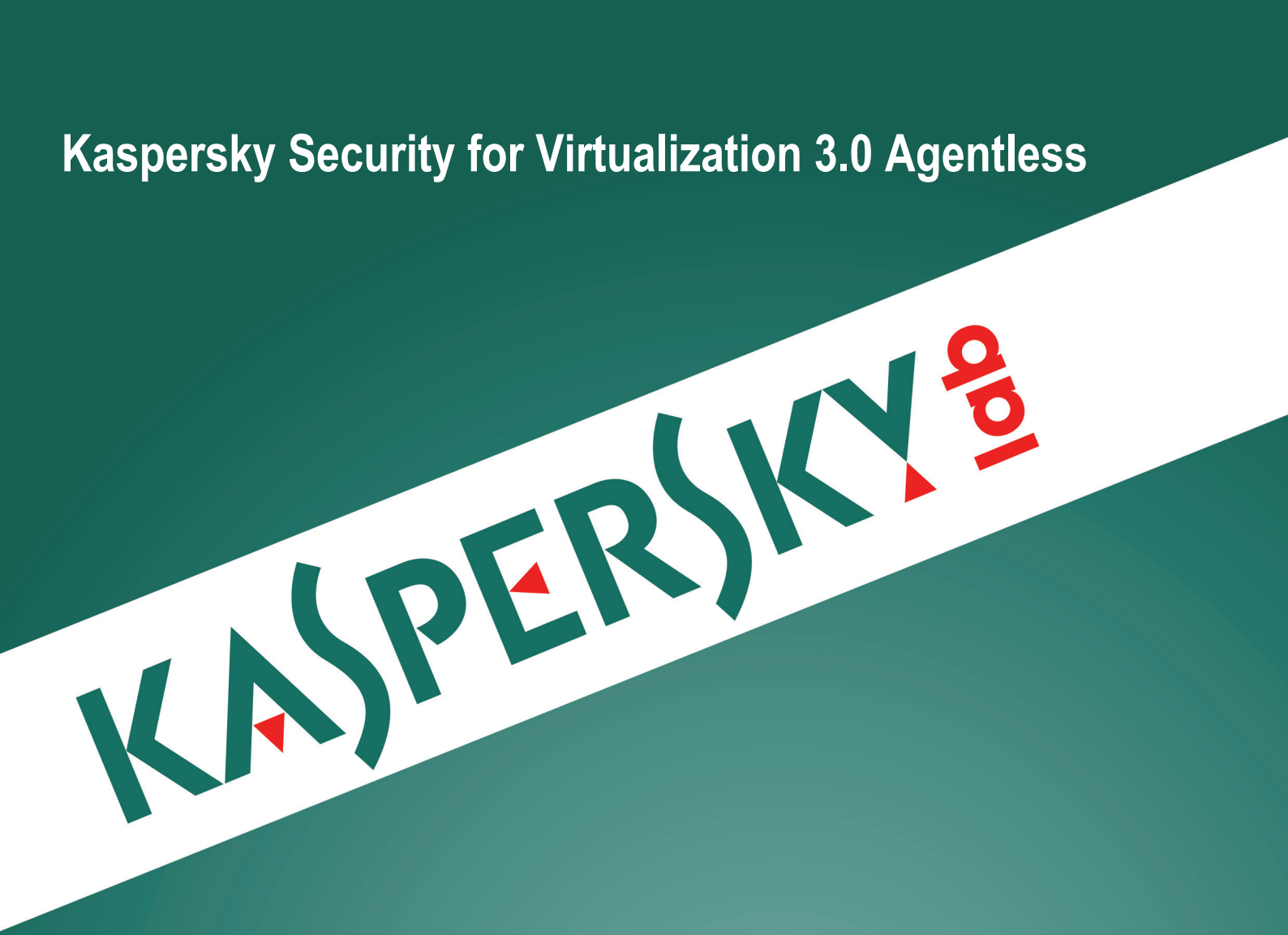
Kaspersky Security for Virtualization 3.0 Agentless



Manuel de l'administrateur

VERSION DE L'APPLICATION : 3.0

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 : 25/04/2014

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

TABLE DES MATIERES

PRESENTATION DU MANUEL

Le présent document constitue le Manuel de l'administrateur de Kaspersky Security for Virtualization 3.0 Agentless (ci-après : Kaspersky Security).

Il est destiné aux techniciens chargés d'installer et d'administrer Kaspersky Security et d'offrir une assistance technique aux sociétés 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.
- Aider à planifier le déploiement de Kaspersky Security sur le réseau de la société.
- Décrire les préparatifs de l'installation de Kaspersky Security, l'installation et l'activation de l'application.
- 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

Ce manuel contient les sections suivantes :

Sources d'informations sur l'application (cf. page 13)

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 15)

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

Architecture de l'application (cf. page 20)

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. 24)

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

Installation de l'application (cf. page 28)

Cette section explique comment installer l'application dans l'infrastructure virtuelle VMware.

Modifier la configuration des machines virtuelles de protection avec le module Antivirus Fichiers (cf. à la page 46)

Cette section explique la modification de la configuration des machines virtuelles de protection dotées du module Antivirus Fichiers.

Mise à jour des versions précédentes de l'application (cf. page 50)

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

Suppression de l'application (cf. page 67)

Cette section comprend des informations sur la suppression des modules Antivirus Fichiers et Détection des menaces réseau de Kaspersky Security.

Elimination des erreurs d'enregistrement des machines virtuelles de protection (cf. page 78)

Cette section contient la description des erreurs d'enregistrement possibles des machines virtuelles de protection dotées du module Antivirus Fichiers dans VMware vShield™ Manager et les moyens pour s'en débarrasser.

Licence de l'application (cf. page 82)

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.

Création d'une stratégie (cf. page 99).

Cette section explique la création et la configuration des stratégies pour l'application Kaspersky Security.

Lancement et arrêt de l'application (cf. page 106)

Cette section explique comment lancer et arrêter l'application.

Administration de la protection (cf. page 107)

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

Protection des fichiers du système de machines virtuelles. Antivirus Fichiers (cf. page 108)

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

Protection des machines virtuelles contre les menaces réseau. Détection des menaces réseau (cf. page 134)

Cette section contient des informations sur la configuration des paramètres du module de détection des menaces réseau.

Sauvegarde (cf. page 139)

Cette section présente la sauvegarde et explique comment la manipuler.

Mise à jour des bases antivirus (cf. page 144)

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 150)

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

Participation au Kaspersky Security Network (cf. page 164)

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 167)

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 170)

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

Kaspersky Lab ZAO (cf. page 174)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (cf. page 175)

Cette section contient des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page 176)

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 document comprend des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le 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. Les avertissements contiennent des informations sur les actions indésirables potentielles qui peuvent amener à la perte d'informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes de paramètres ou des cas particuliers importants pour le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases 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 de touches **ALT+F4**.	Les noms des touches du clavier sont en caractères gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il est nécessaire d'appuyer simultanément sur ces touches.
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 par l'utilisateur.
<Nom de l'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 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.

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 D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- la page du site de Kaspersky Lab ;
- la page sur le site Internet du Support Technique (Base de connaissances) ;
- l'aide électronique ;
- la documentation.

Si vous ne parvenez pas à résoudre vous-même le problème, il est conseillé de contacter le Support technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 167).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

Page sur le site Internet de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page dédiée pour chaque application.

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

La page http://www.kaspersky.com/fr 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 sur le site Internet du Support Technique (Base de connaissances)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations d'utilisation des applications de Kaspersky Lab. La Base de connaissances est composée d'articles d'aide regroupés par thèmes.

La page de l'application dans la Base des connaissances (http://support.kaspersky.com/ksv3a) 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 peuvent répondre à des questions en rapport non seulement avec Kaspersky Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support Technique en général.

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 des 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.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du Service commercial par l'un des moyens suivants :

- En appelant notre siège en France (http://www.kaspersky.com/fr/contacts).
- En envoyant vos questions à l'adresse sales@kaspersky.com.

La réponse vous sera donnée en français ou en anglais suivant votre demande.

CONTACTER PAR COURRIER ELECTRONIQUE LE SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Pour contacter le Service de localisation et de rédaction de la documentation technique, il est nécessaire d'envoyer un message à l'adresse docfeedback@kaspersky.com. L'objet du message doit être "Kaspersky Help Feedback : Kaspersky Security for Virtualization 3.0. Agentless".

KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS

Kaspersky Security for Virtualization 3.0 Agentless est une solution intégrée qui protège les machines virtuelles sur l'hôte VMware ESXi contre les virus et autres programmes dangereux pour la sécurité de l'ordinateur (ci-après "contre les virus et autres programmes dangereux") et les menaces pesant sur le réseau. Les modules 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 17).

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 vShield Endpoint Thin Agent et que celui-ci est 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 : VMware vCenter™ Server, objet Datacenter, cluster VMware, hôte 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 :

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

- *Détection des menaces réseau* : 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 URL sollicitée par l'utilisateur à une base d'adresses URL malveillantes et bloque l'accès aux adresses URL nuisibles. Dans VMware vShield Manager, le module Détection des menaces réseau s'enregistre comme un service de Kaspersky Network Protection.

Kaspersky Security offre les possibilités suivantes :

- **Protection**. L'application protège le système de fichiers du système d'exploitation invité de la machine virtuelle (ci-après, "les fichiers de la machine virtuelle"). Elle analyse tous les fichiers que l'utilisateur ou une autre application ouvre et ferme 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 URL**. L'application confronte les adresses URL ou les applications HTTP sollicitées par l'utilisateur à une base d'adresses URL malveillantes. En cas de détection d'une adresse URL dans la base des adresses URL malveillantes, l'application peut bloquer l'accès à cette adresse. Kaspersky Security transmet les informations sur tous les événements survenus dans le cadre de l'analyse des adresses URL 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 antivirus. 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 antivirus ;
- 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

NOUVEAUTES

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

- Prise en charge complémentaire de VMware vSphere 5.5.
- En cas de détection d'une URL figurant dans la base des URL malveillantes et de blocage de la page Internet, Kaspersky Security fait apparaître un message de blocage de la page Internet dans la fenêtre du navigateur.
- Nouvelle prise en charge des systèmes d'exploitation invités suivants sur les machines virtuelles protégées par le module Antivirus Fichiers :
  - Windows 8 (versions 32 ou 64 bits) ;
  - Windows Server® 2003 R2 (versions 32 ou 64 bits) ;
  - Windows Server 2012 sans prise en charge de ReFS (Resilient File System) (version 64 bits).
- Possibilité de supprimer au cours d'une seule procédure le module Détection des menaces réseau de l'infrastructure virtuelle VMware. Pour supprimer le module Détection des menaces réseau de tous les cluster VMware, il n'est pas nécessaire d'exécuter deux procédures (suppression des machines virtuelles de protection dotées du module Détection des menaces réseau et annulation de l'enregistrement du module Détection des menaces réseau (service Kaspersky Network Protection) dans VMware vShield Manager).

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 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 le fonctionnement de Kaspersky Security sur le réseau local de l'organisation, l'application Kaspersky Security Center 10 Maintenance Release 1 doit être installée.

L'ordinateur sur lequel est installée la Console d'administration du Kaspersky Security Center doit être équipé de Microsoft® .NET Framework 3.5 ou suivant.

Configuration requise pour le composant Antivirus Fichiers

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

- Hyperviseur VMware ESXi 5.5 patch 1 ou hyperviseur VMware ESXi 5.1 patch 2.
- VMware vCenter Server 5.5 patch 1 ou VMware vCenter Server 5.1 patch 2.
- VMware vShield Endpoint du paquet VMware vCloud™ Networking and Security 5.5.2 ou du paquet VMware vCloud Networking and Security 5.1.4.
- VMware vShield Manager du paquet VMware vCloud Networking and Security 5.5.2 ou du paquet VMware vCloud Networking and Security 5.1.4.
- Pilote VMware vShield Endpoint Thin Agent. Le pilote est repris dans la distribution VMware Tools, livrée avec l'hyperviseur VMware ESXi 5.5 patch 1 et l'hyperviseur VMware ESXi 5.1 patch 2. 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 menaces réseau

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

- Hyperviseur VMware ESXi 5.5 patch 1 ou hyperviseur VMware ESXi 5.1 patch 2.
- VMware vCenter Server 5.5 patch 1 ou VMware vCenter Server 5.1 patch 2.
- VMware vShield Manager du paquet VMware vCloud Networking and Security 5.5.2 ou du paquet VMware vCloud Networking and Security 5.1.4.
- VMware Distributed Virtual Switch 5.1.0 et suivante.

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

Le module Antivirus 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 (versions 32 ou 64 bits) ;
  - Windows 8 (versions 32 ou 64 bits) ;
- Systèmes d'exploitation pour serveurs :
  - Windows Server 2003 SP2 ou suivant (versions 32 ou 64 bits) ;
  - Windows Server 2003 R2 (versions 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).

Les exigences du module Détection des menaces réseau envers le système d'exploitation invité de la machine virtuelle protégée correspondent aux exigences des hyperviseurs VMware ESXi 5.5 patch 1 ou VMware ESXi 5.1 patch 2 vis-à-vis des systèmes d'exploitation invités.

Le module Détection des menaces réseau assure uniquement la protection des machines virtuelles utilisées avec l'adaptateur réseau E1000.

Configuration matérielle requise

Il est nécessaire d'octroyer une quantité minimale de ressources système à la machine virtuelle de protection dotée du module Antivirus 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 menaces réseau :

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

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

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

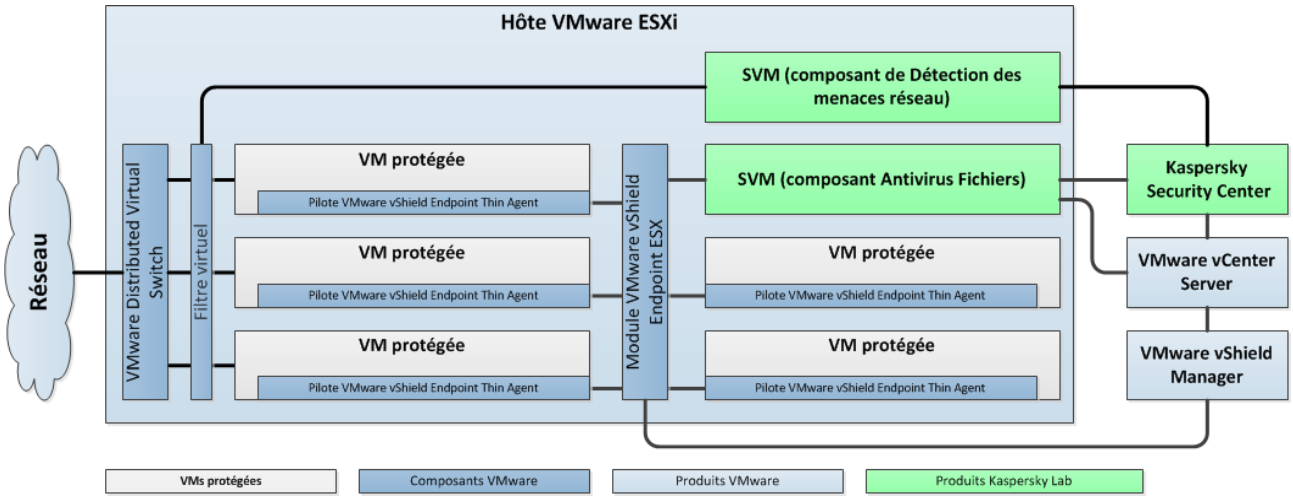


Illustration 1. Architecture de l'application

Kaspersky Security est installé sur un hôte VMware ESXi et garantit la protection des machines virtuelles sur cet hôte 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 21) :

- image de la machine virtuelle de protection assortie du module Antivirus Fichiers ;
- image de la machine virtuelle de protection sur laquelle le module Détection des menaces réseau est installé.

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

Installés sur un hôte VMware ESXi, les modules de l'application Kaspersky Security, garantissent la protection de toutes les machines virtuelles sur cet hôte. 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 hôtes VMware ESXi. Kaspersky Security doit être installé sur chaque hôte VMware ESXi dont vous souhaitez 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 comprenant le module Console d'administration du Kaspersky Security Center (cf. section "Installation des plug-ins d'administration Kaspersky Security" à la page 31).

DANS CETTE SECTION

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 Antivirus Fichiers entrent :

- Le système d'exploitation SUSE Linux® Enterprise Server 11 SP3.
- Le module Kaspersky Security Antivirus 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 menaces réseau entrent :

- Le système d'exploitation SUSE Linux Enterprise Server 11 SP3.
- Module Détection des menaces réseau 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 DE KASPERSKY SECURITY A L'INFRASTRUCTURE VIRTUELLE VMWARE

L'intégration de l'Antivirus Fichiers à l'infrastructure virtuelle de VMware requiert les modules suivants :

- **VMware vShield Endpoint ESX™ Module**. Ce module est installé sur l'hôte VMware ESXi. Il assure l'interaction du pilote VMware vShield Endpoint Thin Agent installé sur la machine virtuelle et de la bibliothèque ESPEC installée sur la machine virtuelle de protection.
- **VMware vCenter Server**. 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. Ce module offre des informations sur les machines virtuelles installées sur les hôtes VMware ESXi.
- **VMware vShield Manager**. Ce module assure l'installation de VMware vShield Endpoint ESX Module sur les hôtes VMware ESXi et l'intégration des machines virtuelles de protection.

Le pilote VMware vShield Endpoint Thin Agent collecte les informations relatives aux 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 vShield Endpoint Thin Agent sur ces dernières. Le pilote est repris dans la distribution VMware Tools, livrée avec l'hyperviseur VMware ESXi 5.5 patch 1 et l'hyperviseur VMware ESXi 5.1 patch 2.

L'intégration du module Détection des menaces réseau 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.
- **VMware vCenter Server**. 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 sur les machines virtuelles installées sur les hôtes VMware ESXi, les clusters VMware, les services installés et les paramètres de VMware Distributed Virtual Switches.
- **VMware vShield Manager**. Ce module garantit l'enregistrement et le déploiement du module Détection des menaces réseau (service Kaspersky Network Protection), le déploiement et l'enregistrement des machines virtuelles de protection sur les hôtes 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 Antivirus 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 vShield Endpoint Thin Agent intercepte les informations relatives à ces événements et les transmet au module VMware vShield Endpoint ESX Module, installé sur l'hôte 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 Antivirus Fichiers installé sur la machine virtuelle de protection et garantit l'accès aux fichiers sur la machine virtuelle.
5. Le module Antivirus 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 25). Par exemple, Kaspersky Security peut réparer ou bloquer le fichier.

Le module Détection des menaces réseau 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 menaces réseau installé sur la machine virtuelle de protection.
2. Le module Détection des menaces réseau 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 25), 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 URL présentes dans les paquets réseaux à la base des adresses URL malveillantes.

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

  - Si une adresse URL figure dans la base des adresses URL malveillantes, 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 25), attribué à cette machine virtuelle. Par exemple, Kaspersky Security bloque ou autorise l'accès à cette adresse URL.

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 VMware vCenter Server.

Les machines virtuelles de protection installées sur les hôtes VMware ESXi sous une plateforme VMware vCenter Server et les machines virtuelles qu'ils 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 de la plateforme VMware vCenter Server correspondante. Les objets d'administration VMware appartenant à cette plateforme VMware vCenter Server forment l'*infrastructure protégée* du cluster KSC.

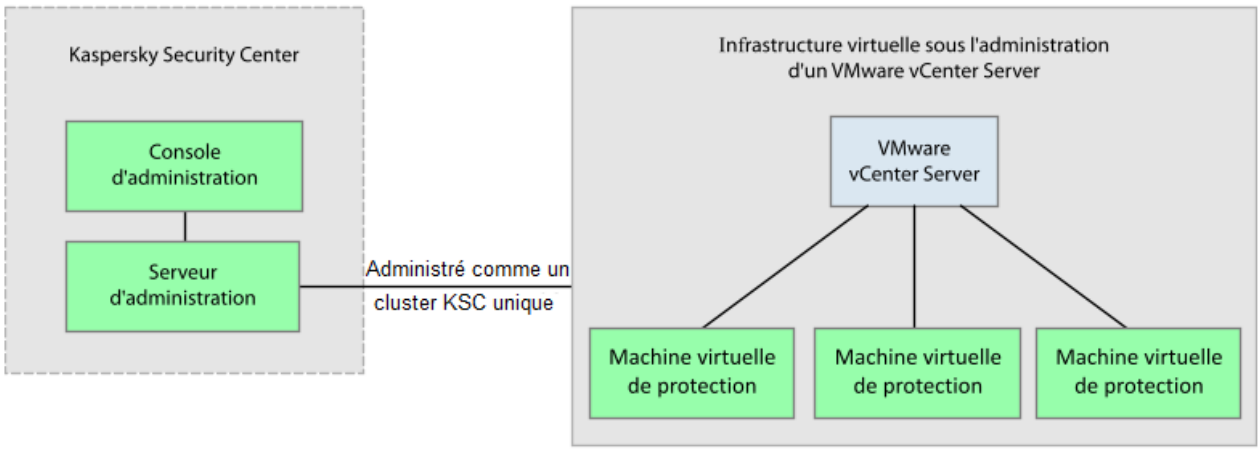


Illustration 2. Cluster KSC

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, les paramètres d'analyse des fichiers compactés (cf. section "Création d'une stratégie" à la page 99), les paramètres de détection des attaques réseau et les paramètres des sauvegardes sur les machines virtuelles de protection (cf. section "A propos de la sauvegarde" à la page 139).

- Les *tâches d'analyse* déterminent les paramètres d'analyse des machines virtuelles (cf. section "Analyse des machines virtuelles" à la page 118).

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 STRATEGIE DE KASPERSKY SECURITY ET DES PROFILS DE PROTECTION

Dans le cas de Kaspersky Security, la stratégie s'applique 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.

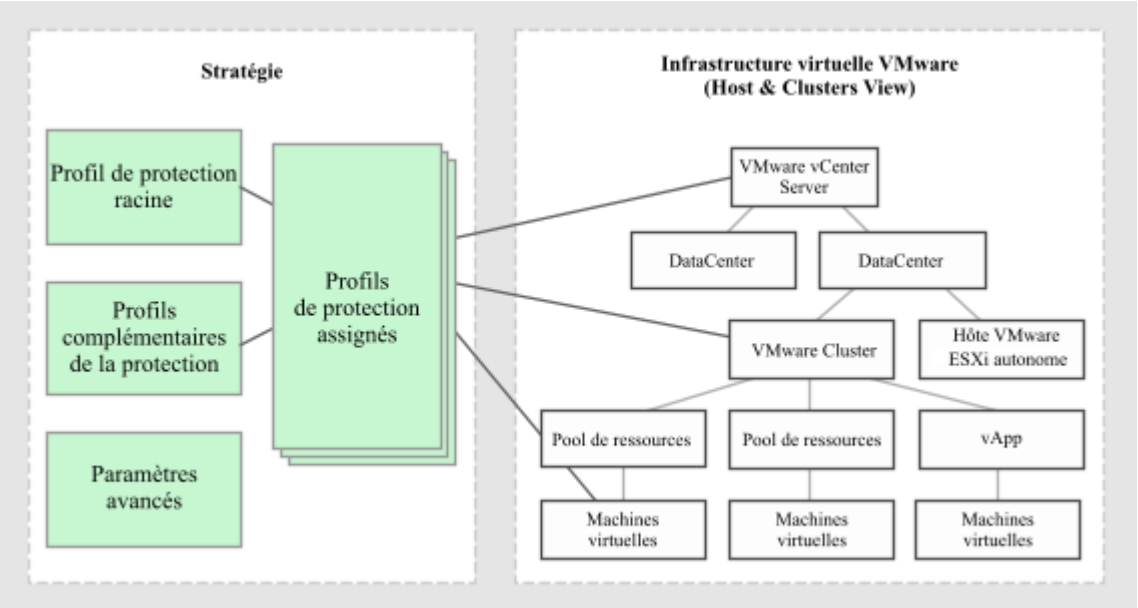


Illustration 3. Profils de protection

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

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 à VMware vCenter Server. Si vous utilisez la hiérarchie complexe des groupes d'administration et des stratégies, la stratégie du niveau inférieur hérite des paramètres incorrects de connexion à VMware vCenter Server, 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

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 117) 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 111). 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 VMware vCenter Server. 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. 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.

INSTALLATION DE L'APPLICATION

Cette section fournit les informations suivantes :

- ordre des étapes d'installation de Kaspersky Security ;
- description de la procédure à suivre avant d'installer l'application ;
- instructions pour l'installation des modules Antivirus Fichiers et Détection des menaces réseau de Kaspersky Security ;
- informations sur la consultation de la liste des machines virtuelles de protection et des machines virtuelles protégées installées dans la Console d'administration du Kaspersky Security Center.

DANS CETTE SECTION

ORDRE DES ETAPES D'INSTALLATION DE L'APPLICATION

L'installation de l'application Kaspersky Security dans l'infrastructure virtuelle VMware comprend les étapes suivantes :

1. Préparation de l'installation des modules de Kaspersky Security (cf. section "Préparation de l'installation" à la page. 29).
2. Installation du module Antivirus Fichiers (cf. section "Procédure d'installation du module Antivirus Fichiers" à la page 32). L'installation du module Antivirus Fichiers se déroule via le déploiement des machines virtuelles de protection dotées du module Antivirus Fichiers sur les hôtes VMware ESXi.
3. Installation du module Détection des menaces réseau (cf. section "Procédure d'installation du module Détection des menaces réseau" à la page 39). L'installation du module Détection des menaces réseau dans l'infrastructure virtuelle VMware se déroule via le déploiement des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi et via l'enregistrement du module Détection des menaces réseau sur le VMware vShield Manager.
4. Activation de l'application sur l'ensemble des machines virtuelles de protection (cf. section "Activation de l'application" à la page 85).
5. Configuration des paramètres de fonctionnement de l'application avec la stratégie (cf. section "Création d'une stratégie" à la page 99). Kaspersky Security commence à protéger les machines virtuelles seulement après la configuration des paramètres de fonctionnement de l'application avec une stratégie.

   Après l'installation du module Détection des menaces réseau, il convient d'activer la détection des attaques réseau (cf. section "Activation et désactivation de la détection des attaques réseau" page 135) et l'analyse des adresses URL (cf. section "Activation et désactivation de l'analyse des adresses URL" page 137) dans les paramètres de la stratégie. Par défaut, Kaspersky Security ne détecte pas les attaques réseau et n'analyse pas les adresses URL.
6. Mise à jour des bases antivirus sur l'ensemble des machines virtuelles de protection (cf. section "Mise à jour des bases antivirus" à la page 144).

PREPARATION DE L'INSTALLATION

Cette section présente les prérequis pour les modules du Kaspersky Security Center et de l'infrastructure virtuelle VMware, ainsi que les préparatifs d'installation de l'application.

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

- Vérifier la sélection de modules du Kaspersky Security Center et de l'infrastructure virtuelle VMware (cf. section "Prérequis pour les modules du Kaspersky Security Center et de l'infrastructure virtuelle VMware" à la page 30).
- Installer le plug-in d'administration de Kaspersky Security (cf. section "Installation du plug-in d'administration de Kaspersky Security" à la page 31).
- Confirmer que la plateforme Microsoft .NET Framework 3.5 ou suivante est installée sur l'ordinateur où est installée la Console d'administration du Kaspersky Security Center. La plateforme Microsoft .NET Framework 3.5 ou suivante est requise pour le fonctionnement de l'Assistant d'installation de l'application.
- Confirmer qu'aucun logiciel antivirus n'est installé sur les machines virtuelles que vous avez l'intention de protéger à l'aide de Kaspersky Security.

  L'utilisation conjointe de Kaspersky Security et d'un logiciel antivirus peut entraîner un conflit.

- Configurer les paramètres de comptes VMware vCenter Server requis pour l'installation et l'utilisation de l'application (cf. section "Comptes utilisateur VMware vCenter Server" à la page 31).
- S'assurer que l'image de la machine virtuelle de protection provient d'une source sûre. Pour en savoir plus sur les procédés de vérification de l'authenticité de l'image de la machine virtuelle de protection, consultez la page de l'application dans la Banque de solutions http://support.kaspersky.com/legacy/fr/find?faq_id=11050.

Si vous souhaitez installer le module Détection des menaces réseau, vous devez réaliser les actions supplémentaires suivantes :

- Configurer les paramètres des groupes de ports distribués (Distributed Virtual Port Groups) dans VMware Distributed Virtual Switches.
- Placer tous les fichiers de l'image de la machine virtuelle de protection dans un dossier sur la ressource réseau accessible par un protocole HTTP.
- Pour chaque hôte VMware ESXi sur lequel sera installé une machine virtuelle de protection, configurer les paramètres Agent VM Settings suivants : choisir le référentiel de données (Datastore) dans lequel seront conservés les fichiers de la machine virtuelle de protection et le réseau qu'elle doit utiliser pour se connecter au Serveur d'administration du Kaspersky Security Center. La configuration s'opère dans VMware vSphere Client sous l'onglet **Configuration**, groupe de paramètres **Agent VM Settings**. Pour en savoir plus sur la configuration des paramètres Agent VM Settings, consultez la documentation des produits VMware.

DANS CETTE SECTION

PREREQUIS POUR LES MODULES DU KASPERSKY SECURITY CENTER ET DE L'INFRASTRUCTURE VIRTUELLE VMWARE

Avant d'installer l'application, il convient de vérifier les éléments suivants :

- la sélection des modules du Kaspersky Security Center ;
- la sélection des modules de l'infrastructure virtuelle VMware ;
- l'adéquation des modules du Kaspersky Security Center et des modules de VMware par rapport à la configuration requise pour l'installation de Kaspersky Security (cf. section " Configuration requise " à la page 17).

Modules du Kaspersky Security Center :

- Serveur d'administration.
- Console d'administration.
- Agent d'administration. Ce module figure dans les images des machines virtuelles de protection Kaspersky Security.

  Pour en savoir plus sur l'installation du Kaspersky Security Center, consultez la documentation du Kaspersky Security Center.

Modules de l'infrastructure virtuelle VMware nécessaires pour la configuration et le fonctionnement du module Antivirus Fichiers :

- VMware vCenter Server.
- VMware vSphere Client.
- VMware vShield Endpoint. Le module s'installe sur les hôtes VMware ESXi et assure l'interaction entre le pilote VMware vShield Endpoint Thin Agent sur les machines virtuelles et la bibliothèque EPSEC sur la machine virtuelle de protection.
- VMware vShield Manager. Ce module permet d'assurer une administration centralisée du réseau VMware vShield.
- Un ou plusieurs hôtes VMware ESXi sur lesquels les machines virtuelles sont déployées.
- Pilote VMware vShield Endpoint Thin Agent. Le pilote est repris dans la distribution VMware Tools, livrée avec l'hyperviseur VMware ESXi 5.5 patch 1 et l'hyperviseur VMware ESXi 5.1 patch 2. Le pilote doit être installé et activé sur les machines virtuelles que vous avez l'intention de protéger à l'aide de Kaspersky Security.

  Pour en savoir plus sur le pilote VMware vShield Endpoint Thin Agent, consultez la documentation des produits VMware.

Modules de l'infrastructure virtuelle VMware nécessaires pour l'installation et le fonctionnement du module Détection des menaces réseau :

- VMware vCenter Server.
- VMware vShield Manager. Le module permet de gérer les modules entrant dans la composition du VMware vCloud Networking and Security, ainsi que d'assurer l'enregistrement et le déploiement du module de Détection des menaces réseau (service Kaspersky Network Protection).
- VMware Distributed Virtual Switch. Le module permet de configurer les paramètres des groupes de ports distribués (Distributed Virtual Port Groups).

Il convient d'utiliser un serveur DHCP dans l'infrastructure VMware pour l'attribution des adresses IP et des noms des machines virtuelles de protection.

COMPTES VMWARE VCENTER SERVER

L'utilisation de l'application requiert la présence des comptes utilisateur VMware vCenter Server suivants :

- Pour installer et supprimer l'application, il est nécessaire de disposer du compte administrateur auquel le rôle système a été attribué avec les privilèges suivants :
  - Global/Licenses.
  - Datastore/Allocate space.
  - vApp/Import.
  - Network/Assign network.
  - Host/Inventory/Modify cluster.
  - Host/Configuration/Virtual machine autostart configuration.
  - Tasks/Create task.
  - Global/Cancel task.
  - Virtual machine/Configuration/Add new disk.
  - Virtual machine/Interaction/Power on.
  - Virtual machine/Inventory/Create new.
  - Virtual machine/Interaction/Power off.
  - VirtualMachine/Inventory/Remove.

  Le nom et le mot de passe de l'administrateur ne sont pas enregistrés dans les paramètres de l'application.
- Pour utiliser l'application et modifier la configuration des machines virtuelles de protection, il est nécessaire de disposer d'un compte auquel le rôle système prédéfini ReadOnly est attribué. Le rôle système ReadOnly possède par défaut les privilèges System.View, System.Read et System.Anonymous. Le nom et le mot de passe du compte sont conservés sous forme chiffrée sur les machines virtuelles de protection.

Les rôles doivent être attribués aux comptes du niveau supérieur dans la hiérarchie des objets d'administration VMware : au niveau de VMware vCenter Server.

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

INSTALLATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY SECURITY

Pour administrer l'application à l'aide du Kaspersky Security Center, il est nécessaire d'installer le plug-in d'administration de Kaspersky Security sur l'ordinateur où est installée la Console d'administration du Kaspersky Security Center.

Pour installer le plug-in d'administration de Kaspersky Security, procédez comme suit :

1. Copiez le fichier d'installation klcfginst.msi du plug-in d'administration de Kaspersky Security depuis la distribution du Kaspersky Security Center sur l'ordinateur où est installée la Console d'administration.

2. Lancez le fichier d'installation du plug-in d'administration Kaspersky Security sur l'ordinateur où figure la Console d'administration.

   L'installation s'opère via l'Assistant d'installation. Le plug-in d'administration de Kaspersky Security sera installé dans le dossier d'installation du Kaspersky Security Center.

Une fois l'installation terminée, le plug-in d'administration de Kaspersky Security apparaît dans la liste des plug-ins d'administration figurant dans les propriétés du Serveur d'administration.

Vous pouvez réinstaller le plug-in. Pour ce faire, saisissez `msiexec /i klcfginst.msi REINSTALLMODE=voums REINSTALL=ALL` sur la ligne de commande de l'ordinateur où est installée la Console d'administration.

PROCEDURE D'INSTALLATION DU MODULE ANTIVIRUS FICHIERS

L'installation du module Antivirus Fichiers dans l'infrastructure virtuelle VMware se déroule via le déploiement des machines virtuelles de protection dotées du module Antivirus Fichiers sur les hôtes VMware ESXi.

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

Pour installer le module Antivirus Fichiers, procédez comme suit :

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

2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.

3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.

4. Dans la fenêtre ouverte, choisissez l'option **Protection du système de fichiers des machines virtuelles** et passez à l'étape suivante de l'Assistant.

5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Installation**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à créer des machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'installation.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur VMware vCenter Server" à la page 31), l'Assistant le signale et ne passe pas à l'étape suivante.

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que VMware vCenter Server est accessible via le réseau, puis relancez l'installation de l'application.

ETAPE 3. SAISIE DE L'ADRESSE IP DU SERVEUR D'ADMINISTRATION DU KASPERSKY SECURITY CENTER

L'Assistant reçoit du Kaspersky Security Center l'adresse de connexion de la machine virtuelle à l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. Cette étape est accessible si l'adresse de connexion au Serveur d'administration du Kaspersky Security Center obtenue à partir du Kaspersky Security Center porte le nom NetBIOS ou DNS de l'ordinateur. Si l'adresse de connexion s'avère être l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center, cette étape est passée.

Désignez l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. L'adresse IP est indiquée au format IPv4.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SELECTION DU FICHIER IMAGE DE LA MACHINE VIRTUELLE DE PROTECTION

A cette étape, désignez le fichier de l'image de la machine virtuelle de protection dotée du module Antivirus Fichiers. Pour ce faire, cliquez sur le bouton **Parcourir** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier image de la machine virtuelle de protection. Il s'agit d'un fichier au format OVA.

L'Assistant vérifie l'image de la machine virtuelle de protection. Si l'image est endommagée ou si sa version n'est pas prise en charge par l'Assistant, il affiche un message d'erreur.

Si l'analyse réussit, les informations suivantes relatives à l'image de la machine virtuelle de protection sélectionnée apparaissent dans la partie inférieure de la fenêtre :

- **Nom de l'application** : nom de l'application installée sur la machine virtuelle de protection.
- **Version de l'application** : numéro de la version de l'application.
- **Version de l'image de la machine virtuelle de protection** : numéro de version de l'image de machine virtuelle de protection.
- **Editeur** : éditeur de l'application installée sur la machine virtuelle de protection.
- **Description** : brève description de l'application.
- **Editeur** : émetteur du certificat utilisé pour signer l'image de la machine virtuelle de protection.
- **Taille de l'image** : taille du fichier de l'image de la machine virtuelle de protection.
- **Taille sur le disque** : volume approximatif d'espace disque requis pour le déploiement de la machine virtuelle de protection dans le référentiel de données de l'hôte VMware ESXi :
  - dans le cadre de la répartition dynamique de l'espace disque avec l'utilisation de VMware vStorage Thin Provisioning ;
  - dans le cadre de la répartition de l'espace disque avec un volume fixe.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. LECTURE DES CONTRATS DE LICENCE

Cette étape vous permet de prendre connaissance des Contrats de licence que vous allez conclure avec Kaspersky Lab et avec la société SUSE LLC. La société SUSE LLC est propriétaire du système d'exploitation SUSE Linux Enterprise Server 11 SP3 installé sur la machine virtuelle de protection.

Lisez attentivement les Contrats de licence et, si vous en acceptez tous les points, cochez la case **J'accepte les conditions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. SELECTION DES HOTES VMWARE ESXI

A cette étape, sélectionnez les hôtes VMware ESXi sur lesquels vous souhaitez installer la machine virtuelle de protection.

Les colonnes du tableau affichent les informations relatives à l'ensemble des hôtes VMware ESXi dans le cadre d'une plateforme VMware vCenter Server :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Etat** : état actuel de l'hôte VMware ESXi : accessible ou inaccessible.
- **Machine virtuelle de protection** : indique si les machines virtuelles de cet hôte VMware ESXi sont protégées ou non :
  - **Installée** : une machine virtuelle de protection est installée sur l'hôte VMware ESXi.
  - **Non installée** : pas de machine virtuelle de protection installée sur l'hôte VMware ESXi.

Vous pouvez sélectionner les hôtes VMware ESXi accessibles via le réseau sur lesquels la machine virtuelle de protection n'est pas installée.

Pour sélectionner un hôte VMware ESXi, cochez la case en regard de son nom dans le tableau.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. SELECTION DE L'OPTION DE PLACEMENT ET DE CONFIGURATION DES PARAMETRES DE DEPLOIEMENT

A cette étape, sélectionnez l'option d'emplacement de la machine virtuelle de protection dans le stockage de données de l'hôte VMware ESXi :

- **Répartition dynamique à l'aide de VMware vStorage Thin Provisioning**. Pendant l'attribution de l'espace dans le stockage de données de l'hôte VMware ESXi pour la machine virtuelle de protection, un volume requis minimal est réservé. Ce volume augmente en fonction des besoins. Cette option est sélectionnée par défaut.
- **Répartition de l'espace disque avec un volume fixe**. Pendant l'attribution de l'espace dans le stockage de données de l'hôte VMware ESXi pour la machine virtuelle de protection, le volume requis est directement réservé.

Configurez les paramètres du processus de déploiement des machines virtuelles de protection. Si vous souhaitez que l'Assistant déploie les machines virtuelles de protection simultanément sur plusieurs VMware ESXi, cochez la case **Autoriser le déploiement en parallèle**. Dans le champ **Déployer simultanément sur un maximum de X hôtes VMware ESXi**, indiquez le nombre d'hôtes VMware ESXi sur lesquels les machines virtuelles de protection doivent être déployées simultanément.

Passez à l'étape suivante de l'Assistant.

ETAPE 8. SELECTION DU STOCKAGE DE DONNEES

A cette étape, sélectionnez pour chaque machine virtuelle de protection un stockage de données dans la liste des stockages connectés aux hôtes VMware ESXi.

Les colonnes du tableau reprennent les informations suivantes :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Nom de la machine virtuelle de protection** : nom de la machine virtuelle de protection installée sur cet hôte VMware ESXi. Les machines virtuelles de protection reçoivent automatiquement le nom ksv-<N> où N représente l'adresse IP ou le nom de domaine de l'hôte VMware ESXi sur lequel se trouve la machine virtuelle de protection. Par exemple, ksv-192-168-0-2 ou ksv-esx-avp-ru.

  Vous pouvez modifier le nom de la machine virtuelle de protection. Pour ce faire, double-cliquez gauche sur la colonne **Nom de la machine virtuelle de protection** et saisissez le nouveau nom.
- Le **référentiel de données** : reprend dans des listes déroulantes les noms des stockages de données connectés à l'hôte VMware ESXi. Si un seul stockage de données est connecté à l'hôte VMware ESXi, la liste déroulante ne contient qu'un seul nom.

Dans la liste déroulante de la colonne **Référentiel de données**, sélectionnez le stockage de données pour chaque machine virtuelle de protection.

Passez à l'étape suivante de l'Assistant.

ETAPE 9. CONFIGURATION DE LA CORRESPONDANCE DES RESEAUX VIRTUELS

A cette étape, définissez la correspondance entre les réseaux virtuels de la machine virtuelle de protection et l'hôte VMware ESXi :

- La colonne **Hôte VMware ESXi** affiche l'adresse IP ou le nom de domaine de l'hôte VMware ESXi sur lequel la machine virtuelle de protection est installée.
- Dans la colonne **Réseau VMware vShield**, sélectionnez dans la liste déroulante le réseau virtuel de l'hôte VMware ESXi que la machine virtuelle de protection doit utiliser pour communiquer avec le module VMware vShield Endpoint ESX Module. Ce module est installé sur l'hôte VMware ESXi. Il assure l'interaction du pilote VMware vShield Endpoint Thin Agent installé sur la machine virtuelle et de la bibliothèque ESPEC installée sur la machine virtuelle de protection.
- Dans la colonne **Réseau Utilisateur**, sélectionnez dans la liste déroulante le réseau virtuel de l'hôte VMware ESXi que la machine virtuelle de protection doit utiliser pour communiquer avec l'environnement externe du réseau et le Serveur d'administration du Kaspersky Security Center.

Passez à l'étape suivante de l'Assistant.

ETAPE 10. SAISIE DES PARAMETRES DE RESEAU

A cette étape, désignez les paramètres de réseau des machines virtuelles de protection :

- **Utiliser DHCP**. Utilisation du protocole de réseau DHCP qui permet aux machines virtuelles de protection d'obtenir automatiquement les paramètres de réseau. Cette option est sélectionnée par défaut.
- **Désigner manuellement pour chaque machine virtuelle de protection**. Les paramètres de réseau sont attribués manuellement pour les machines virtuelles de protection.
- **Distribuer à l'aide des paramètres définis**. Les paramètres de réseau sont attribués manuellement pour les machines virtuelles de protection à partir d'une plage définie. Si vous choisissez cette option, définissez les paramètres de réseau dans les champs **Passerelle**, **Serveur DNS** et **Masque de réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 11. SAISIE MANUELLE DES PARAMETRES DE RESEAU

Cette étape est accessible si, à l'étape précédente de l'Assistant, vous avez choisi le paramètre **Désigner manuellement pour chaque machine virtuelle de protection** ou **Répartir selon les paramètres définis**. Si vous avez choisi l'option **Utiliser DHCP**, cette étape est ignorée.

Si vous avez choisi le paramètre **Désigner manuellement pour chaque machine virtuelle de protection** à l'étape précédente de l'Assistant, indiquez manuellement tous les paramètres de réseau des machines virtuelles de protection. Si vous ne saisissez pas les paramètres de quelconque machine virtuelle de protection sur cette ligne, les paramètres de réseau obtenus via le protocole DHCP seront ceux utilisés pour cette machine virtuelle de protection.

Si vous avez choisi l'option **Répartir selon les paramètres définis** à l'étape précédente, les colonnes **Passerelle**, **Serveur DNS** et **Masque de réseau** du tableau afficheront les valeurs saisies antérieurement. Saisissez manuellement les adresses IP des machines virtuelles de protection.

Passez à l'étape suivante de l'Assistant.

ETAPE 12. MODIFICATION DES MOTS DE PASSE DES COMPTES UTILISATEUR SUR LES MACHINES VIRTUELLES DE PROTECTION

Deux comptes utilisateur sont créés par défaut sur les machines virtuelles de protection : root et klconfig. Ces comptes utilisateur permettent de configurer les machines virtuelles de protection.

A cette étape, modifiez les mots de passe des comptes root et klconfig par défaut sur les machines virtuelles de protection.

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

Pour prévenir l'accès non autorisé à la machine virtuelle de protection, il est recommandé de modifier fréquemment le mot de passe du compte utilisateur klconfig. Vous pouvez modifier le mot de passe du compte utilisateur klconfig à l'aide de la procédure de modification de la configuration des machines virtuelles de protection (cf. section "Modifier la configuration des machines virtuelles de protection avec le module Antivirus Fichiers" à la page 46).

Passez à l'étape suivante de l'Assistant.

ETAPE 13. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

Pour enregistrer les machines virtuelles de protection dans VMware vShield Manager, l'Assistant opère une connexion à VMware vShield Manager.

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'installation.

L'Assistant vérifie la présence du module VMware vShield Endpoint sur tous les hôtes VMware ESXi où il convient d'installer la machine virtuelle de protection, ainsi que la présence de la licence VMware vShield Endpoint. Si le module n'est pas installé ou si la licence est inexistante, l'Assistant le mentionne à l'étape suivante.

ETAPE 14. SAISIE DES PARAMETRES DU COMPTE UTILISATEUR VMWARE VCENTER SERVER

A cette étape, indiquez les paramètres du compte VMware vCenter Server auquel le rôle système préinstallé ReadOnly est désigné. Ce compte est utilisé par les machines virtuelles de protection.

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant le signalera et restera à l'étape actuelle. Si le compte présente plus de privilèges que nécessaire, l'Assistant le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

ETAPE 15. LANCEMENT DU DEPLOIEMENT DES MACHINES VIRTUELLES DE PROTECTION

Tous les paramètres indispensables au déploiement des machines virtuelles de protection sur les hôtes VMware ESXi ont été saisis.

Passez à l'étape suivante de l'Assistant afin de lancer le déploiement des machines virtuelles de protection.

ETAPE 16. DEPLOIEMENT DES MACHINES VIRTUELLES DE PROTECTION

Cette étape correspond au déploiement des machines virtuelles de protection sur les hôtes VMware ESXi. Le processus dure un certain temps. Attendez la fin du processus de déploiement.

Les informations relatives au déploiement des machines virtuelles de protection sont reprises dans le tableau. L'heure de début et l'heure de fin du déploiement sur chacun des hôtes VMware ESXi sont affichées dans les colonnes **Début** et **Fin**. Ces informations permettent d'estimer le temps nécessaire au déploiement des machines virtuelles de protection.

Si une erreur se produit pendant le déploiement de la machine virtuelle de protection sur l'hôte VMware ESXi, l'Assistant réalise le retour à l'état antérieur aux modifications sur cet hôte VMware ESXi et annule l'enregistrement de la machine virtuelle de protection dans VMware vShield Manager, s'il avait été réalisé. Le déploiement des machines virtuelles de protection sur les autres hôtes VMware ESXi se poursuit.

La machine virtuelle de protection s'allume automatiquement après le déploiement.

Passez à l'étape suivante de l'Assistant.

ETAPE 17. FIN DE L'INSTALLATION DU MODULE ANTIVIRUS FICHIERS

A cette étape, les informations relatives au déploiement des machines virtuelles de protection sur les hôtes VMware ESXi sont affichées.

Fermez l'Assistant.

Si le déploiement des machines virtuelles de protection se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Vous pouvez utiliser ce fichier lorsque vous demandez l'aide du Service de Support Technique.

PROCEDURE D'INSTALLATION DU MODULE DETECTION DES MENACES RESEAUX

L'installation du module Détection des menaces réseau dans l'infrastructure virtuelle VMware se déroule via le déploiement des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi et via l'enregistrement du module Détection des menaces réseau sur le VMware vShield Manager. Dans VMware vShield Manager, le module Détection des menaces réseau s'enregistre comme un service de Kaspersky Network Protection.

Les paramètres indispensables à l'installation des machines virtuelles de protection et d'enregistrement du module Détection des menaces réseau sur VMware vShield Manager se définissent à l'aide de l'Assistant d'installation, de mise à jour et de suppression des machines virtuelles de protection. L'Assistant transmet ces paramètres à VMware vShield Manager. VMware vShield Manager effectue le déploiement des images des machines virtuelles de protection sur les hôtes VMware ESXi, entrant dans la composition des clusters VMware, ainsi que l'enregistrement du module Détection des menaces réseau (service de Kaspersky Network Protection).

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des menaces réseau.

Pour installer le module Détection des menaces réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection des machines virtuelles contre les menaces réseau** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Installation, mise à jour ou suppression des machines virtuelles de protection avec le composant Détection des menaces réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à créer des machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'installation.

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que VMware vCenter Server est accessible via le réseau, puis relancez l'installation de l'application.

ETAPE 3. SAISIE DE L'ADRESSE IP DU SERVEUR D'ADMINISTRATION DU KASPERSKY SECURITY CENTER

L'Assistant reçoit du Kaspersky Security Center l'adresse de connexion de la machine virtuelle à l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. Cette étape est accessible si l'adresse de connexion au Serveur d'administration du Kaspersky Security Center obtenue à partir du Kaspersky Security Center porte le nom NetBIOS ou DNS de l'ordinateur. Si l'adresse de connexion s'avère être l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center, cette étape est passée.

Désignez l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. L'adresse IP est indiquée au format IPv4.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'installation.

ETAPE 5. SELECTION DE L'IMAGE DE LA MACHINE VIRTUELLE DE PROTECTION

A cette étape, il convient d'indiquer le chemin vers le fichier OVF de la machine virtuelle de protection dotée du module Détection des menaces réseau sur la ressource réseau accessible par le protocole HTTP.

Si vous procédez pour la première fois à l'installation du module Détection des menaces réseau sur les clusters VMware qui font partie de VMware vCenter Server désigné, indiquez le chemin vers le fichier OVF de la machine virtuelle de protection dans le champ **Fichier OVF**.

Si le module Détection des menaces réseau est déjà installé sur un ou plusieurs clusters VMware faisant partie de VMware vCenter Server sélectionné, le chemin vers le fichier OVF qui a été utilisé lors de la précédente installation du module Détection des menaces réseau s'affiche dans le champ **Fichier OVF**. Vous pouvez choisir l'emplacement de l'autre fichier OVF de la machine virtuelle de protection.

Cliquez sur le bouton **Vérifier**.

L'Assistant vérifie la présence d'un accès à la ressource réseau où se trouve le fichier OVF. Si la ressource réseau est accessible, l'Assistant vérifie l'image de la machine virtuelle de protection. Si l'image est endommagée ou si sa version n'est pas prise en charge par l'Assistant, il affiche un message d'erreur.

Si l'analyse réussit, les informations suivantes relatives à l'image de la machine virtuelle de protection sélectionnée apparaissent dans la partie inférieure de la fenêtre :

- **Nom de l'application** : nom de l'application installée sur la machine virtuelle de protection.
- **Version de l'application** : numéro de la version de l'application.
- **Version de l'image de la machine virtuelle de protection** : numéro de version de l'image de machine virtuelle de protection.
- **Editeur** : éditeur de l'application installée sur la machine virtuelle de protection.
- **Description** : brève description de l'application.
- **Editeur** : émetteur du certificat utilisé pour signer l'image de la machine virtuelle de protection.
- **Taille de l'image** : taille du fichier de l'image de la machine virtuelle de protection.
- **Taille sur le disque** : volume approximatif d'espace disque requis pour le déploiement de la machine virtuelle de protection dans le référentiel de données de l'hôte VMware ESXi :
    - dans le cadre de la répartition dynamique de l'espace disque avec l'utilisation de VMware vStorage Thin Provisioning ;
    - dans le cadre de la répartition de l'espace disque avec un volume fixe.

Si, dans le champ **Fichier OVF**, vous avez modifié le chemin vers le fichier OVF de la machine virtuelle de protection utilisé lors de la précédente installation du module Détection des menaces réseau, une mise à jour des machines virtuelles de protection s'exécutera sur les clusters VMware protégés (cf. section "Procédure de mise à jour du module Détection des menaces réseau" à la page 61). Des machines virtuelles de protection seront installées sur les clusters VMware que vous avez choisis et sur lesquels le module Détection des menaces réseau n'a pas été précédemment installé.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. LECTURE DES CONTRATS DE LICENCE

Cette étape vous permet de prendre connaissance des Contrats de licence que vous allez conclure avec Kaspersky Lab et avec la société SUSE LLC. La société SUSE LLC est propriétaire du système d'exploitation SUSE Linux Enterprise Server 11 SP3 installé sur la machine virtuelle de protection.

Lisez attentivement les Contrats de licence et, si vous en acceptez tous les points, cochez la case **J'accepte les conditions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. SELECTION DES CLUSTERS VMWARE

A cette étape, sélectionnez les clusters VMware des hôtes VMware ESXi sur lesquels il convient d'installer les machines virtuelles de protection.

Les colonnes du tableau affichent les informations relatives à l'ensemble des clusters VMware dans le cadre d'une plateforme VMware vCenter Server :

- **Nom du cluster VMware** – nom du cluster VMware.
- **Chemin d'accès** : chemin vers le cluster VMware dans l'infrastructure virtuelle VMware.
- **Protection** : informations sur l'activation ou non de la protection des machines virtuelles de ce cluster VMware contre les menaces réseau :

- **Protégé** : des machines virtuelles de protection sont installées sur les hôtes VMware ESXi entrant dans la composition de ce cluster VMware.

- **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hôtes VMware ESXi entrant dans la composition de ce cluster VMware.

Pour sélectionner un cluster VMware, cochez la case en regard de son nom dans le tableau.

Si le module Détection des menaces réseau est déjà installé sur une ou plusieurs clusters VMware de VMware vCenter Server sélectionné, les cases sont cochées dans le tableau à gauche du nom des clusters VMware protégés.

Une mise à jour des machines virtuelles de protection sur les clusters VMware protégés sera effectuée si, à l'étape du choix de l'image de la machine virtuelle de protection, vous avez modifié le chemin vers le fichier OVF de la machine virtuelle de protection utilisé lors de la précédente installation du module Détection des menaces réseau (cf. section " Procédure de mise à jour du module Détection des menaces réseau" à la page 61). Des machines virtuelles de protection seront installées sur les clusters VMware choisis et sur lesquels le module Détection des menaces réseau n'est pas installé.

Passez à l'étape suivante de l'Assistant.

ETAPE 8. SELECTION DES GROUPES DE PORTS DISTRIBUES

A cette étape, sélectionnez les groupes de ports distribués (Distributed Virtual Port Groups) qui nécessitent d'activer la protection contre les menaces réseau. Kaspersky Security contrôlera le trafic sur les groupes de ports distribués sélectionnés pour détecter les activités caractéristiques des attaques réseau.

Les colonnes du tableau affichent les informations relatives à l'ensemble des groupes de ports distribués configurés dans VMware Distributed Virtual Switches dans le cadre d'une plateforme VMware vCenter Server :

- **Groupe de ports distribués** : nom du groupe de ports distribués.

- **Chemin d'accès** : emplacement du groupe de ports distribués dans l'infrastructure virtuelle VMware.

- **Protection** : informations sur l'activation ou non de la vérification du trafic des machines virtuelles au sein de ce groupe de ports distribués :

  - **Activée** : Kaspersky Security vérifie le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.

  - **Désactivée** : l'application ne vérifie pas le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.

Pour sélectionner un groupe de ports distribués, dans le tableau, cochez les cases situées à gauche du nom de ce groupe de ports distribués.

Passez à l'étape suivante de l'Assistant.

ETAPE 9. FIN DE LA SAISIE DES PARAMETRES

Tous les paramètres indispensables au déploiement des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi ont été saisis.

A cette étape, les paramètres de déploiement des machines virtuelles de protection par VMware vShield Manager s'affichent : informations sur l'image de la machine virtuelle de protection choisie pour le déploiement, sur les clusters VMware et les groupes de ports distribués VMware (Distributed Virtual Port Groups) pour lesquels la protection contre les menaces réseau sera activée.

S'il convient de modifier les paramètres, revenez aux étapes précédentes de l'Assistant.

Cliquez sur **Exécuter**, pour terminer l'entrée des paramètres indispensables au déploiement des machines virtuelles de protection et passer à l'étape suivante de l'Assistant. L'Assistant transmet ces paramètres à VMware vShield Manager.

ETAPE 10. FIN DU TRAVAIL DE L'ASSISTANT

Cette étape affiche les informations relatives aux résultats de la transmission à VMware vShield Manager des paramètres indispensables au déploiement des machines virtuelles de protection avec le module Détection des menaces réseau.

Si la transmission des paramètres été effectuée avec succès, fermez l'Assistant.

Si la transmission des paramètres à VMware vShield Manager se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Dans ce cas, fermez l'Assistant, corrigez les erreurs en fonction des raisons fournies et relancez à nouveau la procédure d'installation.

Vous pouvez consulter les informations relatives au procédé de déploiement des machines virtuelles de protection sur les hôtes VMware ESXi dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

Après l'installation du module Détection des menaces réseau, un pool de ressources intitulé ESX Agents spécifiant les machines virtuelles de protection installées est créé pour chaque cluster VMware protégé sur la console VMware vSphere Client dans le dossier **vCenter**. Le service Kaspersky Network Protection apparaît sur l'interface Internet de VMware vShield Manager, dans la liste des services, (module Détection des menaces réseau).

Après l'installation du module Détection des menaces réseau, il convient d'activer la détection des attaques réseau (cf. section "Activation et désactivation de la détection des attaques réseau" page 135) et l'analyse des adresses URL (cf. section "Activation et désactivation de l'analyse des adresses URL" page 137) dans les paramètres de la stratégie. Par défaut, Kaspersky Security ne détecte pas les attaques réseau et n'analyse pas les adresses URL.

MODIFICATIONS DANS LE KASPERSKY SECURITY CENTER APRES L'INSTALLATION DE L'APPLICATION

Après l'installation de Kaspersky Security dans l'infrastructure VMware, les machines virtuelles de protection transmettent les informations les concernant au Kaspersky Security Center. Sur la base de ces informations, le Kaspersky Security Center regroupe les machines virtuelles de protection installées sur les hôtes VMware ESXi dans le cadre d'une plateforme VMware vCenter Server et les machines virtuelles qu'elles protègent dans un cluster KSC. Le cluster KSC reçoit le nom de la plateforme VMware vCenter Server correspondante.

Pour chaque cluster KSC, le Kaspersky Security Center crée des dossiers auxquels il attribue le nom des clusters KSC (cf. section "Concept de l'administration de l'application via le Kaspersky Security Center" à la page 24) dans le dossier **Ordinateurs administrés** de la Console d'administration. Lors de la sélection dans l'arborescence de la console du dossier intitulé KSC, la liste des machines virtuelles de protection entrant dans la composition de ce cluster KSC s'affiche dans la zone de travail.

La liste de tous les clusters KSC s'affiche dans le dossier **Clusters et tableaux de serveurs**. Dans la fenêtre des propriétés du cluster KSC, vous pouvez consulter la liste des tâches élaborées pour le cluster, la liste des machines virtuelles de protection et toutes les machines virtuelles entrant dans la composition du cluster KSC (cf. section "Consultation de la liste des machines virtuelles et des machines virtuelles de protection du cluster KSC" à la page 44).

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**.

     La liste des clusters KSC s'affiche dans la zone de travail.

3. Choisissez le cluster KSC dans la liste et ouvrez la fenêtre **Propriétés de <Nom du cluster KSC>** grâce à l'un des procédés suivants :

   - En double-cliquant.
   - A l'aide du lien **Ouvrir les propriétés**, situé à droite de la liste des clusters KSC.
   - Cliquez droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.

4. Dans la liste à gauche, 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 sur les hôtes VMware ESXi entrant dans la composition du cluster KSC sélectionné.

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 vShield Endpoint Thin Agent est installé sur la machine virtuelle et il est activé ;
    - 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 :
    - la machine virtuelle est déconnectée ou arrêtée, ou le pilote 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.

- **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.

  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**.

Lors de la consultation de la liste des machines virtuelles, vous pouvez effectuer les actions suivantes :

- Trier la liste en fonction du nom des machines virtuelles. Pour ce faire, 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.
- Filtrer la liste en fonction de l'état de la protection des machines virtuelles. Pour ce faire, utilisez les boutons suivants :
  -  : indiquer les machines virtuelles protégées.
  -  : indiquer les machines virtuelles de protection et les machines virtuelles non protégées.

  Pour supprimer le filtre appliqué à la liste selon le statut de la protection des machines virtuelles, cliquez sur le bouton  .
- Effectuer une recherche dans la liste en fonction du nom de la machine virtuelle. Pour ce faire, saisissez le nom de la machine virtuelle dans la ligne de recherche.

MODIFICATION DE LA CONFIGURATION DES MACHINES VIRTUELLES DOTEES DU MODULE ANTIVIRUS FICHIERS

Cette section détaille la modification de la configuration des machines virtuelles de protection dotées du module Antivirus Fichiers après l'installation : paramètres de connexion des machines virtuelles de protection à VMware vCenter Server et mot de passe du compte klconfig.

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

Pour modifier la configuration des machines virtuelles de protection, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection du système de fichiers des machines virtuelles** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Modification de la configuration**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de modification de la configuration.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant le signalera et restera à l'étape actuelle. Si le compte présente plus de privilèges que nécessaire, l'Assistant le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que VMware vCenter Server est accessible via le réseau, puis relancez la modification de la configuration.

ETAPE 3. SELECTION DES MACHINES VIRTUELLES DE PROTECTION

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

Les colonnes du tableau reprennent les informations relatives aux hôtes VMware ESXi de la plateforme VMware vCenter Server sélectionnée sur lesquels la machine virtuelle de protection est installée :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hôte VMware ESXi.
- **Etat** : informations sur l'état de la machine virtuelle de protection :
  - **Accessible** : la machine virtuelle de protection est activée.
  - **Eteinte** : la machine virtuelle de protection est désactivée.

Pour sélectionner la machine virtuelle de protection dont la configuration doit être modifiée, cochez la case dans le tableau à gauche du nom de l'hôte VMware ESXi sur lequel la machine virtuelle de protection est installée. Vous pouvez uniquement sélectionner les hôtes VMware ESXi sur lesquels la machine virtuelle de protection présente l'état *Accessible*.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SAISIE DU MOT DE PASSE DU COMPTE KLCONFIG

A cette étape, indiquez le mot de passe du compte klconfig qui a été défini lors de l'installation de l'application. Le compte klconfig est utilisé par les machines virtuelles de protection.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. MODIFICATION DES PARAMETRES DE CONNEXION DES MACHINES VIRTUELLES DE PROTECTION A VMWARE VCENTER SERVER

A cette étape, vous pouvez modifier les paramètres de connexion des machines virtuelles de protection à VMware vCenter Server :

Pour ce faire, sélectionnez l'option **Modifier les paramètres** et définissez les paramètres suivants :

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. MODIFICATION DU MOT DE PASSE DU COMPTE KLCONFIG

Cette étape permet de modifier le mot de passe du compte klconfig utilisé sur les machines virtuelles de protection.

Pour ce faire, choisissez l'option **Modifier le mot de passe** et saisissez le nouveau mot de passe du compte klconfig dans les champs **Nouveau mot de passe** et **Confirmation**.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. LANCEMENT DE LA MODIFICATION DE LA CONFIGURATION DES MACHINES VIRTUELLES DE PROTECTION

Tous les paramètres nécessaires pour modifier la configuration des machines virtuelles de protection ont été saisis.

Passez à l'étape suivante de l'Assistant afin de lancer le déploiement des machines virtuelles de protection.

ETAPE 8. MODIFICATION DE LA CONFIGURATION DES MACHINES VIRTUELLES DE PROTECTION

Cette étape correspond à la modification de la configuration des machines virtuelles de protection sur les hôtes VMware ESXi. Le processus dure un certain temps. Attendez la fin du processus de modification.

Les informations relatives à la modification de la configuration des machines virtuelles de protection sont reprises dans le tableau. L'heure de début et l'heure de fin du processus sur chacun des hôtes VMware ESXi sont affichées dans les colonnes **Début** et **Fin**. Ces informations permettent d'estimer le temps nécessaire à la modification de la configuration des machines virtuelles de protection sélectionnées.

Passez à l'étape suivante de l'Assistant.

ETAPE 9. FIN DE LA MODIFICATION DE LA CONFIGURATION DES MACHINES VIRTUELLES DE PROTECTION

A cette étape, les résultats de la modification des machines virtuelles de protection sur les hôtes VMware ESXi sont affichés.

Fermez l'Assistant.

Si, pendant la modification de la configuration des machines virtuelles de protection, des erreurs sont relevées, l'Assistant affiche un lien vers le fichier contenant le journal de travail de l'Assistant. Vous pouvez utiliser ce fichier lorsque vous demandez l'aide du Service de Support Technique.

MISE A JOUR DE LA VERSION PRECEDENTE DE L'APPLICATION

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

DANS CETTE SECTION

SEQUENCE DE MISE A JOUR DE LA VERSION PRECEDENTE DE L'APPLICATION

Vous pouvez mettre à jour Kaspersky Security for Virtualization 2.0 et Kaspersky Security for Virtualization 2.0 Maintenance Release 1 vers Kaspersky Security for Virtualization 3.0 Agentless.

La mise à jour des applications Kaspersky Security for Virtualization 2.0 et Kaspersky Security for Virtualization 2.0 Maintenance Release 1 vers Kaspersky Security for Virtualization 3.0 Agentless comprend les étapes suivantes :

1. Mise à jour du Kaspersky Security Center 10 vers le Kaspersky Security Center 10 Maintenance Release 1 (informations détaillées dans la documentation du Kaspersky Security Center).

2. Mise à jour du plug-in d'administration de Kaspersky Security.

   La mise à jour du plug-in s'effectue à partir de la ligne de commande sur l'ordinateur où est installée la console d'administration du Kaspersky Security Center, via la commande `msiexec /i klcfginst.msi REINSTALLMODE=voums REINSTALL=ALL`. Le fichier d'installation klcfginst.msi fait partie de la distribution de Kaspersky Security.

   La mise à jour du plug-in d'administration de Kaspersky Security permet de gérer les versions précédentes de Kaspersky Security installées sur les machines virtuelles de protection. Pour les machines virtuelles de protection dont l'application n'a pas été mise à jour, les tâches et stratégies de la version antérieure de l'application s'appliquent mais les paramètres qui n'existaient pas dans la version antérieure sont ignorés. Pour utiliser l'ensemble des fonctions de Kaspersky Security for Virtualization 3.0 Agentless lors de la protection des machines virtuelles, il est nécessaire de mettre à jour toutes les machines virtuelles de protection dotées du module Kaspersky Security.

   > Si la Console d'administration du Kaspersky Security Center est installée sur plusieurs ordinateurs, il est nécessaire de mettre à jour le plug-in d'administration de Kaspersky Security sur chacun d'entre eux. Les paramètres de l'application varient dans les plug-ins d'administration de Kaspersky Security de différentes versions. Ainsi, l'utilisation des plug-ins d'administration des différentes versions peut entraîner une erreur de synchronisation entre les paramètres configurés et utilisés de l'application.

3. Mise à jour du module Antivirus Fichiers. La mise à jour du module Antivirus Fichiers se déroule via la mise à jour des machines virtuelles de protection dotées du module Antivirus Fichiers sur les hôtes VMware ESXi.

   La mise à jour des machines virtuelles de protection s'opère à l'aide de l'Assistant de mise à jour du module Antivirus Fichiers (cf. section "Procédure de mise à jour du module Antivirus Fichiers" à la page 52).

4. Mise à jour du module Détection des menaces réseau. La mise à jour du module Détection des menaces réseau s'effectue via la mise à jour des machines virtuelles de protection dotées de la version précédente du module Détection des menaces réseau.

   Les paramètres indispensables à la mise à jour de toutes les machines virtuelles de protection se définissent à l'aide de l'Assistant d'installation, de mise à jour et de suppression des machines virtuelles de protection (cf. section "Procédure de mise à jour du module Détection des menaces réseau" à la page 61).

5. Activation de l'application sur les machines virtuelles de protection dotées du module Détection des menaces réseau (cf. section "Activation de l'application" à la page 85).

   Si vous avez refusé le transfert des clés lors de la mise à jour des machines virtuelles de protection dotées du module Antivirus Fichiers, il est également nécessaire d'activer l'application sur ces machines virtuelles de protection.

6. Mise à jour des bases antivirus sur les machines virtuelles de protection dotées du module Détection des menaces réseau (cf. section "Mise à jour des bases antivirus" page 144).

   Si vous avez refusé la mise à jour automatique des bases antivirus lors de la mise à jour des machines virtuelles de protection dotées du module Antivirus Fichiers, il est également nécessaire d'exécuter la mise à jour des bases antivirus de ces machines.

7. Conversion des stratégies et des tâches existantes (cf. section "Conversion des stratégies et des tâches lors de la mise à jour de l'application" à la page 66). Après la mise à jour du plug-in d'administration de Kaspersky Security, les stratégies et les tâches de la version précédente sont automatiquement conservées dans les stratégies et les tâches de Kaspersky Security for Virtualization 3.0 Agentless ; ceci dès la première modification et la première sauvegarde des paramètres de protection dans la stratégie et des paramètres d'analyse dans la tâche.

Si vous souhaitez mettre à jour l'hyperviseur VMware ESXi 5.1, VMware ESXi 5.1 patch 1 ou VMware ESXi 5.1 patch 2 vers la version VMware ESXi 5.5 patch 1, vous devrez attendre la mise à jour de l'application Kaspersky Security.

La mise à jour de l'hyperviseur VMware ESXi s'exécute via l'infrastructure virtuelle de VMware.

Suite à la mise à jour de l'hyperviseur VMware ESXi, vous devrez mettre à jour l'enregistrement des machines virtuelles de protection dotées du module Détection des menaces réseau dans VMware vShield Manager. La mise à jour de l'enregistrement des machines virtuelles de protection dans VMware vShield Manager s'exécute à l'aide de l'Assistant d'installation, de mise à jour et de suppression des machines virtuelles de protection (cf. section "Procédure de mise à jour du module Détection des menaces réseau" à la page 61). Pour mettre à jour l'enregistrement des machines virtuelles de protection, vous devrez passer toutes les étapes de l'Assistant. L'Assistant transmet les paramètres indispensables à la mise à jour de l'enregistrement des machines virtuelles dans VMware vShield Manager.

CONSULTATION DE LA LISTE DES IMAGES DE MACHINES VIRTUELLES DE PROTECTION DEFINIES

Kaspersky Security permet de consulter la liste des images des machines virtuelles de protection déployées dans l'infrastructure virtuelle VMware. Dans cette liste, vous pouvez consulter le numéro de version des images des machines virtuelles de protection installées sur les hôtes VMware ESXi.

Pour consulter la liste des images des machines virtuelles de protection, procédez comme suit :

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

2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.

3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.

4. Dans la fenêtre ouverte, choisissez l'option **Consultation de la liste des images installées des machines virtuelles de protection** et passez à l'étape suivante de l'Assistant.

5. Saisissez les paramètres de connexion de l'Assistant au VMware vCenter Server :

   - **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
   - **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
   - **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

6. Passez à l'étape suivante de l'Assistant.

   Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat.

7. Cliquez sur le bouton **Poursuivre**.

   Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

8. S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez queVMware vCenter Server est accessible via le réseau, puis relancez la procédure.

   La liste des images des machines virtuelles de protection déployées sur les hôtes VMware ESXi apparaît dans la fenêtre de l'Assistant. Si, aucune machine virtuelle de protection installée avec le module Antivirus Fichiers ou le module Détection des menaces réseau n'est détectée dans l'infrastructure virtuelle VMware, la liste est vide.

   La liste des images des machines virtuelles de protection se présente sous la forme d'un tableau. Chaque ligne du tableau contient des informations sur les images des machines virtuelles de protection déployées sur un hôte VMware ESXi.

   Les colonnes du tableau reprennent les informations suivantes :

   - **Hôte VMware ESXi** : l'adresse IP de l'hôte VMware ESXi.
   - **Version de l'image (Antivirus Fichiers)** : le numéro de la version de l'image de la machine virtuelle de protection avec le module Antivirus Fichiers installé sur l'hôte VMware ESXi.
   - **Version de l'image (Détection des menaces réseau)** : numéro de la version de l'image de la machine virtuelle de protection dotée du module Détection des menaces réseau installée sur l'hôte VMware ESXi.

   Vous pouvez trier la liste des images des machines virtuelles de protection à partir de n'importe quelle colonne du tableau. Pour ce faire, cliquez sur le bouton gauche de la souris sur le haut de la colonne. La liste est triée par ordre croissant. Si vous cliquez à nouveau sur le haut de la colonne, la liste est triée par ordre décroissant.

PROCEDURE DE MISE A JOUR DU MODULE ANTIVIRUS FICHIERS

La mise à jour du module Antivirus Fichiers se déroule via la mise à jour des machines virtuelles de protection dotées du module Antivirus Fichiers sur les hôtes VMware ESXi.

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

Avant de lancer la mise à jour d'une machine virtuelle de protection, il convient de confirmer l'existence d'une stratégie active qui peut être appliquée à la nouvelle machine virtuelle de protection. Si aucune stratégie active ne figure dans le Kaspersky Security Center, la mise à jour de la machine virtuelle de protection se solde sur une erreur.

L'Assistant de mise à jour de l'Antivirus Fichiers procède comme suit :

1. Il installe des machines virtuelles de protection avec la nouvelle version du module Antivirus Fichiers sur les hôtes VMware ESXi sélectionnés. Les stratégies sont appliquées lors de l'installation des nouvelles machines virtuelles de protection.

2. L'Assistant peut transférer les clés depuis la machine virtuelle de protection mise à jour vers la nouvelle machine virtuelle de protection pour une utilisation prolongée de l'application sous la licence active. Il est également en mesure de mettre à jour les bases antivirus sur la machine virtuelle de protection dotée de la nouvelle version de l'application.

   Si vous avez refusé le transfert des clés et la mise à jour automatique des bases antivirus, la protection des machines virtuelles ne sera pas active au moment de la suppression des machines virtuelles de protection dotées de la version précédente du module Antivirus Fichiers et de l'installation de nouvelles machines virtuelles de protection. Ainsi, lors de la mise à jour, il est conseillé d'arrêter les machines virtuelles protégées ou de migrer les machines virtuelles sur un hôte VMware ESXi protégé.

3. Il supprime les machines virtuelles de protection dotées de la version antérieure du module Antivirus Fichiers sur les hôtes VMware ESXi sélectionnés dans le cadre d'une plateforme VMware Server Center. Les copies de sauvegarde des fichiers et les journaux de traçage enregistrés sur les machines virtuelles de protection sont également supprimés.

   Après que l'Assistant de mise à jour du module Antivirus Fichiers a supprimé les machines virtuelles de protection dotées de la version antérieure du module Antivirus Fichiers sur les hôtes VMware ESXi, les machines virtuelles de protection apparaissent toujours dans la Console d'administration du Kaspersky Security Center. A l'issue du délai défini dans les paramètres du Kaspersky Security Center (pour les détails, reportez-vous à la documentation du Kaspersky Security Center), les machines virtuelles de protection sont automatiquement supprimées de la Console d'administration.

   Vous pouvez supprimer manuellement des machines virtuelles de protection dotées de la version antérieure du module Antivirus Fichiers de la Console d'administration du Kaspersky Security Center directement après la fin de la procédure de mise à jour.

   Avant la suppression des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center, les événements envoyés par ces machines virtuelles de protection sont enregistrés dans le Kaspersky Security Center et figurent dans les rapports et le journal des événements du Kaspersky Security Center. La liste des copies de sauvegarde des fichiers placés dans la sauvegarde sur ces machines virtuelles de protection est également enregistrée dans le Kaspersky Security Center avant la suppression des machines virtuelles de protection de la Console d'administration, mais aucune action ne peut être réalisée sur les copies des fichiers car les copies de sauvegarde ont été supprimées pendant la suppression des machines virtuelles de protection sur les hôtes VMware ESXi.

Pour mettre à jour le module Antivirus Fichiers, procédez comme suit :

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

2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.

3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail dans le groupe **Déploiement**.

4. Dans la fenêtre ouverte, choisissez l'option **Protection du système de fichiers des machines virtuelles** et passez à l'étape suivante de l'Assistant.

5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Mise à jour**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à créer des machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de mise à jour.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur VMware vCenter Server" à la page 31), l'Assistant le signale et ne passe pas à l'étape suivante.

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le VMware vCenter Server est accessible via le réseau, puis relancez la mise à jour du module Antivirus Fichiers.

ETAPE 3. SAISIE DE L'ADRESSE IP DU SERVEUR D'ADMINISTRATION DU KASPERSKY SECURITY CENTER

L'Assistant reçoit du Kaspersky Security Center l'adresse de connexion de la machine virtuelle à l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. Cette étape est accessible si l'adresse de connexion au Serveur d'administration du Kaspersky Security Center obtenue à partir du Kaspersky Security Center porte le nom NetBIOS ou DNS de l'ordinateur. Si l'adresse de connexion s'avère être l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center, cette étape est passée.

Désignez l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. L'adresse IP est indiquée au format IPv4.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SELECTION DU FICHIER IMAGE DE LA MACHINE VIRTUELLE DE PROTECTION

Désignez à cette étape le fichier de l'image de la machine virtuelle de protection avec la nouvelle version du module Antivirus Fichiers. Pour ce faire, cliquez sur le bouton **Parcourir** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier image de la machine virtuelle de protection. Il s'agit d'un fichier au format OVA.

L'Assistant vérifie l'image de la machine virtuelle de protection. Si l'image est endommagée ou si sa version n'est pas prise en charge par l'Assistant, il affiche un message d'erreur.

Si l'analyse réussit, les informations suivantes relatives à l'image de la machine virtuelle de protection sélectionnée apparaissent dans la partie inférieure de la fenêtre :

- **Nom de l'application** : nom de l'application installée sur la machine virtuelle de protection.
- **Version de l'application** : numéro de la version de l'application.
- **Version de l'image de la machine virtuelle de protection** : numéro de version de l'image de machine virtuelle de protection.
- **Editeur** : éditeur de l'application installée sur la machine virtuelle de protection.
- **Description** : brève description de l'application.
- **Editeur** : émetteur du certificat utilisé pour signer l'image de la machine virtuelle de protection.
- **Taille de l'image** : taille du fichier de l'image de la machine virtuelle de protection.

- **Taille sur le disque** : volume approximatif d'espace disque requis pour le déploiement de la machine virtuelle de protection dans le référentiel de données de l'hôte VMware ESXi :
  - dans le cadre de la répartition dynamique de l'espace disque avec l'utilisation de VMware vStorage Thin Provisioning ;
  - dans le cadre de la répartition de l'espace disque avec un volume fixe.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. LECTURE DES CONTRATS DE LICENCE

Cette étape vous permet de prendre connaissance des Contrats de licence que vous allez conclure avec Kaspersky Lab et avec la société SUSE LLC. La société SUSE LLC est propriétaire du système d'exploitation SUSE Linux Enterprise Server 11 SP3 installé sur la machine virtuelle de protection.

Lisez attentivement les Contrats de licence et, si vous en acceptez tous les points, cochez la case **J'accepte les conditions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. SELECTION DES MACHINES VIRTUELLES DE PROTECTION

A cette étape, désignez les machines virtuelles de protection que vous souhaitez mettre à jour.

Les colonnes du tableau reprennent les informations relatives aux hôtes VMware ESXi de la plateforme VMware vCenter Server sélectionnée sur lesquels la machine virtuelle de protection est installée :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hôte VMware ESXi.
- **Etat** : informations sur l'état de la machine virtuelle de protection :
  - **Accessible** : la machine virtuelle de protection est activée.
  - **Eteinte** : la machine virtuelle de protection est désactivée.

Pour sélectionner la machine virtuelle de protection à mettre à jour, cochez la case dans le tableau à gauche du nom de l'hôte VMware ESXi sur lequel la machine virtuelle de protection est installée. Vous pouvez uniquement sélectionner les hôtes VMware ESXi sur lesquels la machine virtuelle de protection présente l'état *Accessible*.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. SELECTION DE L'OPTION DE PLACEMENT ET DE CONFIGURATION DES PARAMETRES DE DEPLOIEMENT

A cette étape, sélectionnez l'option d'emplacement de la machine virtuelle de protection dans le stockage de données de l'hôte VMware ESXi :

- **Répartition dynamique à l'aide de VMware vStorage Thin Provisioning**. Pendant l'attribution de l'espace dans le stockage de données de l'hôte VMware ESXi pour la machine virtuelle de protection, un volume requis minimal est réservé. Ce volume augmente en fonction des besoins. Cette option est sélectionnée par défaut.
- **Répartition de l'espace disque avec un volume fixe**. Pendant l'attribution de l'espace dans le stockage de données de l'hôte VMware ESXi pour la machine virtuelle de protection, le volume requis est directement réservé.

Configurez les paramètres du processus de déploiement des machines virtuelles de protection. Si vous souhaitez que l'Assistant déploie les machines virtuelles de protection simultanément sur plusieurs VMware ESXi, cochez la case **Autoriser le déploiement en parallèle**. Dans le champ **Déployer simultanément sur un maximum de X hôtes VMware ESXi**, indiquez le nombre d'hôtes VMware ESXi sur lesquels les machines virtuelles de protection doivent être déployées simultanément.

Passez à l'étape suivante de l'Assistant.

ETAPE 8. SELECTION DU STOCKAGE DE DONNEES

A cette étape, sélectionnez pour chaque machine virtuelle de protection un stockage de données dans la liste des stockages connectés aux hôtes VMware ESXi.

Les colonnes du tableau reprennent les informations suivantes :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Nom de la machine virtuelle de protection** : nom de la machine virtuelle de protection installée sur cet hôte VMware ESXi. Les machines virtuelles de protection reçoivent automatiquement le nom ksv-<N> où N représente l'adresse IP ou le nom de domaine de l'hôte VMware ESXi sur lequel se trouve la machine virtuelle de protection. Par exemple, ksv-192-168-0-2 ou ksv-esx-avp-ru.

  Vous pouvez modifier le nom de la machine virtuelle de protection. Pour ce faire, double-cliquez gauche sur la colonne **Nom de la machine virtuelle de protection** et saisissez le nouveau nom.
- Le **référentiel de données** : reprend dans des listes déroulantes les noms des stockages de données connectés à l'hôte VMware ESXi. Si un seul stockage de données est connecté à l'hôte VMware ESXi, la liste déroulante ne contient qu'un seul nom.

Dans la liste déroulante de la colonne **Référentiel de données**, sélectionnez le stockage de données pour chaque machine virtuelle de protection.

Passez à l'étape suivante de l'Assistant.

ETAPE 9. CONFIGURATION DE LA CORRESPONDANCE DES RESEAUX VIRTUELS

A cette étape, définissez la correspondance entre les réseaux virtuels de la machine virtuelle de protection et l'hôte VMware ESXi :

- La colonne **Hôte VMware ESXi** affiche l'adresse IP ou le nom de domaine de l'hôte VMware ESXi sur lequel la machine virtuelle de protection est mise à jour.
- Dans la colonne **Réseau VMware vShield**, sélectionnez dans la liste déroulante le réseau virtuel de l'hôte VMware ESXi que la machine virtuelle de protection doit utiliser pour communiquer avec le module VMware vShield Endpoint ESX Module. Ce module est installé sur l'hôte VMware ESXi. Il assure l'interaction du pilote VMware vShield Endpoint Thin Agent installé sur la machine virtuelle et de la bibliothèque ESPEC installée sur la machine virtuelle de protection.
- Dans la colonne **Réseau Utilisateur**, sélectionnez, dans la liste déroulante, le réseau virtuel de l'hôte VMware ESXi que la machine virtuelle de protection doit utiliser pour communiquer avec l'environnement externe du réseau et le Serveur d'administration du Kaspersky Security Center.

Passez à l'étape suivante de l'Assistant.

ETAPE 10. SAISIE DES PARAMETRES DE RESEAU

A cette étape, désignez les paramètres de réseau des machines virtuelles de protection :

- **Utiliser DHCP**. Utilisation du protocole de réseau DHCP qui permet aux machines virtuelles de protection d'obtenir automatiquement les paramètres de réseau. Cette option est sélectionnée par défaut.
- **Désigner manuellement pour chaque machine virtuelle de protection**. Les paramètres de réseau sont attribués manuellement pour les machines virtuelles de protection.
- **Distribuer à l'aide des paramètres définis**. Les paramètres de réseau sont attribués manuellement pour les machines virtuelles de protection à partir d'une plage définie. Si vous choisissez cette option, définissez les paramètres de réseau dans les champs **Passerelle**, **Serveur DNS** et **Masque de réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 11. SAISIE MANUELLE DES PARAMETRES DE RESEAU

Cette étape est accessible si, à l'étape précédente de l'Assistant, vous avez choisi le paramètre **Désigner manuellement pour chaque machine virtuelle de protection** ou **Répartir selon les paramètres définis**. Si vous avez choisi l'option **Utiliser DHCP**, cette étape est ignorée.

Si vous avez choisi le paramètre **Désigner manuellement pour chaque machine virtuelle de protection** à l'étape précédente de l'Assistant, indiquez manuellement tous les paramètres de réseau des machines virtuelles de protection. Si vous ne saisissez pas les paramètres de quelconque machine virtuelle de protection sur cette ligne, les paramètres de réseau obtenus via le protocole DHCP seront ceux utilisés pour cette machine virtuelle de protection.

Si vous avez choisi l'option **Répartir selon les paramètres définis** à l'étape précédente, les colonnes **Passerelle**, **Serveur DNS** et **Masque de réseau** du tableau afficheront les valeurs saisies antérieurement. Saisissez manuellement les adresses IP des machines virtuelles de protection.

Les adresses IP des nouvelles machines virtuelles de protection ne peuvent pas correspondre aux adresses IP des machines virtuelles de protection sélectionnées pour la mise à jour. L'unicité des adresses IP dans l'infrastructure VMware se vérifie dans le cadre d'un seul objet Datacenter.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifie l'unicité des adresses IP des nouvelles machines virtuelles de protection. Si les adresses IP définies pour une ou plusieurs nouvelles machines virtuelles de protection correspondent aux adresses IP d'autres machines virtuelles dans le cadre d'un seul objet Datacenter, l'Assistant affiche un message d'erreur et il est impossible de passer à l'étape suivante. Une icône d'avertissement apparaît dans la colonne contenant l'adresse IP qui correspond à l'adresse IP de l'autre machine virtuelle de protection. Indiquez une autre adresse IP pour la machine virtuelle de protection.

ETAPE 12. MODIFICATION DES MOTS DE PASSE DES COMPTES UTILISATEUR SUR LES MACHINES VIRTUELLES DE PROTECTION

Deux comptes utilisateur sont créés par défaut sur les machines virtuelles de protection : root et klconfig. Ces comptes utilisateur permettent de configurer les machines virtuelles de protection.

A cette étape, modifiez les mots de passe des comptes root et klconfig par défaut sur les machines virtuelles de protection.

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

Pour prévenir l'accès non autorisé à la machine virtuelle de protection, il est recommandé de modifier fréquemment le mot de passe du compte utilisateur klconfig. Vous pouvez modifier le mot de passe du compte utilisateur klconfig à l'aide de la procédure de modification de la configuration des machines virtuelles de protection (cf. section "Modifier la configuration des machines virtuelles de protection avec le module Antivirus Fichiers" à la page 46).

Passez à l'étape suivante de l'Assistant.

ETAPE 13. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

Pour annuler l'inscription des machines virtuelles de protection dotées de la version antérieure du module Antivirus Fichiers dans VMware vShield Manager et inscrire les nouvelles machines virtuelles de protection dans VMware vShield Manager, l'Assistant établit une connexion à VMware vShield Manager.

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de mise à jour.

L'Assistant vérifie la présence du module VMware vShield Endpoint sur tous les hôtes VMware ESXi où il convient de mettre à jour la machine virtuelle de protection, ainsi que la présence de la licence VMware vShield Endpoint. Si le module n'est pas installé ou si la licence est inexistante, l'Assistant le mentionne à l'étape suivante.

ETAPE 14. SAISIE DES PARAMETRES DU COMPTE UTILISATEUR VMWARE VCENTER SERVER

A cette étape, indiquez les paramètres du compte VMware vCenter Server auquel le rôle système préinstallé ReadOnly est désigné. Ce compte est utilisé par les machines virtuelles de protection.

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant le signalera et restera à l'étape actuelle. Si le compte présente plus de privilèges que nécessaire, l'Assistant le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

ETAPE 15. PREPARATION DE L'UTILISATION DES MACHINES VIRTUELLES DE PROTECTION MISES A JOUR

L'Assistant peut transférer les clés depuis les machines virtuelles de protection mises à jour et mettre à jour les bases antivirus des machines virtuelles de protection dotées de la nouvelle version de l'application pour que la protection soit assurée dès la fin de la procédure.

Si vous souhaitez que l'Assistant transfère les clés et mette à jour les bases antivirus, sélectionnez l'option **Préparer le fonctionnement des machines virtuelles de protection qui peuvent être mises à jour (recommandé)** et indiquez le mot de passe du compte utilisateur klconfig utilisé sur l'ensemble de ces machines.

Si vous souhaitez refuser le transfert des clés et la mise à jour automatique des bases antivirus lors de l'exécution de l'Assistant, sélectionnez l'option **Ne pas préparer le fonctionnement des machines virtuelles de protection qui peuvent être mises à jour**. Dans ce cas, après la mise à jour du module Antivirus Fichiers, vous devrez activer l'application (cf. section "Activation de l'application" à la page 85) et mettre à jour les bases antivirus sur les machines virtuelles de protection (cf. section "Mise à jour des bases antivirus" à la page 144).

Passez à l'étape suivante de l'Assistant afin de continuer la mise à jour ou retournez à l'étape de sélection des machines virtuelles de protection pour modifier les paramètres.

ETAPE 16. LANCEMENT DE LA MISE A JOUR DES MACHINES VIRTUELLES DE PROTECTION

A cette étape, la fenêtre de l'Assistant affiche les informations relatives au nombre de machines virtuelles de protection qui sera mis à jour.

Passez à l'étape suivante de l'Assistant afin de lancer la mise à jour des machines virtuelles de protection.

ETAPE 17. MISE A JOUR DES MACHINES VIRTUELLES DE PROTECTION

Cette étape correspond à la mise à jour des machines virtuelles de protection sur les hôtes VMware ESXi. Le processus dure un certain temps. Attendez la fin de la mise à jour.

Les informations relatives à la mise à jour des machines virtuelles de protection sont reprises dans le tableau. L'heure de début et l'heure de fin de la mise à jour sur chacun des hôtes VMware ESXi sont affichées dans les colonnes **Début** et **Fin**. Ces informations permettent d'estimer le temps nécessaire à la mise à jour des machines virtuelles de protection.

La stratégie est appliquée après la mise à jour sur la machine virtuelle de protection. La machine virtuelle de protection s'active automatiquement.

Si une erreur survient pendant la mise à jour d'une machine virtuelle de protection sur un hôte VMware ESXi (y compris lors du transfert des clés ou de la mise à jour des bases antivirus) ou pendant l'application d'une stratégie sur la nouvelle machine virtuelle de protection, l'Assistant exécute les actions suivantes :

1. Il annule les modifications introduites sur cet hôte VMware ESXi ;
2. Il annule l'inscription de la nouvelle machine virtuelle de protection sur VMware vShield Manager, si celle-ci avait eu lieu ;
3. Il enregistre la machine virtuelle de protection avec la version antérieure de l'application dans VMware vShield Manager.

   La stratégie appliquée à cette machine virtuelle de protection avant la mise à jour de l'application s'applique sur la machine virtuelle de protection dotée de la version antérieure de l'application. La machine virtuelle de protection avec la version antérieure de l'application est activée automatiquement.

La mise à jour des machines virtuelles de protection sur les autres hôtes VMware ESXi se poursuit.

Passez à l'étape suivante de l'Assistant.

ETAPE 18. FIN DE LA MISE A JOUR DES MACHINES VIRTUELLES DE PROTECTION

A cette étape, les informations relatives aux résultats de la mise à jour des machines virtuelles de protection sur les hôtes VMware ESXi sont affichées.

Fermez l'Assistant.

Si la mise à jour des machines virtuelles de protection se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Vous pouvez utiliser ce fichier lorsque vous demandez l'aide du Service de Support Technique.

Si vous avez refusé le transfert des clés et la mise à jour automatique des bases antivirus lors de la mise à jour des machines virtuelles de protection, vous devrez activer l'application (cf. section "Activation de l'application" à la page 85) et mettre à jour les bases antivirus sur l'ensemble des machines virtuelles de protection mises à jour (cf. section "Mise à jour des bases antivirus" à la page144) après la mise à jour du module Antivirus Fichiers.

PROCEDURE DE MISE A JOUR DU MODULE DETECTION DES MENACES RESEAU

La mise à jour du module Détection des menaces réseau se déroule via la mise à jour des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des menaces réseau.

Avant de commencer la mise à jour du module Détection des menaces réseau, il est important de placer l'ensemble des fichiers d'image de machine virtuelle de protection dotés de la nouvelle version du module Détection des menaces réseau dans un dossier d'une ressource réseau accessible via le protocole HTTP.

Les paramètres indispensables à la mise à jour des machines virtuelles de protection se définissent à l'aide de l'Assistant d'installation, de mise à jour et de suppression des machines virtuelles de protection. L'Assistant transmet ces paramètres à VMware vShield Manager. VMware vShield Manager exécute les actions suivantes :

1. Installe les machines virtuelles de protection dotées de la nouvelle version du module Détection des menaces réseau sur les hôtes VMware ESXi des clusters VMware sélectionnés.

2. Supprime les machines virtuelles de protection dotées de l'ancienne version du module Détection des menaces réseau sur les hôtes VMware ESXi des clusters VMware sélectionnés.

   Pendant la suppression des machines virtuelles de protection sur les hôtes VMware ESXi entrant dans la composition du cluster VMware, VMware vShield Manager supprime également les fichiers de traçage.

   Après la suppression sur les hôtes VMware ESXi, les machines virtuelles de protection apparaissent toujours dans la Console d'administration Kaspersky Security Center. A l'issue du délai défini dans les paramètres du Kaspersky Security Center (cf. Documentation du Kaspersky Security Center), les machines virtuelles de protection sont automatiquement supprimées de la Console d'administration.

   Vous pouvez supprimer manuellement des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center directement après la fin de la procédure de suppression du module Détection des menaces réseau.

   Avant la suppression des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center, les événements envoyés par ces machines virtuelles de protection sont enregistrés dans le Kaspersky Security Center et figurent dans les rapports et le journal des événements du Kaspersky Security Center.

Pour mettre à jour le module Détection des menaces réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail dans le groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection des machines virtuelles contre les menaces réseau** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Installation, mise à jour ou suppression des machines virtuelles de protection avec le composant Détection des menaces réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à créer des machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de mise à jour.

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le VMware vCenter Server est accessible via le réseau, puis relancez la mise à jour de l'application.

ETAPE 3. SAISIE DE L'ADRESSE IP DU SERVEUR D'ADMINISTRATION DU KASPERSKY SECURITY CENTER

L'Assistant reçoit du Kaspersky Security Center l'adresse de connexion de la machine virtuelle à l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. Cette étape est accessible si l'adresse de connexion au Serveur d'administration du Kaspersky Security Center obtenue à partir du Kaspersky Security Center porte le nom NetBIOS ou DNS de l'ordinateur. Si l'adresse de connexion s'avère être l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center, cette étape est passée.

Désignez l'adresse IP de l'ordinateur sur lequel est installé le Serveur d'administration du Kaspersky Security Center. L'adresse IP est indiquée au format IPv4.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de mise à jour.

ETAPE 5. SELECTION DE L'IMAGE DE LA MACHINE VIRTUELLE DE PROTECTION

A cette étape, il convient d'indiquer le chemin vers le fichier OVF de la machine virtuelle de protection dotée de la nouvelle version du module Détection des menaces réseau sur la ressource réseau accessible par le protocole HTTP.

Le chemin vers le fichier OVF utilisé pour l'installation de la version précédente du module Détection des menaces réseau s'affiche dans le champ **Fichier OVF**.

Le chemin vers le fichier OVF de la machine virtuelle de protection dotée de la nouvelle version du module Détection des menaces réseau doit différer du chemin vers le fichier OVF utilisé pour l'installation de la version précédente de ce module.

Dans le champ **Fichier OVF**, indiquez le chemin vers le fichier OVF de la machine virtuelle de protection dotée de la nouvelle version du module Détection des menaces réseau et cliquez sur **Vérifier**.

L'Assistant vérifie la présence d'un accès à la ressource réseau où se trouve le fichier OVF. Si la ressource réseau est accessible, l'Assistant vérifie l'image de la machine virtuelle de protection. Si l'image est endommagée ou si sa version n'est pas prise en charge par l'Assistant, il affiche un message d'erreur.

Si l'analyse réussit, les informations suivantes relatives à l'image de la machine virtuelle de protection sélectionnée apparaissent dans la partie inférieure de la fenêtre :

- **Nom de l'application** : nom de l'application installée sur la machine virtuelle de protection.
- **Version de l'application** : numéro de la version de l'application.
- **Version de l'image de la machine virtuelle de protection** : numéro de version de l'image de machine virtuelle de protection.
- **Editeur** : éditeur de l'application installée sur la machine virtuelle de protection.
- **Description** : brève description de l'application.
- **Editeur** : émetteur du certificat utilisé pour signer l'image de la machine virtuelle de protection.
- **Taille de l'image** : taille du fichier de l'image de la machine virtuelle de protection.
- **Taille sur le disque** : volume approximatif d'espace disque requis pour le déploiement de la machine virtuelle de protection dans le référentiel de données de l'hôte VMware ESXi :
    - dans le cadre de la répartition dynamique de l'espace disque avec l'utilisation de VMware vStorage Thin Provisioning ;
    - dans le cadre de la répartition de l'espace disque avec un volume fixe.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. LECTURE DES CONTRATS DE LICENCE

Cette étape vous permet de prendre connaissance des Contrats de licence que vous allez conclure avec Kaspersky Lab et avec la société SUSE LLC. La société SUSE LLC est propriétaire du système d'exploitation SUSE Linux Enterprise Server 11 SP3 installé sur la machine virtuelle de protection.

Lisez attentivement les Contrats de licence et, si vous en acceptez tous les points, cochez la case **J'accepte les conditions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. SELECTION DES CLUSTERS VMWARE

A cette étape, sélectionnez les clusters VMware sur les hôtes VMware ESXi qui nécessitent de mettre à jour les machines virtuelles de protection.

Les colonnes du tableau affichent les informations relatives à l'ensemble des clusters VMware dans le cadre d'une plateforme VMware vCenter Server :

- **Nom du cluster VMware** – nom du cluster VMware.
- **Chemin d'accès** : chemin vers le cluster VMware dans l'infrastructure virtuelle VMware.

- **Protection** : informations sur l'activation ou non de la protection des machines virtuelles de ce cluster VMware contre les menaces réseau :
  - **Protégé** : machines virtuelles de protection dotées de l'ancienne version du module Détection des menaces réseau et installées sur les hôtes VMware ESXi de ce cluster VMware.
  - **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hôtes VMware ESXi entrant dans la composition de ce cluster VMware.

Dans le tableau, cases cochées à gauche des noms des clusters VMware protégées. Les machines virtuelles de protection seront mises à jour sur les hôtes VMware ESXi entrant dans la composition de ces clusters VMware.

Passez à l'étape suivante de l'Assistant.

ETAPE 8. SELECTION DES GROUPES DE PORTS DISTRIBUES

A cette étape, sélectionnez les groupes de ports distribués (Distributed Virtual Port Groups) qui nécessitent d'activer la protection contre les menaces réseau. Kaspersky Security contrôlera le trafic sur les groupes de ports distribués sélectionnés pour détecter les activités caractéristiques des attaques réseau.

Les colonnes du tableau affichent les informations relatives à l'ensemble des groupes de ports distribués configurés dans VMware Distributed Virtual Switches dans le cadre d'une plateforme VMware vCenter Server :

- **Groupe de ports distribués** : nom du groupe de ports distribués.
- **Chemin d'accès** : emplacement du groupe de ports distribués dans l'infrastructure virtuelle VMware.
- **Protection** : informations sur l'activation ou non de la vérification du trafic des machines virtuelles au sein de ce groupe de ports distribués :
  - **Activée** : Kaspersky Security vérifie le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.
  - **Désactivée** : l'application ne vérifie pas le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.

Pour sélectionner un groupe de ports distribués, dans le tableau, cochez les cases situées à gauche du nom de ce groupe de ports distribués.

Passez à l'étape suivante de l'Assistant.

ETAPE 9. FIN DE LA SAISIE DES PARAMETRES

Tous les paramètres indispensables à la mise à jour des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi ont été saisis.

A cette étape, les paramètres de déploiement des machines virtuelles de protection par VMware vShield Manager s'affichent : informations sur l'image de la machine virtuelle de protection choisie pour le déploiement, sur les clusters VMware où seront installées les machines virtuelles de protection dotées de la nouvelle version du module Détection des menaces réseau et sur les groupes de ports distribués VMware (Distributed Virtual Port Groups) pour lesquels la protection contre les menaces réseau sera activée.

S'il convient de modifier les paramètres, revenez aux étapes précédentes de l'Assistant.

Cliquez sur **Exécuter** pour terminer la configuration de la mise à jour des machines virtuelles de protection et passer à l'étape suivante de l'Assistant. L'Assistant transmet ces paramètres à VMware vShield Manager.

ETAPE 10. FIN DU TRAVAIL DE L'ASSISTANT

Cette étape affiche les informations relatives aux résultats de la transmission à VMware vShield Manager des paramètres indispensables à la mise à jour des machines virtuelles de protection dotées du module Détection des menaces réseau.

Si la transmission des paramètres été effectuée avec succès, fermez l'Assistant.

Si la transmission des paramètres à VMware vShield Manager se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Dans ce cas, fermez l'Assistant, corrigez les erreurs en fonction des raisons fournies et relancez à nouveau la procédure de mise à jour.

Vous pouvez consulter les informations relatives au procédé de déploiement des machines virtuelles de protection sur les hôtes VMware ESXi dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

Suite à la mise à jour du module Détection des menaces réseau, il est nécessaire d'activer l'application (cf. section "Activation de l'application" à la page 85) et d'exécuter la mise à jour des bases antivirus (à la page 144) sur les machines virtuelles avec le module Détection des menaces réseau.

CONVERSION DES STRATEGIES ET DES TACHES LORS DE LA MISE A JOUR DE L'APPLICATION

Lors de la mise à jour de l'application Kaspersky Security for Virtualization 2.0 ou Kaspersky Security for Virtualization 2.0 Maintenance Release 1 vers la version Kaspersky Security for Virtualization 3.0 Agentless, vous pouvez convertir les stratégies et les tâches afin d'utiliser leurs paramètres de configuration dans la version précédente de l'application.

Les stratégies et les tâches de Kaspersky Security for Virtualization 2.0 sont automatiquement conservées dans les stratégies et les tâches de Kaspersky Security for Virtualization 3.0 Agentless ; ceci dès la première modification et la première sauvegarde des paramètres de protection dans la stratégie, et des paramètres d'analyse dans les tâches.

Les stratégies et les tâches converties utilisent les paramètres des stratégies et des tâches de la version antérieure de l'application.

Les paramètres inexistants dans les stratégies et les tâches de Kaspersky Security for Virtualization 2.0 se traduisent ainsi dans les stratégies et les tâches converties :

- **Activer l'analyse des URL** : désactivé.
- **Ne pas bloquer l'accès aux URL suivantes** : adresses URL inconnues.
- **Analyser les disques amovibles et les clés (CD, DVD, Blu-Ray, USB)** : désactivé.

Les paramètres des actions à entreprendre lors de la détection d'une menace définis dans les stratégies et les tâches de Kaspersky Security for Virtualization 2.0 se traduisent ainsi dans les stratégies et les tâches converties :

- **Réparer. Supprimer si la réparation est impossible** : si l'action **Réparer** était sélectionnée dans la stratégie ou la tâche de Kaspersky Security for Virtualization 2.0. **Supprimer si la réparation est impossible**.
- **Réparer. Bloquer si la réparation est impossible** : si l'action **Réparer** était sélectionnée dans la stratégie ou la tâche de Kaspersky Security for Virtualization 2.0. **Bloquer si la réparation est impossible** ou action **Ignorer**.
- **Supprimer. Bloquer si la suppression est impossible** : si l'action **Supprimer** était sélectionnée dans la stratégie ou la tâche de Kaspersky Security for Virtualization 2.0.
- **Bloquer** : si l'action **Bloquer** était sélectionnée dans la stratégie ou la tâche de Kaspersky Security for Virtualization 2.0.

SUPPRESSION DE L'APPLICATION

Cette section comprend des informations sur la suppression des modules Antivirus Fichiers et Détection des menaces réseau de Kaspersky Security.

DANS CETTE SECTION

SUPPRESSION DU MODULE ANTIVIRUS FICHIERS

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

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

La suppression du module Antivirus Fichiers s'effectue via la suppression des machines virtuelles de protection dotées du module Antivirus Fichiers sur les hôtes VMware ESXi (cf. section "Procédure de suppression du module Antivirus Fichiers" à la page 68). Vous pouvez supprimer les machines virtuelles de protection sur tous les hôtes VMware ESXi qui appartiennent au cluster KSC ou procéder à une sélection.

Pendant la suppression des machines virtuelles de protection sur les hôtes VMware ESXi, l'Assistant de suppression de l'application supprime également les copies de sauvegarde des fichiers de la sauvegarde ainsi que les fichiers de traçage enregistrés sur les machines virtuelles de protection.

Après la suppression sur les hôtes VMware ESXi, les machines virtuelles de protection apparaissent toujours dans la Console d'administration Kaspersky Security Center. A l'issue du délai défini dans les paramètres du Kaspersky Security Center (cf. Documentation du Kaspersky Security Center), les machines virtuelles de protection sont automatiquement supprimées de la Console d'administration.

Vous pouvez supprimer manuellement des machines virtuelles de protection de la console d'administration du Kaspersky Security Center directement après la fin de la procédure de suppression de l'application.

Avant la suppression des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center, les événements envoyés par ces machines virtuelles de protection sont enregistrés dans le Kaspersky Security Center et figurent dans les rapports et le journal des événements du Kaspersky Security Center. La liste des copies de sauvegarde des fichiers placés dans la sauvegarde sur ces machines virtuelles de protection est également enregistrée dans le Kaspersky Security Center, mais aucune action ne peut être réalisée sur les copies des fichiers car les copies de sauvegarde ont été supprimées pendant la suppression des machines virtuelles de protection sur les hôtes VMware ESXi.

Il est conseillé de supprimer les machines virtuelles de protection à l'aide du Kaspersky Security Center, il est déconseillé de supprimer les machines virtuelles de protection manuellement à l'aide de VMware.

Pour supprimer le module Antivirus Fichiers, les modules suivants de l'infrastructure virtuelle VMware doivent être accessibles :

- **VMware vCenter Server**. Offre des informations au sujet des hôtes VMware ESXi sur lesquels la machine virtuelle de protection est installée.
- **VMware vShield Manager**. Permet d'annuler l'enregistrement des machines virtuelles de protection dans VMware vShield Server.

PROCEDURE DE SUPPRESSION DU MODULE ANTIVIRUS FICHIERS

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

Pour supprimer le module Antivirus Fichiers, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection du système de fichiers des machines virtuelles** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

Choisissez l'option **Suppression**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à supprimer les machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de suppression.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant le signalera et restera à l'étape actuelle. Si le compte présente plus de privilèges que nécessaire, l'Assistant le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le VMware vCenter Server est accessible via le réseau, puis relancez la suppression de l'application.

ETAPE 3. SELECTION DES HOTES VMWARE ESXI

A cette étape, sélectionnez les hôtes VMware ESXi sur lesquels vous souhaitez supprimer la machine virtuelle de protection.

Les colonnes du tableau reprennent les informations relatives aux hôtes VMware ESXi de la plateforme VMware vCenter Server sélectionnée sur lesquels la machine virtuelle de protection est installée :

- **Hôte VMware ESXi** : l'adresse IP ou le nom de domaine de l'hôte VMware ESXi.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hôte VMware ESXi.
- **Etat** : informations sur l'état de la machine virtuelle de protection :
  - **Accessible** : la machine virtuelle de protection est activée.
  - **Eteinte** : la machine virtuelle de protection est désactivée.

Pour sélectionner un hôte VMware ESXi, cochez la case en regard de son nom dans le tableau. Vous pouvez uniquement sélectionner les hôtes VMware ESXi sur lesquels la machine virtuelle de protection présente l'état *Accessible*.

Passez à l'étape suivante de l'Assistant.

ETAPE 4. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

Pour bien supprimer une machine virtuelle de protection, l'Assistant doit annuler l'enregistrement de celle-ci dans VMware vShield Manager. Pour annuler l'enregistrement, l'Assistant se connecte à VMware vShield Manager.

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse IP de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de suppression.

ETAPE 5. CONFIRMATION DE LA SUPPRESSION

A cette étape, la fenêtre de l'Assistant affiche les informations relatives au nombre de machines virtuelles de protection qui sera supprimé.

Passez à l'étape suivante de l'Assistant afin de confirmer la suppression ou revenez à l'étape précédente de l'Assistant.

ETAPE 6. SUPPRESSION DES MACHINES VIRTUELLES DE PROTECTION

Cette étape correspond à la suppression des machines virtuelles de protection sur les hôtes VMware ESXi. Le processus dure un certain temps. Attendez la fin du processus de suppression.

Les informations relatives à la suppression des machines virtuelles de protection sont reprises dans le tableau. L'heure de début et l'heure de fin de la suppression sur chacun des hôtes VMware ESXi sont affichées dans les colonnes **Début** et **Fin**. Ces informations permettent d'estimer le temps nécessaire à la suppression de toutes les machines virtuelles de protection sélectionnées.

Une fois que la suppression de l'application sur tous les hôtes VMware ESXi sélectionnés est terminée, passez à l'étape suivante de l'Assistant.

ETAPE 7. FIN DE LA SUPPRESSION DES MACHINES VIRTUELLES DE PROTECTION

Au cours de cette étape, les informations relatives au résultat de la suppression des machines virtuelles de protection sur les hôtes VMware ESXi sont affichées.

Fermez l'Assistant.

Si la suppression des machines virtuelles de protection se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Vous pouvez utiliser ce fichier lorsque vous demandez l'aide du Service de Support Technique.

SUPPRESSION DU MODULE DETECTION DES MENACES RESEAU

Cette section contient des informations sur la suppression du module Détection des menaces réseau.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des menaces réseau.

Vous pouvez supprimer le module Détection des menaces réseau sur tous les clusters VMware ou sur certains seulement.

La suppression du module Détection des menaces réseau sur tous les clusters VMware passe par la suppression totale de ce module de l'infrastructure virtuelle VMware. Les paramètres indispensables à la suppression totale du module Détection des menaces réseau se définissent à l'aide de l'Assistant de suppression totale (cf. section "Procédure de suppression totale du module Détection des menaces réseau" page 75). L'Assistant transmet ces paramètres à VMware vShield Manager. VMware vShield Manager exécute les actions suivantes :

- supprime les machines virtuelles de protection sur tous les hôtes VMware ESXi entrant dans la composition de toutes les grappes VMware ;
- annule l'enregistrement des machines virtuelles de protection du module Détection des menaces réseau (service de Kaspersky Network Protection) dans VMware vShield Manager.

La suppression sélective du module Détection des menaces réseau s'effectue via la suppression des machines virtuelles de protection dotées du module Détection des menaces réseau sur les hôtes VMware ESXi entrant dans la composition des clusters VMware sélectionnés. Les paramètres de suppression des machines virtuelles de protection sur les hôtes VMware ESXi se définissent à l'aide de l'Assistant d'installation, de mise à jour et de suppression des machines virtuelles de protection (cf. section "Procédure de suppression des machines virtuelles de protection dotées du module Détection des menaces réseau" page 72). L'Assistant transmet ces paramètres à VMware vShield Manager. VMware vShield Manager exécute les actions suivantes :

- supprime les machines virtuelles de protection sur tous les hôtes VMware ESXi entrant dans la composition des grappes VMware sélectionnées ;
- annule l'enregistrement des machines virtuelles de protection dans VMware vShield Manager.

Lors de la suppression sélective du module Détection des menaces réseau, l'enregistrement du module Détection des menaces réseau (service de Kaspersky Network Protection) n'est pas annulé.

Pendant la suppression des machines virtuelles de protection sur les hôtes VMware ESXi entrant dans la composition du cluster VMware, VMware vShield Manager supprime également les fichiers de traçage.

Après la suppression sur les hôtes VMware ESXi, les machines virtuelles de protection apparaissent toujours dans la Console d'administration Kaspersky Security Center. A l'issue du délai défini dans les paramètres du Kaspersky Security Center (cf. Documentation du Kaspersky Security Center), les machines virtuelles de protection sont automatiquement supprimées de la Console d'administration.

Vous pouvez supprimer manuellement des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center directement après la fin de la procédure de suppression du module Détection des menaces réseau.

Avant la suppression des machines virtuelles de protection de la Console d'administration du Kaspersky Security Center, les événements envoyés par ces machines virtuelles de protection sont enregistrés dans le Kaspersky Security Center et figurent dans les rapports et le journal des événements du Kaspersky Security Center.

Il est conseillé de supprimer les machines virtuelles de protection à l'aide du Kaspersky Security Center, il est déconseillé de supprimer les machines virtuelles de protection manuellement à l'aide de VMware.

Pour supprimer le module Détection des menaces réseau, les modules suivants de l'infrastructure virtuelle VMware doivent être accessibles :

- **VMware vCenter Server**. Fournit des informations au sujet des hôtes VMware ESXi sur lesquels les machines virtuelles de protection sont installées.
- **VMware vShield Manager**. S'utilise pour la suppression des machines virtuelles de protection sur les hôtes VMware ESXi, l'annulation de l'enregistrement des machines virtuelles de protection et du module Détection des menaces réseau (service de Kaspersky Network Protection) dans VMware vShield Manager.

PROCEDURE DE SUPPRESSION DES MACHINES VIRTUELLES DE PROTECTION DOTEES DU MODULE DETECTION DES MENACES RESEAU

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des menaces réseau.

Pour supprimer les machines virtuelles de protection dotées du module Détection des menaces réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection des machines virtuelles contre les menaces réseau** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Installation, mise à jour ou suppression des machines virtuelles de protection avec le composant Détection des menaces réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**. Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
- **Nom de l'utilisateur**. Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère.
- **Mot de passe**. Mot de passe du compte utilisateur sous lequel s'opère la connexion à VMware vCenter Server.

Dans les deux cas, choisissez le compte utilisateur d'un administrateur autorisé à supprimer les machines virtuelles.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de suppression.

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le VMware vCenter Server est accessible via le réseau, puis relancez la procédure de suppression.

ETAPE 3. SAISIE DES PARAMETRES DE CONNEXION A VMWARE VSHIELD MANAGER

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure de suppression.

ETAPE 4. CONSULTATION DES INFORMATIONS RELATIVES A L'IMAGE DE LA MACHINE VIRTUELLE DE PROTECTION

A cette étape, la fenêtre de l'Assistant affiche le chemin vers le fichier OVF de la machine virtuelle de protection déployée sur les clusters VMware qui font partie du VMware vCenter Server sélectionné.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. LECTURE DES CONTRATS DE LICENCE

Cette étape vous permet de prendre connaissance du texte des Contrats de licence que vous allez conclure avec Kaspersky Lab et la société SUSE LLC. La société SUSE LLC est propriétaire du système d'exploitation SUSE Linux Enterprise Server 11 SP3 installé sur la machine virtuelle de protection.

Pour poursuivre la suppression, choisissez l'option **J'accepte les conditions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 6. SELECTION DES CLUSTERS VMWARE

A cette étape, indiquez les clusters VMware sur les hôtes VMware ESXi pour lesquels il faut supprimer les machines virtuelles de protection dotées du module Détection des menaces réseau.

Les colonnes du tableau affichent les informations relatives à l'ensemble des clusters VMware dans le cadre d'une plateforme VMware vCenter Server :

- **Nom du cluster VMware** – nom du cluster VMware.
- **Chemin d'accès** : chemin vers le cluster VMware dans l'infrastructure virtuelle VMware.
- **Protection** : informations sur l'activation ou non de la protection des machines virtuelles de ce cluster VMware contre les menaces réseau :
  - **Protégé** : des machines virtuelles de protection sont installées sur les hôtes VMware ESXi entrant dans la composition de ce cluster VMware.
  - **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hôtes VMware ESXi entrant dans la composition de ce cluster VMware.

Pour désigner le cluster VMware sur lequel il convient de supprimer les machines virtuelles de protection, dans le tableau, décochez la case située à gauche du nom de ce cluster VMware.

Passez à l'étape suivante de l'Assistant.

ETAPE 7. SELECTION DES GROUPES DE PORTS DISTRIBUES

A cette étape, désignez les groupes de ports distribués (Distributed Virtual Port Groups) qui nécessitent de désactiver la protection contre les menaces réseau. Kaspersky Security ne contrôlera pas le trafic des machines virtuelles qui passe par les groupes sélectionnés de ports distribués.

Les colonnes du tableau affichent les informations relatives à l'ensemble des groupes de ports distribués configurés dans Distributed Virtual Switches dans le cadre d'une plateforme VMware vCenter Server :

- **Groupe de ports distribués** : nom du groupe de ports distribués.
- **Chemin d'accès** : emplacement du groupe de ports distribués dans l'infrastructure virtuelle VMware.

- **Protection** : informations sur l'activation ou non de la vérification du trafic des machines virtuelles au sein de ce groupe de ports distribués :

  - **Activée** : Kaspersky Security vérifie le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.

  - **Désactivée** : l'application ne vérifie pas le trafic au sein de ce groupe de ports distribués en vue de détecter les activités caractéristiques des attaques réseau.

Pour désigner le groupe de ports distribués nécessitant de désactiver la protection contre les menaces réseau, dans le tableau, décochez la case située à gauche du nom de ce groupe de ports distribués.

Passez à l'étape suivante de l'Assistant.

ETAPE 8. FIN DE LA SAISIE DES PARAMETRES

Tous les paramètres indispensables à la suppression des machines virtuelles de protection sur les hôtes VMware ESXi ont été saisis.

A cette étape, les paramètres de suppression des machines virtuelles de protection par VMware vShield Manager s'affichent : informations sur l'image de la machine virtuelle de protection déployée sur les hôtes VMware ESXi, sur les clusters VMware et sur les groupes de ports distribués (Distributed Virtual Port Groups) pour lesquels la protection contre les menaces réseau sera activée.

S'il convient de modifier les paramètres, revenez aux étapes précédentes de l'Assistant.

Cliquez sur **Exécuter**, pour terminer la saisie des paramètres de suppression des machines virtuelles de protection et passer à l'étape suivante de l'Assistant. L'Assistant transmet ces paramètres à VMware vShield Manager.

ETAPE 9. FIN DU TRAVAIL DE L'ASSISTANT

Cette étape affiche les informations relatives aux résultats de la transmission à VMware vShield Manager des paramètres de suppression des machines virtuelles de protection sur les hôtes VMware ESXi.

Si la transmission des paramètres été effectuée avec succès, fermez l'Assistant.

Si la transmission des paramètres à VMware vShield Manager se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Dans ce cas, fermez l'Assistant, corrigez les erreurs en fonction des raisons fournies et relancez à nouveau la procédure de suppression.

Les informations relatives au procédé de suppression des machines virtuelles de protection sur les hôtes VMware ESXi peuvent être consultées dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

PROCEDURE DE SUPPRESSION TOTALE DU MODULE DETECTION DES MENACES RESEAU

Pour supprimer complètement le module Détection des menaces réseau, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection des machines virtuelles contre les menaces réseau** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

A cette étape, choisissez l'option **Suppression totale du module Détection des menaces réseau**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VSHIELD MANAGER

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine du module VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Pour poursuivre la procédure de suppression totale du module Détection des menaces réseau, cliquez que le bouton **Continuer**.

Si l'infrastructure virtuelle VMware présente des machines virtuelles de protection dotées du module Détection des menaces réseau, une fenêtre s'ouvre avec un message notifiant la désactivation de la protection des clusters VMware et des groupes de ports distribués. Au cours de la suppression totale du module Détection des menaces réseau, l'Assistant transmet les paramètres nécessaires à la désactivation de la protection des clusters VMware et des groupes de ports distribués à VMware vShield Manager . VMware vShield Manager désactive la protection de tous les clusters VMware et groupes de ports distribués. Cliquez sur le bouton **OK** pour confirmer la désactivation de la protection.

ETAPE 3. FIN DE LA SAISIE DES PARAMETRES

Tous les paramètres indispensables à la suppression totale du module Détection des menaces réseau de l'infrastructure virtuelle VMware ont été saisis.

S'il convient de modifier les paramètres, revenez aux étapes précédentes de l'Assistant.

Cliquez sur **Exécuter**, pour terminer saisie des paramètres et passer à l'étape suivante de l'Assistant. L'Assistant transmet ces paramètres à VMware vShield Manager.

ETAPE 4. FIN DU TRAVAIL DE L'ASSISTANT

Cette étape affiche les informations relatives aux résultats de la transmission à VMware vShield Manager des paramètres de suppression totale du module Détection des menaces réseau.

Si la transmission des paramètres été effectuée avec succès, fermez l'Assistant.

Si la transmission des paramètres à VMware vShield Manager se termine avec une erreur, l'Assistant affiche un lien vers le fichier contenant son journal de travail. Dans ce cas, fermez l'Assistant, corrigez les erreurs en fonction des raisons fournies et relancez à nouveau la procédure de suppression total du module Détection des menaces réseau.

Le service Kaspersky Network Protection (module Détection des menaces réseau) est supprimé de la liste des services après la suppression totale du module Détection des menaces réseau dans l'interface Internet VMware vShield Manager.

ELIMINATION DES ERREURS D'ENREGISTREMENT DES MACHINES VIRTUELLES DE PROTECTION

Cette section contient la description des erreurs d'enregistrement possibles des machines virtuelles de protection dotées du module Antivirus Fichiers dans VMware vShield Manager et les moyens pour s'en débarrasser.

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

DANS CETTE SECTION

A PROPOS DES ERREURS POTENTIELLES D'ENREGISTREMENT DES MACHINES VIRTUELLES DE PROTECTION

Compte tenu des particularités liées à l'utilisation commune de l'application Kaspersky Security et de VMware vShield Manager, des erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager sont possibles pendant l'installation de l'application, ainsi qu'une annulation incorrecte de leur enregistrement pendant la suppression de l'application.

Les erreurs suivantes ainsi que les solutions suivantes sont possibles :

- Les machines virtuelles de protection ne sont pas enregistrées dans VMware vShield Manager. La solution est d'enregistrer ces machines virtuelles de protection dans VMware vShield Manager.
- Les machines virtuelles de protection sont mal enregistrées dans VMware vShield Manager : elles sont enregistrées comme des machines virtuelles de protection de Kaspersky Lab mais ne possèdent pas d'indices d'installation de l'application Kaspersky Security. La solution est de supprimer les enregistrements sur de telles machines virtuelles de protection depuis VMware vShield Manager.
- Les machines virtuelles de protection sont mal supprimées : les machines virtuelles de protection sont absentes de VMware vCenter Server, mais les enregistrements concernant ces machines restent dans VMware vShield Manager. La solution est de supprimer les enregistrements sur de telles machines virtuelles de protection depuis VMware vShield Manager.

Les erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager peuvent provoquer un échange incorrect d'événements entre l'application Kaspersky Security et VMware vShield Manager.

Pour éliminer de telles erreurs, un Assistant d'élimination des erreurs est prévu.

PROCEDURE D'ELIMINATION DES ERREURS D'ENREGISTREMENT DES MACHINES VIRTUELLES DE PROTECTION

Pour éliminer les erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le Serveur d'administration.
3. Cliquez sur le lien **Administrer Kaspersky Security for Virtualization Agentless** pour lancer l'Assistant. Le lien se trouve dans la zone de travail du groupe **Déploiement**.
4. Dans la fenêtre ouverte, choisissez l'option **Protection du système de fichiers des machines virtuelles** et passez à l'étape suivante de l'Assistant.
5. Suivez les instructions de l'Assistant.

DANS CETTE SECTION

ETAPE 1. SELECTION DE L'ACTION

Sélectionnez l'option **Elimination des erreurs d'enregistrement** à cette étape.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION A VMWARE VCENTER SERVER

Cette étape permet de définir les paramètres de connexion de l'Assistant à VMware vCenter Server :

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

Passez à l'étape suivante de l'Assistant.

Si le certificat reçu de VMware vCenter Server n'est pas approuvé, une fenêtre s'ouvre et affiche un message sur l'erreur de certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'élimination des erreurs.

L'Assistant vérifiera la possibilité de se connecter à VMware vCenter Server avec le nom et le mot de passe du compte indiqué. Si le compte ne présente pas assez de privilèges, l'Assistant le signalera et restera à l'étape actuelle. Si le compte présente plus de privilèges que nécessaire, l'Assistant le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

Ensuite, l'Assistant établira la connexion à VMware vCenter Server.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le VMware vCenter Server est accessible via le réseau, puis relancez l'élimination des erreurs.

ETAPE 3. CONNEXION A VMWARE VSHIELD MANAGER

Pour rechercher et éliminer les éventuelles erreurs d'enregistrement des machines virtuelles de protection, l'Assistant requiert la connexion à VMware vShield Manager.

A cette étape, indiquez les paramètres de connexion à VMware vShield Manager :

- **Adresse IP de VMware vShield Manager**. Adresse IP au format IPv4 ou nom de domaine VMware vShield Manager pour lequel les machines virtuelles de protection se trouvent dans la zone d'action.
- **Nom de l'utilisateur**. Nom de compte d'administrateur pour la connexion à VMware vShield Manager.
- **Mot de passe**. Mot de passe de compte administrateur pour la connexion à VMware vShield Manager.

Passez à l'étape suivante de l'Assistant.

Si le certificat, obtenu à partir du VMware vShield Manager, n'est pas approuvé, une fenêtre s'ouvre avec un message spécifiant l'erreur contenue dans le certificat. Le lien dans cette fenêtre permet de consulter les informations relatives au certificat. Cliquez sur **Poursuivre** pour continuer la procédure d'élimination des erreurs.

L'Assistant établira la connexion à VMware vShield Manager.

S'il n'est pas possible d'établir la connexion à VMware vCenter Server, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vShield Manager est accessible via le réseau, puis recommencez l'élimination des erreurs.

ETAPE 4. SELECTION DES ERREURS A ELIMINER

A cette étape l'Assistant exécute la collecte d'informations et l'analyse des erreurs détectées. Le processus dure un certain temps. Attendez la fin du processus de modification.

Finalement, l'Assistant affiche la liste des machines virtuelles de protection pour lesquelles les erreurs d'enregistrement dans VMware vShield Manager ont été détectées :

- Les machines virtuelles de protection ne sont pas enregistrées dans VMware vShield Manager. Sélectionnez ces machines virtuelles de protection pour les enregistrer dans VMware vShield Manager.
- Les machines virtuelles de protection sont mal enregistrées dans VMware vShield Manager. Sélectionnez ces machines virtuelles de protection pour supprimer leur enregistrement dans VMware vShield Manager.
- Les machines virtuelles de protection sont mal supprimées. Sélectionnez ces machines virtuelles de protection pour supprimer leur enregistrement dans VMware vShield Manager.

La liste indique l'identificateur et le nom de chaque machine virtuelle dans l'infrastructure virtuelle VMware. Si les machines virtuelles de protection sont mal supprimées, seul leur identificateur est indiqué.

Pour sélectionner la machine virtuelle de protection, cochez la case à gauche de son identificateur.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. CONFIRMATION DES ACTIONS

A cette étape, la fenêtre de l'Assistant affiche les informations sur les conséquences, dans l'infrastructure virtuelle VMware, qu'entraînera l'élimination des erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager.

Passez à l'étape suivante de l'Assistant afin de confirmer l'élimination de l'erreur ou revenez à l'étape précédente de l'Assistant.

ETAPE 6. ELIMINATION DES ERREURS

A cette étape, définissez l'élimination des erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager. Le processus dure un certain temps. Attendez la fin du processus de modification.

Une fois le processus terminé, l'Assistant passe automatiquement à l'étape suivante.

ETAPE 7. FIN DE L'ELIMINATION DES ERREURS

Cette étape affiche les informations sur les résultats de l'élimination des erreurs d'enregistrement des machines virtuelles de protection dans VMware vShield Manager.

Si des erreurs se sont produites dans l'Assistant, les informations suivantes s'affichent :

- l'identificateur de la machine virtuelle de protection dans l'infrastructure virtuelle VMware ;
- le nom de la machine virtuelle de protection ;
- le code et la description de l'erreur apparue générés par VMware vShield Manager.

Fermez l'Assistant.

LICENCE DE L'APPLICATION

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.

DANS CETTE SECTION

A PROPOS DU CONTRAT DE LICENCE

Le *contrat de licence* 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.

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

- Pendant l'installation de l'application (cf. section "Etape 5. Consultation des contrats de licence" à la page 35).
- En lisant le document license.txt. Ce document est repris dans la distribution de l'application (cf. section "Distribution" à la page. 17).

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 conditions du Contrat de licence, vous devez interrompre l'installation de l'application.

PRESENTATION 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 hôtes VMware ESXi.

  Kaspersky Security protège uniquement les machines virtuelles de l'infrastructure virtuelle VMware sur lesquelles le pilote 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 hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées. 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 85). 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 hôtes 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 dans le cadre d'une même plateforme VMware vCenter Server. .

PRESENTATION DU CERTIFICAT DE LICENCE

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

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

- numéro de 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.

PRESENTATION DE LA CLE

La clé est une séquence unique de chiffres et de lettres. La clé permet l'utilisation de l'application conformément aux conditions figurant dans le Certificat de licence (au type de licence, à la durée de validité de la licence, aux restrictions imposées par la licence).

Elle peut être ajoutée via un code d'activation ou un fichier clé.

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

La clé peut être bloquée par Kaspersky Lab si vous avez enfreint les conditions du Contrat de licence. Si la clé est bloquée, il est nécessaire d'ajouter une autre clé pour utiliser l'application.

Clés actives et clés complémentaires.

Clé active : clé utilisée lors du fonctionnement de l'application. Une clé active peut être ajoutée pour la licence d'évaluation ou la licence commerciale.

Clé complémentaire : clé confirmant le droit d'utilisation de l'application mais qui ne s'utilise pas au moment donné. A la fin de la validité de la clé active, la clé complémentaire s'active automatiquement.

La clé complémentaire peut être ajoutée uniquement en présence d'une clé active.

La clé de la licence d'évaluation peut être utilisée uniquement en tant que clé active et ne peut en aucun cas servir de clé complémentaire. La clé de la licence d'évaluation ne peut en aucun cas remplacer la clé active d'une licence commerciale.

Kaspersky Security accepte les types de clés suivants :

- *Clé pour serveur* : clé prévue pour l'utilisation de l'application afin de protéger les machines virtuelles dotées d'un système d'exploitation pour serveurs.
- *Clé pour poste de travail* : clé prévue pour l'utilisation de l'application pour protéger les machines virtuelles dotées d'un système d'exploitation pour postes de travail.
- *Clé avec limitation en fonction du nombre de cœurs* : clé prévue pour l'utilisation de l'application afin de protéger les 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 hôtes VMware ESXi dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

PRESENTATION DU CODE D'ACTIVATION

Le *Code d'activation* est un code qui vous est fourni par Kaspersky Lab. Vous recevez un code d'activation lors de l'achat d'une licence commerciale pour Kaspersky Security ou lors de la commande d'une version d'évaluation de l'application. Ce code sert à activer l'application.

Le code d'activation constitue une suite de vingt chiffres et lettres selon le format xxxxx-xxxxx-xxxxx-xxxxx.

Pour activer l'application avec un code d'activation, il convient de se connecter aux serveurs d'activation Kaspersky Lab.

Vous saisissez le code d'activation pour ajouter une clé.

En cas de perte ou de suppression du code d'activation après l'activation, vous pouvez le restaurer en envoyant une demande au Support Technique (cf. section "Contacter le Support Technique" page 167).

PRESENTATION DU FICHIER CLE

Le *Fichier clé* est un fichier de type xxxxxxxx.key qui vous est fourni par Kaspersky Lab. Vous recevez un fichier clé lors de l'achat d'une licence commerciale pour Kaspersky Security ou lors de la commande d'une version d'évaluation de l'application. Ce fichier clé sert à activer l'application.

Le fichier clé comporte toutes les informations nécessaires à l'activation de l'application. Pour activer l'application avec un fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation Kaspersky Lab et de disposer d'un accès à Internet.

En cas de suppression accidentelle du fichier clé, vous pouvez le restaurer en envoyant une demande au Support Technique (cf. section "Contacter le Support Technique" à la page 167).

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. La 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 hôtes VMware ESXi dans le cadre d'une plateforme VMware vCenter Server.

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

Si vous utilisez le mode de licence en fonction du nombre de cœurs de processeurs de l'hôte 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.

Pour activer l'application, procédez comme suit :

1. Créez une tâche d'ajout de clé pour chaque cluster KSC reprenant les machines virtuelles auxquelles vous souhaitez ajouter une clé (cf. section "Création d'une tâche d'ajout de clé" à la page 86).

2. Lancez la tâche d'ajout de clé (cf. section "Lancement de la tâche d'ajout de clé" la page 89).

Si le nombre de machines virtuelles protégées ou le nombre de cœurs de processeur utilisés sur les hôtes 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

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. 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 de l'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 connexion suivante au serveur proxy, l'authentification s'effectuera automatiquement avec les 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**.

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 ou commerciale.
- **Restriction** : dépend du type de clé.
  - pour une clé serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;
  - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.
- **Durée de validité de la licence** : durée d'utilisation de l'application indiquée dans le Certificat de licence. Par exemple, 365 jours.
- **Date d'expiration de la 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.

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 le temps de retard maximal de 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 10000 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 le temps de retard maximal de 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 le temps de retard maximal de 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 89).

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. 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**.

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 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. Si aucune clé active n'a déjà été ajoutée à la machine virtuelle, si la clé active correspond à un autre mode de licence ou si le type de la clé complémentaire ajoutée ne correspond pas au type de clé active précédemment ajouté, la tâche d'ajout de la clé sur une telle machine virtuelle de protection se soldera par une erreur et la clé complémentaire ne sera pas ajoutée.

La clé de la licence d'évaluation ne peut en aucun cas servir de clé complémentaire. La clé de la licence d'évaluation ne peut en aucun cas remplacer la clé active d'une licence commerciale.

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.

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'hôte VMware ESXi, 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. 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 86).

2. Lancez la tâche d'ajout de clé (cf. section "Lancement de la tâche d'ajout de clé" la page 89).

   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.

   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.

CONSULTATION DES INFORMATIONS RELATIVES AUX CLES AJOUTEES

Les informations relatives aux clés ajoutées sont accessibles :

- dans le dossier **Stockages** de l'arborescence de la console, dans le sous-répertoire **Clés** ;
- 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 A LA CLE DANS LE DOSSIER CLES

Pour consulter les informations relatives à la clé dans le dossier Clés, procédez comme suit :

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Stockages** de l'arborescence de la console, choisissez le sous-répertoire **Clés**.

   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** : type de licence, évaluation ou commerciale.
   - **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 d'expiration de la 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 cette clé.

- **Restriction** : dépend du type de clé.

    - pour une clé serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;

    - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.

- **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.

Le Kaspersky Security Center permet d'afficher dans le dossier **Clés** 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 d'expiration de la 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.

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. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
   - Cliquez sur le lien **Propriétés de l'ordinateur** pour ouvrir la fenêtre des propriétés de la machine virtuelle de protection. Le lien se trouve à droite de la liste des machines virtuelles de protection.

   La fenêtre **Propriétés : <nom de la machine virtuelle de protection>** s'ouvre.
6. Dans la liste de gauche, choisissez l'option **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. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de l'application Kaspersky Security for Virtualization 3.0 Agentless** s'ouvre.
9. Dans la liste de gauche, choisissez 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 ou commerciale.
   - **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 serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;
    - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.

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 serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;
    - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 autorisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.

Le Kaspersky Security Center permet d'afficher les informations relatives à une clé dans les propriétés de l'application. 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).
- **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. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.
   - Cliquez sur le lien **Modifier les paramètres de la tâche** pour ouvrir la fenêtre des propriétés de la tâche. Le lien se trouve à droite de la liste des tâches dans le groupe **Exécution de la tâche**.

   La fenêtre **Propriétés : <Nom de la tâche>** s'ouvre.
6. Dans la liste de gauche, choisissez 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 ou commerciale.
   - **Restriction** : dépend du type de clé.
     - pour une clé serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;
     - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.
   - **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.
   - **Date d'expiration de la 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.

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 : nombre de cœurs de processeur physique utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.
- **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 serveur : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour serveurs fonctionnant en même temps et pour lesquelles la protection est activée ;
  - pour une clé poste de travail : la restriction correspond au nombre maximal de machines virtuelles dotées d'un système d'exploitation pour postes de travail fonctionnant en même temps 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 utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.
- **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.
- **Date d'expiration de la 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 reprennent le nombre maximal de machines virtuelles avec système d'exploitation pour serveur ou poste de travail qui peuvent être exécutées simultanément et pour lesquelles la protection est activée ; ou le nombre maximal de cœurs de processeurs physiques utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées. 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 de machines virtuelles dotées d'un système d'exploitation pour serveurs ou pour postes de travail ou par rapport au nombre de cœurs de processeurs physique utilisés sur tous les hôtes 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 d'expiration de la 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 : nombre de cœurs de processeur physique utilisés sur tous les hôtes VMware ESXi sur lesquels des machines virtuelles de protection sont installées.
- **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.

Le Kaspersky Security Center permet d'afficher les informations relatives à une clé pour chaque machine virtuelle de protection dans le rapport sur l'utilisation des clés. 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 d'expiration de la 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.

CREATION D'UNE STRATEGIE

Une fois Kaspersky Security installé, il est nécessaire de configurer le fonctionnement de l'application à l'aide des stratégies.

Kaspersky Security ne commencera à protéger les machines virtuelles qu'après que vous aurez configuré les paramètres de fonctionnement de l'application à l'aide de stratégies, puis activé l'application (cf. section "Activation de l'application" à la page 85). Si aucune clé n'est ajoutée sur la machine virtuelle de protection ou si elle ne présente aucune base antivirus, l'application ne protège pas les machines virtuelles.

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

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. 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 protection**, 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 protection** :

   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 analysé**.

  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 :

- **Niveau d'analyse heuristique**.

  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*.

  Niveau d'analyse heuristique défini pour ce niveau de protection :

  - **Superficiel**. 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 spécification de l'analyse heuristique, la possibilité de détecter une menace est faible par rapport aux niveaux de spécification de l'analyse heuristique **Moyen** et **Minutieux**. L'analyse requiert moins de ressources de la machine virtuelle et s'exécute plus rapidement.

  - **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.

  - **Minutieux**. Pendant la recherche du code malveillant dans les fichiers, l'analyseur heuristique exécute dans les fichiers exécutables un nombre d'instructions qui dépasse le nombre d'instructions pour des niveaux d'analyse heuristique **Superficiel** et **Moyen**. A ce niveau d'analyse heuristique, la possibilité de détecter une menace est plus importante qu'aux niveaux **Superficiel** et **Moyen**. L'analyse requiert plus de ressources de la machine virtuelle de protection et prend plus de temps.

  Par défaut, la valeur **Moyen** est attribuée aux profils de protection, et **Minutieux** aux tâches d'analyse.

- **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 analyser**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à analyser** qui apparaît :

- **Utilitaires malveillants**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation de la protection contre les programmes numéroteurs.

  Les *programmes numéroteurs* peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.

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

  La case est cochée par défaut.

- **Autres**.

  Activation 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 d'autres applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  La case est décochée 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 analyser**.

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

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 protection** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action à réaliser suite à la 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 n'importe quel fichier des machines virtuelles de protection, cliquez sur le bouton **Configuration** dans le groupe **Exclusions de l'analyse**.

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

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

      - **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.

      - **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.

   b. Dans le tableau **Dossiers**, saisissez la liste des extensions de fichiers à ne pas analyser dans le cadre de la protection de la machine virtuelle. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure les sous-dossiers de la protection.

4. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de l'analyse**.

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

ETAPE 4. CONFIGURATION DES PARAMETRES D'ANALYSE DES FICHIERS COMPACTES

Kaspersky Security peut analyser les fichiers compactés et le module compacteur présents dans les archives autoextractibles SFX.

Pour empêcher la découverte des applications malveillantes, les individus malintentionnés les compactent à l'aide de compacteurs spéciaux ou compactent le même fichier plusieurs fois. Les experts de Kaspersky Lab ont identifié les compacteurs que les individus malintentionnés utilisent le plus souvent.

Si Kaspersky Security découvre un fichier compacté plusieurs fois ou un fichier compacté à l'aide d'un compacteur spécial, 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.

Kaspersky Security définit les types de fichiers compactés de la manière suivante :

- *Fichiers compactés qui peuvent nuire* : le fichier a été compacté par un programme spécial qui sert à compacter des programmes malveillants (virus, vers, chevaux de Troie).

- *Fichiers compactés à plusieurs reprises* (niveau de danger moyen) : le fichier est compacté trois fois au moins par un ou plusieurs compacteurs.

Cette étape permet de définir les paramètres d'analyse des fichiers compactés sur les machines virtuelles :

- **Fichiers compactés qui peuvent nuire**.

  Exclusion ou inclusion de l'analyse des fichiers compactés à l'aide de compacteurs spéciaux qui servent à compacter des applications malveillantes (virus, vers, chevaux de Troie).

  Si la case est cochée, la protection contre les compacteurs que des individus malintentionnés peuvent utiliser pour nuire à la machine virtuelle ou aux données de l'utilisateur est activée et l'analyse des fichiers compactés par leur biais est autorisée.

  La case est cochée par défaut.

- **Fichiers compactés à plusieurs reprises**.

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

  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.

  La case est cochée par défaut.

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

ETAPE 5. 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 164).

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 6. 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 hôtes VMware ESXi conformément au profil de protection racine qui leur a été attribué.

Si aucune clé n'est ajoutée à la machine virtuelle de protection (cf. section "Activation de l'application" à la page 85) ou s'il manque des bases antivirus, l'application ne protège pas les machines virtuelles.

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*.

La fonction de protection des machines virtuelles s'active automatiquement lors du lancement de l'application si vous avez configuré les paramètres de Kaspersky Security à l'aide d'une stratégie (cf. section "Création d'une stratégie" à la page 99) et que vous avez activé l'application (cf. section "Activation de l'application" à la page 85).

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

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

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 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 150).

PROTECTION DU SYSTEME DE FICHIERS DES MACHINES VIRTUELLES. ANTIVIRUS 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 Antivirus Fichiers.

DANS CETTE SECTION

PROTECTION DES MACHINES VIRTUELLES

Cette section présente le mécanisme de protection des machines virtuelles par Kaspersky Security sur les hôtes 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

Une machine virtuelle de protection dotée du module Antivirus Fichiers protège le système de fichiers du système d'exploitation invité des machines virtuelles sur l'hôte 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 24).

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.

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 150).

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 suspendre temporairement la protection de ces machines virtuelles (cf. section "Désactivation de la protection sur la machine virtuelle" à la p. 111).

MODIFICATION DES PARAMETRES D'ANALYSE DES FICHIERS COMPACTES

Les paramètres d'analyse des fichiers compactés sont indiqués dans les paramètres de la stratégie lors de sa création (cf. section "Création d'une stratégie" à la page 99). Une fois la stratégie créée, vous pouvez modifier les paramètres d'analyse des fichiers compactés.

Pour modifier les paramètres d'analyse des fichiers compactés, 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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez la section **Détection de fichiers compactés**.
6. Dans la partie droite de la fenêtre, définissez les paramètres suivants :
   - **Fichiers compactés qui peuvent nuire**.

     Exclusion ou inclusion de l'analyse des fichiers compactés à l'aide de compacteurs spéciaux qui servent à compacter des applications malveillantes (virus, vers, chevaux de Troie).

     Si la case est cochée, la protection contre les compacteurs que des individus malintentionnés peuvent utiliser pour nuire à la machine virtuelle ou aux données de l'utilisateur est activée et l'analyse des fichiers compactés par leur biais est autorisée.

     La case est cochée par défaut.
   - **Fichiers compactés à plusieurs reprises**.

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

     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.

     La case est cochée par défaut.
7. Cliquez sur le bouton **OK**.

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez l'option **Infrastructure protégée** dans la liste de gauche.
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 VMware vCenter Server :
   - **Adresse de VMware vCenter Server**.

     Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.
   - **Nom de l'utilisateur**.

     Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.
8. Si nécessaire, définissez la valeur du paramètre **Enregistrer les paramètres de connexion**.

   Activation ou désactivation de l'enregistrement des paramètres de connexion à VMware vCenter Server.

   Si la case est cochée, Kaspersky Security enregistre les derniers paramètres saisis pour la connexion à VMware vCenter Server indiqué dans le champ **Adresse de VMware vCenter Server** : adresse de VMware vCenter Server, nom et mot de passe du compte utilisateur. Lors des connexions ultérieures à VMware vCenter Server, les paramètres enregistrés seront affichés 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 du Kaspersky Security Center.

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

   Si vous décochez cette case, les paramètres de connexion à VMware vCenter Server précédemment enregistrés sont supprimés par Kaspersky Security.

   La case est décochée par défaut.

9. Cliquez sur le bouton **OK**.

   Kaspersky Security Center établit la connexion à VMware vCenter Server. Si la connexion n'est pas établie, vérifiez que le VMware vCenter Serveur est accessible via le réseau et retentez la connexion.

   Dans la partie droite de la fenêtre, l'infrastructure protégée du cluster KSC s'affiche : VMware vCenter Server, objets Datacenter, clusters VMware, hôtes 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'hôtes 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 110).
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)*.

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

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez 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 protection**, 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 protection** :

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 analysé**.

  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 :

- **Niveau d'analyse heuristique**.

  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*.

  Niveau d'analyse heuristique défini pour ce niveau de protection :

  - **Superficiel**. 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 spécification de l'analyse heuristique, la possibilité de détecter une menace est faible par rapport aux niveaux de spécification de l'analyse heuristique **Moyen** et **Minutieux**. L'analyse requiert moins de ressources de la machine virtuelle et s'exécute plus rapidement.

- **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.

- **Minutieux**. Pendant la recherche du code malveillant dans les fichiers, l'analyseur heuristique exécute dans les fichiers exécutables un nombre d'instructions qui dépasse le nombre d'instructions pour des niveaux d'analyse heuristique **Superficiel** et **Moyen**. A ce niveau d'analyse heuristique, la possibilité de détecter une menace est plus importante qu'aux niveaux **Superficiel** et **Moyen**. L'analyse requiert plus de ressources de la machine virtuelle de protection et prend plus de temps.

Par défaut, la valeur **Moyen** est attribuée aux profils de protection, et **Minutieux** aux tâches d'analyse.

- **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 analyser**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à analyser** qui apparaît :

- **Utilitaires malveillants**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation de la protection contre les programmes numéroteurs.

  Les *programmes numéroteurs* peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.

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

  La case est cochée par défaut.

- **Autres**.

  Activation 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 d'autres applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  La case est décochée 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 analyser**.

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

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 protection** sera remplacé par **Utilisateur**.

9. Dans le groupe **Action à réaliser suite à la 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 n'importe quel fichier des machines virtuelles de protection, cliquez sur le bouton **Configuration** dans le groupe **Exclusions de l'analyse**.

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

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

- **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.

- **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.

b. Dans le tableau **Dossiers**, saisissez la liste des extensions de fichiers à ne pas analyser dans le cadre de la protection de la machine virtuelle. Pour chaque dossier, vous pouvez indiquer s'il est nécessaire d'exclure les sous-dossiers de la protection.

11. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de l'analyse**.

12. 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 117).

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :

   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.

   - En double-cliquant.

   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. 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 dans la liste de gauche 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 100).

     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** dans la liste de gauche.

        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 112).

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. 26). 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 110).

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la fenêtre **Propriétés: <Nom de la stratégie>**, sélectionnez la section **Profils de protection** dans la liste de gauche.

   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 l'analyse par Kaspersky Security des fichiers des machines virtuelles sur les hôtes VMware ESXi et explique comme configurer les paramètres de l'analyse.

DANS CETTE SECTION

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.

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.

Les paramètres d'analyse des fichiers compactés sont définis dans les paramètres de la stratégie (cf. section "Modification des paramètres d'analyse des fichiers compactés" à la page 109).

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 dans 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'hôte 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.
- Le système d'exploitation hôte installé sur la machine virtuelle ne correspond pas aux configurations requises de Kaspersky Security.
- Le pilote 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 est affichée sous l'onglet **Tâches** de la zone de travail du dossier portant le nom du cluster KSC contenant les machines virtuelles pour lesquelles vous avez lancé la tâche d'analyse (cf. documentation du Kaspersky Security Center).

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 150).

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 VMware vCenter Server, 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. 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 protection**, 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 protection** :

   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 analysé**.

  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 :

- **Niveau d'analyse heuristique**.

  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*.

  Niveau d'analyse heuristique défini pour ce niveau de protection :

  - **Superficiel**. 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 spécification de l'analyse heuristique, la possibilité de détecter une menace est faible par rapport aux niveaux de spécification de l'analyse heuristique **Moyen** et **Minutieux**. L'analyse requiert moins de ressources de la machine virtuelle et s'exécute plus rapidement.

  - **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.

  - **Minutieux**. Pendant la recherche du code malveillant dans les fichiers, l'analyseur heuristique exécute dans les fichiers exécutables un nombre d'instructions qui dépasse le nombre d'instructions pour des niveaux d'analyse heuristique **Superficiel** et **Moyen**. A ce niveau d'analyse heuristique, la possibilité de détecter une menace est plus importante qu'aux niveaux **Superficiel** et **Moyen**. L'analyse requiert plus de ressources de la machine virtuelle de protection et prend plus de temps.

  Par défaut, la valeur **Moyen** est attribuée aux profils de protection, et **Minutieux** aux tâches d'analyse.

- **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 analyser**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à analyser** qui apparaît :

- **Utilitaires malveillants**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation de la protection contre les programmes numéroteurs.

  Les *programmes numéroteurs* peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.

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

  La case est cochée par défaut.

- **Autres**.

  Activation 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 d'autres applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

La case est décochée 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 analyser**.

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

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 protection** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action à réaliser suite à la 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 et les clés, cochez la case **Analyser les fichiers sur les disques amovibles et les clés (CD, DVD, Blu-Ray, USB)** dans le groupe **Disques amovibles et clés**.

Si la case **Analyser les fichiers sur les disques amovibles et les clés (CD, DVD, Blu-Ray, USB)** est cochée, mais qu'une zone d'analyse a été définie et que celle-ci ne contient pas le chemin d'accès à un disque amovible ou à une clé, Kaspersky Security n'analyse pas ce disque amovible ou cette clé.

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, sauf ceux indiqués**. Les boutons **Ajouter**, **Modifier** et **Supprimer** permettent de composer la liste des dossiers de la machine virtuelle à exclure de l'analyse pendant l'exécution de la tâche. Dans le groupe **Extensions des fichiers**, indiquez les extensions de fichiers que vous souhaitez inclure dans l'analyse ou en exclure.

  Les dossiers exclus de l'analyse présentent une priorité supérieure à celle des extensions de fichiers à analyser. Autrement dit, un fichier figurant dans un dossier exclu de l'analyse 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 le temps de retard maximal de 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 10000 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 le temps de retard maximal de 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 le temps de retard maximal de 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 132).

CREATION D'UNE TACHE D'ANALYSE PERSONNALISEE

En cas de remplacement ou de réinstallation de la plateforme VMware vCenter Server, les tâches d'analyse personnalisée créées antérieurement ne fonctionneront plus. 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. 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 A VMWARE VCENTER SERVER

A cette étape, définissez les paramètres de connexion de Kaspersky Security à VMware vCenter Server.

- **Adresse de VMware vCenter Server**.

  Adresse IP au format IPv4 ou nom de domaine complet de VMware vCenter Server auquel la connexion s'opère.

- **Nom de l'utilisateur**.

  Nom du compte utilisateur sous lequel la connexion à VMware vCenter Server s'opère. 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 s'opère la connexion à VMware vCenter Server.

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

Activation ou désactivation de l'enregistrement des paramètres de connexion à VMware vCenter Server.

Si la case est cochée, Kaspersky Security enregistre les derniers paramètres saisis pour la connexion à VMware vCenter Server indiqué dans le champ **Adresse de VMware vCenter Server** : adresse de VMware vCenter Server, nom et mot de passe du compte utilisateur. Lors des connexions ultérieures à VMware vCenter Server, les paramètres enregistrés seront affichés 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 du Kaspersky Security Center.

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

Si vous décochez cette case, les paramètres de connexion à VMware vCenter Server 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 à VMware vCenter Server 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. Si le compte possède plus de privilèges qu'il n'en faut, l'Assistant de création de la tâche le signalera à l'étape suivante (cf. section "Comptes de VMware vCenter Server" à la page 31).

L'Assistant de création de la tâche établira la connexion à VMware vCenter Server.

Si la connexion n'a pas été établie, quittez l'Assistant de création de tâche d'analyse personnalisée, vérifiez que le VMware vCenter Server 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 d'une plateforme VMware vCenter Server s'affiche dans le tableau sous la forme d'une arborescence d'objets : serveur VMware vCenter Server, objets Datacenter, clusters VMware, hôtes 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 protection**, 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 protection** :

   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 analysé**.

  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 :

- **Niveau d'analyse heuristique**.

  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*.

  Niveau d'analyse heuristique défini pour ce niveau de protection :

  - **Superficiel**. 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 spécification de l'analyse heuristique, la possibilité de détecter une menace est faible par rapport aux niveaux de spécification de l'analyse heuristique **Moyen** et **Minutieux**. L'analyse requiert moins de ressources de la machine virtuelle et s'exécute plus rapidement.

  - **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.

- **Minutieux**. Pendant la recherche du code malveillant dans les fichiers, l'analyseur heuristique exécute dans les fichiers exécutables un nombre d'instructions qui dépasse le nombre d'instructions pour des niveaux d'analyse heuristique **Superficiel** et **Moyen**. A ce niveau d'analyse heuristique, la possibilité de détecter une menace est plus importante qu'aux niveaux **Superficiel** et **Moyen**. L'analyse requiert plus de ressources de la machine virtuelle de protection et prend plus de temps.

Par défaut, la valeur **Moyen** est attribuée aux profils de protection, et **Minutieux** aux tâches d'analyse.

- **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 analyser**, cliquez sur le bouton **Configuration** et définissez les paramètres suivants dans la fenêtre **Objets à analyser** qui apparaît :

- **Utilitaires malveillants**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation 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.

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation de la protection contre les programmes numéroteurs.

  Les *programmes numéroteurs* peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.

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

  La case est cochée par défaut.

- **Autres**.

  Activation 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 d'autres applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur est activée.

  La case est décochée 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 analyser**.

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

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 protection** sera remplacé par **Utilisateur**.

2. Dans le groupe **Action à réaliser suite à la 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 et les clés, cochez la case **Analyser les fichiers sur les disques amovibles et les clés (CD, DVD, Blu-Ray, USB)** dans le groupe **Disques amovibles et clés**.

Si la case **Analyser les fichiers sur les disques amovibles et les clés (CD, DVD, Blu-Ray, USB)** est cochée, mais qu'une zone d'analyse a été définie et que celle-ci ne contient pas le chemin d'accès à un disque amovible ou à une clé, Kaspersky Security n'analyse pas ce disque amovible ou cette clé.

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, sauf ceux indiqués**. Les boutons **Ajouter**, **Modifier** et **Supprimer** permettent de composer la liste des dossiers de la machine virtuelle à exclure de l'analyse pendant l'exécution de la tâche. Dans le groupe **Extensions des fichiers**, indiquez les extensions de fichiers que vous souhaitez inclure dans l'analyse ou en exclure.

  Les dossiers exclus de l'analyse présentent une priorité supérieure à celle des extensions de fichiers à analyser. Autrement dit, un fichier figurant dans un dossier exclu de l'analyse 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 le temps de retard maximal de 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 10000 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 le temps de retard maximal de 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 le temps de retard maximal de 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 132).

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 la tâche 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 :
   - Sélectionnez le dossier **Ordinateurs administrés** de l'arborescence de la console si vous souhaitez lancer ou arrêter une analyse complète des machines virtuelles de protection de tous les clusters KSC.
   - 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 lancer ou arrêter l'analyse complète ou personnalisée.
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. Si vous souhaitez lancer une tâche, exécutez l'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**.
6. Si vous souhaitez arrêter une tâche, exécutez l'une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Arrêter**.
   - Cliquez sur le bouton **Arrêter**. Le bouton se trouve à droite de la liste des tâches dans le groupe **Exécution de la tâche**.

PROTECTION DES MACHINES VIRTUELLES CONTRE LES MENACES RESEAU. DETECTION DES MENACES RESEAU

Cette section contient des informations sur la configuration des paramètres du module de détection des menaces réseau.

Dans cette section, l'expression machine virtuelle de protection désigne la machine virtuelle de protection dotée du module Détection des menaces réseau.

DANS CETTE SECTION

CONCERNANT LA PROTECTION DES MACHINES VIRTUELLES CONTRE LES MENACES RESEAU

Le module Détection des menaces réseau 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 URL sollicitée par l'utilisateur à une base d'adresses URL malveillantes.

Une machine virtuelle de protection dotée du module Détection des menaces réseau, installée sur un hôte VMware ESXi, protège toutes les machines virtuelles présentes sur cet hôte VMware ESXi contre les menaces réseau.

Si vous souhaitez protéger les machines virtuelles des menaces réseau : après l'installation du module Détection des menaces réseau, il convient d'activer la détection des attaques réseau (cf. section "Activation et désactivation de la détection des attaques réseau" page135) et l'analyse des adresses URL(cf. section "Activation et désactivation de l'analyse des adresses URL" page 137) dans les paramètres de la stratégie. Par défaut, Kaspersky Security ne détecte pas les attaques réseau et n'analyse pas les adresses URL.

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 136).

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 URL est activée, Kaspersky Security confronte chaque adresse URL sollicitée par l'utilisateur ou certaines applications HTTP à une base d'adresses URL malveillantes :

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

- Si une adresse URL figure dans la base des adresses URL malveillantes, l'application effectue l'action définie dans les paramètres Kaspersky Security (cf. section "Configuration des paramètres de l'analyse des adresses URL" à la page 137). Par exemple, elle bloque ou autorise l'accès à cette adresse URL.

Vous pouvez composer une liste des adresses URL auxquelles l'accès ne doit pas être bloqué par Kaspersky Security si elles apparaissent dans la base des adresses URL 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 150).

Les descriptions des types connus d'attaques réseau, les méthodes de lutte contre ces attaques et la base des adresses URL malveillantes figurent dans les bases antivirus. La liste des attaques réseau détectées par le module Détection des menaces réseau et la base des adresses URL 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" page 144).

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :

   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.

   - En double-cliquant.

   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. Dans la liste de gauche, choisissez 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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez 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 URL

Pour activer ou désactiver la fonction d'analyse des adresses URL, 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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez la section **Analyse des adresses URL**.
6. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'analyse des adresses URL**, si vous souhaitez que Kaspersky Security confronte une adresse URL à la base des adresses URL malveillantes.
   - Décochez la case **Activer l'analyse des adresses URL**, si vous ne souhaitez pas que Kaspersky Security confronte une adresse URL à la base des adresses URL malveillantes.
7. Cliquez sur le bouton **OK**.

CONFIGURATION DES PARAMETRES DE L'ANALYSE DES ADRESSES URL

Si l'analyse des adresses URL est activée et qu'une adresse URL ou une application sollicitée par l'utilisateur est détectée dans la base des adresses URL malveillantes, Kaspersky Security bloque par défaut l'accès à cette adresse URL. Vous pouvez modifier l'action par défaut ou composer une liste des adresses URL auxquelles l'accès ne sera pas bloqué par Kaspersky Security si elles apparaissent dans la base des adresses URL malveillantes.

Pour modifier les paramètres d'analyse des adresses URL, 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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.

- En double-cliquant.
- Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. Dans la liste de gauche, choisissez la section **Analyse des adresses URL**.
6. Dans le groupe **Action à réaliser suite à la détection d'une menace**, sélectionnez les actions que Kaspersky Security doit exécuter en cas de détection d'une adresse URL dans la base des adresses URL malveillantes :
   - **Sélectionner l'action automatiquement**.

     En cas de détection d'une adresse URL dans la base des adresses URL malveillantes, Kaspersky Security exécute l'action par défaut définie par les spécialistes de Kaspersky Lab. Il s'agit de **Bloquer**.

     Cette option est sélectionnée par défaut.
   - **Bloquer**.

     Kaspersky Security bloque l'accès à l'adresse URL apparaissant dans la base des adresses URL malveillantes.
   - **Ignorer**.

     Kaspersky Security autorise l'accès à l'adresse URL apparaissant dans la base des adresses URL malveillantes.
7. Dans le tableau **Ne pas bloquer les adresses URL suivantes** indiquez les adresses URL auxquelles l'accès ne doit pas être bloqué si ces dernières apparaissent dans la base des adresses URL malveillantes. Pour ajouter une adresse URL au tableau, procédez comme suit :
   a. Cliquez sur le bouton **Ajouter** ou pressez la touche **INSERT**.
   b. Entrez l'adresse URL dans la colonne **Adresse URL**.
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 Antivirus Fichiers.

DANS CETTE SECTION

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 une copie de 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.

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 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 140).

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez la section **Sauvegarde**.
6. Dans la partie droite de la fenêtre, définissez les paramètres suivants :
   - **Placer les objets 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

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, utilisez les touches **SHIFT** et **CTRL** pour sélectionner les fichiers que vous souhaitez enregistrer sur le disque.
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 à l'aide des touches **SHIFT** et **CTRL**.

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 **Mettre à jour**, vous pouvez mettre à jour la liste des copies de sauvegarde des fichiers pour voir les modifications dans la liste.

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

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 antivirus 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 antivirus 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 antivirus (cf. section "Création de la tâche de diffusion des mises à jour" à la page 145).

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 antivirus.

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. 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 le temps de retard maximal de 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 10000 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 le temps de retard maximal de 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 le temps de retard maximal de 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.

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 147).

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 149).

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 qui comprend les machines virtuelles de protection que vous souhaitez remettre à l'état antérieur à dernières 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. 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 dernière 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 le temps de retard maximal de 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 10000 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 le temps de retard maximal de 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 le temps de retard maximal de 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 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 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.

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 95).
- **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 URL malveillantes consignées par le module Détection des menaces réseau 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 d'administration de VMware vCenter Server.

DANS CETTE SECTION

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 de protection qui a détecté le virus ou un autre programme dangereux 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 comportant un virus ou une autre application présentant une menace.
- **Nom NetBIOS** : nom de la machine virtuelle de protection comportant un virus ou une autre application présentant une menace.
- **Nom de domaine** : nom de la machine virtuelle de protection comportant un virus ou une autre application présentant une menace.
- **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).

  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 depuis lesquelles la machine virtuelle de protection qui a détecté l'objet 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 l'objet.
- **Nom NetBIOS** : nom de la machine virtuelle de protection ayant détecté l'objet.
- **Nom de domaine** : nom de la machine virtuelle de protection ayant détecté l'objet.
- **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 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 depuis lesquelles la machine virtuelle de protection qui a détecté l'objet 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 l'objet.
- **Nom NetBIOS** : nom de la machine virtuelle de protection ayant détecté l'objet.
- **Nom de domaine** : nom de la machine virtuelle de protection ayant détecté l'objet.
- **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 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 antivirus 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 attaques réseau de Kaspersky Security.

RAPPORT SUR LE FONCTIONNEMENT DU CONTROLE WEB

Le rapport sur le fonctionnement du contrôle Web contient des renseignements sur les connexions des utilisateurs ou des applications installées sur les machines virtuelles de protection à des adresses URL malveillantes reprises dans la base des URL 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 URL malveillante.
- **Règle** : règle réseau régissant l'action de l'application lors de la détection d'une tentative de connexion à une adresse URL malveillante. Pour Kaspersky Security, ce champ indique : *KSV : n'importe quelle activité réseau via le protocole HTTP*.
- **Tentatives** : nombre de tentatives de connexion à une adresse URL malveillante.
- **Comptes utilisateurs** : nombre de machines virtuelles à partir desquelles les tentatives de connexion à l'adresse URL malveillante ont été lancées.
- **URL** – adresse URL reprise dans la base des URL malveillantes.
- **Postes** : nombre de machines virtuelles de protection ayant détecté les tentatives de connexion à l'adresse URL 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 URL malveillante.
- **Dernière tentative** : date et heure de la dernière tentative de connexion à l'adresse URL 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 URL malveillante. Pour Kaspersky Security ce champ indique : *1*.
  - **Blocages** : nombre de connexions aux adresses URL malveillantes ayant été bloquées par Kaspersky Security.
  - **Avertissements** : nombre de connexions aux adresses URL malveillantes ayant été autorisées conformément aux paramètres de l'application.
  - **URL bloquées** : nombre d'adresses URL malveillantes ayant été bloquées par Kaspersky Security.
  - **Avertissements sur les URL** : nombre d'adresses URL 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 URL bloquées ont été lancées.
  - **Avertissements sur les utilisateurs** : nombre de machines virtuelles ayant été autorisées par Kaspersky Security à accéder aux adresses URL malveillantes, conformément aux paramètres de l'application.
  - **Premier blocage** : date et heure du premier blocage de la tentative de connexion à l'adresse URL malveillante.
  - **Dernier blocage** : date et heure du dernier blocage de la tentative de connexion à l'adresse URL malveillante.

- **Premier avertissement** : date et heure de la première connexion à l'adresse URL malveillante ayant été autorisée conformément aux paramètres de l'application.
- **Dernier avertissement** : date et heure de la dernière connexion à l'adresse URL 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 URL malveillante.
- **Règle** : règle réseau régissant l'action de l'application lors de la détection d'une tentative de connexion à une adresse URL malveillante. Pour Kaspersky Security, ce champ indique : *KSV : n'importe quelle 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 URL malveillante ont été lancées.
- **URL** : adresse URL reprise dans la base des URL malveillantes.
- **Circonstances** : date et heure de la détection de la tentative de connexion à l'adresse URL malveillante.
- **Groupe** : cluster KSC auquel appartient la machine virtuelle de protection ayant détecté la tentative de connexion à une adresse URL malveillante.
- **Poste client** : nom de la machine virtuelle de protection ayant détecté la tentative de connexion à l'adresse URL malveillante.
- **Application** : nom de l'application ayant détecté la tentative de connexion à l'adresse URL malveillante.
- **Numéro de version** : numéro de la version du module Détection des attaques réseau 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 URL 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 URL 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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.
5. Dans la liste de gauche, choisissez la section **Evénements**.
6. Dans la liste déroulante, sélectionnez le niveau d'importance des événements pour lesquels vous souhaitez être prévenu :
   - **Evénements critiques**.
   - **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.

    - **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**.

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

CONCERNANT 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 165).

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 :

- les informations sur les sommes de contrôle des fichiers traités (MD5) ;
- l'identifiant unique de l'installation de l'application ;
- le numéro de version de l'application ;
- le type d'application.

Les informations transmises à Kaspersky Lab par l'application Kaspersky Security sont uniquement utilisées pour évaluer la réputation des fichiers traités et ne sont pas conservées par Kaspersky Lab.

Kaspersky Lab protège les informations reçues conformément aux exigences réglementaires.

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 des stratégies, sélectionnez une stratégie et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** de l'une des manières suivantes :
   - Cliquez sur le lien **Modifier les paramètres de la stratégie**. Le lien **Modifier les paramètres de la stratégie** se trouve à droite de la liste de stratégies dans le groupe contenant les paramètres de la stratégie.
   - En double-cliquant.
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Choisissez l'option **Propriétés**.

5. Dans la liste de gauche, choisissez 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 présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Support Technique.

DANS CETTE SECTION

MODES D'OBTENTION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans l'une des sources d'informations relatives à l'application (cf. section "Sources d'informations sur l'application "à la page 13), 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.

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 :

- Par téléphone (cf. section "Assistance technique par téléphone" à la page 167). Vous pouvez contacter les experts du Support Technique en France.
- Envoyer une demande via le service Web Kaspersky CompanyAccount sur le site Internet du Support Technique (cf. section "Obtention du support technique via Kaspersky CompanyAccount" à la page 168).

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.

SUPPORT TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique français (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). Ceci permettra à nos experts à vous venir en aide le plus vite possible.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount est un service Web (https://companyaccount.kaspersky.com) conçu pour l'envoi de demandes électroniques à Kaspersky Lab et le suivi de leur traitement par les spécialistes.

Une connexion Internet est nécessaire pour utiliser Kaspersky CompanyAccount.

Pour accéder à Kaspersky CompanyAccount, il vous est demandé de vous inscrire (https://support.kaspersky.com/companyaccount/register?LANG=fr). Vous pouvez vous inscrire seul ou par l'intermédiaire d'un utilisateur disposant des droits d'administrateur sur le compte utilisateur de votre entreprise dans Kaspersky CompanyAccount.

Dans Kaspersky CompanyAccount, le compte utilisateur de votre entreprise est créé dès le premier enregistrement de la licence Kaspersky CompanyAccount de Kaspersky Security acquise par votre société. Tous les employés enregistrés dans Kaspersky CompanyAccount sont associés à ce compte utilisateur.

Si un nouveau compte utilisateur est créé pour votre entreprise lors de l'inscription à Kaspersky CompanyAccount, les privilèges concernant son administration vous sont attribués par défaut. Il s'agit des privilèges couvrant l'ensemble des actions possibles avec ce compte utilisateur. Si, lors de l'inscription, vous vous ajoutez à un compte utilisateur existant, des privilèges restreints vous sont attribués par défaut.

Pour en savoir plus sur Kaspersky CompanyAccount et les actions qu'il vous permet de réaliser, consultez la page du site Internet du Support Technique http://support.kaspersky.com/fr/faq/companyaccount_help.

Demande adressée par email au Support Technique

Kaspersky CompanyAccount vous permet de :

- envoyer des demandes au Support Technique ;
- échanger des messages avec le Support Technique ;
- suivre la progression du traitement des demandes et de consulter leur historique.

Un spécialiste du Support Technique vous répond via le système Kaspersky CompanyAccount à l'adresse électronique que vous avez indiquée lors de l'inscription.

Demande électronique adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer des demandes au Laboratoire d'étude des virus dans les cas suivants :

- Si vous soupçonnez un fichier ou une ressource Internet de contenir un virus ou une autre application présentant une menace mais que Kaspersky Security ne la détecte pas. Les spécialistes du Laboratoire d'étude des virus analysent le fichier ou la ressource Web envoyé et, s'ils détectent un virus ou une application auparavant inconnu et présentant une menace, ils en intègrent les informations dans la base de données. Cette base de données est accessible lors de la mise à jour des bases antivirus de l'application Kaspersky Lab.
- Si Kaspersky Security identifie un fichier ou une ressource Web comme porteur d'un virus ou d'une autre application présentant une menace mais que vous êtes sûr que ce n'est pas le cas.

Vous pouvez également envoyer une demande au Laboratoire d'étude des virus depuis le formulaire de demande (https://my.kaspersky.com/fr/kpc/support/viruslab) sur le site Internet du Support Technique sans vous enregistrer dans Kaspersky CompanyAccount. Les demandes formulées via Kaspersky CompanyAccount sont traitées prioritairement par rapport aux demandes transmises via le formulaire de demande.

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 de la plateforme VMware vCenter Server ;
- 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 le système Kaspersky Security Center est installé : la version du système d'exploitation et la version de Microsoft .NET Framework.

Le rapport obtenu doit ensuite être envoyé au Support technique.

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/legacy/fr/find?faq_id=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/legacy/fr/find?faq_id=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 hôtes VMware ESXi sous l'administration d'une plateforme VMware vCenter Server 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 prévue pour l'utilisation de l'application en vue de protéger les 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 hôtes 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 prévue pour l'utilisation de l'application en vue de protéger les machines virtuelles dotées d'un système d'exploitation pour postes de travail.

CLE POUR SERVEUR

Clé prévue pour l'utilisation de 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

Accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions selon lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

COPIE DE SAUVEGARDE DU FICHIER

Copie de fichier de la machine virtuelle 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

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 dans le cadre de la plateforme VMware vCenter Server 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 un hôte VMware ESXi où est installé un 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 attribué automatiquement à l'objet racine de la structure des objets d'administration VMware, à savoir le VMware vCenter Server.

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 protection des machines virtuelles et les paramètres d'analyse des fichiers compactés.

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 hôtes VMware ESXi dans le cadre d'une plateforme VMware vCenter Server.

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, LTD

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), Critical Path (Irlande), D-Link (Taïwan), M86 Security (E-U), GFI (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), NETASQ (France), NETGEAR (E-U), Parallels (Russie), 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 :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets potentiellement infectés sous forme d'archive)
	https://my.kaspersky.com/fr/kpc/support/viruslab
	(pour les questions aux experts de la lutte contre les virus)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

AVIS DE MARQUES 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, vShield Endpoint, 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

R

S

T