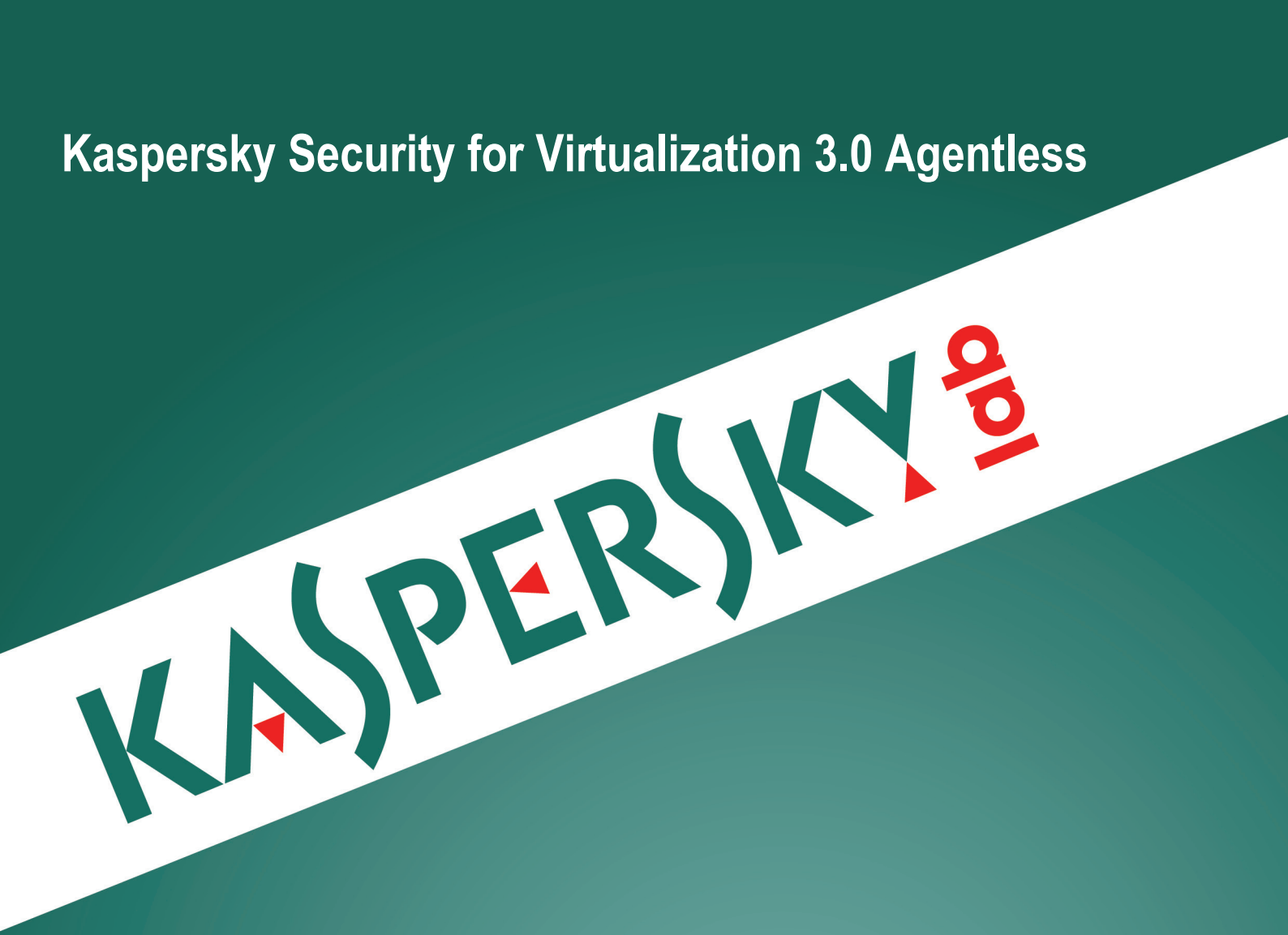
Kaspersky Security for Virtualization 3.0 Agentless



Manuel d'implantation

VERSION DE L'APPLICATION : 3.0 SERVICE PACK 1

Cher utilisateur,

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

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

Date d'édition : 21/05/2015

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

TABLE DES MATIERES

PRESENTATION DU MANUEL

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

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

- planification de l'installation de Kaspersky Security dans le réseau de l'organisation (en tenant compte des principes de fonctionnement de Kaspersky Security, de la configuration requise, des particularités de l'intégration de Kaspersky Security aux autres applications) ;
- préparation de l'installation, installation et activation de Kaspersky Security ;
- configuration de Kaspersky Security après l'installation ;
- mise à jour et suppression de Kaspersky Security.

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

DANS CETTE SECTION

DANS CE DOCUMENT

Ce manuel contient les sections suivantes :

Sources d'informations sur l'application (cf. page 10)

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 12)

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

Configuration logicielle et matérielle (cf. page 15)

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

Architecture de l'application (cf. page 18)

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™.

Information sur le code tiers (cf. page 118)

Cette section contient des informations sur le code tiers.

Notifications sur les marques de commerce (cf. page 119)

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

Index

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

CONVENTIONS

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

Tableau 1. Conventions

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

SOURCES D'INFORMATIONS SUR L'APPLICATION

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

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

DANS CETTE SECTION

SOURCES POUR DES CONSULTATIONS INDEPENDANTES

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

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

Si vous ne trouvez pas la réponse à votre question, il est recommandé de contacter le Support Technique de Kaspersky Lab.

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

Page de Kaspersky Security sur le site de Kaspersky Lab

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

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

Page de Kaspersky Security dans la base de connaissances

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

La page de Kaspersky Security dans la Base des connaissances (http://support.kaspersky.com/fr/ksv3nola) permet de trouver les articles qui proposent des informations utiles, des recommandations et une foire aux questions sur l'achat, l'installation et l'utilisation de l'application.

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

Aide électronique

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

Documentation

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

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications sur notre forum (http://forum.kaspersky.fr).

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

KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS

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

Kaspersky Security protège les machines virtuelles avec les systèmes d'exploitation invités Windows®, notamment les systèmes d'exploitation pour serveurs.

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

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

Kaspersky Security comprend les modules suivants :

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

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

Kaspersky Security offre les possibilités suivantes :

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

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

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

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

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

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

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

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

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

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

Le Kaspersky Security Center permet de réaliser les opérations suivantes :

- installer l'application dans l'infrastructure virtuelle VMware ;
- configurer les paramètres de fonctionnement de l'application ;
- administrer le fonctionnement de l'application ;
  - administrer la protection des machines virtuelles ;
  - administrer avec les tâches d'analyse ;
  - administrer les clés de l'application ;
- mettre à jour les bases anti-virus de l'application ;
- utiliser les copies de sauvegarde des fichiers dans la sauvegarde ;
- créer des rapports sur les événements survenus pendant le fonctionnement de l'application ;
- supprimer l'application de l'infrastructure virtuelle VMware.

DANS CETTE SECTION

NOUVEAUTES

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

- Ajout de la compatibilité avec les composants de VMware vSphere 6.0.
- Nouveau module de l'application Kaspersky Security : Serveur d'intégration. Ce module est destiné aux infrastructures virtuelles comportant de nombreuses machines virtuelles de protection et vise à alléger la charge pesant sur le serveur VMware vCenter. Le serveur d'intégration se connecte au serveur VMware vCenter, obtient des informations sur l'infrastructure virtuelle VMware et transmet ces informations aux machines virtuelles de protection dès qu'elles en ont besoin. Cette opération permet de diminuer le nombre de requêtes que les machines virtuelles de protection envoient au serveur VMware vCenter.
- Possibilité d'utiliser l'application par abonnement. L'application peut être activée à l'aide du code d'activation fourni sur abonnement.

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

DISTRIBUTION

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

La distribution contient les éléments suivants :

- les fichiers de l'application ;
- les fichiers de documentation sur l'application ;
- Le Contrat de licence utilisateur final reprenant les conditions d'utilisation de l'application.

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

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

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

CONFIGURATIONS LOGICIELLE ET MATERIELLE

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

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

Configuration requise pour le composant Anti-Virus Fichiers

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

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

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

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

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

Configuration requise pour le module Détection des intrusions

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

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

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

Configuration requise pour le module Serveur d'intégration

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

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

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

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

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

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

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

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

Configuration matérielle requise

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

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

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

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

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

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

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

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

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

ARCHITECTURE DE L'APPLICATION

Cette section décrit les modules de Kaspersky Security leur interaction.

DANS CETTE SECTION

PRESENTATION DE L'ARCHITECTURE DE L'APPLICATION

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

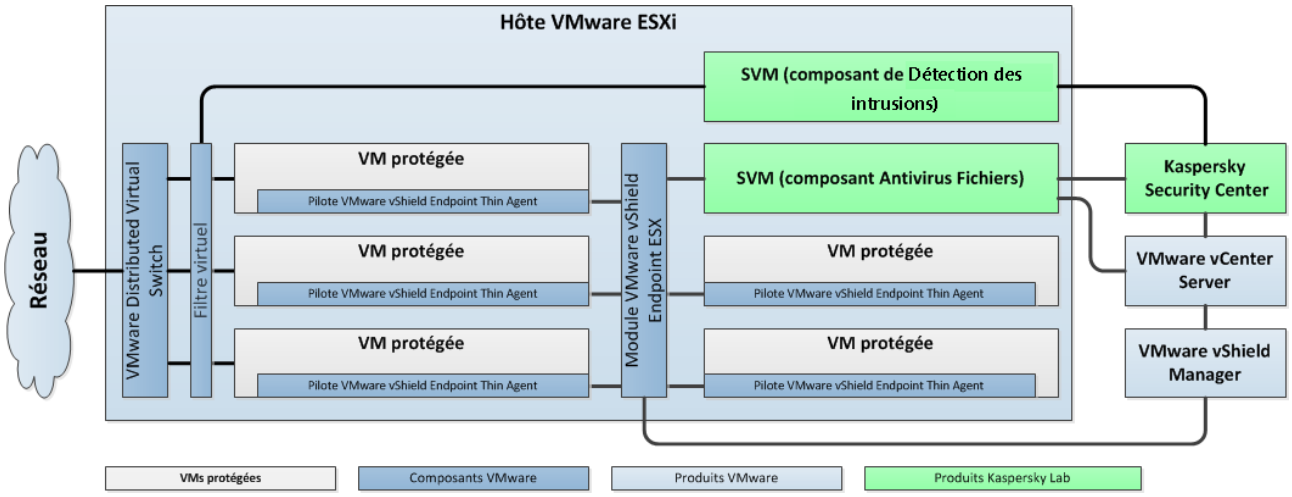


Illustration 1. Architecture de l'application

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

Kaspersky Security se présente sous la forme de deux images de machines virtuelles de protection (voir la section "Composition des images des machines virtuelles de protection Kaspersky Security" page 19) :

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

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

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

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

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

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

L'interface d'administration de l'application Kaspersky Security via le Kaspersky Security Center est assurée par le plug-in d'administration de Kaspersky Security. Le plug-in d'administration de Kaspersky Security fait partie de la distribution de Kaspersky Security. Le plug-in d'administration de Kaspersky Security doit être installé sur l'ordinateur comprenant le module Console d'administration du Kaspersky Security Center (cf. section "Installation des plug-ins d'administration Kaspersky Security" à la page 27).

COMPOSITION DES IMAGES DES MACHINES VIRTUELLES DE PROTECTION KASPERSKY SECURITY

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

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

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

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

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

Composants VMware

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

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

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

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

  Si un grand nombre de machines virtuelles échangent avec le serveur VMware vCenter, ce dernier peut subir une surcharge. Si votre infrastructure virtuelle comporte un grand nombre de machines virtuelles de protection, il est recommandé d'utiliser le module Serveur d'intégration de Kaspersky Security pour obtenir des informations relatives à l'infrastructure virtuelle VMware (cf. section "A propos du Serveur d'intégration" à la page 22).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    - Si les fichiers contiennent des virus ou autres programmes dangereux, Kaspersky Security exécute l'action définie dans les paramètres du profil de protection attribué à cette machine virtuelle. Par exemple, Kaspersky Security peut réparer ou bloquer le fichier.

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

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

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

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

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

        - En cas de détection d'une activité caractéristique des attaques réseau, Kaspersky Security exécute l'action définie dans les paramètres du profil de protection attribué à cette machine virtuelle. Par exemple, Kaspersky Security bloque ou ignore les paquets réseau dont l'adresse IP est à l'origine d'une attaque réseau.

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

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

        - S'il s'avère que l'adresse Internet figure dans la base des adresses Internet malveillantes, Kaspersky Security exécute l'action définie dans les paramètres du profil de protection attribué à cette machine virtuelle. Par exemple, Kaspersky Security bloque ou autorise l'accès à cette 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.

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

- Une *stratégie* définit les paramètres de la protection des machines virtuelles contre les virus et autres programmes dangereux, les paramètres de protection des machines virtuelles contre les intrusions et les paramètres des sauvegardes sur les machines virtuelles de protection.

- Les *tâches d'analyse* déterminent les paramètres d'analyse des machines virtuelles.

Les informations relatives à la configuration des tâches et des stratégies figurent dans le *Manuel de l'administrateur de Kaspersky Security for Virtualization 3.0 Agentless*.

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

A PROPOS DU SERVEUR D'INTEGRATION

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

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

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

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

Une fois que le Serveur d'intégration aura été installé et configuré (cf. section "Installation du Serveur d'intégration" à la page 28), vous devrez configurer la connexion des machines virtuelles de protection dotées de l'Anti-Virus Fichiers au Serveur d'intégration. Vous pouvez configurer la connexion lors de l'installation, de la mise à jour ou de la modification de la configuration des machines virtuelles de protection.

PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

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 23).
- S'assurer que la plateforme Microsoft .NET Framework 4.0 ou suivante est installée sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center. La plateforme Microsoft .NET Framework version 4.0 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 des comptes du serveur VMware vCenter requis pour l'installation et l'utilisation de l'application (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24).
- 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/fr/11050.

Si vous souhaitez installer le module Détection des intrusions, 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 hyperviseur VMware ESXi sur lequel sera installée 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.

Si vous souhaitez installer le module Serveur d'intégration, il est nécessaire d'autoriser les connexions via le port qui sera utilisé pour la connexion à ce serveur. Cette opération s'effectue dans les paramètres de la configuration réseau ou de l'application contrôlant le trafic. Le port utilisé par défaut est le port 7271.

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 ;
- la compatibilité des modules de 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 15).

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 Anti-Virus Fichiers :

- Serveur VMware vCenter.
- VMware vSphere Client.
- VMware vShield Endpoint. Le module est installé sur les hyperviseurs VMware ESXi et assure l'interaction entre le pilote VMware Guest Introspection Thin Agent (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 hyperviseurs VMware ESXi sur lesquels les machines virtuelles sont déployées.
- Pilote VMware Guest Introspection Thin Agent ou pilote VMware vShield Endpoint Thin Agent. Le pilote VMware Guest Introspection Thin Agent fait partie de la distribution VMware Tools livrée avec l'hyperviseur VMware ESXi 6.0 et l'hyperviseur VMware ESXi 5.5 patch 2d. Le pilote VMware vShield Endpoint Thin Agent fait partie de la distribution VMware Tools livrée avec l'hyperviseur VMware ESXi 5.1 patch 3. Le pilote doit être installé 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 Guest Introspection Thin Agent (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 intrusions :

- Serveur VMware vCenter.
- 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 intrusions (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 UTILISATEUR DU SERVEUR VMWARE VCENTER

L'utilisation de l'application requiert la présence des comptes utilisateur VMware vCenter 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 du serveur VMware vCenter.

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

INSTALLATION DE L'APPLICATION

Cette section fournit les informations suivantes :

- ordre des étapes d'installation de Kaspersky Security ;
- instructions pour l'installation des modules de Kaspersky Security ;
- informations sur les modifications dans le Kaspersky Security Center après l'installation de l'application.

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. Installation du plug-in d'administration de Kaspersky Security (cf. section "Installation du plug-in d'administration de Kaspersky Security" à la page 27).

2. Installation du module Serveur d'intégration (cf. section "Installation du serveur d'intégration" à la page 28). Vous pouvez ignorer cette étape si vous souhaitez que les machines virtuelles de protection reçoivent les informations relatives à l'infrastructure virtuelle directement du serveur VMware vCenter.

3. Installation du module Anti-Virus Fichiers (cf. section "Installation du module Anti-Virus Fichiers" à la page 32). L'installation du module Anti-Virus Fichiers se déroule via le déploiement des machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi.

4. Installation du module Détection des intrusions (cf. section "Installation du module Détection des intrusions" à la page 41). L'installation du module Détection des intrusions dans l'infrastructure virtuelle VMware se déroule via le déploiement des machines virtuelles de protection dotées du module Détection des intrusions sur les hyperviseurs VMware ESXi et via l'enregistrement du module Détection des intrusions dans VMware vShield Manager.

Une fois que l'application a été installée, il faut l'activer sur l'ensemble des machines virtuelles de protection (cf. section "Activation de l'application" à la page 47).

Une fois que l'application a été installée et activée, il faut préparer l'application en vue de son utilisation (cf. section "Préparation pour l'utilisation de l'application" à la page 53).

Une fois que le module Détection des intrusions a été installé, il faut activer la détection des attaques réseau et l'analyse des adresses Internet dans les paramètres de la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 3.0 Agentless*). Par défaut, Kaspersky Security ne détecte pas les intrusions et n'analyse pas les adresses Internet.

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.

DANS CETTE SECTION

PROCEDURE D'INSTALLATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY SECURITY

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 le paquet d'installation de Kaspersky Security sur l'ordinateur où est installée la Console d'administration.

2. Exécutez le fichier d'installation du plug-in d'administration de Kaspersky Security.

   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.

Après l'installation, le plug-in d'administration de Kaspersky Security apparaît dans la liste des plug-ins d'administrations dans les propriétés du Serveur d'administration (cf. section "Consultation de la liste des plug-ins d'administration installés" à la page 27).

CONSULTATION DE LA LISTE DES PLUG-INS D'ADMINISTRATION INSTALLES

Pour consulter la liste des plug-ins d'administration installés, procédez comme suit :

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

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

3. Ouvrez la fenêtre **Propriétés: Serveur d'administration** via le lien **Propriétés du serveur d'administration** dans la zone de travail de la section **Serveur d'administration**.

4. Dans la section **Avancés** de la fenêtre des propriétés du Serveur d'administration, sélectionnez la rubrique **Informations sur les plug-ins d'administration des applications installés**.

   La liste des plug-ins d'administration installés qui apparaît dans la partie droite de la fenêtre reprend le plug-in d'administration de Kaspersky Security for Virtualization 3.0 Agentless.

INSTALLATION DU SERVEUR D'INTEGRATION

Avant de commencer l'installation du Serveur d'intégration, il est nécessaire d'autoriser les connexions via le port qui sera utilisé pour la connexion à ce serveur. Cette opération s'effectue dans les paramètres de la configuration réseau ou de l'application contrôlant le trafic. Le port utilisé par défaut est le port 7271.

Pour installer le module Serveur d'intégration de Kaspersky Security et le préparer à son utilisation, procédez comme suit :

1. Installez le Serveur d'intégration et la Console de gestion du Serveur d'intégration sur n'importe quel ordinateur du réseau local de l'organisation. L'installation est exécutée à l'aide d'un Assistant d'installation (cf. section "Procédure d'installation du Serveur d'intégration et de la Console de gestion" à la page 28). Lors de l'installation du Serveur d'intégration, vous pouvez installer la Console de gestion sur le même ordinateur que le Serveur d'intégration ou refuser son installer et l'installer plus tard séparément (cf. section "Installation de la console de gestion" à la page 31).

2. Configurez les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter (cf. section "Configuration initiale du serveur d'intégration" à la page 32). La configuration des paramètres de connexion s'opère dans la Console de gestion du Serveur d'intégration.

3. Configurez pour chaque machine virtuelle de protection dotée du module Anti-Virus Fichiers la connexion au Serveur d'intégration qui garantira l'interaction entre le serveur VMware vCenter et les machines virtuelles de protection. Vous pouvez configurer la connexion des machines virtuelles de protection au Serveur d'intégration pendant l'installation, pendant la mise à jour ou pendant la modification de la configuration des machines virtuelles de protection.

DANS CETTE SECTION

PROCEDURE D'INSTALLATION DU SERVEUR D'INTEGRATION ET DE LA CONSOLE DE GESTION

Avant de lancer l'installation du Serveur d'intégration, assurez-vous que la configuration logicielle de l'ordinateur répond à la configuration requise pour le Serveur d'intégration (cf. section "Configurations logicielles et matérielles requises" à la page 15).

Pour installer le Serveur d'intégration sur l'ordinateur, procédez comme suit :

1. Sur l'ordinateur, copiez le fichier d'installation KsvServerService.msi du Serveur d'intégration depuis la distribution de Kaspersky Security.

2. Exécutez le fichier d'installation du Serveur d'intégration.

   L'installation s'opère via l'Assistant d'installation.

   L'Assistant vérifie si la plateforme Microsoft .NET Framework 4.0 ou suivant est installée sur l'ordinateur. Si ce n'est pas le cas, l'Assistant vous le signale et s'arrête. Dans ce cas, installez la plateforme Microsoft .NET Framework 4.0 ou suivant et relancez l'Assistant d'installation.

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

DANS CETTE SECTION

ETAPE 1. FENETRE D'ACCUEIL DE L'ASSISTANT D'INSTALLATION

Si les conditions répondent à la configuration requise pour installer le module Serveur d'intégration, la fenêtre de bienvenue de l'Assistant d'installation s'ouvre. Celle-ci contient les informations relatives au début de l'installation du Serveur d'intégration sur l'ordinateur.

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

ETAPE 2. SELECTION DU DOSSIER D'INSTALLATION

Choisissez lors de cette étape le dossier dans lequel les modules du Serveur d'intégration seront installés.

L'installation a lieu par défaut dans le dossier C:\Program Files\Kaspersky Lab\Viis\.

Si vous souhaitez choisir un autre dossier, cliquez sur le bouton **Modifier** et sélectionnez le nouveau dossier d'installation dans la fenêtre qui s'ouvre.

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

ETAPE 3. SELECTION DES MODULES DE L'APPLICATION A INSTALLER

Cette étape permet de modifier la sélection de modules de l'application qui va être installée. Les deux modules (le Serveur d'intégration et la Console de gestion du Serveur d'intégration) sont installés par défaut.

Pour sélectionner le module à installer, ouvrez le menu contextuel en cliquant sur l'icône située en regard du nom du module et sélectionnez l'option **Le module sera installé sur** le disque dur local.

Pour connaître l'espace requis sur le disque dur pour installer le module, consultez la partie inférieure de la fenêtre de l'Assistant d'installation.

Si vous ne souhaitez pas installer un des deux modules, ouvrez le menu contextuel en cliquant avec le bouton gauche de la souris sur l'icône située en regard du nom du module et sélectionnez l'option **Le module sera complètement indisponible**.

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

ETAPE 4. SAISIE DES PARAMETRES DU SERVEUR D'INTEGRATION

Cette étape est proposée si vous avez choisi le module Serveur d'intégration ou les deux, à savoir le Serveur d'intégration et la Console de gestion du Serveur d'intégration, à l'étape "Sélection des modules de l'application à installer". Si vous n'avez choisi que la Console de gestion, l'Assistant passe cette étape.

A cette étape, indiquez les paramètres que le Serveur d'intégration devra utiliser pour établir la connexion réseau :

- **Adresse du Serveur d'intégration** : adresse IP sur laquelle le Serveur d'intégration recevra les connexions entrantes en provenance de la Console de gestion du Serveur d'intégration et des machines virtuelles de protection. Sélectionnez une des options suivantes dans la liste déroulante :
  - **Toutes les interfaces réseau**. Si vous choisissez cette option, le Serveur d'intégration acceptera les connexions entrantes sur n'importe quelle des adresses IP de l'ordinateur sur lequel le Serveur d'intégration est installé (en présence de plusieurs adresses IP).
  - Adresse IP de l'ordinateur sur lequel le Serveur d'intégration est installé. Si vous avez choisi cette option, le Serveur d'intégration acceptera les connexions entrantes uniquement sur l'adresse IP indiquée.
- **Port** : port de connexion au serveur d'intégration. Le port utilisé par défaut est le port 7271.

L'adresse et le port de connexion au Serveur d'intégration ne peuvent être modifiés après l'installation du Serveur d'intégration.

Saisissez le mot de passe du compte utilisateur de l'administrateur du Serveur d'intégration dans les champs **Mot de passe** et **Confirmation du mot de passe**.

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

Le compte de l'administrateur du Serveur d'intégration est nécessaire pour configurer les paramètres du Serveur d'intégration. Le nom d'utilisateur du compte de l'administrateur est *admin*. Le nom d'utilisateur ne peut pas être modifié.

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

ETAPE 5. LANCEMENT DE L'INSTALLATION

Tous les paramètres indispensables à l'installation du Serveur d'intégration ont été saisis.

Cliquez sur **Installer** pour lancer l'installation du Serveur d'intégration.

ETAPE 6. INSTALLATION DES MODULES DU SERVEUR D'INTEGRATION

Cette étape correspond à l'installation des modules du Serveur d'intégration. L'installe dure un certain temps. Veuillez attendre jusque sa fin.

L'Assistant réalise les opérations suivantes pendant l'installation :

- Si vous avez choisi le module Serveur d'intégration ou les deux, à l'étape "Sélection des modules de l'application à installer", l'Assistant d'installation crée deux comptes utilisateur du Serveur d'intégration :
  - Compte utilisateur d'administration du Serveur d'intégration. Ce compte est indispensable pour configurer les paramètres du Serveur d'intégration. Le nom d'utilisateur du compte de l'administrateur est *admin*.
  - Compte utilisateur pour la connexion des machines virtuelles de protection au Serveur d'intégration. Ce compte utilisateur possède le nom d'utilisateur *svm* et le mot de passe par défaut *svm*.

Les comptes utilisateur du Serveur d'intégration sont conservés sous une forme chiffrée dans la base de registres du système d'exploitation de l'ordinateur où est installé le Serveur d'intégration.

Pour prévenir l'accès non autorisé au Serveur d'intégration après l'installation, il est recommandé de modifier le mot de passe attribué par défaut au compte de connexion des machines virtuelles de protection au Serveur d'intégration. Vous pouvez modifier ce mot de passe dans la Console de gestion du Serveur d'intégration (cf. section "Modification des paramètres du Serveur d'intégration" à la page 86). Les noms des comptes utilisateur ne peuvent pas être modifiés.

- Le certificat SSL du Serveur d'intégration est installé dans la base de registres du système d'exploitation de l'ordinateur où sont installés les modules du Serveur d'intégration. Le certificat permet d'ouvrir une connexion sécurisée entre le Serveur d'intégration et la Console de gestion ou les machines virtuelles de protection. Le certificat est enregistré sur le disque dur dans le dossier <dossier d'installation des modules du Serveur d'intégration>\ssl\certs.

Le certificat du Serveur d'intégration est créé une seule fois, lors de l'installation du Serveur d'intégration. En cas de perte du Serveur d'intégration, la seule manière de le récupérer consiste à installer à nouveau le Serveur d'intégration ou à installer un autre certificat (la procédure de substitution d'un certificat est décrite dans la base des connaissances http://support.kaspersky.com/fr/11698).

ETAPE 7. FIN DU TRAVAIL DE L'ASSISTANT

Cette étape affiche les informations relatives aux résultats de l'installation des modules du Serveur d'intégration.

Si l'installation a été interrompue ou si une erreur s'est produite durant celle-ci, l'Assistant d'installation annule toutes les modifications introduites.

Pour pouvoir utiliser le Serveur d'intégration pendant le fonctionnement de Kaspersky Security, il faut configurer les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter après l'installation du serveur d'intégration. La configuration des paramètres de connexion s'opère dans la Console de gestion du Serveur d'intégration (cf. section "Configuration initiale du Serveur d'intégration" à la page 32).

Quittez l'Assistant d'installation.

INSTALLATION DE LA CONSOLE DE GESTION

La Console de gestion permet de configurer les paramètres du Serveur d'intégration. Vous pouvez installer la Console de gestion sur l'ordinateur hébergeant le Serveur d'intégration, ou sur un autre ordinateur.

Si la Console de gestion du Serveur d'intégration est installée sur l'ordinateur où se trouve la Console d'administration de Kaspersky Security Center, vous pouvez lancer la Console de gestion du Serveur d'intégration en cliquez sur le lien situé dans la zone de travail de la Console d'administration de Kaspersky Security Center.

Si la Console de gestion du Serveur d'intégration est installée sur un autre ordinateur, vous pouvez la lancer depuis le dossier d'installation.

L'installation de la Console de gestion s'opère à l'aide de l'Assistant d'installation du Serveur d'intégration.

Pour installer la Console de gestion du Serveur d'intégration, procédez comme suit :

1. Lancez l'Assistant d'installation du Serveur d'intégration (cf. section "Procédure d'installation du Serveur d'intégration et de la Console de gestion" à la page 28).

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

A l'étape de sélection des modules à installer, sélectionnez le module Console de gestion et refusez d'installer le module Serveur d'intégration.

CONFIGURATION INITIALE DU SERVEUR D'INTEGRATION

Pour pouvoir utiliser le Serveur d'intégration pendant le fonctionnement de Kaspersky Security, il faut configurer les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter après l'installation du serveur d'intégration.

Pour configurer les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter, procédez comme suit :

1. Lancez la Console de gestion du Serveur d'intégration d'une des manières suivantes :

   - Si la Console de gestion est installée sur l'ordinateur où se trouve la Console d'administration de Kaspersky Security Center, procédez comme suit :

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

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

     c. Lancez la Console de gestion du Serveur d'intégration via le lien **Console de gestion du Serveur d'intégration**. Le lien se trouve dans la zone de travail du groupe **Déploiement**.

   - Si la Console de gestion du serveur d'intégration est installé sur un autre ordinateur que celui de la Console d'administration de Kaspersky Security Center, exécutez le fichier KsvServerConsole.exe depuis le dossier d'installation du Serveur d'intégration.

   La fenêtre de saisie des paramètres de connexion au Serveur d'intégration s'ouvre.

2. Etablissez la connexion au Serveur d'intégration (cf. section "Connexion au Serveur d'intégration" à la page 86).

3. Définissez les paramètres suivants sous l'onglet **Paramètres de connexion au serveur VMware vCenter** :

   - adresse du serveur VMware vCenter auquel le Serveur d'intégration se connecte ;

   - nom d'utilisateur et mot de passe du compte utilisateur sous lequel le Serveur d'intégration se connecte au serveur VMware vCenter ;

   - action exécutée par le Serveur d'intégration lors de la connexion au serveur VMware vCenter, si le certificat SSL du serveur VMware vCenter contient une erreur ou ne correspond pas à un certificat installé antérieurement.

4. Cliquez sur le bouton **OK** pour appliquer les modifications et fermer la Console de gestion.

INSTALLATION DU MODULE ANTI-VIRUS FICHIERS

L'installation du module Anti-Virus Fichiers dans l'infrastructure virtuelle VMware se déroule via le déploiement de machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi.

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

Pour installer le module Anti-Virus 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Le cas échéant, cochez la case **Consigner les informations détaillées dans les journaux de fonctionnement de Kaspersky Security** de cette fenêtre, puis passez à l'étape suivante de l'Assistant.

Il est conseillé d'activer la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security uniquement à la demande des experts du Support Technique.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Anti-Virus Fichiers** 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 AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure d'installation.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter 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 transmise par 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 Anti-Virus 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'hyperviseur 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 HYPERVISEURS VMWARE ESXI.

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

Les colonnes du tableau reprennent les informations relatives à l'ensemble des hyperviseurs VMware ESXi placés sous l'administration d'un serveur VMware vCenter :

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

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

Pour sélectionner un hyperviseur, 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'hyperviseur 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'hyperviseur 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'hyperviseur 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 hyperviseurs VMware ESXi, cochez la case **Autoriser le déploiement en parallèle**. Dans le champ **Déployer simultanément sur un maximum de X hyperviseurs VMware ESXi**, indiquez le nombre d'hyperviseurs 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 hyperviseurs VMware ESXi.

Les colonnes du tableau reprennent les informations suivantes :

- **Hyperviseur VMware ESXi** : adresse IP ou nom de domaine de l'hyperviseur.
- **Nom de la machine virtuelle de protection** : nom de la machine virtuelle de protection qui sera installée sur cet hyperviseur. 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'hyperviseur VMware ESXi. Si un seul stockage de données est connecté à l'hyperviseur, 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'hyperviseur VMware ESXi :

- La colonne **Hyperviseur VMware ESXi** affiche l'adresse IP ou le nom de domaine de l'hyperviseur 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'hyperviseur 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'hyperviseur VMware ESXi. Il assure l'interaction du pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) installé sur la machine virtuelle et de la bibliothèque EPSEC installée sur la machine virtuelle de protection.
- Dans la colonne **Réseau d'administration**, sélectionnez dans la liste déroulante le réseau virtuel de l'hyperviseur 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 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

Le mot de passe klconfig et le mot de passe du compte utilisateur root sont définis par défaut sur les machines virtuelles de protection. Le mot de passe klconfig est le mot de passe nécessaire pour apporter des modifications à la configuration de la machine virtuelle de protection. Le compte root est utilisé dans le cadre de la configuration des machines virtuelles de protection.

Cette étape permet de modifier le mot de passe klconfig et le mot de passe du compte utilisateur root définis 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 klconfig. Vous pouvez modifier le mot de passe 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 Anti-Virus Fichiers" à la page 90).

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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure d'installation.

L'Assistant vérifie la présence du module VMware vShield Endpoint sur tous les hyperviseurs 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 DE CONNEXION DES MACHINES VIRTUELLES DE PROTECTION A L'INFRASTRUCTURE VIRTUELLE

Au cours de cette étape, indiquez les paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle VMware. Ces paramètres interviennent dans le fonctionnement des machines virtuelles de protection en vue d'obtenir des informations sur l'infrastructure virtuelle.

Dans la fenêtre **Type de connexion**, sélectionnez une des options suivantes :

- **Connexion au serveur VMware vCenter**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection reçoivent les informations relatives à l'infrastructure virtuelle directement du serveur VMware vCenter.

- **Connexion au Serveur d'intégration**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection obtiennent les informations sur l'infrastructure virtuelle auprès du Serveur d'intégration connecté au serveur VMware vCenter (cf. section "A propos du Serveur d'intégration" à la page 22).

  Si vous souhaitez utiliser la connexion au Serveur d'intégration, il faudra, avant de lancer l'installation du module Anti-Virus Fichiers, installer le Serveur d'intégration et configurer les paramètres de connexion au serveur VMware vCenter (cf. section "Installation du Serveur d'intégration" à la page 28).

Définissez les paramètres de connexion au serveur VMware vCenter :

- **Adresse** : l'adresse du serveur VMware vCenter ou adresse du Serveur d'intégration :

  - Si vous avez choisi la connexion au serveur VMware vCenter, le contenu du champ ne peut être modifié : l'adresse utilisée est l'adresse du serveur VMware vCenter que vous avez renseignée à l'étape "Connexion au serveur VMware vCenter".

  - Si vous avez choisi la connexion au Serveur d'intégration, indiquez l'adresse IP au format IPv4 ou le nom de domaine complet du Serveur d'intégration.

- **Nom d'utilisateur** : nom du compte utilisateur sous lequel la connexion des machines virtuelles au serveur VMware vCenter s'opère.

  - Si vous avez choisi la connexion au serveur VMware vCenter, 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.

  - Si vous avez choisi la connexion au Serveur d'intégration, indiquez le nom d'utilisateur *svm*.

- **Mot de passe** : mot de passe du compte utilisateur sous lequel la connexion des machines virtuelles au serveur VMware vCenter s'opère.

- **Action de la machine virtuelle de protection en cas de détection d'une erreur de certificat** : action que va exécuter la machine virtuelle de protection lors de la connexion au serveur VMware vCenter ou au Serveur d'intégration si le certificat de serveur obtenu contient une erreur ou ne correspond pas à un certificat installé antérieurement. Options possibles :

  - **Annuler la connexion, indiquer une erreur** : la machine virtuelle de protection annule la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center.

  - **Poursuivre la connexion, indiquer une erreur** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center. Cette option est sélectionnée par défaut.

  - **Ignorer** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter ou au Serveur d'intégration 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 du serveur VMware vCenter" à la page 24).

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure d'installation.

ETAPE 15. LANCEMENT DU DEPLOIEMENT DES MACHINES VIRTUELLES DE PROTECTION

Tous les paramètres indispensables au déploiement des machines virtuelles de protection sur les hyperviseurs 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 hyperviseurs 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 hyperviseurs 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'hyperviseur VMware ESXi, l'Assistant réalise le retour à l'état antérieur aux modifications sur cet hyperviseur 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 hyperviseurs 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 ANTI-VIRUS FICHIERS

A cette étape, les informations relatives au déploiement des machines virtuelles de protection sur les hyperviseurs 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.

INSTALLATION DU MODULE DETECTION DES INTRUSIONS

L'installation du module Détection des intrusions dans l'infrastructure virtuelle VMware se déroule via le déploiement des machines virtuelles de protection dotées du module Détection des intrusions sur les hyperviseurs VMware ESXi et via l'enregistrement du module Détection des intrusions dans VMware vShield Manager. Dans VMware vShield Manager, le module Détection des intrusions 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 intrusions 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 hyperviseurs VMware ESXi, entrant dans la composition des clusters VMware, ainsi que l'enregistrement du module Détection des intrusions (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 intrusions.

Pour installer le module Détection des intrusions, 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.
4. Dans la fenêtre qui s'ouvre, choisissez l'option **Détection des intrusions** 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 intrusions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure d'installation.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter 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 transmise par 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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** 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 intrusions sur la ressource réseau accessible par le protocole HTTP.

Si vous procédez pour la première fois à l'installation du module Détection des intrusions sur les clusters VMware administré par le serveur VMware vCenter sélectionné, indiquez le chemin d'accès au fichier OVF de la machine virtuelle de protection dans le champ **Fichier OVF**.

Si le module Détection des intrusions est déjà installé sur un ou plusieurs clusters VMware administrés par le serveur VMware vCenter sélectionné, le chemin d'accès au fichier OVF qui a été utilisé lors de la précédente installation du module Détection des intrusions 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'hyperviseur 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 intrusions, 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 intrusions" à la page 78). Des machines virtuelles de protection seront installées sur les clusters VMware que vous avez choisis et sur lesquels le module Détection des intrusions 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 hyperviseurs 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 administré par un serveur VMware vCenter :

- **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 hyperviseurs VMware ESXi entrant dans la composition de ce cluster VMware.
  - **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hyperviseurs 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 intrusions est déjà installé sur un ou plusieurs clusters VMware administré par le serveur VMware vCenter sélectionné, les cases à gauche du nom des clusters VMware protégés sont cochées dans le tableau.

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 intrusions (cf. section " Procédure de mise à jour du module Détection des intrusions" à la page 78). Des machines virtuelles de protection seront installées sur les clusters VMware choisis et sur lesquels le module Détection des intrusions 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 administrés par un serveur VMware vCenter :

- **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 intrusions 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 intrusions.

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 hyperviseurs VMware ESXi dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

Après l'installation du module Détection des intrusions, 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 intrusions).

Une fois que le module Détection des intrusions a été installé, il faut activer la détection des attaques réseau et l'analyse des adresses Internet dans les paramètres de la stratégie. Par défaut, Kaspersky Security ne détecte pas les intrusions et n'analyse pas les adresses Internet. Les informations relatives à la configuration des tâches et des stratégies figurent dans le *Manuel de l'administrateur de Kaspersky Security for Virtualization 3.0 Agentless*.

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 hyperviseurs VMware ESXi administrés par un serveur VMware vCenter et les machines virtuelles qu'elles protègent dans un cluster KSC. Le cluster KSC reçoit le nom du serveur VMware vCenter correspondant.

Kaspersky Security Center un dossier dans le dossier **Ordinateurs administrés** de la Console d'administration pour chaque cluster KSC et lui donne le nom de ce cluster KSC. Lors de la sélection dans l'arborescence de la console du dossier portant le nom d'un cluster KSC, la liste des machines virtuelles de protection entrant dans la composition de ce cluster KSC s'affiche dans la zone de travail sous l'onglet **Ordinateurs**.

Il est possible d'ouvrir la fenêtre des propriétés du cluster depuis le sous-dossier **Clusters et tableau de serveurs** du dossier portant le nom du cluster KSC. La fenêtre des propriétés du cluster KSC permet de consulter la liste des tâches créées pour le cluster, la liste des machines virtuelles de protection et de toutes les machines virtuelles qui appartiennent au cluster KSC.

ACTIVATION DE L'APPLICATION

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

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

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

- fichier clé ;
- code d'activation.

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

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

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

Si vous utilisez un plan de licence en fonction du nombre de machines virtuelles protégées, le type de clé doit correspondre au système d'exploitation invité des machines virtuelles :

- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour serveur, il faut ajouter à la machine virtuelle de protection une clé pour serveur ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour ordinateur de bureau, il faut ajouter à la machine virtuelle de protection une clé pour ordinateur de bureau ;
- pour assurer la protection des machines virtuelles dotées d'un système d'exploitation pour serveur et d'un système pour ordinateur de bureau, il faut ajouter à la machine virtuelle de protection une clé pour serveur et une clé pour ordinateur de bureau.

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

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

Si vous ajoutez une clé pour serveur ou poste de travail et qu'une clé en fonction du nombre de cours avait été ajoutée à la machine virtuelle de protection, la clé active et complémentaire (le cas échéant) en fonction du nombre de cœurs est supprimée suite à l'exécution de la tâche. Elle est remplacée par une clé active pour serveur ou poste de travail.

Si vous achetez une clé commerciale et qu'une clé d'abonnement avait déjà été ajoutée sur la machine virtuelle de protection, la clé d'abonnement sera supprimée. La clé commerciale la remplacera.

Si vous ajoutez une clé d'abonnement et qu'une ou plusieurs clés commerciales avaient déjà été ajoutées sur la machine virtuelle de protection, toutes les clés actives et, le cas échéant, les clés complémentaires, seront supprimées. La clé d'abonnement les remplacera.

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

Pour activer l'application, procédez comme suit :

1. Créez une tâche d'ajout de clé pour chaque cluster KSC reprenant les machines virtuelles de protection auxquelles vous souhaitez ajouter une clé (cf. section "Création d'une tâche d'ajout de clé" à la page 48).

2. Lancez la tâche d'ajout de clé (cf. section "Lancement de la tâche d'ajout de clé" à la page 51).

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

DANS CETTE SECTION

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

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

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

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

Après que vous avez sélectionné le fichier clé ou entré le code d'activation, les informations suivantes s'affichent dans la partie inférieure de la fenêtre :

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

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

ETAPE 5. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

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

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

  Si la case est décochée, le lancement de la tâche pour le mode **Manuel** est exécuté uniquement sur les machines virtuelles de protection visibles dans le réseau.
- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :
  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;

- De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
- De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
- De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
- De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
- Plus de 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 3 heures.

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

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

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

ETAPE 6. FIN DE LA CREATION DE LA TACHE

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

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

Si, dans la fenêtre **Programmation de l'exécution de la tâche**, vous avez défini une planification pour l'exécution de la tâche d'ajout de clé, cette tâche sera exécutée conformément à la programmation. Vous pouvez également lancer à n'importe quel moment la tâche d'ajout de clé manuellement (cf. section "Lancement de la tâche d'ajout de clé " à la page 51).

LANCEMENT DE LA TACHE D'AJOUT DE CLE

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

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

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

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

- Si vous ajoutez une clé pour serveur ou poste de travail et qu'une clé en fonction du nombre de cours avait été ajoutée à la machine virtuelle de protection, la clé active et complémentaire (le cas échéant) en fonction du nombre de cœurs est supprimée suite à l'exécution de la tâche. Elle est remplacée par une clé active pour serveur ou poste de travail.

- Si vous achetez une clé commerciale et qu'une clé d'abonnement avait déjà été ajoutée sur la machine virtuelle de protection, l'exécution de la tâche de la clé d'abonnement sera annulée. La clé commerciale la remplacera.

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

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

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

- il manque une clé active ;

- une clé par abonnement a été ajoutée en tant que clé active ;

- une clé d'évaluation est ajoutée en tant que clé complémentaire ;

- le type de la clé complémentaire ajoutée ne correspond pas au type de la clé active ajoutée antérieurement.

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

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

- Dans la fenêtre **Résultats de l'exécution de la tâche**. Pour ouvrir la fenêtre, cliquez sur le bouton **Consulter les résultats** situé à droite de la liste des tâches, sous l'onglet **Tâches**.

- Dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les machines virtuelles de protection. La liste des événements apparaît dans le dossier **Rapports et notifications/Evénements** de l'arborescence de la Console d'administration du Kaspersky Security Center.

PREPARATIFS DE L'APPLICATION EN VUE DE SON UTILISATION

Cette section contient les informations sur les actions à réaliser avant de commencer à utiliser l'application Kaspersky Security.

Il convient de réaliser les opérations suivantes après l'installation et l'activation de Kaspersky Security :

- Configurer les paramètres de fonctionnement de l'application à l'aide d'une stratégie (cf. section "Création d'une stratégie" à la page 53).
- Mettre à jour les bases anti-virus sur l'ensemble des machines virtuelles de protection (cf. section "Mise à jour des bases anti-virus" à la page 59).

DANS CETTE SECTION

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

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

Le profil de protection racine est formé pendant la création de la stratégie. Les paramètres de protection indiqués dans le profil de protection racine sont appliqués à toutes les machines virtuelles de l'infrastructure protégée du cluster KSC.

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

- les paramètres de détection des attaques réseau et d'analyse des adresses Internet ;
- les paramètres de la sauvegarde ;
- les paramètres d'utilisation des services KSN.

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 sécurité**, effectuez l'une des actions suivantes :
   - Si vous souhaitez utiliser l'un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.

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

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

- **Analyser les archives**.

  Activation ou désactivation de l'analyse des archives.

  La case est décochée par défaut.

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

  Suppression des archives dont la réparation est impossible.

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

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

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

  La case est décochée par défaut.

- **Analyser les archives autoextractibles**.

  Activation/désactivation de l'analyse des archives autoextractibles.

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

- **Analyser les objets OLE intégrés**.

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

  La case est cochée par défaut.

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

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

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

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

  La case est cochée par défaut.

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

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

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

  La valeur par défaut est de 8 Mo.

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

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

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

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

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

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

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

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

  La valeur par défaut est de 60 secondes.

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

- **Utilitaires malveillants**.

  Activation/désactivation de la protection contre les utilitaires malveillants.

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

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

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

  La case est cochée par défaut.

- **Programmes publicitaires**.

  Activation/désactivation de la protection contre les programmes publicitaires.

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

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

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

  La case est cochée par défaut.

- **Programmes numéroteurs**.

  Activation/désactivation de la protection contre les programmes numéroteurs.

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

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

  La case est cochée par défaut.

- **Autres**.

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

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

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

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

  La case est décochée par défaut.

- **Fichiers compactés plusieurs fois**.

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

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

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

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

  La case est cochée par défaut.

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

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

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

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

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

- **Sélectionner l'action automatiquement**.

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

  Cette option est sélectionnée par défaut.

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

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

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

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

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

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

- **Bloquer**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ETAPE 4. ACCORD DE PARTICIPATION A KASPERSKY SECURITY NETWORK

Cette étape est une invitation à participer au programme 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.

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

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

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

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

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

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

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

Si aucune clé n'est ajoutée à la machine virtuelle de protection (cf. section "Activation de l'application" à la page 47) ou s'il manque des bases anti-virus, l'application ne protège pas les machines virtuelles.

MISE A JOUR DES BASES ANTIVIRUS

Une fois que les machines virtuelles de protection ont été installées ou mises à jour sur les hyperviseurs VMware ESXi, il faut obligatoirement mettre à jour les bases anti-virus sur les machines virtuelles de protection.

La mise à jour requiert une licence d'utilisation de l'application (cf. section "Activation de l'application" à la page 47).

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.

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 actualiser les bases anti-virus sur les machines virtuelles de protection, 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. Lancez manuellement la tâche de chargement des mises à jour dans le référentiel ou attendez le lancement planifié. Assurez-vous que la tâche de chargement des mises à jour dans le référentiel a réussi (pour les détails, consultez la documentation de Kaspersky Security Center).
3. Créez une tâche de diffusion des mises à jour pour chaque cluster KSC reprenant les machines virtuelles sur lesquelles vous souhaitez mettre à jour les bases anti-virus (cf. section "Création de la tâche de diffusion des mises à jour" à la page 60).
4. Attendez l'exécution planifiée de la tâche de diffusion des mises à jour ou lancez la tâche manuellement (cf. section "Lancement manuel de la tâche de diffusion des mises à jour" à la page 62).
5. Assurez-vous que la tâche de diffusion des mises à jour a réussi (cf. section "Consultation des résultats d'exécution de la tâche de diffusion des mises à jour" à la page 62).

DANS CETTE SECTION

CREATION DE LA TACHE DE DIFFUSION DES MISES A JOUR

Pour créer une tâche de diffusion des mises à jour, procédez comme suit :

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

DANS CETTE SECTION

ETAPE 1. DEFINITION DU NOM DE LA TACHE

Saisissez le nom de la tâche de diffusion des mises à jour dans le champ **Nom**.

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

ETAPE 2. SELECTION DU TYPE DE TACHE

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

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

ETAPE 3. DEFINITION DES PARAMETRES DE PROGRAMMATION DE LA TACHE

Cette étape correspond à la configuration du mode de lancement de la tâche de diffusion des mises à jour :

- **Lancement programmé**. Dans la liste déroulante, sélectionnez **Lors du téléchargement des mises à jour dans le stockage**.
- **Lancement des tâches ignorées**. Cochez la case si une tentative de lancement des tâches doit avoir lieu lors du prochain démarrage de l'application sur la machine virtuelle de protection.

  Si la case est cochée, la tâche sur la machine virtuelle de protection sera lancée uniquement selon la programmation.
- **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. Par défaut, le lancement des tâches sur les machines virtuelles de protection s'étale sur une durée précise. Cette durée est calculée automatiquement en fonction du nombre de machines virtuelles de protection couvertes par la tâche :
  - De 0 à 200 machines virtuelles de protection : le lancement de la tâche est immédiat ;
  - De 200 à 500 machines virtuelles de protection : le lancement de la tâche s'étale sur 5 minutes ;
  - De 500 à 1000 machines virtuelles de protection : le lancement de la tâche s'étale sur 10 minutes ;
  - De 1000 à 2000 machines virtuelles de protection : le lancement de la tâche s'étale sur 15 minutes ;
  - De 2000 à 5000 machines virtuelles de protection : le lancement de la tâche s'étale sur 20 minutes ;
  - De 5000 à 10 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 30 minutes ;
  - De 10 000 à 20 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 1 heure ;
  - De 20 000 à 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 2 heures ;
  - Plus de 50 000 machines virtuelles de protection : le lancement de la tâche s'étale sur 3 heures.

  S'il n'est pas nécessaire d'étaler le lancement de la tâche sur une période calculée automatiquement, décochez la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche**. La case est cochée par défaut.
- **Démarrage aléatoire de la tâche avec intervalle (min.)**. Si vous voulez que la tâche soit lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment du lancement supposé de la tâche, cochez cette case et, dans le champ de saisie, indiquez le temps de retard maximal de lancement de la tâche. Dans ce cas, la tâche sera lancée à une heure aléatoire dans l'intervalle indiqué à partir du moment supposé de lancement. La case est accessible si la case **Déterminer automatiquement l'intervalle de répartition du lancement de la tâche** n'est pas cochée.

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

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

ETAPE 4. FIN DE LA CREATION DE LA TACHE

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

Après l'installation ou la mise à jour de Kaspersky Security, les machines virtuelles de protection transmettent au Kaspersky Security Center les informations relatives aux bases anti-virus requises pour le fonctionnement de Kaspersky Security. Le traitement des informations du côté de Kaspersky Security Center dure un certain temps. Si Kaspersky Security Center, au moment du lancement de la tâche de diffusion des mises à jour, n'avait pas encore traité les informations obtenues, la tâche pourrait se solder sur une erreur (cf. section "Consultation des résultats d'exécution de la tâche de diffusion des mises à jour" à la page 62). Dans ce cas, vous pouvez attendre le prochain lancement de la tâche selon la programmation ou lancer la tâche manuellement (cf. section "Lancement manuel de la tâche de diffusion des mises à jour" à la page 62). Si Kaspersky Security Center, au moment du lancement de la tâche de diffusion des mises à jour, a reçu et traité toutes les informations requises, la tâche de diffusion réussira.

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 est lancée à chaque chargement d'un paquet de mise à jour dans le stockage du Serveur d'administration. Suite à l'exécution de cette tâche, les mises à jour des bases antivirus sont diffusées et installées sur les machines virtuelles de protection.

CONSULTATION DES RESULTATS D'EXECUTION DE LA TACHE DE DIFFUSION DES MISES A JOUR

- *Pour consulter les résultats de l'exécution de la tâche de diffusion des mises à jour, procédez comme suit :*

1. Ouvrez la Console d'administration du Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, choisissez le dossier portant le nom du cluster KSC qui comprend les machines virtuelles de protection pour lesquelles la tâche de mise à jour a été configurée.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
4. Dans la liste des tâches, sélectionnez la tâche de diffusion des mises à jour dont vous souhaitez consulter les résultats d'exécution.
5. Cliquez sur le bouton **Consulter les résultats** situé à droite de la liste des tâches.

La fenêtre **Résultats de l'exécution de la tâche** s'ouvre.

Si la tâche de diffusion de la mise à jour s'est terminée sur une erreur, vous pouvez attendre le prochain lancement de la tâche selon la programmation ou lancer la tâche manuellement (cf. section "Lancement manuel de la tâche de diffusion des mises à jour" à la page 62).

Les résultats de l'exécution de la tâche peuvent également être consultés dans la liste des événements envoyés au Serveur d'administration de Kaspersky Security Center par les machines virtuelles de protection. La liste des événements apparaît dans le dossier **Rapports et notifications/Evénements** de l'arborescence de la Console d'administration du Kaspersky Security Center.

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

LANCEMENT MANUEL DE LA TACHE DE DIFFUSION DES MISES A JOUR

Si la tâche de diffusion des mises à jour lancée selon la programmation s'est terminée sur une erreur, vous pouvez la lancer manuellement.

Pour lancer manuellement une tâche de diffusion des mises à jour, procédez comme suit :

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

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 53) et que vous avez activé l'application (cf. section "Activation de l'application" à la page 47).

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

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

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

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 actualiser les versions suivantes de l'application jusque Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 :

- Kaspersky Security for Virtualization 2.0
- Kaspersky Security for Virtualization 2.0 Maintenance Release 1
- Kaspersky Security for Virtualization 3.0 Agentless

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

1. Mise à jour du Kaspersky Security Center 10 vers le Kaspersky Security Center 10 Service Pack 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 d'administration de Kaspersky Security s'effectue via l'installation d'une nouvelle version du plug-in sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center (cf. section "Installation du plug-in d'administration de Kaspersky Security" à la page 27). Il n'est pas nécessaire de supprimer les versions précédentes du plug-in.

   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 Service Pack 1 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 Anti-Virus Fichiers. La mise à jour du module Anti-Virus Fichiers se déroule via la mise à jour des machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs 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 Anti-Virus Fichiers (cf. section "Procédure de mise à jour du module Anti-Virus Fichiers" à la page 68).

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

   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 intrusions" à la page 78).

5. Activation de l'application sur les machines virtuelles de protection dotées du module Détection des intrusions (cf. section "Activation de l'application" à la page 47).

   Si vous avez refusé le transfert des clés lors de la mise à jour des machines virtuelles de protection dotées du module Anti-Virus 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 intrusions (cf. section "Mise à jour des bases antivirus" page 59).

   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 Anti-Virus 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 83). 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 Service Pack 1 ; ceci dès la première modification et la première sauvegarde des paramètres de protection dans la stratégie et des paramètres d'analyse dans la tâche.

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. Cette liste permet de consulter le numéro de version des images des machines virtuelles de protection installées sur les hyperviseurs 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.

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 serveur VMware vCenter :

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

   - **Nom d'utilisateur**. Nom du compte utilisateur sous lequel la connexion au serveur VMware vCenter est établie.

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

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

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

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

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

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

   La liste des images des machines virtuelles de protection déployées sur les hyperviseurs VMware ESXi apparaît dans la fenêtre de l'Assistant. Si, aucune machine virtuelle de protection installée avec le module Anti-Virus Fichiers ou le module Détection des intrusions 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 hyperviseur VMware ESXi.

   Les colonnes du tableau reprennent les informations suivantes :

   - **Hyperviseur VMware ESXi** : adresse IP de l'hyperviseur.

   - **Version de l'image (Anti-Virus Fichiers)** : le numéro de la version de l'image de la machine virtuelle de protection avec le module Anti-Virus Fichiers installé sur l'hyperviseur VMware ESXi.

   - **Version de l'image (Détection des intrusions)** : numéro de la version de l'image de la machine virtuelle de protection dotée du module Détection des intrusions installée sur l'hyperviseur 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 sera triée par ordre décroissant.

PROCEDURE DE MISE A JOUR DU MODULE ANTI-VIRUS FICHIERS

La mise à jour du module Anti-Virus Fichiers se déroule via la mise à jour des machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi.

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

1. Il installe des machines virtuelles de protection avec la nouvelle version du module Anti-Virus Fichiers sur les hyperviseurs 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 anti-virus 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 Anti-Virus 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 hyperviseur VMware ESXi protégé.

3. Il supprime les machines virtuelles de protection dotées de la version antérieure du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi administrés par un serveur VMware vCenter. 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 Anti-Virus Fichiers a supprimé les machines virtuelles de protection dotées de la version antérieure du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi, les machines virtuelles de protection supprimées 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 Anti-Virus 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 hyperviseurs VMware ESXi.

Pour mettre à jour le module Anti-Virus 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Le cas échéant, cochez la case **Consigner les informations détaillées dans les journaux de fonctionnement de Kaspersky Security** de cette fenêtre, puis passez à l'étape suivante de l'Assistant.

   Il est conseillé d'activer la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security uniquement à la demande des experts du Support Technique.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Anti-Virus Fichiers** 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 AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de mise à jour.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter est accessible via le réseau, puis relancez la mise à jour du module Anti-Virus 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 transmise par 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 Anti-Virus 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'hyperviseur 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 hyperviseurs VMware ESXi administrés par le serveur VMware vCenter sélectionné sur lesquels la machine virtuelle de protection est installée :

- **Hyperviseur VMware ESXi** : adresse IP ou nom de domaine de l'hyperviseur.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hyperviseur.

- **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'hyperviseur VMware ESXi sur lequel la machine virtuelle de protection est installée. Vous pouvez uniquement sélectionner les hyperviseurs 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'hyperviseur 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'hyperviseur 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'hyperviseur 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 hyperviseurs VMware ESXi, cochez la case **Autoriser le déploiement en parallèle**. Dans le champ **Déployer simultanément sur un maximum de X hyperviseurs VMware ESXi**, indiquez le nombre d'hyperviseurs 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 hyperviseurs VMware ESXi.

Les colonnes du tableau reprennent les informations suivantes :

- **Hyperviseur VMware ESXi** : adresse IP ou nom de domaine de l'hyperviseur.
- **Nom de la machine virtuelle de protection** : nom de la machine virtuelle de protection installée sur cet hyperviseur. 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'hyperviseur VMware ESXi. Si un seul stockage de données est connecté à l'hyperviseur, 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'hyperviseur VMware ESXi :

- La colonne **Hyperviseur 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'hyperviseur 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'hyperviseur VMware ESXi. Il assure l'interaction du pilote VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) installé sur la machine virtuelle et de la bibliothèque EPSEC installée sur la machine virtuelle de protection.
- Dans la colonne **Réseau d'administration**, sélectionnez dans la liste déroulante le réseau virtuel de l'hyperviseur 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 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

Le mot de passe klconfig et le mot de passe du compte utilisateur root sont définis par défaut sur les machines virtuelles de protection. Le mot de passe klconfig est le mot de passe nécessaire pour apporter des modifications à la configuration de la machine virtuelle de protection. Le compte root est utilisé dans le cadre de la configuration des machines virtuelles de protection.

Cette étape permet de modifier le mot de passe klconfig et le mot de passe du compte utilisateur root définis 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 klconfig. Vous pouvez modifier le mot de passe 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 Anti-Virus Fichiers" à la page 90).

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 Anti-Virus 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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de mise à jour.

L'Assistant vérifie la présence du module VMware vShield Endpoint sur tous les hyperviseurs 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 DE CONNEXION DES MACHINES VIRTUELLES DE PROTECTION A L'INFRASTRUCTURE VIRTUELLE

Au cours de cette étape, indiquez les paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle VMware. Ces paramètres interviennent dans le fonctionnement des machines virtuelles de protection en vue d'obtenir des informations sur l'infrastructure virtuelle.

Dans la fenêtre **Type de connexion**, sélectionnez une des options suivantes :

- **Connexion au serveur VMware vCenter**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection reçoivent les informations relatives à l'infrastructure virtuelle directement du serveur VMware vCenter.

- **Connexion au Serveur d'intégration**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection obtiennent les informations sur l'infrastructure virtuelle auprès du Serveur d'intégration connecté au serveur VMware vCenter (cf. section "A propos du Serveur d'intégration" à la page 22).

  Si vous souhaitez utiliser la connexion au Serveur d'intégration, il faudra, avant de lancer la mise à jour du module Anti-Virus Fichiers, installer le Serveur d'intégration et configurer les paramètres de connexion au serveur VMware vCenter (cf. section "Installation du Serveur d'intégration" à la page 28).

Définissez les paramètres de connexion au serveur VMware vCenter :

- **Adresse** : l'adresse du serveur VMware vCenter ou adresse du Serveur d'intégration :

  - Si vous avez choisi la connexion au serveur VMware vCenter, le contenu du champ ne peut être modifié : l'adresse utilisée est l'adresse du serveur VMware vCenter que vous avez renseignée à l'étape "Connexion au serveur VMware vCenter".

  - Si vous avez choisi la connexion au Serveur d'intégration, indiquez l'adresse IP au format IPv4 ou le nom de domaine complet du Serveur d'intégration.

- **Nom d'utilisateur** : nom du compte utilisateur sous lequel la connexion des machines virtuelles au serveur VMware vCenter s'opère.

  - Si vous avez choisi la connexion au serveur VMware vCenter, 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.

  - Si vous avez choisi la connexion au Serveur d'intégration, indiquez le nom d'utilisateur *svm*.

- **Mot de passe** : mot de passe du compte utilisateur sous lequel la connexion des machines virtuelles au serveur VMware vCenter s'opère.

- **Action de la machine virtuelle de protection en cas de détection d'une erreur de certificat** : action que va exécuter la machine virtuelle de protection lors de la connexion au serveur VMware vCenter ou au Serveur d'intégration si le certificat de serveur obtenu contient une erreur ou ne correspond pas à un certificat installé antérieurement. Options possibles :

  - **Annuler la connexion, indiquer une erreur** : la machine virtuelle de protection annule la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center.

- **Poursuivre la connexion, indiquer une erreur** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center. Cette option est sélectionnée par défaut.

- **Ignorer** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter ou au Serveur d'intégration 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 du serveur VMware vCenter" à la page 24).

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de mise à jour.

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 anti-virus 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 anti-virus, sélectionnez l'option **Préparer le fonctionnement des machines virtuelles de protection qui peuvent être mises à jour (recommandé)** et indiquez le mot de passe 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 Anti-Virus Fichiers, vous devrez activer l'application (cf. section "Activation de l'application" à la page 47) et mettre à jour les bases anti-virus sur les machines virtuelles de protection (cf. section "Mise à jour des bases anti-virus" à la page 59).

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 hyperviseurs 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 hyperviseurs 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 hyperviseur 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 hyperviseur 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 hyperviseurs 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 hyperviseurs 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 47) et mettre à jour les bases anti-virus sur l'ensemble des machines virtuelles de protection mises à jour (cf. section "Mise à jour des bases anti-virus" à la page59) après la mise à jour du module Anti-Virus Fichiers.

PROCEDURE DE MISE A JOUR DU MODULE DETECTION DES INTRUSIONS

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

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

Avant de commencer la mise à jour du module Détection des intrusions, 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 intrusions 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 intrusions sur les hyperviseurs VMware ESXi des clusters VMware sélectionnés.

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

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

   Après la suppression sur les hyperviseurs, 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 intrusions.

   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 intrusions, 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Détection des intrusions** 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 intrusions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de mise à jour.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter 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 transmise par 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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** 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 intrusions 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 intrusions 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 intrusions 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 intrusions 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'hyperviseur 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 hyperviseurs desquels il faut mettre à jour les machines virtuelles de protection.

Les colonnes du tableau affichent les informations relatives à l'ensemble des clusters VMware administré par un serveur VMware vCenter :

- **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 intrusions et installées sur les hyperviseurs VMware ESXi de ce cluster VMware.
  - **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hyperviseurs 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 hyperviseurs 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 administrés par un serveur VMware vCenter :

- **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 intrusions 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 intrusions 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 intrusions.

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 hyperviseurs VMware ESXi dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

Suite à la mise à jour du module Détection des intrusions, il est nécessaire d'activer l'application (cf. section "Activation de l'application" à la page 47) et d'exécuter la mise à jour des bases antivirus (cf. section "Mise à jour des bases antivirus" à la page 59) sur les machines virtuelles avec le module Détection des intrusions.

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

Une fois que Kaspersky Security a été mis à jour, vous pouvez utiliser les paramètres des stratégies et des tâches de la version précédente de l'application. Il est possible de convertir les stratégies et les tâches créées sur une des versions suivantes :

- Kaspersky Security for Virtualization 2.0
- Kaspersky Security for Virtualization 2.0 Maintenance Release 1
- Kaspersky Security for Virtualization 3.0 Agentless

Les stratégies et les tâches de la version précédente sont automatiquement converties en stratégies et tâches de Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 ; ceci dès la première modification et la première sauvegarde des paramètres de protection dans la stratégie et des paramètres d'analyse dans la tâche.

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 adresses Internet** : désactivé.
- **Ne pas bloquer l'accès aux adresses Internet suivantes** : adresses Internet inconnues.
- **Analyser les disques amovibles** : désactivé.

- **Analyser les disques réseau** : activé.
- **Respecter la casse dans les chemins d'accès aux dossiers réseau** : activé.
- **Langue du message relatif au blocage de l'adresse Internet** : la langue choisie par défaut est la langue qui correspond à la version linguistique du plug-in d'administration de Kaspersky Security.

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.

Les paramètres inexistants dans les stratégies et les tâches de Kaspersky Security for Virtualization 2.0 Maintenance Release 1 et Kaspersky Security for Virtualization 3.0 Agentless se traduisent ainsi dans les stratégies et les tâches converties :

- **Analyser les disques réseau** : activé.
- **Respecter la casse dans les chemins d'accès aux dossiers réseau** : activé.
- **Langue du message relatif au blocage de l'adresse Internet** : la langue choisie par défaut est la langue qui correspond à la version linguistique du plug-in d'administration de Kaspersky Security.

Les stratégies et les tâches de Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 ne prévoient pas la configuration du paramètre **Niveau d'analyse heuristique**. L'analyse heuristique intervient dans le cadre de la protection des machines virtuelles et lors de l'exécution de la tâche d'analyse. Les stratégies converties utilisent un des niveaux d'analyse heuristique suivants en fonction du niveau de sécurité choisi :

- Niveau d'analyse heuristique **Superficiel** quand le niveau de sécurité choisi est **Faible**.
- Niveau d'analyse heuristique **Moyen** quand le niveau de sécurité sélectionné est **Recommandé**, **Elevé** et **Personnalisé**.

Les tâches converties utilisent le niveau d'analyse heuristique **Minutieux** quel que soit le niveau de sécurité choisi.

Les valeurs des paramètres des fichiers compactés à plusieurs reprises et des fichiers compactés par des compacteurs spéciaux ont été modifiés dans les stratégies et les tâches de Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1. Dans les stratégies et les tâches converties, les paramètres d'analyse des fichiers compactés prennent les valeurs suivantes :

- Analyse des fichiers compactés par des compacteurs spéciaux : toujours activée. Le paramètre ne peut être modifié dans l'interface de l'application.
- l'analyse des fichiers compactés à plusieurs reprises est activée par défaut dans les propriétés de la tâche.
- L'analyse des fichiers compactés à plusieurs reprises est activée par défaut dans les propriétés de la stratégie si le niveau de sécurité **Faible**, **Recommandé** ou **Elevé** était sélectionné dans la stratégie de la version antérieure de l'application. Si le niveau de sécurité **Utilisateur** était configuré dans la stratégie de la version antérieure de l'application, le paramètre **Fichiers compactés plusieurs fois** prend la valeur définie dans la section **Détection de fichiers compactés** de la stratégie de la version antérieure de l'application.

  Le paramètre **Fichiers compactés plusieurs fois** se configure dans les propriétés de la stratégie et dans la tâche d'analyse via la fenêtre **Objets à détecter**.

Les stratégies de Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 prévoient une exclusion par défaut pour le profil de protection racine. La liste des exclusions de la protection du profil de protection racine contient les objets recommandés par Microsoft. Ces objets sont exclus de la protection sur toutes les machines virtuelles auxquelles le profil de protection racine a été attribué, quel que soit le système d'exploitation invité des machines virtuelles.

Les paramètres des exclusions de la protection du profil de protection racine dans les stratégies converties prennent les valeurs suivantes :

- Si le profil de protection racine d'une stratégie d'une version antérieure de Kaspersky Security contenait une liste d'exclusions, les objets repris dans cette liste seront exclus de la protection.

- Si aucune exclusion n'est définie dans le profil de protection racine d'une stratégie d'une version antérieure de Kaspersky Security; les objets recommandés par Microsoft sont ajoutés à la liste des exclusions.

MODIFICATION DES PARAMETRES DU SERVEUR D'INTEGRATION

Cette section contient des informations sur la modification des paramètres du serveur d'intégration.

DANS CETTE SECTION

PRESENTATION DES MODIFICATIONS DES PARAMETRES DU SERVEUR D'INTEGRATION

La modification des paramètres du Serveur d'intégration s'opère dans la Console de gestion du Serveur d'intégration (cf. section "Connexion au Serveur d'intégration" à la page 86).

Vous pouvez modifier les paramètres suivants :

- les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter ;
- le mot de passe du compte utilisateur de l'administrateur du Serveur d'intégration ;
- le mot de passe du compte utilisateur pour la connexion des machines virtuelles de protection au Serveur d'intégration ;

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

Le cas échéant, vous pouvez remplacer le certificat SSL du serveur d'intégration installé par défaut lors de l'installation du Serveur d'intégration. Le certificat du Serveur d'intégration permet d'ouvrir une connexion sécurisée entre le Serveur d'intégration et la Console de gestion ou les machines virtuelles de protection. Pour en savoir plus sur le remplacement du certificat, consultez la base de connaissances http://support.kaspersky.com/fr/11698.

L'adresse et le port de connexion au Serveur d'intégration ne peuvent être modifiés une fois l'installation du Serveur d'intégration terminée. Si vous souhaitez modifier l'adresse ou le port de connexion au Serveur d'intégration, il faut supprimer le Serveur d'intégration et l'installer à nouveau.

CONNEXION AU SERVEUR D'INTEGRATION.

Pour vous connecter au Serveur d'intégration, procédez comme suit :

1. Lancez la Console de gestion du Serveur d'intégration d'une des manières suivantes :
   - Si la Console de gestion est installée sur l'ordinateur où se trouve la Console d'administration de Kaspersky Security Center, procédez comme suit :
     a. Ouvrez la Console d'administration du Kaspersky Security Center.

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

c. Lancez la console de gestion en cliquant sur le lien **Console de gestion du Serveur d'intégration** dans le groupe **Déploiement**.

- Si la Console de gestion du serveur d'intégration est installé sur un autre ordinateur que celui de la Console d'administration de Kaspersky Security Center, exécutez le fichier KsvServerConsole.exe depuis le dossier d'installation du Serveur d'intégration.

La fenêtre de saisie des paramètres de connexion au Serveur d'intégration s'ouvre.

2. Saisissez les paramètres suivants dans la fenêtre de saisie des paramètres de connexion :

- **Adresse du serveur d'intégration**.

  Adresse IP au format IPv4 ou nom de domaine complet du Serveur d'intégration dont vous souhaitez configurer les paramètres.

- **Nom d'utilisateur**.

  Le nom du compte utilisateur d'administration du Serveur d'intégration (*admin*).

- **Mot de passe**.

  Mot de passe du compte utilisateur de l'administrateur du Serveur d'intégration.

La console de gestion conserve les paramètres de connexion au Serveur d'intégration saisi (sauf le mot de passe). Les paramètres de connexion sont enregistrés dans la base de Registres système sous forme chiffrée. Lors du prochain lancement de la Console de gestion, les paramètres enregistrés s'afficheront dans la fenêtre de saisie des paramètres de connexion.

3. Cliquez sur le bouton **Connecter**.

La Console de gestion vérifie le certificat SSL obtenu du Serveur d'intégration. La fenêtre **Vérification du certificat** s'ouvre avec un message d'erreur si le certificat reçu contient une erreur ou s'il n'est pas compatible avec le certificat précédemment installé. Vous pouvez consulter les informations sur le certificat reçu. Pour ce faire, cliquez sur le bouton **Afficher le certificat reçu** dans la fenêtre du message d'erreur.

Vous pouvez installer le certificat reçu en tant que certificat de confiance afin de ne pas recevoir de message relatif à une erreur de certificat lors de la prochaine connexion au Serveur d'intégration. Pour ce faire, cochez la case **Installer le certificat reçu et ne plus afficher les avertissements relatifs au serveur <adresse du Serveur d'intégration>**. Une fois que vous avez cliqué sur le bouton **Ignorer**, le certificat est enregistré dans la base de registres du système d'exploitation de l'ordinateur sur lequel la Console de gestion du Serveur d'intégration est installée.

Pour maintenir la connexion au Serveur d'intégration, cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat**.

La Console de gestion réalise la connexion au Serveur d'intégration. En cas d'échec d'ouverture de la connexion, vérifiez les paramètres saisis et retentez la connexion au Serveur d'intégration. Quand la connexion au Serveur d'intégration est ouverte, la fenêtre de configuration des paramètres du Serveur d'intégration s'ouvre.

La fenêtre des paramètres permet de modifier les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter (cf. section "Modification des paramètres de connexion du Serveur d'intégration au serveur VMware vCenter" à la page 88) et les mots de passe des comptes utilisateur du Serveur d'intégration (cf. section "Modification des mots de passe des comptes utilisateur du Serveur d'intégration" à la page 89).

MODIFICATION DES PARAMETRES DE CONNEXION DU SERVEUR D'INTEGRATION AU SERVEUR VMWARE VCENTER

Pour configurer les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter, procédez comme suit :

1. Lancez la Console de gestion du Serveur d'intégration, puis ouvrez la fenêtre de configuration des paramètres du Serveur d'intégration (cf. section "Connexion au Serveur d'intégration" à la page 86).

2. Définissez les paramètres suivants sous l'onglet **Paramètres de connexion au serveur VMware vCenter** :

   - **Adresse de VMware vCenter Server**.

     Adresse IP au format IPv4 ou nom de domaine complet du serveur VMware vCenter auquel le Serveur d'intégration se connecte pour obtenir les informations sur l'infrastructure virtuelle.

   - **Nom d'utilisateur**.

     Nom du compte utilisateur sous lequel le Serveur d'intégration se connecte au serveur VMware vCenter. 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 le Serveur d'intégration se connecte au serveur VMware vCenter.

   - **Action du Serveur d'intégration en cas de détection d'une erreur de certificat**.

     Action exécutée par le Serveur d'intégration lors de la connexion au serveur VMware vCenter, si le certificat du serveur VMware vCenter contient une erreur ou ne correspond pas à un certificat installé antérieurement.

     Options possibles :

     - **Ignorer** : le Serveur d'intégration maintient la connexion au serveur VMware vCenter.
     - **Annuler la connexion** : le Serveur d'intégration annule la connexion au serveur VMware vCenter.
     - **Poursuivre la connexion, consigner dans le journal** : le Serveur d'intégration maintient la connexion au serveur VMware vCenter et consigne les informations relatives à l'erreur dans le journal des événements du système d'exploitation. Cette option est sélectionnée par défaut.

3. Pour appliquer les modifications, cliquez sur **Appliquer**. Pour appliquer les modifications et fermer la Console de gestion, cliquez sur le bouton **OK**.

Les paramètres saisis de connexion au serveur VMware vCenter (sauf le mot de passe) sont consignées dans la base de Registres du système d'exploitation sous forme chiffrée.

MODIFICATION DES MOTS DE PASSE DES COMPTES UTILISATEUR DU SERVEUR D'INTEGRATION

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

1. Lancez la Console de gestion du Serveur d'intégration, puis ouvrez la fenêtre de configuration des paramètres du Serveur d'intégration (cf. section "Connexion au Serveur d'intégration" à la page 86).

2. Sous l'onglet **Paramètres du Serveur d'intégration**, modifiez le cas échéant les mots de passe des comptes utilisateur suivants du Serveur d'intégration :

   - Mot de passe du compte utilisateur de l'administrateur du Serveur d'intégration. Pour ce faire, cochez la case **Modifier le mot de passe du compte administrateur du Serveur d'intégration** et indiquez le nouveau mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.

   - Le mot de passe du compte utilisateur employé pour connecter les machines virtuelles de protection au Serveur d'intégration. Pour ce faire, cochez la case **Modifier le mot de passe du compte de connexion des machines virtuelles de protection** et indiquez le nouveau mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**.

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

   Si vous avez modifié le mot de passe du compte de connexion des machines virtuelles de protection, il faudra indiquer le nouveau mot de passe dans la configuration des machines virtuelles de protection qui se connectent à ce Serveur d'intégration. Réalisez la procédure de modification de la configuration de toutes les machines virtuelles de protection qui utilisent ce Serveur d'intégration pour obtenir les informations relatives à l'infrastructure virtuelle VMware. A l'étape "Modification des paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle", indiquez le nouveau mot de passe de connexion au Serveur d'intégration (cf. section "Modification de la configuration des machines virtuelles de protection dotées du module Anti-Virus Fichiers" à la page 90).

3. Pour appliquer les modifications, cliquez sur **Appliquer**. Pour appliquer les modifications et fermer la Console de gestion, cliquez sur le bouton **OK**.

MODIFICATION DE LA CONFIGURATION DES MACHINES VIRTUELLES DOTEES DU MODULE ANTI-VIRUS FICHIERS

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

Vous pouvez modifier les paramètres suivants de la configuration des machines virtuelles de protection déployées sur les hyperviseurs VMware ESXi :

- les paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle ;
- le mot de passe de configuration.

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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.
4. Dans la fenêtre qui s'ouvre, choisissez l'option **Anti-Virus Fichiers** 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 AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

- **Adresse de VMware vCenter Server**.

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

- **Nom d'utilisateur**.

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

- **Mot de passe**.

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

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. 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 du serveur VMware vCenter" à la page 24).

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de modification de la configuration.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter 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 hyperviseurs VMware ESXi administrés par le serveur VMware vCenter sélectionné sur lesquels la machine virtuelle de protection est installée :

- **Hyperviseur VMware ESXi** : adresse IP ou nom de domaine de l'hyperviseur.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hyperviseur 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'hyperviseur VMware ESXi sur lequel la machine virtuelle de protection est installée. Vous pouvez uniquement sélectionner les hyperviseurs 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 KLCONFIG

A cette étape, indiquez le mot de passe klconfig qui a été défini lors de l'installation de l'application.

Passez à l'étape suivante de l'Assistant.

ETAPE 5. MODIFICATION DES PARAMETRES DE CONNEXION DES MACHINES VIRTUELLES DE PROTECTION A L'INFRASTRUCTURE VIRTUELLE

Cette étape permet de modifier les paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle VMware. Ces paramètres interviennent dans le fonctionnement des machines virtuelles de protection en vue d'obtenir des informations sur l'infrastructure virtuelle.

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

- Dans la fenêtre **Type de connexion**, sélectionnez une des options suivantes :
  - **Connexion au serveur VMware vCenter**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection reçoivent les informations relatives à l'infrastructure virtuelle directement du serveur VMware vCenter.
  - **Connexion au Serveur d'intégration**. Sélectionnez cette option si vous souhaitez que les machines virtuelles de protection obtiennent les informations sur l'infrastructure virtuelle auprès du Serveur d'intégration connecté au serveur VMware vCenter (cf. section "A propos du Serveur d'intégration" à la page 22).

Si vous souhaitez utiliser la connexion au Serveur d'intégration, il faudra, avant de lancer la modification de la configuration des machines virtuelles de protection, installer le Serveur d'intégration et configurer les paramètres de connexion de celui-ci au serveur VMware vCenter (cf. section "Installation du Serveur d'intégration" à la page 28).

Les machines virtuelles de protection dotées de la version antérieure de l'application ne prennent pas en charge la connexion au Serveur d'intégration. Si vous avez choisi dans le cadre de la modification de la configuration des machines virtuelles de protection dotées d'une version de l'application inférieure à Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1, l'Assistant affiche un message d'erreur. Vous pouvez modifier la liste des machines virtuelles de protection dont il faut modifier la configuration ou sélectionner une connexion directe au serveur VMware vCenter pour toutes les machines virtuelles de protection.

- **Adresse** : adresse IP au format IPv4 ou nom de domaine complet du nom du serveur VMware vCenter ou du Serveur d'intégration.
- **Nom d'utilisateur** : nom du compte utilisateur sous lequel la connexion de la machine virtuelle de protection au serveur VMware vCenter ou au Serveur d'intégration s'opère :
  - Si vous avez choisi la connexion au serveur VMware vCenter, 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.
  - Si vous avez choisi la connexion au Serveur d'intégration, indiquez le nom d'utilisateur *svm*.
- **Mot de passe** : mot de passe du compte utilisateur sous lequel la connexion des machines virtuelles au serveur VMware vCenter s'opère.
- **Action de la machine virtuelle de protection en cas de détection d'une erreur de certificat** : action que va exécuter la machine virtuelle de protection lors de la connexion au serveur VMware vCenter ou au Serveur d'intégration si le certificat de serveur obtenu contient une erreur ou ne correspond pas à un certificat installé antérieurement. Options possibles :
  - **Annuler la connexion, indiquer une erreur** : la machine virtuelle de protection annule la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center.
  - **Poursuivre la connexion, indiquer une erreur** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration et transmet les informations relatives à l'erreur à Kaspersky Security Center. Cette option est sélectionnée par défaut.
  - **Ignorer** : la machine virtuelle de protection maintient la connexion au serveur VMware vCenter ou au Serveur d'intégration.

Passez à l'étape suivante de l'Assistant.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter ou au Serveur d'intégration avec les paramètres définis.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de modification de la configuration.

ETAPE 6. MODIFICATION DU MOT DE PASSE KLCONFIG

Cette étape permet de modifier le mot de passe utilisé pour modifier la configuration des machines virtuelles de protection.

Pour ce faire, choisissez l'option **Modifier le mot de passe** et saisissez le nouveau mot de passe 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 la modification de la configuration 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 hyperviseurs 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 hyperviseurs 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 de la configuration des machines virtuelles de protection sur les hyperviseurs 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.

SUPPRESSION DE L'APPLICATION

Cette section comprend des informations sur la suppression des modules Anti-Virus Fichiers et Détection des intrusions de Kaspersky Security.

DANS CETTE SECTION

ORDRE DES ETAPES DE SUPPRESSION DE L'APPLICATION

La suppression de l'application Kaspersky Security de l'infrastructure virtuelle VMware comprend les étapes suivantes :

1. suppression du module (cf. section "Procédure d'installation du Serveur d'intégration et de la Console de gestion" à la page 28) Anti-Virus Fichiers. (cf. section "Suppression du module Anti-Virus Fichiers" à la page 96) La suppression du module Anti-Virus Fichiers s'opère via la suppression de machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi.

2. Procédure de suppression du module Détection des intrusions. La suppression du module Détection des intrusions de l'infrastructure virtuelle VMware s'opère à l'aide de la procédure de suppression totale (cf. section "Procédure de suppression totale du module Détection des intrusions" à la page 104).

   Si vous souhaitez supprimer le module Détection des intrusions uniquement sur les hyperviseurs VMware ESXi qui figurent dans les clusters VMware sélectionnés, utilisez la procédure de suppression sélective (cf. section "Procédure de suppression des machines virtuelles de protection dotées du module Détection des intrusions" à la page 100).

3. Suppression du plug-in d'administration de Kaspersky Security. Vous pouvez supprimer le plug-in d'administration de Kaspersky Security à l'aide des méthodes standard de suppression des applications du système d'exploitation.

4. Suppression du module Serveur d'intégration (cf. section "Suppression du serveur d'intégration" à la page 105).

Après la suppression sur les hyperviseurs, 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 dotées du module Anti-Virus Fichiers 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 hyperviseurs 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.

SUPPRESSION DU MODULE ANTI-VIRUS FICHIERS

Cette section contient des informations sur la suppression du module Anti-Virus Fichiers.

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

PRESENTATION DE LA SUPPRESSION DU MODULE ANTI-VIRUS FICHIERS

La suppression du module Anti-Virus Fichiers s'effectue via la suppression des machines virtuelles de protection dotées du module Anti-Virus Fichiers sur les hyperviseurs VMware ESXi (cf. section "Procédure de suppression du module Anti-Virus Fichiers" à la page 96). Vous pouvez supprimer les machines virtuelles de protection sur tous les hyperviseurs VMware ESXi qui appartiennent au cluster KSC ou procéder à une sélection.

Pendant la suppression des machines virtuelles de protection sur les hyperviseurs 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.

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

- **Serveur VMware vCenter**. Offre des informations sur les hyperviseurs 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 Manager.

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 Anti-Virus Fichiers.

Pour supprimer le module Anti-Virus 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.
4. Dans la fenêtre qui s'ouvre, choisissez l'option **Anti-Virus Fichiers** 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 AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de suppression.

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

ETAPE 3. SELECTION DES HYPERVISEURS VMWARE ESXI.

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

Les colonnes du tableau reprennent les informations relatives aux hyperviseurs VMware ESXi administrés par le serveur VMware vCenter sélectionné sur lesquels la machine virtuelle de protection est installée :

- **Hyperviseur VMware ESXi** : adresse IP ou nom de domaine de l'hyperviseur.
- **Version de l'application** : numéro de la version de l'application Kaspersky Security installée sur la machine virtuelle de protection de cet hyperviseur.
- **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 hyperviseur VMware ESXi, cochez la case en regard de son nom dans le tableau. Vous pouvez uniquement sélectionner les hyperviseurs 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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** 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 hyperviseurs 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 hyperviseurs 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 hyperviseurs 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 hyperviseurs 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.

PROCEDURE DE SUPPRESSION DU MODULE DETECTION DES INTRUSIONS

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

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

PRESENTATION DE LA SUPPRESSION DU MODULE DETECTION DES INTRUSIONS

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

La suppression du module Détection des intrusions 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 intrusions se définissent à l'aide de l'Assistant de suppression totale (cf. section "Procédure de suppression totale du module Détection des intrusions" page 104). 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 hyperviseurs VMware ESXi entrant dans la composition de toutes les clusters VMware ;
- annule l'enregistrement des machines virtuelles de protection du module Détection des intrusions (service de Kaspersky Network Protection) dans VMware vShield Manager.

La suppression sélective du module Détection des intrusions s'effectue via la suppression des machines virtuelles de protection dotées du module Détection des intrusions sur les hyperviseurs VMware ESXi entrant dans la composition des clusters VMware sélectionnés. Les paramètres de suppression des machines virtuelles de protection sur les hyperviseurs 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 intrusions" page 100). 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 hyperviseurs VMware ESXi entrant dans la composition des clusters VMware sélectionnées ;
- annule l'enregistrement des machines virtuelles de protection dans VMware vShield Manager.

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

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

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

- **Serveur VMware vCenter**. Fournit des informations au sujet des hyperviseurs 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 hyperviseurs VMware ESXi, l'annulation de l'enregistrement des machines virtuelles de protection et du module Détection des intrusions (service de Kaspersky Network Protection) dans VMware vShield Manager.

PROCEDURE DE SUPPRESSION DES MACHINES VIRTUELLES DE PROTECTION DOTEES DU MODULE DETECTION DES INTRUSIONS

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

Pour supprimer les machines virtuelles de protection dotées du module Détection des intrusions, 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Détection des intrusions** 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 intrusions**.

Passez à l'étape suivante de l'Assistant.

ETAPE 2. CONNEXION AU SERVEUR VMWARE VCENTER

Cette étape permet de définir les paramètres de connexion de l'Assistant au serveur VMware vCenter :

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

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.

L'Assistant vérifiera la possibilité de se connecter au serveur VMware vCenter avec le nom et le mot de passe du compte indiqué. Si ce compte ne possède pas les autorisations suffisantes (cf. section "Comptes utilisateur du serveur VMware vCenter" à la page 24), l'Assistant le signale et ne passe pas à l'étape suivante.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** pour continuer la procédure de suppression.

S'il n'est pas possible d'établir la connexion au serveur VMware vCenter, vérifiez les paramètres de connexion saisis. Si les paramètres de connexion ont été correctement saisis, quittez l'Assistant, vérifiez que le serveur VMware vCenter 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 d'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.

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

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

Cliquez sur **Poursuivre** dans la fenêtre **Analyse du certificat** 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 d'accès au fichier OVF de la machine virtuelle de protection déployée sur les clusters VMware administrés par le serveur VMware vCenter 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 hyperviseurs desquels il faut supprimer les machines virtuelles de protection dotées du module Détection des intrusions.

Les colonnes du tableau affichent les informations relatives à l'ensemble des clusters VMware administré par un serveur VMware vCenter :

- **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 hyperviseurs VMware ESXi entrant dans la composition de ce cluster VMware.
  - **Non protégé** : des machines virtuelles de protection ne sont pas installées sur les hyperviseurs 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 administrés par un serveur VMware vCenter :

- **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 hyperviseurs 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 hyperviseurs 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 hyperviseurs 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 hyperviseurs VMware ESXi peuvent être consultées dans VMware vSphere Client (dans la fenêtre **Recent Tasks**).

PROCEDURE DE SUPPRESSION TOTALE DU MODULE DETECTION DES INTRUSIONS

Pour supprimer complètement le module Détection des intrusions, 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** dans la zone de travail du groupe **Déploiement** pour lancer l'Assistant.

   Si vous aviez configuré l'enregistrement des informations détaillées dans l'Assistant (cf. section "Collecte des informations détaillées pendant le fonctionnement de l'Assistant" à la page 110), la fenêtre **Collecte des informations détaillées pendant le fonctionnement de l'Assistant** s'ouvre. Passez à l'étape suivante de l'Assistant.

   L'activation de la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security est possible uniquement lors de l'installation et de la mise à jour du module Anti-Virus Fichiers.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Détection des intrusions** 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 intrusions**.

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 d'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.

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

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

Pour poursuivre la procédure de suppression totale du module Détection des intrusions, cliquez que le bouton **Continuer** dans la fenêtre **Analyse du certificat**.

ETAPE 3. FIN DE LA SAISIE DES PARAMETRES

Tous les paramètres indispensables à la suppression totale du module Détection des intrusions 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 intrusions.

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 intrusions.

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

SUPPRESSION DU SERVEUR D'INTEGRATION

Vous pouvez supprimer le Serveur d'intégration et la Console de gestion du Serveur d'intégration à l'aide des méthodes standard de suppression des applications du système d'exploitation.

Lors de la suppression du Serveur d'intégration de l'ordinateur, toutes les données conservées sont supprimées :

- les paramètres de connexion du Serveur d'intégration au serveur VMware vCenter ;
- les paramètres de connexion des machines virtuelles de protection et de la Console de gestion du Serveur d'intégration ;
- le certificat SSL du Serveur d'intégration ;
- les journaux de fonctionnement du Serveur d'intégration et de la Console de gestion du Serveur d'intégration, si vous aviez activé la consignation des informations relatives au fonctionnement du Serveur d'intégration dans les journaux de fonctionnement (cf. section "Collecte des informations sur le fonctionnement du Serveur d'intégration" à la page 111).

Si la Console de gestion a été installée séparément, vous pouvez la supprimer à l'aide des outils standard de suppression d'applications du système d'exploitation. Lors de la suppression de la Console de gestion de l'ordinateur, toutes les données conservées par celle-ci pendant son fonctionnement sont également supprimées.

Si votre infrastructure virtuelle contient des machines virtuelles de protection qui reçoivent les informations relatives à l'infrastructure virtuelle depuis le Serveur d'intégration, vous devrez, après la suppression du Serveur d'intégration, réaliser une procédure de modification de la configuration pour ces machines virtuelles de protection (cf. section "Modification de la configuration des machines virtuelles de protection dotées du module Anti-Virus Fichiers" à la page 90). A l'étape "Modification des paramètres de connexion des machines virtuelles de protection à l'infrastructure virtuelle", configurez la connexion des machines virtuelles de protection au serveur VMware vCenter.

CONTACTER LE SUPPORT TECHNIQUE

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

DANS CETTE SECTION

PRESENTATION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans d'autres sources d'informations relatives à l'application (cf. section "Sources d'informations sur l'application "à la page 10), contactez le Support Technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Le support technique est offert uniquement aux utilisateurs qui ont acheté une licence commerciale de l'application. Les utilisateurs qui disposent d'une licence d'évaluation n'ont pas droit au support technique.

Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du Support Technique de l'une des manières suivantes :

- contacter le Support Technique de Kaspersky Lab par téléphone ;
- envoyer une requête au Support Technique de Kaspersky Lab via le service Internet Kaspersky CompanyAccount.

SUPPORT TECHNIQUE PAR TELEPHONE

Vous pouvez téléphoner aux experts du Support Technique de Kaspersky Lab dans la plupart des régions. Vous pouvez trouver des informations sur les moyens de bénéficier de l'aide du Support technique dans votre région ainsi que les coordonnées du Support technique sur le site Internet du Support Technique de Kaspersky Lab" (http://support.kaspersky.com/fr/b2b).

Avant de contacter le Support technique, il est recommandé de lire les règles d'octroi du support technique (http://support.kaspersky.com/fr/support/rules). Ces règles contiennent des informations telles que les heures d'appel au Support Technique de Kaspersky Lab ou les données dont les experts du Support Technique de Kaspersky Lab auront besoin pour vous aider.

SUPPORT TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un service en ligne réservé aux organisations qui utilisent des applications de Kaspersky Lab. Le service en ligne Kaspersky CompanyAccount est destiné à l'interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le service en ligne Kaspersky CompanyAccount permet de suivre l'état du traitement des requêtes électroniques par les experts de Kaspersky Lab et de conserver un historique des requêtes électroniques.

Vous pouvez inscrire tous les collaborateurs de votre organisation au sein d'un seul compte Kaspersky CompanyAccount. Un compte permet de gérer centralement les requêtes électroniques envoyées par les collaborateurs de l'organisation à Kaspersky Lab et de gérer les autorisations de ces collaborateurs dans le Kaspersky CompanyAccount.

Le service en ligne Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;
- français ;
- japonais.

Pour en savoir plus sur Kaspersky CompanyAccount, consultez le site du Support Technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

COLLECTE D'INFORMATIONS POUR LE SUPPORT TECHNIQUE

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander de générer un rapport contenant les informations suivantes :

- paramètres de configuration de l'image de la machine virtuelle ;
- version de l'hyperviseur VMware ESXi ;
- version du serveur VMware vCenter ;
- version du module VMware vShield Endpoint ;
- version de la distribution VMware Tools installée sur la machine virtuelle protégée ;
- liste des technologies VMware utilisées (View, DRS, DPM, HA, FT) ;
- version du Kaspersky Security Center ;
- pour l'ordinateur sur lequel l'application Kaspersky Security Center est installée : la version du système d'exploitation et la version de Microsoft .NET Framework.

Le rapport obtenu doit ensuite être envoyé au Support technique.

Il peut être nécessaire de désactiver la fonction d'annulation des modifications en vue de l'analyse des erreurs survenues au cours de l'installation ou de la mise à jour de la machine virtuelle de protection. Pour désactiver la fonction d'annulation des modifications, vous devez modifier le fichier KsvInstaller.exe.config. Ce fichier est situé sur l'ordinateur hébergeant la Console d'administration de Kaspersky Security Center qui est à l'origine de l'installation des machines virtuelles de protection (cf. informations détaillées sur la page de l'application dans la Base de connaissances http://support.kaspersky.com/fr/11696).

Pour analyser les erreurs de fonctionnement de Kaspersky Security, les spécialistes du Support Technique peuvent vous demander de recourir aux utilitaires suivants inclus dans la distribution de l'application :

- inventory_view_format_client, inventory_view_tree_client : utilitaires permettant de collecter des informations à propos de l'infrastructure virtuelle VMware ;
- licenser_client : utilitaire destiné à l'administration des clés et à la consultation des informations relatives à la licence ;
- qb_client : utilitaire destiné à l'utilisation des copies de sauvegarde des fichiers dans la sauvegarde ;
- tracer_configurator_client : utilitaire permettant de configurer les paramètres de saisie des journaux de Kaspersky Security ;
- updater_client : utilitaire permettant d'exécuter la mise à jour des bases antivirus ou la remise à l'état antérieur à la mise à jour ;
- vcenter_creds : utilitaire destiné à la consultation ou à la modification des paramètres de connexion de la machine virtuelle de protection au serveur VMware vCenter ou au Serveur d'intégration ;
- vcenter_creds_test_client : utilitaire permettant d'établir une connexion test entre la machine virtuelle de protection et le serveur VMware vCenter ou le Serveur d'intégration en vue de la vérification des paramètres de connexion ;
- vshield_manager_client : utilitaire permettant d'exécuter l'enregistrement, l'annulation de l'enregistrement et la vérification de l'enregistrement des machines virtuelles de protection dotées du module Anti-Virus Fichiers dans VMware vShield Manager ;
- klmover : utilitaire permettant de modifier l'adresse du Serveur d'administration de Kaspersky Security Center et le mode d'échange des données dans les paramètres de configuration des machines virtuelles de protection.

Des informations détaillées sur l'exploitation des utilitaires sont disponibles sur la page dédiée à l'application dans la base de connaissances (http://support.kaspersky.com/fr/11079).

JOURNAUX DE KASPERSKY SECURITY

Par défaut, les journaux suivants reprennent les informations relatives au déroulement de l'installation, de la mise à jour, de la suppression et de la modification de la configuration des machines virtuelles de protection, ainsi que les informations relatives au fonctionnement des modules de l'application Kaspersky Security :

- Journal de fonctionnement de l'Assistant. Le journal contient les informations relatives aux actions de l'Assistant et aux erreurs survenues pendant son fonctionnement. Le journal de fonctionnement de l'Assistant est enregistré dans le fichier ksvinst_aaaa-mm-jj-hh-mm-ss.log, où aaaa-mm-jj-hh-mm-ss représente la date et l'heure d'enregistrement du fichier. Le fichier du journal de fonctionnement de l'Assistant se trouve sur l'ordinateur doté de la Console d'administration de Kaspersky Security Center à partir de laquelle vous réalisez les tâches d'installation, de mise à jour, de suppression et de modification de la configuration des machines virtuelles de protection. Le dossier d'enregistrement du fichier du journal de fonctionnement de l'Assistant varie en fonction du système d'exploitation utilisé :
  - pour les systèmes d'exploitation 64 bits : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV2.plg\Installer\DeploymentTrace ;
  - pour les systèmes d'exploitation 32 bits : %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV2.plg\Installer\DeploymentTrace.

- Journaux de fonctionnement de Kaspersky Security. Ces journaux reprennent les informations relatives au fonctionnement des modules de Kaspersky Security, notamment les données concernant les menaces détectées et les erreurs survenues au cours de l'exécution de ces modules. Par défaut, les journaux de fonctionnement de Kaspersky Security sont enregistrés sur les machines virtuelles de protection dans les fichiers suivants :
  - Machine virtuelle de protection dotée du module Anti-Virus Fichiers :
    - /var/log/ksv ;
    - /var/log/klnagent ;
    - /var/log/kaspersky/ksv/connector.log ;
    - /var/log/messages ;
    - /var/log/kaspersky/ksv/wdserver.log ;
  - machine virtuelle de protection dotée du module Détection des intrusions :
    - /var/log/ksvns ;
    - /var/log/klnagent ;
    - /var/log/kaspersky/ksvns/connector.log.

Les informations consignées dans le journal de fonctionnement de l'Assistant et dans les journaux de fonctionnement de Kaspersky Security ne sont pas envoyées automatiquement à Kaspersky Lab. Vous pouvez utiliser les journaux lorsque vous demandez l'aide du Service de Support Technique. Les informations consignées dans les journaux peuvent être requises pour analyser et comprendre les erreurs survenues pendant l'exécution des modules de l'application, ainsi qu'au cours de la mise à jour, de la suppression ou de la modification de la configuration des machines virtuelles de protection.

Les journaux ne sont pas chiffrés. Il est dès lors conseillé de garantir la protection de ces données contre les accès non autorisé.

DANS CETTE SECTION

COLLECTE DES INFORMATIONS DETAILLEES PENDANT LE FONCTIONNEMENT DE L'ASSISTANT

Avant de lancer l'installation, la mise à jour, la suppression ou la modification de la configuration des machines virtuelles de protection, vous pouvez configurer la consignation des informations détaillées dans le journal de fonctionnement de l'application. Kaspersky Security consigne dans les journaux toutes les informations indispensables au diagnostic du fonctionnement de l'application, à savoir tous les paramètres saisis par l'utilisateur (à l'exception des mots de passe=, les informations relatives aux actions des machines virtuelles de protection, les informations relatives aux erreurs, ainsi que les informations relatives aux échanges réseau avec VMware vShield Manager.

Les explications sur la configuration de la consignation des détails dans le journal de fonctionnement de l'Assistant peuvent être obtenues auprès des experts du Support Technique (cf. section "Présentation du support technique" à la page 107).

Si vous avez configuré la consignation des informations détaillées dans le journal de fonctionnement de l'Assistant, un message qui rappelle que les informations détaillées seront consignées dans le journal de fonctionnement s'affiche après le lancement de l'Assistant.

Cette fenêtre permet de configurer la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security sur la machine virtuelle de protection dotée du module Anti-Virus Fichiers. Les experts du Support Technique peuvent solliciter la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security afin de pouvoir analyser les erreurs d'installation du module Anti-Virus Fichiers.

Il est conseillé d'activer la consignation des informations détaillées dans les journaux de fonctionnement de Kaspersky Security uniquement à la demande des experts du Support Technique.

Si vous avez configuré la consignation des informations détaillées, les journaux de fonctionnement de Kaspersky Security sont enregistrés dans les fichiers suivants sur les machines virtuelles de protection :

- /var/log/kaspersky/ksv/ksvmain.log ;
- /var/log/kaspersky/ksv/connector.log ;
- /var/log/kaspersky/klnagent/klnagent.log.

COLLECTE DES INFORMATIONS SUR LE FONCTIONNEMENT DU SERVEUR D'INTEGRATION

En cas de problème lors du fonctionnement du Serveur d'intégration, les experts du Support Technique pourrait vous demander d'envoyer le journal de fonctionnement du Serveur d'intégration et/ou de la Console de gestion du Serveur d'intégration. Par défaut, la consignation d'informations dans les journaux de fonctionnement du Serveur d'intégration et de sa console de gestion est désactivée.

Pour activer la consignation des informations sur le fonctionnement des modules du Serveur d'intégration dans les journaux, procédez comme suit :

1. Ouvrez les fichiers KsvServerConsole.exe.config et KsvServerService.exe.config, situés dans le dossier d'installation du Serveur d'intégration, dans un éditeur de texte en vue de les modifier.

   Si la Console de gestion a été installée séparément du Serveur d'intégration, le fichier KsvServerConsole.exe.config se trouvera dans le dossier d'installation de la Console de gestion du Serveur d'intégration.

2. Modifiez les fichiers sur la base des instructions des experts du Support Technique ou selon les recommandations reprises dans les fichiers.

3. Enregistrez et fermez les fichiers KsvServerConsole.exe.config et KsvServerService.exe.config.

4. Relancez la Console de gestion du Serveur d'intégration et le service *Serveur d'intégration de Kaspersky Security for Virtualization*.

Kaspersky Security consignera désormais les informations relatives au fonctionnement des modules du Serveur d'intégration dans les journaux de fonctionnement du Serveur d'intégration. Ces journaux sont enregistrés dans le dossier %ProgramData%\Kaspersky Lab\VIIS\traces\ de l'ordinateur où sont installés les modules du Serveur d'intégration.

UTILISATION DU FICHIER DE TRAÇAGE

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander d'envoyer le fichier de traçage de la machine virtuelle de protection.

Pour savoir comment obtenir le fichier de traçage de la machine virtuelle de protection, consultez la page dédiée à l'application dans la Base des connaissances http://support.kaspersky.com/fr/11049.

UTILISATION DES FICHIERS DE STATISTIQUES SYSTEME

Une fois que les experts du Support Technique sont au courant du problème survenu, ils peuvent vous demander d'envoyer le fichier de statistiques système de la machine virtuelle de protection.

Pour savoir comment obtenir le fichier de statistiques système de la machine virtuelle de protection, consultez la page dédiée à l'application dans la Base des connaissances http://support.kaspersky.com/fr/11051.

GLOSSAIRE

A

ACTIVATION DE L'APPLICATION

Procédure d'activation de la licence permettant l'utilisation de l'ensemble des fonctions de la version de l'application tout au long de la durée de validité de la licence.

AGENT D'ADMINISTRATION

Module de l'application Kaspersky Security Center qui crée une interaction entre le Serveur d'administration et les modules de l'application Kaspersky Security installés sur les machines virtuelles de protection. Le module Agent d'administration est unique pour tous les programmes Windows faisant partie des produits de Kaspersky Lab. Pour les applications Novell®-, Unix™- et Mac® de Kaspersky Lab, il existe d'autres versions de l'Agent d'administration.

C

CERTIFICAT DE LICENCE

Document qui vous est transmis avec le fichier clé ou le code d'activation de Kaspersky Lab. Le document contient les informations sur la licence fournie.

CLUSTER KSC

Regroupement dans l'application Kaspersky Security Center de machines virtuelles de protection installées sur des hyperviseurs VMware ESXi administrés par un serveur VMware vCenter et des machines virtuelles qu'elles protègent.

CLE

Séquence unique de chiffres et de lettres. La clé permet l'utilisation de l'application conformément aux conditions du Contrat de licence (au type de licence, à la durée de validité de la licence, aux restrictions imposées par la licence).

CLE ACTIVE

Clé utilisée lors du fonctionnement de l'application.

CLE AVEC LIMITATION EN FONCTION DU NOMBRE DE CŒURS

Clé de l'application de protection des machines virtuelles, quel que soit le type de système d'exploitation installé. En fonction des restrictions imposées par la licence, l'application intervient dans la protection de toutes les machines virtuelles avec des systèmes d'exploitation invités Windows installés sur les hyperviseurs VMware ESXi dans lesquels un nombre défini de cœurs de processeurs physiques est utilisé.

CLE COMPLEMENTAIRE

Clé confirmant le droit d'utilisation de l'application mais qui ne s'utilise pas lors du fonctionnement.

CLE POUR POSTE DE TRAVAIL

Clé de l'application en vue de protéger les machines virtuelles dotées d'un système d'exploitation pour postes de travail.

CLE POUR SERVEUR

Clé l'application en vue de protéger les machines virtuelles dotées d'un système d'exploitation pour serveurs.

CODE D'ACTIVATION

Code vous offrant un accès à Kaspersky Lab suite à l'activation d'une licence d'évaluation ou à l'acquisition de la licence commerciale pour l'utilisation de Kaspersky Security. Ce code est nécessaire pour l'activation de l'application.

Le code d'activation est une suite de 20 caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

CONTRAT DE LICENCE UTILISATEUR FINAL

Accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions selon lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

COPIE DE SAUVEGARDE DU FICHIER

Copie d'un fichier de la machine virtuelle, créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde sont conservées dans la sauvegarde sous un format spécial et ne présentent aucun danger.

F

FICHIER CLE

Fichier de type xxxxxxxx.key vous offrant un accès à Kaspersky Lab suite à l'activation d'une licence d'évaluation ou à l'acquisition de la licence commerciale pour l'utilisation de Kaspersky Security. Le fichier clé est nécessaire pour l'activation de l'application.

G

GROUPE D'ADMINISTRATION

Ensemble d'ordinateurs reliés au Kaspersky Security Center conformément aux fonctions exécutables et aux applications Kaspersky Lab installées. Les ordinateurs sont regroupés pour plus de facilité, dans la mesure où ils sont gérés comme une seule entité. Le groupe d'administration peut inclure d'autres groupes. Pour chacune des applications installées dans le groupe d'administration, des stratégies propres à chaque groupe peuvent être définies. Chaque groupe peut également se voir attribuer des tâches.

I

INFRASTRUCTURE PROTEGEE DU CLUSTER KSC

Objets d'administration VMware administré par le serveur VMware vCenter correspondant au cluster KSC.

K

KASPERSKY COMPANYACCOUNT

Service Internet conçu pour l'envoi de demandes électroniques à Kaspersky Lab et le suivi de leur traitement par les spécialistes.

KASPERSKY SECURITY NETWORK (KSN)

Infrastructure de services en ligne et de services fournissant un accès à la base opérationnelle de connaissances de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit le nombre de faux positifs.

L

LICENCE

Droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du contrat de licence.

M

MACHINE VIRTUELLE DE PROTECTION

Machine virtuelle sur l'hyperviseur VMware ESXi hébergeant le module de l'application Kaspersky Security.

O

OBJET OLE

Objet qui est lié à un autre fichier ou inclus dans un autre fichier utilisant la technologie Object Linking and Embedding (OLE). Par exemple, l'objet OLE peut être un tableau Microsoft Office Excel® inclus dans un document Microsoft Office Word.

P

PROFIL DE PROTECTION

Le profil de protection détermine dans la stratégie les paramètres de protection des machines virtuelles. Une stratégie peut contenir plusieurs profils de protection. Un profil de protection est attribué aux objets d'administration de VMware appartenant à l'infrastructure protégée du cluster KSC. Un objet d'administration VMware ne peut se voir attribuer qu'un seul profil de protection. La machine virtuelle de protection protège la machine virtuelle selon les paramètres définis dans le profil de protection qui lui a été attribué.

PROFIL DE PROTECTION RACINE

Profil de protection racine que vous générez pendant la création d'une stratégie. Le profil de protection racine est automatiquement attribué à l'objet racine de la structure des objets d'administration de VMware, à savoir le serveur VMware vCenter.

S

SAUVEGARDE

Sauvegarde spécialisée des copies des fichiers qui ont été supprimés ou modifiés durant la réparation.

SERVEUR D'ADMINISTRATION

Module de l'application Kaspersky Security Center qui remplit la fonction de sauvegarde centralisée des informations relatives aux applications Kaspersky Lab installées sur le réseau de l'organisation et qui gère ces informations.

SOURCE DES MISES A JOUR

Ressource qui contient les mises à jour des bases et des modules des applications de Kaspersky Lab. La source de mises à jour pour Kaspersky Security est un stockage du Serveur d'administration du Kaspersky Security Center.

STRATEGIE

Définit les paramètres de la protection des machines virtuelles contre les virus et autres programmes dangereux, les paramètres de la protection des machines virtuelles contre les intrusions et les paramètres des sauvegardes sur les machines virtuelles de protection.

T

TACHE D'AJOUT DE CLE

Ajoute la clé sur toutes les machines virtuelles de protection dans le cadre d'un cluster KSC, c'est à dire sur toutes les machines virtuelles installées sur les hyperviseurs VMware ESXi administrés par un serveur VMware vCenter.

TACHE D'ANALYSE COMPLETE

Définit les paramètres d'analyse des machines virtuelles de tous les clusters.

TACHE D'ANALYSE PERSONNALISEE

Définit les paramètres d'analyse des machines virtuelles qui appartiennent au cluster KSC indiqué.

TACHE DE DIFFUSION DES MISES A JOUR

Au cours de cette tâche, le Kaspersky Security Center peut diffuser et installer automatiquement les mises à jour des bases antivirus sur les machines virtuelles de protection.

TACHE DE REMISE A L'ETAT ANTERIEUR A LA DERNIERE MISE A JOUR

Au cours de cette tâche, le Kaspersky Security Center revient à l'état antérieur à la dernière mise à jour des bases antivirus sur les machines virtuelles de protection.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de systèmes de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

PRODUITS. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les réseaux informatiques d'entreprise.

La gamme de logiciels pour particuliers reprend des applications antivirus pour ordinateurs de bureau et ordinateurs portables, ainsi que des applications pour la protection des tablettes, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace et automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de multiples plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils détectent des centaines de nouvelles menaces informatiques, développent des outils d'identification et de neutralisation contre ces menaces, et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont mises à jour toutes les heures*, tandis que *les bases antispam* sont mises à jour *toutes les 5 minutes*.

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (E-U), Alt-N Technologies (E-U), Blue Coat Systems (E-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (E-U), Openwave Messaging (Irlande), D-Link (Taïwan), M86 Security (E-U), GFI Software (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), Netasq+Arkoon (France), NETGEAR (E-U), Parallels (E-U), SonicWALL (E-U), WatchGuard Technologies (E-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. La société compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.viruslist.com/fr
Laboratoire d'étude des virus :	http://newvirus.kaspersky.com/fr (pour l'analyse des fichiers et sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATION SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

AVIS DE MARQUES COMMERCIALES

Les marques et marques de service déposées appartiennent à leurs propriétaires respectifs.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans d'autres pays.

Mac : marque déposée Apple Inc.

Microsoft, Windows, Excel et Windows Server sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Novell est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

SUSE est une marque commerciale de SUSE LLC déposée aux Etats-Unis et dans d'autres pays.

UNIX est une marque utilisant une licence X/Open Company Limited déposée aux Etats-Unis et dans d'autres pays.

VMware, VMware vSphere, vShield, vCenter, VMware vCloud, ESX sont des marques commerciales ou déposées de VMware, Inc, enregistrées aux Etats-Unis ou dans d'autres juridictions de VMware, Inc.

INDEX