements correspondant au type que vous avez sélectionné.
11. Saisissez dans le champ le nombre de jours de conservation des événements sur le Serveur d'administration. Le Kaspersky Security Center supprime les événements à l'issue de ce délai.
12. Sélectionnez le mode de notification dans le groupe **Notification relative à un événement** :
    - **Notifier par courrier électronique**.

      Si la case est cochée, les notifications sont envoyées par courrier électronique.
    - **Notifier via SMS**.

      Si la case est cochée, les notifications sont envoyées par SMS.

      La case est décochée par défaut.
    - **Notifier via le lancement d'un fichier exécutable ou d'un script**.

      Si la case est cochée, l'application ou le fichier exécutable indiqué est lancé lorsque l'événement survient.

      La case est décochée par défaut.

- **Notifier via SNMP**.

  Si la case est cochée, la notification est envoyée via le réseau (TCP/IP) selon le protocole d'administration SNMP.

  La case est décochée par défaut.

13. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés <N événements>**.

14. Cliquez sur le bouton **OK**.

CONSULTATION DES STATISTIQUES DU FONCTIONNEMENT DE L'APPLICATION

Les machines virtuelles de protection envoient les statistiques d'information suivantes concernant le fonctionnement de Kaspersky Security au Serveur d'administration du Kaspersky Security Center :

- informations relatives à la version de la bibliothèque EPSEC installée sur la machine virtuelle de protection dotée du module Anti-Virus Fichiers ;
- informations relatives à la durée de validité de la licence ;
- nombre de fichiers analysés au cours de la protection des machines virtuelles ;
- nombre de fichiers analysés au cours des tâches d'analyse ;
- nombre de paquets réseau traités ;
- informations sur l'état des bases antivirus.

Vous pouvez consulter les statistiques de Kaspersky Security sur chaque machine virtuelle de protection dans la Console d'administration du Kaspersky Security Center.

Pour consulter les statistiques de fonctionnement de l'application, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC comprenant les machines virtuelles de protection pour lesquelles vous souhaitez consulter les statistiques de l'application.
3. Dans la zone de travail, sélectionnez l'onglet **Ordinateurs**.
4. Dans la liste des machines virtuelles de protection, sélectionnez la machine virtuelle de protection pour laquelle vous souhaitez consulter les statistiques de l'application.
5. Ouvrez la fenêtre **Propriétés : <nom de la machine virtuelle de protection>** en cliquant sur le lien **Propriétés de l'ordinateur**, situé à droite de la liste des machines virtuelles de protection.
6. Dans la fenêtre des propriétés de la machine virtuelle de protection, choisissez la section **Applications**.
7. La liste des applications installées sur cette machine virtuelle de protection apparaît dans la partie droite de la fenêtre.
8. Sélectionnez l'application Kaspersky Security for Virtualization 3.0 Agentless.
9. Cliquez sur le bouton **Statistiques** sous de la liste des applications.

   La fenêtre **Statistiques** s'ouvre.

Si vous avez sélectionné une machine virtuelle de protection dotée du module Anti-Virus Fichiers, la fenêtre **Statistiques** affiche les informations suivantes :

- **Statistiques générales** : nombre de fichiers analysés par la machine virtuelle de protection depuis l'installation de l'application ; que ce soit au cours de la protection ou lors de l'exécution des tâches d'analyse.
- **Informations relatives à la version** : version de la bibliothèque EPSEC installée sur la machine virtuelle de protection.
- **Informations sur la licence** : le champ **Durée restante de validité de la licence** affiche le nombre de jours restants avant la fin de validité de la licence ou des informations indiquant que la licence a déjà expiré. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *Non définie*.
- **Informations relatives aux bases antivirus** / **Etat des bases anti-virus** : date et heure de diffusion des bases anti-virus, nombre d'enregistrements dans ces bases ou informations indiquant que les bases anti-virus sont corrompues.
- **Statistiques des dernières 24 h** : nombre de fichiers analysés par la machine virtuelle de protection pendant les dernières 24 h ; que ce soit au cours de la protection ou lors de l'exécution des tâches d'analyse.
- **Statistiques des 30 derniers jours** : nombre de fichiers analysés par la machine virtuelle de protection pendant les 30 derniers jours ; que ce soit au cours de la protection ou lors de l'exécution des tâches d'analyse.
- **Statistiques des 7 derniers jours** : nombre de fichiers analysés par la machine virtuelle de protection pendant les sept derniers jours ; que ce soit au cours de la protection ou lors de l'exécution des tâches d'analyse.

Si vous avez sélectionné une machine virtuelle de protection dotée du module Détection des intrusions, la fenêtre **Statistiques** affiche les informations suivantes :

- **Statistiques générales** : nombre de paquets réseau traités par la machine virtuelle de protection depuis l'installation de l'application au cours de la protection.
- **Informations sur la licence** : le champ **Durée restante de validité de la licence** affiche le nombre de jours restants avant la fin de validité de la licence ou des informations indiquant que la licence a déjà expiré. Si vous utilisez l'application avec un abonnement illimité, le champ affiche *Non définie*.
- **Informations relatives aux bases antivirus** / **Etat des bases anti-virus** : date et heure de diffusion des bases anti-virus, nombre d'enregistrements dans ces bases ou informations indiquant que les bases anti-virus sont corrompues.
- **Statistiques pour les dernières 24 heures** : nombre de paquets réseau traités par la machine virtuelle de protection au cours des dernières 24 heures.
- **Statistiques pour les 30 derniers jours** : nombre de paquets réseau traités par la machine virtuelle de protection au cours des 30 derniers jours.
- **Statistiques pour les 7 derniers jours** : nombre de paquets réseau traités par la machine virtuelle de protection au cours des sept derniers jours.

PARTICIPATION A KASPERSKY SECURITY NETWORK

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

DANS CETTE SECTION

A propos de la participation à Kaspersky Security Network 113

Présentation des données 114

Activation et désactivation de l'utilisation de Kaspersky Security Network 114

A PROPOS DE LA PARTICIPATION A KASPERSKY SECURITY NETWORK

Pour améliorer l'efficacité de la protection des machines virtuelles, Kaspersky Security peut utiliser des données obtenues auprès d'utilisateurs d'applications de Kaspersky Lab dans le monde entier. Ces données sont recueillies via le réseau *Kaspersky Security Network*.

Kaspersky Security Network (KSN) est une infrastructure de services et de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network permet d'accélérer le temps de réaction de Kaspersky Security aux nouvelles menaces, d'améliorer l'efficacité de plusieurs modules de protection et de diminuer les risques de faux positifs.

Votre participation à Kaspersky Security Network permet de repérer plus aisément les nouvelles menaces complexes, leurs sources, ainsi que les attaques ciblées.

La participation à Kaspersky Security Network est volontaire. La décision de participer ou non à Kaspersky Security Network est prise lors de la définition de la stratégie de Kaspersky Security. Vous pouvez changer d'avis à tout moment (cf. section "Activation et désactivation de l'utilisation de Kaspersky Security Network" à la page 114).

L'interaction entre l'infrastructure de Kaspersky Security Network et les machine virtuelles de protection gérées par le Kaspersky Security Center est garantie par le service *KSN Proxy*. La configuration du service KSN Proxy s'opère dans les propriétés du serveur d'administration du Kaspersky Security Center.

Si le service KSN Proxy est désactivé, l'échange de données entre Kaspersky Security et les services de Kaspersky Security Network n'a pas lieu. Si l'utilisation de KSN est activée dans l'application Kaspersky Security et que le service KSN Proxy est désactivé dans le Kaspersky Security Center, il se peut que les performances de l'application Kaspersky Security diminuent.

Vous pouvez consulter les informations détaillées sur le service KSN Proxy dans la documentation du Kaspersky Security Center.

PRESENTATION DES DONNEES

En acceptant les conditions de participation au programme Kaspersky Security Network, vous autorisez la transmission automatique des renseignements suivants à Kaspersky Lab :

- numéro de version et type de l'application ;
- nom et version du système d'exploitation installé sur la machine virtuelle de protection dotée du module Anti-Virus Fichiers et des paquets de mises à jour pour le système d'exploitation ;
- adresse IP de la machine virtuelle de protection assortie du composant Antivirus Fichiers ;
- version du système d'exploitation de la machine virtuelle protégée sur laquelle le fichier a été analysé ;
- identificateur unique de l'installation de l'application (identificateur unique du BIOS de la machine virtuelle de protection dotée du module Anti-Virus Fichiers) ;
- Hachage de fichier MD5;
- informations relatives aux fichiers infectés détectés (nom du fichier infecté, taille du fichier décompressé en octets, chemin d'accès complet au fichier, état du fichier, code du type de fichier, identificateur du type de fichier, nom de l'objet détecté, date et heure d'émission des bases antivirus, version des bases antivirus, type, identificateur et version des enregistrements des bases antivirus, identificateur du type de tâche de mise à jour des bases) ;
- nombre de tentatives de mise à jour s'étant soldées sur un échec ;
- résultat de la mise à jour des bases antivirus.

Pour de plus amples informations sur le traitement des données, consultez le site Internet de Kaspersky Lab (http://www.kaspersky.com/fr/privacy).

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Kaspersky Lab utilise les informations obtenues uniquement sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas de données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme cryptée et sont supprimées au fur et à mesure de leur accumulation (deux fois par an). Les données des statistiques générales sont conservées de manière illimitée.

Les données relatives à l'utilisateur et les informations confidentielles ne sont ni recueillies, ni traitées, ni enregistrées. Pour connaître les données transmises par Kaspersky Security au Kaspersky Security Network, lisez les conditions de Kaspersky Security Network avant de décider d'y participer ou non.

ACTIVATION ET DESACTIVATION DE L'UTILISATION DE KASPERSKY SECURITY NETWORK

L'activation ou la désactivation de l'utilisation des services de Kaspersky Security Network est définie dans les paramètres de la stratégie. Si l'utilisation de KSN est activée dans la stratégie active du cluster KSC, les services KSN sont utilisés par Kaspersky Security dans le cadre de la protection des machines virtuelles et dans le cadre de l'exécution des tâches d'analyse des machines virtuelles.

Si la stratégie dans laquelle l'utilisation de KSN est activée n'est pas active, les services de KSN ne sont pas utilisés par Kaspersky Security.

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

Pour activer ou désactiver l'utilisation de Kaspersky Security Network, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC de la stratégie que vous souhaitez modifier.
3. Dans la zone de travail, choisissez l'onglet **Stratégies**.
4. Dans la liste, sélectionnez une stratégie et double-cliquez dessus pour ouvrir la fenêtre **Propriétés: <Nom de la stratégie>**.
5. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Paramètres KSN**.
6. Exécutez une des actions suivantes :
   - Cochez la case **Utiliser KSN** si vous souhaitez activer l'utilisation des services de Kaspersky Security Network.
   - Décochez la case **Utiliser KSN** si vous souhaitez désactiver l'utilisation des services de Kaspersky Security Network.

   En cochant la case **Utiliser KSN**, vous marquez votre accord avec les dispositions du programme Kaspersky Security Network présentées dans les Conditions de participation à Kaspersky Security Network.
7. Cliquez sur le bouton **OK**.

CONTACTER LE SUPPORT TECHNIQUE

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

DANS CETTE SECTION

Présentation du Support technique....116

Support Technique par téléphone 116

Support Technique via Kaspersky CompanyAccount 117

Collecte d'informations pour le Support Technique....117

Utilisation du fichier de traçage 118

Utilisation des fichiers de statistiques système....118

PRESENTATION 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 9), contactez le Support Technique de Kaspersky Lab. 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 Support Technique, il est recommandé de lire les règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

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

- contacter le Support Technique de Kaspersky Lab par téléphone ;
- envoyer une requête au Support Technique de Kaspersky Lab via le service Internet Kaspersky CompanyAccount.

SUPPORT TECHNIQUE PAR TELEPHONE

Vous pouvez téléphoner aux experts du Support Technique de Kaspersky Lab dans la plupart des régions. 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). Ces règles contiennent des informations telles que les heures d'appel au Support Technique de Kaspersky Lab ou les données dont les experts du Support Technique de Kaspersky Lab auront besoin pour vous aider.

SUPPORT TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un service en ligne réservé aux organisations qui utilisent des 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. Un compte permet de gérer centralement les requêtes électroniques envoyées par les collaborateurs de l'organisation à Kaspersky Lab et de gérer les autorisations de ces collaborateurs dans le Kaspersky CompanyAccount.

Le service en ligne 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).

COLLECTE D'INFORMATIONS POUR LE SUPPORT TECHNIQUE

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander de générer un rapport contenant les informations suivantes :

- paramètres de configuration de l'image de la machine virtuelle ;
- version de l'hyperviseur VMware ESXi ;
- version du serveur VMware vCenter ;
- version du module VMware vShield Endpoint ;
- version de la distribution VMware Tools installée sur la machine virtuelle protégée ;
- liste des technologies VMware utilisées (View, DRS, DPM, HA, FT) ;
- version du Kaspersky Security Center ;
- pour l'ordinateur sur lequel l'application Kaspersky Security Center est installée : la version du système d'exploitation et la version de Microsoft .NET Framework.

Le rapport obtenu doit ensuite être envoyé au Support technique.

Il peut être nécessaire de désactiver la fonction d'annulation des modifications en vue de l'analyse des erreurs survenues au cours de l'installation ou de la mise à jour de la machine virtuelle de protection. Pour désactiver la fonction d'annulation des modifications, vous devez modifier le fichier KsvInstaller.exe.config. Ce fichier est situé sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center qui est à l'origine de l'installation des machines virtuelles de protection (cf. informations détaillées sur la page de l'application dans la Base de connaissances http://support.kaspersky.com/fr/11696).

Pour analyser les erreurs de fonctionnement de Kaspersky Security, les spécialistes du Support Technique peuvent vous demander de recourir aux utilitaires suivants inclus dans la distribution de l'application :

- inventory_view_format_client, inventory_view_tree_client : utilitaires permettant de collecter des informations à propos de l'infrastructure virtuelle VMware ;
- licenser_client : utilitaire destiné à l'administration des clés et à la consultation des informations relatives à la licence ;
- qb_client : utilitaire destiné à l'utilisation des copies de sauvegarde des fichiers dans la sauvegarde ;
- tracer_configurator_client : utilitaire permettant de configurer les paramètres de saisie des journaux de Kaspersky Security ;
- updater_client : utilitaire permettant d'exécuter la mise à jour des bases antivirus ou la remise à l'état antérieur à la mise à jour ;
- vcenter_creds : utilitaire destiné à la consultation ou à la modification des paramètres de connexion de la machine virtuelle de protection au serveur VMware vCenter ou au Serveur d'intégration ;
- vcenter_creds_test_client : utilitaire permettant d'établir une connexion test entre la machine virtuelle de protection et le serveur VMware vCenter ou le Serveur d'intégration en vue de la vérification des paramètres de connexion ;
- vshield_manager_client : utilitaire permettant d'exécuter l'enregistrement, l'annulation de l'enregistrement et la vérification de l'enregistrement des machines virtuelles de protection dotées du module Anti-Virus Fichiers dans VMware vShield Manager ;
- klmover : utilitaire permettant de modifier l'adresse du Serveur d'administration de Kaspersky Security Center et le mode d'échange des données dans les paramètres de configuration des machines virtuelles de protection.

Des informations détaillées sur l'exploitation des utilitaires sont disponibles sur la page dédiée à l'application dans la base de connaissances (http://support.kaspersky.com/fr/11079).

UTILISATION DU FICHIER DE TRAÇAGE

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander d'envoyer le fichier de traçage de la machine virtuelle de protection.

Pour savoir comment obtenir le fichier de traçage de la machine virtuelle de protection, consultez la page dédiée à l'application dans la Base des connaissances http://support.kaspersky.com/fr/11049.

UTILISATION DES FICHIERS DE STATISTIQUES SYSTEME

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander d'envoyer le fichier de statistiques système de la machine virtuelle de protection.

Pour savoir comment obtenir le fichier de statistiques système de la machine virtuelle de protection, consultez la page dédiée à l'application dans la Base des connaissances http://support.kaspersky.com/fr/11051.

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.

AGENT D'ADMINISTRATION

Module de l'application Kaspersky Security Center qui crée une interaction entre le Serveur d'administration et les modules de l'application Kaspersky Security installés sur les machines virtuelles de protection. Le module Agent d'administration est unique pour tous les programmes Windows faisant partie des produits de Kaspersky Lab. Pour les applications Novell®-, Unix™- et Mac® de Kaspersky Lab, il existe d'autres versions de l'Agent d'administration.

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.

CLUSTER KSC

Regroupement dans l'application Kaspersky Security Center de machines virtuelles de protection installées sur des hyperviseurs VMware ESXi administrés par un serveur VMware vCenter et des machines virtuelles qu'elles protègent.

CLE

Séquence unique de chiffres et de lettres. La clé permet l'utilisation de l'application conformément aux conditions du Contrat de licence (au type de licence, à la durée de validité de la licence, aux restrictions imposées par la licence).

CLE ACTIVE

Clé utilisée lors du fonctionnement de l'application.

CLE 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 avec des systèmes d'exploitation invités Windows installés sur les hyperviseurs VMware ESXi dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

CLE COMPLEMENTAIRE

Clé confirmant le droit d'utilisation de l'application mais qui ne s'utilise pas lors du fonctionnement.

CLE 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.

CLE 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 20 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 d'un fichier de la machine virtuelle, créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde sont conservées dans la sauvegarde sous un format spécial et ne présentent aucun danger.

F

FICHIER CLE

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.

G

GLOSSAIRE

GROUPE D'ADMINISTRATION

Ensemble d'ordinateurs reliés au Kaspersky Security Center conformément aux fonctions exécutables et aux applications Kaspersky Lab installées. Les ordinateurs sont regroupés pour plus de facilité, dans la mesure où ils sont gérés comme une seule entité. Le groupe d'administration peut inclure d'autres groupes. Pour chacune des applications installées dans le groupe d'administration, des stratégies propres à chaque groupe peuvent être définies. Chaque groupe peut également se voir attribuer des tâches.

I

INFRASTRUCTURE PROTEGEE DU CLUSTER KSC

Objets d'administration VMware administré par le serveur VMware vCenter correspondant au cluster KSC.

K

KASPERSKY COMPANYACCOUNT

Service Internet conçu pour l'envoi de demandes électroniques à Kaspersky Lab et le suivi de leur traitement par les spécialistes.

KASPERSKY SECURITY NETWORK (KSN)

Infrastructure de services en ligne et de services fournissant un accès à la base opérationnelle de connaissances de Kaspersky Lab sur la réputation des fichiers, des ressources Internet 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 inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit le nombre de faux positifs.

L

LICENCE

Droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du contrat de licence.

M

MACHINE VIRTUELLE DE PROTECTION

Machine virtuelle sur l'hyperviseur VMware ESXi hébergeant le module de l'application Kaspersky Security.

O

OBJET OLE

Objet qui est lié à un autre fichier ou inclus dans un autre fichier utilisant la technologie Object Linking and Embedding (OLE). Par exemple, l'objet OLE peut être un tableau Microsoft Office Excel® inclus dans un document Microsoft Office Word.

P

PROFIL DE PROTECTION

Le profil de protection détermine dans la stratégie les paramètres de protection des machines virtuelles. Une stratégie peut contenir plusieurs profils de protection. Un profil de protection est attribué aux objets d'administration de VMware appartenant à l'infrastructure protégée du cluster KSC. Un objet d'administration VMware ne peut se voir attribuer qu'un seul profil de protection. La machine virtuelle de protection protège la machine virtuelle selon les paramètres définis dans le profil de protection qui lui a été attribué.

PROFIL DE PROTECTION RACINE

Profil de protection racine que vous générez pendant la création d'une stratégie. Le profil de protection racine est automatiquement attribué à l'objet racine de la structure des objets d'administration de VMware, à savoir le serveur VMware vCenter.

S

SAUVEGARDE

Sauvegarde spécialisée des copies des fichiers qui ont été supprimés ou modifiés durant la réparation.

SERVEUR D'ADMINISTRATION

Module 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 A JOUR

Ressource qui contient les mises à jour des bases et des modules 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.

STRATEGIE

Définit les paramètres de la protection des machines virtuelles contre les virus et autres programmes dangereux, les paramètres de la protection des machines virtuelles contre les intrusions et les paramètres des sauvegardes sur les machines virtuelles de protection.

T

TACHE D'AJOUT DE CLE

Ajoute la clé sur toutes les machines virtuelles de protection dans le cadre d'un cluster KSC, c'est à dire sur toutes les machines virtuelles installées sur les hyperviseurs VMware ESXi administrés par un serveur VMware vCenter.

TACHE D'ANALYSE COMPLETE

Définit les paramètres d'analyse des machines virtuelles de tous les clusters.

TACHE D'ANALYSE PERSONNALISEE

Définit les paramètres d'analyse des machines virtuelles qui appartiennent au cluster KSC indiqué.

TACHE DE DIFFUSION DES MISES A JOUR

Au cours de cette tâche, le Kaspersky Security Center peut diffuser et installer automatiquement les mises à jour des bases antivirus sur les machines virtuelles de protection.

TACHE DE REMISE A L'ETAT ANTERIEUR A LA DERNIERE MISE A JOUR

Au cours de cette tâche, le Kaspersky Security Center revient à l'état antérieur à la dernière mise à jour des bases antivirus sur les machines virtuelles de protection.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les 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 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de systèmes de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

PRODUITS. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les réseaux informatiques d'entreprise.

La gamme de logiciels pour particuliers reprend des applications antivirus 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 propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace et automatisée de l'organisation 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 multiples plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils détectent des centaines de nouvelles menaces informatiques, développent des outils d'identification et de neutralisation contre ces menaces, et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont mises à jour toutes les heures*, tandis que *les bases antispam* sont mises à jour *toutes les 5 minutes*.

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (E-U), Alt-N Technologies (E-U), Blue Coat Systems (E-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (E-U), Openwave Messaging (Irlande), D-Link (Taïwan), M86 Security (E-U), GFI Software (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), Netasq+Arkoon (France), NETGEAR (E-U), Parallels (E-U), SonicWALL (E-U), WatchGuard Technologies (E-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. 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 300 millions d'utilisateurs. La société compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.viruslist.com/fr
Laboratoire d'étude des virus :	http://newvirus.kaspersky.com/fr (pour l'analyse des fichiers et sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATION 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 COMMERCIALES

Les marques et marques de service déposées appartiennent à leurs propriétaires respectifs.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans d'autres pays.

Mac : marque déposée Apple Inc.

Microsoft, Windows, Excel et Windows Server sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Novell est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

SUSE est une marque commerciale de SUSE LLC déposée aux Etats-Unis et dans d'autres pays.

UNIX est une marque utilisant une licence X/Open Company Limited déposée aux Etats-Unis et dans d'autres pays.

VMware, VMware vSphere, vShield, vCenter, VMware vCloud, ESX sont des marques commerciales ou déposées de VMware, Inc, enregistrées aux Etats-Unis ou dans d'autres juridictions de VMware, Inc.

INDEX

A

Activation de l'application 30
Analyse des machines virtuelles 65
Anti-Virus Fichiers 57
Architecture de l'application 17

C

Clé 28
Clé avec limitation en fonction du nombre de cœurs 29
Clé pour poste de travail 29
Clé pour serveur 29
Cluster KSC 22
Contrat de licence utilisateur final 26

D

Détection des intrusions 82

F

Fichier clé 29

H

Héritage des profils de protection 24

I

Image de la machine virtuelle 18
Infrastructure protégée du cluster KSC 22, 53

K

Kaspersky Security Network 113

L

Licence 26
  code d'activation 29
  renouvellement 36

M

Machine virtuelle de protection 17
Modules de Kaspersky Security 11

P

Profil de protection 23, 58
Profil de protection racine 24
Protection des machines virtuelles 57

R

Rapports 99

S

Sauvegarde ... 87
Source des mises à jour ... 91
Stratégie ... 23
  création ... 46

T

Tâche
  analyse complète ... 65
  analyse personnalisée ... 65
  diffusion des mises à jour ... 91
  remise à l'état antérieur à la dernière mise à jour ... 94
Tâche d'ajout de clé ... 30