KASPERSKY lab

Kaspersky Security for Virtualization 4.0 Light Agent for Windows

Manuel de l'utilisateur pour Windows

Version de l'application : 4.0

Cher utilisateur,

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

Date d'édition : 20/01/2017

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

Table des matières

Présentation du manuel

Le manuel de l'utilisateur Kaspersky Security for Virtualization 4.0 Light Agent (ci-après, " Kaspersky Security ") est adressé aux spécialistes qui réalisent la configuration du Light Agent installé sur la machine virtuelle dotée du système d'exploitation Microsoft® Windows® (ci-après, " Light Agent for Windows ").

Pour utiliser Kaspersky Security, l'utilisateur doit connaître l'interface du système d'exploitation Microsoft Windows, maîtriser ses fonctionnalités principales, et savoir utiliser une messagerie électronique et Internet.

Dans cette section

Dans ce document

Ce document contient les sections suivantes :

Kaspersky Security for Virtualization 4.0 Light Agent (cf. page 17)

Cette section contient des informations sur le rôle, les capacités principales et le contenu de l'application ainsi qu'un aperçu de ses fonctions et de ses modules.

Interface de l'application (à la page 21)

Cette section explique les éléments fondamentaux de l'interface de l'application.

Lancement et arrêt de l'application (cf. page 26)

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

Etat de la protection de la machine virtuelle (cf. page 30)

Cette section contient des informations sur la configuration de la détection des menaces de sécurité et sur les options de protection contre ces menaces.

Connexion de la machine virtuelle protégée à la SVM (cf. page 34)

Cette section contient des informations sur les particularités et la configuration de la connexion de la machine virtuelle protégée à la SVM.

Protection du système de fichiers de la machine virtuelle. Antivirus Fichiers (cf. page 38)

Cette section contient des informations sur l'Antivirus Fichiers et des instructions sur la configuration du module.

Protection du courrier. Antivirus Courrier (cf. page 54)

Cette section contient des informations sur l'Antivirus Courrier et les instructions sur la configuration du module.

Protection du trafic Internet de la machine virtuelle. Antivirus Internet (cf. page 68)

Cette section contient des informations sur l'Antivirus Internet et les instructions sur la configuration du module.

Protection du trafic des clients IM. Antivirus IM (cf. page 80)

Cette section contient des informations sur l'Antivirus IM et les instructions sur la configuration des paramètres du module.

Protection réseau (cf. page 86)

Cette section contient les informations sur les principes de fonctionnement et sur la configuration des modules Pare-feu, Prévention des intrusions et Surveillance du réseau, ainsi que sur le contrôle du trafic réseau.

Surveillance du système (cf. page 131)

Cette section contient des informations sur la Surveillance du système et les instructions sur la configuration des paramètres du module.

Contrôle du lancement des applications (cf. page 136)

Cette section contient des informations sur le Contrôle du lancement des applications et les instructions sur la configuration du module.

Contrôle de l'activité des applications (cf. page 152)

Cette section contient des informations sur le Contrôle de l'activité des applications et les instructions sur la configuration des paramètres du module.

Contrôle des périphériques (cf. page 172)

Cette section contient des informations sur le Contrôle des périphériques et les instructions sur la configuration du module.

Contrôle Internet (cf. page 189)

Cette section contient des informations sur le Contrôle Internet et les instructions sur la configuration du module.

Analyse de la machine virtuelle (cf. page 209)

Cette section présente les particularités et la configuration des tâches d'analyse, les niveaux de sécurité ainsi que les méthodes et technologies d'analyse. Elle explique également comment manipuler les fichiers non traités par Kaspersky Security lors de la recherche sur la machine virtuelle de virus et autres applications malveillantes.

Mise à jour des bases de données et des modules de l'application (cf. page 235)

Cette section contient des informations sur la mise à jour des bases et des modules de l'application (ci-après mises à jour) et les instructions sur la configuration de la mise à jour.

Zone de confiance (cf. page 241)

Cette section présente des informations sur la zone de confiance et explique comment configurer les règles d'exclusion et composer une liste d'applications de confiance.

Sauvegarde (cf. page 253)

Cette section explique comment configurer les paramètres de la Sauvegarde et comment utiliser celle-ci.

Utilisation des rapports (cf. page 260)

Cette section explique comment utiliser les rapports et en configurer les paramètres.

Notifications (cf. page 270)

Cette section contient des informations sur les notifications qui signalent les événements dans le fonctionnement de Kaspersky Security, ainsi que des instructions sur la configuration des notifications relatives aux événements.

Performances de Kaspersky Security et compatibilité avec d'autres applications (cf. page 275)

Cette section contient des informations sur les performances de Kaspersky Security et sur la compatibilité avec d'autres applications, ainsi que les instructions sur la sélection des types d'objets à détecter et le mode de fonctionnement de Kaspersky Security.

Autodéfense Kaspersky Security (cf. page 279)

Cette section contient des informations sur les mécanismes de l'autodéfense de l'application Kaspersky Security et de la protection contre l'administration externe de l'application, ainsi que les instructions sur la configuration de ces mécanismes.

Protection par mot de passe (cf. page 283)

Cette section contient des informations sur les restrictions d'accès à Kaspersky Security à l'aide d'un mot de passe.

Gestion des paramètres de l'application Kaspersky Security (cf. page 287)

Cette section contient les instructions pour le transfert des paramètres vers une application Kaspersky Security installée sur une autre machine virtuelle et pour la réinitialisation des paramètres par défaut de l'application.

Participation au Kaspersky Security Network (cf. page 291)

Cette section contient des informations relatives à la participation au Kaspersky Security Network et les instructions pour la vérification de la connexion au Kaspersky Security Network.

Glossaire (cf. page 294)

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

AO Kaspersky Lab (cf. page 298)

Cette section contient des informations sur AO Kaspersky Lab.

Information sur le code tiers (cf. page 300)

Cette section contient des informations sur le code tiers utilisé dans l'application.

Notifications sur les marques de commerce (cf. page 301)

Cette section présente une liste des marques commerciales d'autres propriétaires cités dans le document.

Index

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

Conventions

Des conventions sont utilisées dans ce document (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple du texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui peuvent avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations supplémentaires et de l'aide.
Exemple : …	Les exemples sont présentés sur un fond bleu sous le titre “Exemple”.

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

Kaspersky Security for Virtualization 4.0 Light Agent

Kaspersky Security for Virtualization 4.0. Light Agent est une solution intégrée assurant une protection avancée des machines virtuelles régies par les hyperviseurs Microsoft® Windows Server® avec Hyper-V® (ci-après “ Microsoft Windows Server (Hyper-V) “), Citrix® XenServer ou VMware ESXi™ ou KVM (Kernel-base Virtual Machine) contre différentes sortes de menaces, d'escroqueries et d'attaques réseau.

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

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

En plus de la protection en temps réel assurée par les modules de l'application, vous pouvez réaliser une recherche périodique d'éventuels virus et autres programmes dangereux sur votre machine virtuelle. Cette opération s'impose pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par l'application en raison, par exemple, d'un niveau de sécurité faible ou pour toute autre raison.

Modules de l'application

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

- **Contrôle du lancement des applications**. Ce module recense vos tentatives de lancement d'applications et régule le lancement d'applications.
- **Contrôle de l'activité des applications**. Ce module enregistre les actions réalisées par les applications sous le système d'exploitation de la machine virtuelle protégée et gère l'activité des applications en fonction du groupe dans lequel le module place chaque application. Il existe un ensemble de règles défini pour chaque groupe. Ces règles gèrent l'accès des applications à vos données personnelles et aux ressources du système d'exploitation. Les données personnelles de l'utilisateur comprennent le dossier “Mes documents”, les fichiers cookie, les informations sur l'activité du système d'exploitation,

ainsi que les fichiers, les dossiers et les clés de registre contenant les paramètres de fonctionnement et les informations importantes sur les applications les plus utilisées.

- **Contrôle des périphériques**. Ce module permet de définir des restrictions d'accès souples aux périphériques de stockage de données (tels que les disques durs, les disques amovibles, les CD/DVD), aux périphériques réseau (tels que les modems), aux périphériques d'impression (tels que les imprimantes) et aux interfaces permettant la connexion des périphériques à la machine virtuelle protégée (telles que les connexions USB, Bluetooth, FireWire®).

- **Contrôle Internet**. Ce module permet de configurer en toute souplesse des restrictions d'accès aux ressources Web pour différents groupes d'utilisateurs.

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

- Le Contrôle du lancement des applications utilise les règles de contrôle du lancement des applications.

- Le Contrôle de l'activité des applications utilise les règles du contrôle des applications.

- Le Contrôle des périphériques utilise les règles d'accès aux périphériques et les règles d'accès aux bus de connexion.

- Le Contrôle Internet utilise les règles d'accès aux ressources Web.

Les modules de protection sont les modules suivants :

- **Antivirus Fichiers**. Ce module permet d'éviter l'infection du système de fichiers du système d'exploitation de la machine virtuelle protégée. Le module est lancé au démarrage de Kaspersky Security. Il se trouve en permanence dans la mémoire opérationnelle et il analyse tous les fichiers ouverts, enregistrés et exécutés sous le système d'exploitation de la machine virtuelle protégée. L'Antivirus Fichiers intercepte toute sollicitation du fichier et recherche dans ce fichier la présence éventuelle de virus et d'autres applications malveillantes.

- **Surveillance du système**. Ce module récolte des données sur l'activité des applications sous le système d'exploitation de la machine virtuelle protégée et transmet ces informations aux autres modules afin de garantir une protection plus efficace.

- **Antivirus Courrier**. Ce module analyse l'ensemble des messages électroniques entrants et sortants à la recherche de virus et d'autres applications malveillantes.

- **Antivirus Internet**. Ce module analyse le trafic qui arrive sur la machine virtuelle protégée via les protocoles HTTP et FTP et définit si un lien appartient à la base des adresses Internet dangereuses ou de phishing.

- **Antivirus IM**. Ce module analyse le trafic entrant et sortant de la machine virtuelle protégée transmis via les clients IM. Ce module fonctionne en toute sécurité avec de nombreux clients IM.

- **Pare-feu**. Ce module assure la protection des données personnelles stockées dans le système d'exploitation de la machine virtuelle protégée de l'utilisateur en bloquant toutes les menaces éventuelles pour le système d'exploitation lorsque la machine virtuelle protégée est connectée à Internet ou au réseau local. Le module filtre toute activité réseau conformément à deux types de règles : règles réseau de l'application et règles pour les paquets réseau (voir section “A propos des règles réseau” p. 90).

- **Surveillance du réseau**. Ce module est prévu pour consulter en temps réel les informations sur l'activité réseau de la machine virtuelle protégée.

- **Prévention des intrusions**. Ce module recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre la machine virtuelle protégée, Kaspersky Security bloque l'activité réseau de l'ordinateur attaquant.

Tâches et fonctions de l'application

L'application Kaspersky Security prévoit les tâches suivantes :

- **Analyse complète**. Kaspersky Security effectue une analyse minutieuse du système d'exploitation de la machine virtuelle protégée, y compris la mémoire système, les objets chargés au démarrage, la sauvegarde du système d'exploitation et tous les disques durs et amovibles.

- **Analyse personnalisée**. Kaspersky Security analyse les objets sélectionnés par l'utilisateur.

- **Analyse des zones critiques**. Kaspersky Security analyse par défaut les objets chargés au démarrage du système d'exploitation de la machine virtuelle protégée, la mémoire système et les objets potentiellement infectés par les outils de dissimulation d'activité.

- **Mise à jour**. Kaspersky Security charge les mises à jour de la base et des modules de l'application. Ceci garantit que la protection du système d'exploitation de la machine virtuelle protégée est à jour contre les nouveaux virus et autres applications malveillantes.

Kaspersky Security inclut une série de fonctions de service qui servent à maintenir l'application à jour, à élargir les fonctions de l'application et à fournir de l'aide pendant l'utilisation de l'application :

- **Rapports**. Pendant le fonctionnement de l'application, celle-ci génère un rapport pour chaque module et chaque tâche de l'application. Le rapport contient la liste des événements survenus pendant le fonctionnement de Kaspersky Security et de toutes les opérations exécutées par l'application. En cas de problème, vous pouvez envoyer ces rapports aux experts du Support Technique de Kaspersky Lab afin qu'ils analysent la situation plus en détail.

- **Stockage des données**. Si l'application Kaspersky Security détecte des fichiers infectés lors de la recherche de virus et d'autres applications malveillantes dans le système d'exploitation de la machine virtuelle protégée, elle bloque les fichiers en question. Kaspersky Security sauvegarde les copies des fichiers réparés ou supprimés dans le *dossier de sauvegarde*. Kaspersky Security place les fichiers qui n'ont pas été traités, pour quelque raison que ce soit, sur la liste des fichiers non traités. Vous pouvez restaurer les fichiers dans leur dossier d'origine et nettoyer le stockage des données.

- **Notifications**. Les notifications vous informent sur l'état actuel de la protection du système d'exploitation de la machine virtuelle protégée et sur le fonctionnement de Kaspersky Security. Les notifications peuvent être affichées sur l'écran ou envoyées par email.

- **Support Technique**. Tous les utilisateurs inscrits de Kaspersky Security peuvent bénéficier de l'aide des experts du Support Technique de Kaspersky Lab. Vous pouvez envoyer une requête via le portail de Kaspersky CompanyAccount sur le site du Support Technique ou recevoir une assistance par téléphone (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

Interface de l'application

Cette section explique les éléments fondamentaux de l'interface de l'application.

Dans cette section

Icône de l'application dans la zone de notification

Dès que Kaspersky Security a été lancé, l'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows®.

L'icône de l'application remplit les fonctions suivantes :

- Elle indique le fonctionnement de l'application.
- Elle permet d'accéder au menu contextuel de l'icône de l'application et à la fenêtre principale de l'application.

L'icône de l'application renseigne l'état de la protection de la machine virtuelle et affiche les actions que l'application exécute actuellement :

- L'icône  indique que tous les modules de protection de l'application sont activés.
- L'icône  indique que Kaspersky Security analyse le message électronique.

- L'icône  indique que Kaspersky Security vérifie le trafic réseau entrant ou sortant.
- L'icône  indique que Kaspersky Security met à jour les bases et les modules de l'application.
- L'icône  indique que des événements importants se sont déroulés dans Kaspersky Security et qu'il faut y prêter attention. Par exemple, l'Antivirus Fichiers est désactivé ou les bases et les modules de l'application sont dépassés.
- L'icône  indique que des événements critiques se sont produits durant le fonctionnement de Kaspersky Security. Par exemple, échec d'un ou de plusieurs des modules, bases et modules endommagés.

L'animation de l'icône de l'application est désactivée par défaut. Vous pouvez activer l'animation de l'icône de l'application (cf. section " Activation et désactivation de l'animation de l'icône de l'application " à la page 22).

Activation et désactivation de l'animation de l'icône de l'application

► *Pour activer ou désactiver l'animation de l'icône de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Paramètres complémentaires** de la partie gauche de la fenêtre, sélectionnez la section **Interface**.

   Les paramètres de l'interface de l'application sont repris dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Si vous souhaitez activer l'animation de l'icône de l'application, cochez la case **Animer l'icône durant l'exécution des tâches**.
   - Si vous souhaitez désactiver l'animation de l'icône de l'application, décochez la case **Animer l'icône durant l'exécution des tâches**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Menu contextuel de l'icône de l'application

Pour ouvrir le menu contextuel de l'icône de l'application, placez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows, puis cliquez avec le bouton droit de la souris.

Le menu contextuel de l'icône de l'application reprend les options suivantes :

- **Kaspersky Security for Virtualization 4.0 Light Agent**. Ouvre la fenêtre principale de l'application à l'onglet **Statut de la protection**. L'onglet **Statut de la protection** vous permet de gérer le fonctionnement des modules et des tâches de l'application, et de consulter les statistiques relatives aux fichiers traités et aux menaces détectées.
- **Configuration**. Ouvre la fenêtre principale de l'application à l'onglet **Configuration**. L'onglet **Configuration** vous permet de modifier les paramètres par défaut de l'application.
- **Suspension de la protection et du contrôle/Rétablissement de la protection et du contrôle**. Désactive temporairement ou rétablit le fonctionnement des modules de protection et des modules de contrôle de l'application. Cette option du menu contextuel n'a aucune influence sur l'exécution de la mise à jour et des analyses. Elle est uniquement accessible lorsque la stratégie de Kaspersky Security Center est désactivée.
- **Désactivation de la stratégie/Activation de la stratégie**. Désactive ou active la stratégie de Kaspersky Security Center. Cet option est disponible si Kaspersky Security fonctionne selon la stratégie de Kaspersky Security Center et qu'un mot de passe pour désactiver la stratégie a été créé dans les paramètres de la stratégie.
- **A propos de l'application**. Ouvre une fenêtre contenant des informations sur l'application.
- **Terminer**. Entraîne l'arrêt de Kaspersky Security. Si vous choisissez cette option du menu contextuel, l'application est déchargée de la mémoire vive de la machine virtuelle.

Fenêtre principale de l'application

La fenêtre principale de Kaspersky Security réunit les éléments de l'interface qui vous permettent d'accéder aux principales fonctionnalités de l'application.

► *Pour ouvrir la fenêtre principale de Kaspersky Security, procédez d'une des manières suivantes :*

- positionnez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et cliquez avec le bouton gauche de la souris ;
- sélectionnez l'option **Kaspersky Security for Virtualization 4.0 Light Agent** dans le menu contextuel de l'icône de l'application (cf. section “ Menu contextuel de l'icône de l'application “ à la page 23) ;
- sélectionnez dans le menu **Démarrer** l'option **Applications** → **Kaspersky Security for Virtualization 4.0 Light Agent**.

La fenêtre principale de l'application contient trois parties :

- La partie supérieure de la fenêtre contient les éléments de l'interface qui permettent d'accéder aux informations suivantes :
  - informations sur l'application ;
  - statistiques des bases de données de réputation ;
  - liste des fichiers non traités ;
  - dossier de sauvegarde des fichiers infectés supprimés ou modifiés lors du fonctionnement de l'application ;
  - rapports sur les événements survenus pendant le fonctionnement de l'application dans son ensemble, de modules distincts et des tâches.
- La partie centrale de la fenêtre présente les onglets **Statut de la protection** et **Configuration** :
  - L'onglet **Statut de la protection** permet de réguler le fonctionnement des modules et des tâches de l'application. Lorsque vous ouvrez la fenêtre principale de l'application, l'onglet **Statut de la protection** s'affiche.
  - L'onglet **Configuration** permet de modifier les paramètres par défaut de l'application.

- La partie inférieure de la fenêtre regroupe les liens suivants :
  - **Aide**. Cliquez sur ce lien pour accéder à l'aide de Kaspersky Security.
  - **Support Technique**. Cliquez sur ce lien pour ouvrir la fenêtre **Support Technique** contenant les informations relatives au système d'exploitation, à la version actuelle de Kaspersky Security et des liens vers les ressources d'informations de Kaspersky Lab.
  - **Licence**. Cliquez sur ce lien pour ouvrir la fenêtre **Licence** contenant les informations relatives à la licence active.

Fenêtre de configuration des paramètres de l'application

La fenêtre de configuration de Kaspersky Security permet de configurer les paramètres de fonctionnement de l'application dans son ensemble, de ses modules distincts, des rapports et des stockages, des tâches d'analyse et des tâches de mise à jour.

► *Pour ouvrir la fenêtre de configuration de l'application, procédez d'une des manières suivantes :*

- sélectionnez l'onglet **Configuration** dans la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- sélectionnez l'option **Configuration** du menu contextuel de l'icône de l'application (cf. section “Menu contextuel de l'icône de l'application” à la page 23).

La fenêtre de configuration de l'application comprend deux parties :

- La partie gauche de la fenêtre contient des modules de l'application, des tâches et d'autres éléments qui peuvent être configurés.
- La partie droite de la fenêtre contient des éléments de gestion qui permettent de configurer le fonctionnement de l'élément sélectionné dans la partie gauche de la fenêtre.

Lancement et arrêt de l'application

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

Dans cette section

Activation et désactivation du lancement automatique de l'application

Le concept de lancement automatique de l'application désigne le lancement de Kaspersky Security sans intervention de votre part après le démarrage du système d'exploitation. Cette option de lancement de l'application est définie par défaut.

La première fois, Kaspersky Security est lancé automatiquement après son installation. Ensuite, l'application est lancée automatiquement après le démarrage du système d'exploitation.

► *Pour activer ou désactiver le lancement automatique de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Si vous souhaitez activer le lancement automatique de l'application, cochez la case **Lancer Kaspersky Security for Virtualization 4.0 Light Agent au démarrage de l'ordinateur**.

- Si vous souhaitez désactiver le lancement automatique de l'application, décochez la case **Lancer Kaspersky Security for Virtualization 4.0 Light Agent au démarrage de l'ordinateur**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement et arrêt manuels de l'application

Les experts de Kaspersky Lab déconseillent de quitter Kaspersky Security car cela mettrait en danger votre machine virtuelle et vos données personnelles. En cas de nécessité, vous pouvez suspendre la protection (cf. section “Suspension et rétablissement de la protection et du contrôle de la machine virtuelle” à la page 28) de la machine virtuelle pendant l'intervalle que vous souhaitez, sans quitter l'application.

► *Pour arrêter l'application manuellement, procédez comme suit :*

1. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel de l'icône de l'application (à la page 23) située dans la zone de notification de la barre des tâches.

2. Sélectionnez **Terminer** dans le menu contextuel.

Le lancement manuel de Kaspersky Security s'impose si vous avez désactivé le lancement automatique de l'application (cf. section “Activation et désactivation du lancement automatique de l'application” à la page 26).

► *Pour démarrer l'application manuellement,*

sélectionnez dans le menu **Démarrer** l'option **Applications** → **Kaspersky Security for Virtualization 4.0 Light Agent**.

Suspension et rétablissement de la protection et du contrôle de la machine virtuelle

La suspension de la protection de la machine virtuelle et du contrôle implique la désactivation pendant un certain temps de tous les modules de protection et des modules de contrôle de Kaspersky Security.

L'icône dans la zone de notification de la barre des tâches indique le fonctionnement de l'application (cf. section “Icône de l'application dans la zone de notification” à la page 21) :

- L'icône  signale la suspension de la protection et du contrôle de la machine virtuelle.
- L'icône  signale le rétablissement de la protection et du contrôle de la machine virtuelle.

La suspension et le rétablissement de la protection et du contrôle de la machine virtuelle n'ont aucune influence sur l'exécution des tâches d'analyse et de mise à jour de l'application.

Si des connexions réseau étaient ouvertes au moment de la suspension et du rétablissement de la protection et du contrôle de la machine virtuelle, un message s'affiche pour indiquer l'interruption de ces connexions.

► *Pour suspendre ou rétablir la protection et le contrôle de la machine virtuelle, procédez comme suit :*

1. Si vous souhaitez suspendre la protection et le contrôle de la machine virtuelle, procédez comme suit :

   a. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

   b. Sélectionnez **Suspension de la protection et du contrôle** dans le menu contextuel.

      La fenêtre **Suspension de la protection** s'ouvre.

   c. Choisissez l'une des options suivantes :

      - **Suspendre pendant la période indiquée** : la protection et le contrôle de la machine virtuelle seront activés à l'issue de l'intervalle de temps défini dans la liste déroulante en dessous. Sélectionnez l'intervalle requis dans la liste déroulante.

- **Suspendre jusqu'au redémarrage** : la protection et le contrôle de la machine virtuelle sont activés après le redémarrage de l'application ou du système d'exploitation. Pour pouvoir utiliser cette fonctionnalité, le lancement automatique de l'application doit être activé.
- **Reprendre manuellement** : la protection et le contrôle de la machine virtuelle sont activés quand vous décidez de les rétablir.

2. Si vous souhaitez rétablir la protection et le contrôle de la machine virtuelle, vous pouvez le faire à tout moment, quelle que soit l'option de suspension de la protection et du contrôle de la machine virtuelle que vous aviez sélectionnée. Pour rétablir la protection et le contrôle de la machine virtuelle, procédez comme suit :

   a. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

   b. Sélectionnez **Lancement de la protection et du contrôle** dans le menu contextuel.

Etat de la protection de la machine virtuelle

Cette section contient des informations sur la configuration de la détection des menaces de sécurité et sur les options de protection contre ces menaces.

Dans cette section

Indication de l'état de la protection de la machine virtuelle

Kaspersky Security vous informe des événements déterminant l'état actuel de la protection de la machine virtuelle à l'aide de différents indicateurs dans la fenêtre principale de l'application.

Kaspersky Security utilise les indicateurs d'état de la protection de la machine virtuelle suivants :

- Indication à l'aide d'icônes de statut du fonctionnement des modules et des états de fonctionnement des modules Kaspersky Security. Les différents types d'indicateurs sont les suivants :
  - Une icône verte indiquant le statut du fonctionnement du module s'affiche sur la ligne du module activé. Les statistiques relatives au nombre d'objets analysés par ce module et de menaces détectés, ainsi que les statistiques sur les actions exécutées par le module pour éliminer ces menaces s'affichent sur la droite.
  - Une icône jaune indiquant le statut du fonctionnement du module s'affiche sur la ligne du module désactivé. Dans ce cas, les statistiques relatives au fonctionnement du module ne s'affichent pas.

- Si tous les modules de contrôle ou de protection sont désactivés, le statut *désactivée* s'affichera dans l'en-tête des groupes **Protection Endpoint** ou **Administration de la protection**.
- Si un ou plusieurs modules de contrôle ou de protection sont désactivés, le statut *partiellement désactivée (modules en fonctionnement : <nombre de module du groupe activés> sur <nombre total de modules du groupe>)* s'affichera dans l'en-tête des groupes **Protection Endpoint** ou **Administration de la protection**.

- Indication de présence de menaces détectées par les modules de Kaspersky Security (par exemple, *lancements d'application autorisés, lancements d'application bloqués, objets analysés, menaces détectées*) :
  - Si vous réduisez les groupes **Protection Endpoint** ou **Administration de la protection**, l'indication de présence de menaces s'affiche sur la ligne des statistiques générales de fonctionnement des modules, sous l'en-tête du groupe.
  - Si vous rétablissez les groupes **Protection Endpoint** ou **Administration de la protection**, l'indication de présence de menaces s'affiche sur la ligne des statistiques de fonctionnement de chacun des modules.

  En fonction de la menace, les informations relatives à cette dernière et son niveau d'importance sont consignées en tant qu'événement et apparaissent sous un des onglets de la fenêtre **Rapports et stockages** :
  - **Rapports**.
  - **Sauvegarde**.
  - **Fichiers non traités**.
- Indication à l'aide de messages sur les événements dans le fonctionnement des modules de protection de Kaspersky Security, liés à l'état de la machine virtuelle protégée (par exemple, *Redémarrage de la machine virtuelle nécessaire* ou *Aucune connexion à la SVM*). Les messages s'affichent de la manière suivante :
  - Si vous réduisez le groupe **Administration de la protection**, le message s'affiche à la place de la ligne des statistiques sous l'en-tête du groupe.
  - Si vous déployez le groupe **Administration de la protection**, le message s'affiche à la place de la ligne des statistiques du module Antivirus Fichiers.

- Indication à l'aide de messages sur les événements liés à l'exécution des tâches de Kaspersky Security ou aux problèmes de fonctionnements de l'application (par exemple, les bases et les modules de l'application sont devenus obsolètes). Les messages s'affichent de la manière suivante :

  - Si vous réduisez le groupe **Gestion des tâches**, les messages s'affichent dans la zone d'information sous l'en-tête du groupe.

  - Si vous rétablissez le groupe **Gestion des tâches**, les messages s'affichent à la place de la ligne des statistiques et de la planification des tâches de mise à jour.

- Indication à l'aide de messages relatifs à des problèmes de licence.

  Si vous avez des problèmes de licence, par exemple l'expiration de sa validité, l'avis sous forme de message mis en évidence en rouge apparaît dans la fenêtre **Licence** qui s'ouvre via le lien **Licence** situé en bas de la fenêtre principale de l'application.

Résolution des problèmes liés à la protection de la machine virtuelle

Afin de résoudre les problèmes de protection de la machine virtuelle, vous pouvez sélectionner une des actions suivantes :

- Résoudre le problème immédiatement. En cas de découverte d'informations sur des événements importants ou critiques concernant la protection de la machine virtuelle, vous pouvez passer directement à la résolution du problème :

  - Si le module de l'application détecte des problèmes au niveau de la protection de la machine virtuelle, vous pouvez consulter les informations sur les fichiers dans lesquels l'application Kaspersky Security a détecté une menace à l'aide de l'option **Rapports** dans le menu contextuel du module, puis sélectionner l'action à effectuer sur ces fichiers (par exemple, supprimer le fichier ou rétablir le fichier dans le dossier d'origine).

  - Si un redémarrage de la machine virtuelle est exigé, vous pouvez fermer toutes les applications et redémarrer la machine virtuelle.

- Si les bases et les modules de l'application sont dépassés, vous pouvez lancer la tâche de mise à jour.

- En cas de problèmes au niveau de la licence, un message s'affiche dans la fenêtre **Licence**, ouverte via le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application. Contactez l'administrateur pour régler les problèmes liés à la licence.

- Reporter la résolution des problèmes. Si, pour quelque raison que ce soit, il est impossible de résoudre les problèmes immédiatement, vous pouvez reporter cette action et l'effectuer plus tard.

  En cas de problèmes graves, il est impossible de reporter la résolution. Cette catégorie de problèmes comprend par exemple l'échec du fonctionnement d'un ou plusieurs modules de l'application, l'endommagement des fichiers de l'application ou l'expiration de la durée de validité de la licence.

Connexion de la machine virtuelle protégée à la SVM

Cette section contient des informations sur les particularités de la connexion de la machine virtuelle protégée à la SVM.

Dans cette section

A propos de la connexion de la machine virtuelle protégée à la SVM

Le fonctionnement de l'application exige la connexion de la machine virtuelle protégée à la SVM dotée du Serveur de protection.

Si la machine virtuelle protégée n'est connectée à aucune SVM, l'application n'analyse pas les fichiers qu'elle contient. Les fichiers à analyser conformément aux paramètres de la protection sont envoyés pour analyse après la connexion à la SVM.

Pour sélectionner une SVM à laquelle se connecter, la machine virtuelle protégée doit recevoir les informations sur les SVM du réseau. La machine virtuelle protégée sélectionne la SVM optimale pour la connexion, conformément à l'algorithme de sélection des SVM. Pour en savoir plus sur la connexion de la machine virtuelle protégée à la SVM, reportez-vous au *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*.

Vous pouvez configurer les paramètres de détection des SVM qu'utilise la machine virtuelle protégée (voir section “Configuration des paramètres de détection des SVM” à la p. 35).

Configuration des paramètres de détection des SVM

► *Pour configurer les paramètres de détection des SVM du réseau et recevoir les informations qui les concernent, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche de la fenêtre du groupe **Paramètres complémentaires**, sélectionnez la section **Paramètres de détection des SVM**.

   Les paramètres de détection des SVM s'afficheront dans la partie droite de la fenêtre.

3. Sélectionnez le moyen que la machine virtuelle protégée utilisera pour la détection des SVM et la réception des informations les concernant :

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

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

     Cette option est sélectionnée par défaut.

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

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

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

     Si vous avez choisi cette option, vous pouvez désigner la liste des SVM auxquelles peut se connecter la machine virtuelle protégée.

4. Si vous avez sélectionné la variante **Utiliser le Serveur d'intégration**, indiquez les paramètres de connexion de la machine virtuelle protégée au Serveur d'intégration. Pour ce faire, procédez comme suit :

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

   b. Si le port de connexion au Serveur d'intégration est différent de celui utilisé par défaut (7271), indiquez le numéro de port dans le champ **Port**.

   c. Si l'ordinateur sur lequel la Console d'administration Kaspersky Security Center n'appartient pas au domaine ou si votre compte n'appartient pas au groupe KLAdmins ou au groupe d'administrateurs locaux, la fenêtre **Connexion au Serveur d'intégration** s'ouvre. Indiquez le mot de l'administrateur du Serveur d'intégration (mot de passe du compte admin). La connexion au Serveur d'intégration avec les autorisations d'administrateur est requise pour recevoir de celui-ci les paramètres du compte utilisé pour la connexion de la machine virtuelle protégée au Serveur d'intégration.

      Lors de l'enregistrement des paramètres de réception des informations sur les SVM, la possibilité d'une connexion au Serveur d'intégration est analysée. Si cette analyse échoue ou s'il est impossible d'établir une connexion au Serveur d'intégration, vérifiez les paramètres de connexion saisis. Les informations concernant les erreurs de connexion au Serveur d'intégration sont consignées dans le journal de fonctionnement du Serveur d'intégration. Vous pouvez consulter le journal de fonctionnement du Serveur d'intégration dans la Console de gestion du Serveur d'intégration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent)*.

5. Si vous avez sélectionné l'option **Utiliser une liste d'adresses de SVM établie manuellement**, composez la liste des SVM. Pour ce faire, procédez comme suit :

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

      Ouvre la fenêtre **Adresses des SVM**.

b. Saisissez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM à laquelle la machine virtuelle protégée peut se connecter. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

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

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

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

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

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection du système de fichiers de la machine virtuelle. Antivirus Fichiers

Cette section contient des informations sur l'Antivirus Fichiers et des instructions sur la configuration du module.

Dans cette section

A propos de l'Antivirus Fichiers

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de la machine virtuelle protégée. L'Antivirus Fichiers est lancé par défaut au démarrage de Kaspersky Security. Il se trouve en permanence dans la mémoire vive de la machine virtuelle et analyse tous les fichiers ouverts, enregistrés et exécutés sur la machine virtuelle protégée à la recherche de virus et d'autres programmes malveillants.

L'Antivirus Fichiers utilise les méthodes de l'analyse sur la base de signatures et de l'analyse heuristique, ainsi que la technologie iSwift. Avant l'analyse du fichier, l'Antivirus Fichiers recherche les données relatives à celui-ci dans les bases iSwift et, sur la base des données obtenues, décide d'analyser ou non le fichier. Si l'analyse du fichier ne révèle aucun virus ou autre programme malveillant, Kaspersky Security octroie l'accès à ce fichier.

Si, suite à l'analyse, l'Antivirus Fichiers détecte une menace dans un fichier, Kaspersky Security attribue au fichier un statut désignant le type d'objet détecté (par exemple, *virus*, *cheval de Troie*).

L'application affiche ensuite à l'écran une notification sur la menace détectée dans le fichier (si l'option a été définie dans les paramètres des notifications) et exécute sur le fichier l'action définie dans les paramètres de l'Antivirus Fichiers.

Activation et désactivation de l'Antivirus Fichiers

Par défaut, l'Antivirus Fichiers est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Fichiers le cas échéant.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver l'Antivirus Fichiers sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne **Antivirus Fichiers** avec les informations sur le module Antivirus Fichiers.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Fichiers.

     L'icône de l'état de fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Fichiers**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Fichiers.

     L'icône de l'état de fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Fichiers**, sera modifiée sur l'icône .

Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver l'Antivirus Fichiers depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

   Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'Antivirus Fichiers** pour activer l'Antivirus Fichiers.
   - Décochez la case **Activer l'Antivirus Fichiers** pour désactiver l'Antivirus Fichiers.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'Antivirus Fichiers

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Fichiers :

- Configurer la suspension automatique, par planification ou lors du lancement des applications, du fonctionnement de l'Antivirus Fichiers.
- Modifier le niveau de sécurité des fichiers.

  Vous pouvez sélectionner un des niveaux de sécurité prédéfinis pour les fichiers ou personnaliser les paramètres du niveau de sécurité des fichiers. Après avoir modifié les paramètres du niveau de sécurité des fichiers, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité des fichiers.
- Modifier l'action que l'Antivirus Fichiers exécute en cas de détection d'un fichier infecté.
- Composer la zone de protection de l'Antivirus Fichiers.

  Vous pouvez élargir ou restreindre la zone de protection en ajoutant ou en supprimant des objets ou en modifiant le type de fichiers à analyser.
- Configurer l'utilisation de l'analyse heuristique.

  L'Antivirus Fichiers utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, l'Antivirus Fichiers compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, l'Antivirus Fichiers analyse l'activité des objets dans le système d'exploitation. L'Analyse heuristique permet de détecter de nouveaux objets malveillants dont les enregistrements n'ont pas encore été ajoutés aux bases de l'application.
- Configurer l'utilisation de la technologie d'analyse iSwift.

  Vous pouvez activer la technologie iSwift qui permet d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse. L'activation de la technologie iSwift implique l'utilisation de la technologie SharedCache qui permet d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers ayant déjà été analysés sur une autre machine virtuelle.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers avec l'Antivirus Fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

- Configurer l'analyse des fichiers composés.
- Modifier le mode d'analyse des fichiers.

Dans cette section

Arrêt automatique de l'Antivirus Fichiers

Vous pouvez configurer la suspension automatique du module Antivirus Fichiers à l'heure indiquée ou en cas d'utilisation d'applications spécifiques.

La suspension de l'Antivirus Fichiers en cas de conflit avec certaines applications est une mesure extrême. Si des conflits se manifestent pendant l'utilisation du module, veuillez contacter le Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/#s_tab4).

► *Pour configurer l'arrêt automatique de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.
5. Dans le groupe **Suspension**, procédez comme suit :

   - Cochez la case **Selon la planification** et cliquez sur le bouton **Planification** pour configurer la suspension automatique de l'Antivirus Fichiers à l'heure indiquée.

     La fenêtre **Suspension** s'ouvre.
   - Cochez la case **Au lancement des applications** et cliquez sur le bouton **Sélectionner** pour configurer la suspension automatique de l'Antivirus Fichiers au lancement des applications indiquées.

     La fenêtre **Applications** s'ouvre.
6. Exécutez une des actions suivantes :

   - Pour configurer la suspension automatique de l'Antivirus Fichiers à l'heure indiquée, dans la fenêtre **Suspension** indiquez dans les champs **Pause à partir de** **et Reprendre à** indiquez la période (au format HH:MM) pendant laquelle il faut suspendre le fonctionnement de l'Antivirus Fichiers. Cliquez ensuite sur le bouton **OK**.
   - Pour configurer la suspension automatique de l'Antivirus Fichiers au lancement des applications indiquées, composez dans la fenêtre **Applications** à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer** la liste des applications dont l'utilisation nécessite la suspension de l'Antivirus Fichiers. Cliquez ensuite sur le bouton **OK**.

7. Dans la fenêtre **Antivirus Fichiers**, cliquez sur **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du niveau de protection des fichiers

Pour protéger le système de fichiers de la machine virtuelle, l'Antivirus Fichiers utilise différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de sécurité des fichiers*. Trois niveaux de sécurité des fichiers sont prévus : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité des fichiers **Recommandé** sont considérés comme optimaux et ils sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité des fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour définir un des niveaux prédéfinis de protection des fichiers (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.

   - Pour personnaliser le niveau de sécurité des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Fichiers** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité des fichiers, le nom du niveau de sécurité des fichiers dans le groupe **Niveau de sécurité** devient **Autre**.

   - Pour sélectionner le niveau de sécurité des fichiers **Recommandé**, cliquez sur le bouton **Par défaut**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action de l'Antivirus Fichiers sur les fichiers infectés

► *Pour modifier l'action que l'Antivirus Fichiers va exécuter sur les fichiers infectés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :

   - **Sélectionner l'action automatiquement**.

     Cette option est sélectionnée par défaut. Suite à la détection d'une menace, l'application exécute l'action **Réparer. Supprimer si la réparation est impossible**.

   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible**.

   - **Exécuter l'action : Réparer**.

     > Pour les fichiers qui font partie d'une application Windows Store, Kaspersky Security exécute l'action **Supprimer** quelle que soit l'option sélectionnée.

   - **Exécuter l'action : Supprimer**.

   - **Exécuter l'action : Bloquer**.

   > Lors de la suppression ou de la réparation, des copies des fichiers sont conservées dans la sauvegarde.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Formation de la zone de protection de l'Antivirus Fichiers

Le terme de *zone de protection* désigne les objets que le composant analyse pendant son exécution. Les propriétés de la zone de protection des modules différents peuvent varier.
Les propriétés de la zone de protection de l'Antivirus Fichiers correspondent à l'emplacement et au type des fichiers analysés. Par défaut, l'Antivirus Fichiers analyse uniquement les fichiers potentiellement infectés et exécutés sur tous les disques durs, les disques amovibles et les disques réseau de la machine virtuelle.

► *Pour former la zone de protection de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Types de fichiers**, sélectionnez le type de fichiers que vous souhaitez analyser avec l'Antivirus Fichiers :

   - Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
   - Sélectionnez **Fichiers analysés selon le format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
   - Sélectionnez **Fichiers analysés selon l'extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

Au moment de choisir le type d'objet à analyser, il convient de ne pas oublier les éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, les formats EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.
- L'individu malintentionné peut envoyer un virus ou une autre application malveillante sur votre machine virtuelle dans un fichier exécutable renommé avec une extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Ce fichier est scrupuleusement analysé pour la recherche de virus et d'autres applications malveillantes.

6. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :
   - Si vous souhaitez ajouter un nouvel objet à la liste des objets analysés, cliquez sur le bouton **Ajouter**.

     La fenêtre **Sélection de l'objet** s'ouvre.
   - Pour modifier le chemin de l'objet, sélectionnez-le dans la liste des objets et cliquez sur le bouton **Modifier**.

     La fenêtre **Sélection de l'objet** s'ouvre.
   - Pour supprimer un objet de la zone d'analyse, sélectionnez-le dans la liste des objets et cliquez sur **Supprimer**.

     La fenêtre de confirmation de suppression s'ouvre.
7. Exécutez une des actions suivantes dans la fenêtre **Sélection de l'objet** :
   - Pour ajouter un nouvel objet, sélectionnez-le dans la fenêtre **Sélection de l'objet** et cliquez sur le bouton **Ajouter**.

     Tous les objets sélectionnés dans la fenêtre **Sélection de l'objet** seront affichés dans la liste **Zone de protection** dans la fenêtre **Antivirus Fichiers**.

     Cliquez sur le bouton **OK**.

- Si vous souhaitez modifier le chemin vers un objet de la liste des objets, indiquez un autre chemin dans le champ **Objet et** cliquez sur le bouton **OK**.
- Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

8. Le cas échéant, répétez les points 6 et 7 pour ajouter des objets, modifier leur chemin ou les supprimer de la liste des objets de la zone de protection.
9. Si vous souhaitez exclure un objet de la zone de protection, décochez la case en regard de l'objet dans la liste **Zone de protection**. Dans ce cas, l'objet reste dans la liste des objets analysés mais sera exclu de l'analyse par l'Antivirus Fichiers.
10. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Fichiers

► *Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Performance**.

5. Dans le groupe **Méthodes d'analyse**, exécutez une des actions suivantes :

   - Si vous voulez que l'Antivirus Fichiers utilise l'analyse heuristique, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

   - Si vous voulez que l'Antivirus Fichiers n'utilise pas l'analyse heuristique, décochez la case **Analyse heuristique**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'utilisation de la technologie iSwift lors du fonctionnement de l'Antivirus Fichiers

► *Pour configurer l'utilisation de la technologie iSwift dans le fonctionnement de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

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

4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Technologie d'analyse**, exécutez une des actions suivantes :

   - Si vous souhaitez utiliser cette technologie pendant le fonctionnement de l'Antivirus Fichiers, cochez la case **Technologie iSwift**.

- Si vous ne souhaitez pas utiliser cette technologie pendant le fonctionnement de l'Antivirus Fichiers, décochez la case **Technologie iSwift**.

> L'activation de la technologie iSwift entraîne également l'activation de la technologie SharedCache.

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Optimisation de l'analyse des fichiers avec l'Antivirus Fichiers

► *Pour optimiser l'analyse des fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Choisissez l'onglet **Performance**.
5. Dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés avec l'Antivirus Fichiers

L'insertion de virus et d'autres applications malveillantes dans des fichiers composés tels que des archives ou les bases de données est une pratique de dissimulation très répandue. Pour détecter les virus dissimulés et les autres applications malveillantes, vous devez décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limites le cercle des fichiers composés analysés pour accélérer l'analyse.

► *Pour configurer l'analyse des fichiers composés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

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

4. Dans la fenêtre **Antivirus Fichiers**, sous l'onglet **Performance** du groupe **Analyse des fichiers composés**, indiquez les fichiers composés que vous voulez analyser : les archives, les paquets d'installation ou les objets OLE joints en cochant les cases correspondantes.

5. Si dans le groupe **Optimisation de l'analyse** la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est décochée, vous pouvez indiquer pour chaque type de fichier composé s'il faut analyser tous les fichiers de ce type ou uniquement les nouveaux fichiers. Pour réaliser la sélection, cliquez sur le lien **tous/nouveaux**, situé à côté du nom de type du fichier composé. Le lien change de valeur après tout clic dessus avec le bouton gauche de la souris.

   Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée, l'application analyse uniquement les nouveaux fichiers.

6. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

7. Dans le groupe **Tâches d'analyse en arrière-plan**, exécutez une des actions suivantes :

   - Si vous ne souhaitez pas que l'Antivirus Fichiers décompresse les fichiers composés en arrière-plan, décochez la case **Décompresser les fichiers composés en arrière-plan**.

   - Si vous souhaitez que l'Antivirus Fichiers décompresse les fichiers composés de grande taille en arrière-plan, cochez la case **Décompresser les fichiers composés en arrière-plan**, indiquez la valeur requise dans le champ **Taille minimale du fichier**.

8. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Si vous ne souhaitez que l'Antivirus Fichiers décompresse les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

   - Si vous souhaitez que l'Antivirus Fichiers décompresse les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

     Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

   > L'Antivirus Fichiers analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

9. Cliquez sur le bouton **OK** dans la fenêtre **Fichiers composés**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Antivirus Fichiers**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du mode d'analyse des fichiers

Le *mode d'analyse* désigne la condition dans laquelle l'Antivirus Fichiers va commencer l'analyse des fichiers. Par défaut, Kaspersky Security utilise le mode intelligent d'analyse des fichiers. Dans ce mode d'analyse des fichiers, l'Antivirus Fichiers prend une décision sur la base de l'analyse des opérations exécutées par vous, par l'application en votre nom ou au nom d'un autre utilisateur (sur la base des données avec lesquelles l'entrée dans le système d'exploitation a eu lieu) ou par le système d'exploitation sur les fichiers. Par exemple, dans le cas d'un fichier Microsoft Office Word, Kaspersky Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.

► *Afin de modifier le mode d'analyse des fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.
5. Dans le groupe **Mode d'analyse**, sélectionnez le mode requis :
   - **Intelligent**.
   - **A l'ouverture et en cas de modification**.
   - **A l'accès**.
   - **A l'exécution**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection du courrier. Antivirus Courrier

Ce module est disponible si vous avez installé Kaspersky Security sur une machine virtuelle sous système d'exploitation Windows pour poste de travail.

Cette section contient des informations sur l'Antivirus Courrier et les instructions sur la configuration du module.

Dans cette section

A propos de l'Antivirus Courrier

L'Antivirus Courrier analyse l'ensemble des messages électroniques entrants et sortants (ci-après, “messages” et “courrier”) pour y rechercher des virus et d'autres applications malveillantes.
Il démarre au lancement de Kaspersky Security. Il se trouve en permanence dans la mémoire vive de la machine virtuelle et analyse tous les messages reçus ou envoyés via les protocoles POP3, SMTP, IMAP et NNTP.

L'Antivirus Courrier ne prend pas en compte les protocoles offrant un transfert des données sécurisé.

L'icône de l'application dans la zone de notification de la barre des tâches indique le fonctionnement de l'Antivirus Courrier (cf. section “Icône de l'application dans la zone de notification” à la page 21).
L'icône de l'application prend la forme  lors de chaque analyse de message, si l'animation de l'icône de l'application est activée (cf. section “ Activation et désactivation de l'animation de l'icône de l'application “ à la page 22).

L'Antivirus Courrier intercepte et analyse chaque message électronique que vous recevez ou envoyez. Si aucune menace n'a été détectée dans le message, vous pouvez y accéder.

Si, suite à l'analyse, l'Antivirus Courrier détecte une menace dans un message, Kaspersky Security attribue au message un statut désignant le type d'objet détecté (par exemple, *virus*, *cheval de Troie*).

Ensuite, l'application bloque le message, affiche sur l'écran une notification (si cela a été défini dans les paramètres des notifications) sur la menace détectée et exécute l'action définie dans les paramètres de l'Antivirus Courrier (cf. section " Changement d'action sur les messages électroniques infectés " à la page 60).

Pour l'application Microsoft Office Outlook®, un plug-in est prévu, permettant une configuration plus détaillée des paramètres d'analyse des messages. Le plug-in de l'Antivirus Courrier est intégré à l'application Microsoft Office Outlook lors de l'installation de Kaspersky Security.

Activation et désactivation de l'Antivirus Courrier

Par défaut, l'Antivirus Courrier est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Courrier le cas échéant.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 25).

► *Pour activer ou désactiver l'Antivirus Courrier sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Antivirus Courrier.

   Le menu de sélection des actions avec le module.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Courrier.

     L'icône de l'état de fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Courrier**, sera modifiée sur l'icône .

   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Courrier.

     L'icône de l'état de fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Courrier**, sera modifiée sur l'icône .

   > Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver l'Antivirus Courrier depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.

   > Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

    - Cochez la case **Activer l'Antivirus Courrier** pour activer l'Antivirus Courrier.
    - Décochez la case **Activer l'Antivirus Courrier** pour désactiver l'Antivirus Courrier.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'Antivirus Courrier

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Courrier :

- Modifier le niveau de sécurité du courrier.

  Vous pouvez sélectionner un des niveaux de sécurité prédéfinis pour le courrier ou personnaliser le niveau de sécurité du courrier.

  Après avoir modifié les paramètres du niveau de sécurité du courrier, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du courrier.

- Modifier l'action que Kaspersky Security exécutera sur les messages électroniques infectés.
- Composer la zone de protection de l'Antivirus Courrier.
- Configurer l'analyse des pièces jointes aux messages.

  Vous pouvez activer ou désactiver l'analyse des archives jointes aux messages, limiter la taille maximale des objets analysés joints aux messages et la période maximale d'analyse de ces objets.

- Configurer le filtrage par type de pièces jointes dans les messages électroniques.

  Le filtrage selon le type de pièces jointes aux messages permet de renommer ou de supprimer automatiquement les fichiers des types indiqués. Une fois la pièce jointe du type concerné renommée, Kaspersky Security peut protéger votre machine virtuelle contre le lancement automatique de programmes malveillants.

- Configurer l'utilisation de l'analyse heuristique.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier dans les messages de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases Kaspersky Security.

- Configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook.

  Vous pouvez intégrer dans l'application Microsoft Office Outlook le plug-in qui permet de configurer les paramètres d'analyse du courrier.

  S'agissant des autres applications (dont Microsoft Outlook Express, Windows Mail et Mozilla™ Thunderbird™), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

  > En travaillant avec l'application Mozilla Thunderbird, l'Antivirus Courrier n'analyse pas les messages transmis selon le protocole IMAP pour y rechercher des virus et d'autres applications malveillantes si des filtres déplaçant les messages du dossier “Entrants” sont utilisés.

Dans cette section

Modification du niveau de sécurité du courrier

L'Antivirus Courrier utilise différents ensembles de paramètres afin de protéger votre courrier. Ces ensembles de paramètres sont appelés *niveaux de sécurité du courrier*. Trois niveaux de sécurité du courrier sont prévus : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité du courrier **Recommandé** sont considérés comme optimaux et ils sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité du courrier, exécutez l'opération suivante :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour définir un des niveaux prédéfinis de protection du courrier (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Courrier** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité du courrier, le nom du niveau de sécurité du courrier dans le groupe **Niveau de sécurité** devient **Autre**.
   - Pour sélectionner le niveau de sécurité du courrier **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Changement d'action sur les messages électroniques infectés

► *Pour modifier l'action à exécuter sur les messages électroniques infectés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que l'application Kaspersky Security exécutera en cas de découverte d'un message électronique infecté :

   - **Sélectionner l'action automatiquement**.
   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible.**
   - **Exécuter l'action : Réparer.**
   - **Exécuter l'action : Supprimer.**
   - **Exécuter l'action : Bloquer.**

   L'option **Exécuter l'action : Réparer** est sélectionnée par défaut. **Supprimer si la réparation est impossible**.

   > Lors de la suppression ou de la réparation, des copies des messages sont conservées dans la sauvegarde.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Formation de la zone de protection de l'Antivirus Courrier

La zone de protection fait référence aux objets analysés par le module. les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection de l'Antivirus Courrier sont les paramètres d'intégration de l'Antivirus Courrier aux clients de messagerie, le type de messages électroniques et les protocoles d'email dont le trafic est analysé par l'Antivirus Courrier. Par défaut, Kaspersky Security analyse l'ensemble des messages entrants et sortants, le trafic des protocoles d'email POP3, SMTP, IMAP et NNTP, et s'intègre à l'application Microsoft Office Outlook.

► *Pour former la zone de protection de l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
4. Dans la fenêtre **Antivirus Courrier**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :

   - Sélectionnez l'option **Messages entrants et sortants** si vous souhaitez que l'Antivirus Courrier analyse tous les messages entrants et sortants sur votre machine virtuelle.
   - Sélectionnez l'option **Analyser uniquement les messages entrants** si vous souhaitez que l'Antivirus Courrier analyse uniquement les messages entrants sur votre machine virtuelle.

> Si vous sélectionnez l'analyse des messages entrants uniquement, nous vous recommandons d'analyser une fois tous les messages sortants car le risque existe que votre machine virtuelle abrite des vers de messagerie qui se propagent via email. Cela permettra d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre machine virtuelle.

6. Dans le groupe **Intégration au système** procédez comme suit :

   - Cochez la case **Trafic POP3/SMTP/NNTP/IMAP** si vous souhaitez que l'Antivirus Courrier analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils atteignent votre machine virtuelle.

     Décochez la case **Trafic POP3/SMTP/NNTP/IMAP** si vous ne souhaitez pas que l'Antivirus Courrier analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils atteignent votre machine virtuelle. Dans ce cas, les messages sont analysés par le plug-in de l'Antivirus Courrier intégré à Microsoft Office Outlook après leur arrivée sur votre machine virtuelle.

     > Si vous utilisez un autre client de messagerie que Microsoft Office Outlook, l'Antivirus Courrier n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP lorsque la case **Trafic POP3/SMTP/NNTP/IMAP** est décochée.

     > Si la case **Avancé : Plugin dans Microsoft Office Outlook** est décochée, l'Antivirus Courrier s'abstiendra également d'analyser les messages transmis via les protocoles de messages POP3, SMTP, NNTP et IMAP.

   - Cochez la case **Avancé : Plugin dans Microsoft Office Outlook**, si vous souhaitez donner l'accès à la configuration de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et activer l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP et IMAP après leur réception sur votre machine virtuelle à partir du plug-in intégré à l'application Microsoft Office Outlook.

Décochez la case **Avancé : Plugin dans Microsoft Office Outlook**, si vous souhaitez bloquer l'accès à la configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et désactiver la possibilité d'analyser les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP après leur réception sur votre machine virtuelle à partir du plug-in intégré dans l'application Microsoft Office Outlook.

> Le plug-in de l'Antivirus Courrier est intégré à l'application Microsoft Office Outlook lors de l'installation de Kaspersky Security.

7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

► *Pour configurer l'analyse des objets joints aux messages, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
4. Dans la fenêtre **Antivirus Courrier**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Analyse des fichiers composés**, procédez comme suit :

   - Décochez la case **Analyser les archives jointes** si vous souhaitez que l'Antivirus Courrier n'analyse pas les archives jointes aux messages.
   - Cochez la case **Ne pas analyser les archives jointes de plus de N Mo** si vous souhaitez que l'Antivirus Courrier n'analyse pas les objets joints aux messages dont la taille dépasse N mégaoctets. Si vous avez coché cette case, indiquez la taille maximale des archives dans le champ à côté du nom de la case.

- Cochez la case **Ne pas analyser les archives plus de N s.** si vous ne souhaitez pas que l'Antivirus Courrier analyse les archives jointes aux messages pendant plus de N secondes. Si vous avez coché cette case, indiquez la durée maximale de l'analyse des archives dans le champ à côté du nom de la case.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Filtrage des pièces jointes dans les messages

Les programmes malveillants peuvent se diffuser par email sous forme de pièces jointes dans les messages. Vous pouvez configurer le filtrage selon le type des pièces jointes présentes dans les messages électroniques permettant ainsi de renommer automatiquement ou de supprimer les fichiers des types indiqués.

► *Pour configurer le filtrage des pièces jointes, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.

4. Dans la fenêtre **Antivirus Courrier** sélectionnez l'onglet **Filtre des pièces jointes**.

5. Exécutez une des actions suivantes :

   - Sélectionnez l'option **Désactiver le filtre** si vous souhaitez que l'Antivirus Courrier ne filtre pas les pièces jointes dans les messages.

- Sélectionnez l'option **Renommer les types de pièces jointes indiqués** si vous souhaitez que l'Antivirus Courrier modifie les noms des fichiers des types indiqués joints aux messages.

- Sélectionnez l'option **Supprimer les types de pièces jointes indiqués** si vous souhaitez que l'Antivirus Courrier supprime les fichiers des types indiqués joints aux messages.

6. Si dans le paragraphe 5 des instructions vous avez sélectionné l'option **Renommer les types de pièces jointes indiqués** ou l'option **Supprimer les types de pièces jointes indiqués**, la liste des types de fichiers devient active. Cochez les cases en regard des types requis de fichiers.

   Vous pouvez modifier la liste des types de fichiers avec les boutons **Ajouter**, **Modifier**, **Supprimer**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Courrier

► *Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.

4. Dans la fenêtre **Antivirus Courrier**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Méthode d'analyse**, procédez comme suit :

    - Si vous voulez que l'Antivirus Courrier utilise l'analyse heuristique, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

    - Si vous ne voulez pas que l'Antivirus Courrier utilise l'analyse heuristique, décochez la case **Analyse heuristique**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse du courrier dans Microsoft Office Outlook

Lors de l'installation de Kaspersky Security, un plug-in spécial est intégré à l'application Microsoft Office Outlook. Il permet de passer à la configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et d'indiquer le moment auquel il convient de rechercher parmi les messages électroniques la présence de virus et d'autres applications malveillantes.
Le plug-in de messagerie Microsoft Office Outlook peut analyser les messages entrants et sortants transmis via les protocoles POP3, SMTP, NNTP et IMAP.

> La configuration de l'Antivirus Courrier depuis Microsoft Office Outlook est disponible si la case **Avancé : Plugin dans Microsoft Office Outlook** est cochée dans l'interface de l'application Kaspersky Security.

Les messages entrants dans Microsoft Office Outlook sont d'abord analysés par l'Antivirus Courrier (si la case **Trafic POP3/SMTP/NNTP/IMAP** est cochée dans l'interface de l'application Kaspersky Security), puis par le plug-in de messagerie de l'application Microsoft Office Outlook.
Si l'Antivirus Courrier détecte un objet malveillant dans un message électronique, il vous en avertit.

Les messages sortants sont analysés d'abord par le plug-in de messagerie de l'application Microsoft Office Outlook, puis par l'Antivirus Courrier.

L'action sélectionnée dans la fenêtre de notification détermine le module qui élimine la menace dans le message : l'Antivirus Courrier ou le plug-in de l'application Microsoft Office Outlook :

- Si, dans la fenêtre de notification de l'Antivirus Courrier, vous sélectionnez l'action **Réparer** ou **Supprimer**, l'action de suppression de la menace sera exécutée par l'Antivirus Courrier.
- Si, dans la fenêtre de notification de l'Antivirus Courrier, vous sélectionnez l'action **Ignorer**, l'action liée à la suppression de la menace sera exécutée par le plug-in de messagerie de l'application Microsoft Office Outlook.

► *Pour configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook, procédez comme suit :*

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Dans le menu de l'application, sélectionnez l'option **Services** → **Paramètres**.

   La fenêtre **Paramètres** s'ouvre.
3. Dans la fenêtre **Paramètres**, sélectionnez l'onglet **Protection du courrier**.

Protection du trafic Internet de la machine virtuelle. Antivirus Internet

Ce module est disponible si vous avez installé Kaspersky Security sur une machine virtuelle sous système d'exploitation Windows pour poste de travail.

Cette section contient des informations sur l'Antivirus Internet et les instructions sur la configuration du module.

Dans cette section

À propos de l'Antivirus Internet

Chaque fois que vous travaillez sur Internet, les informations enregistrées sur votre machine virtuelle sont exposées à un risque d'infection par des virus et par d'autres applications présentant une menace. Ces menaces peuvent s'introduire dans la machine virtuelle lors du téléchargement d'applications gratuites ou lors de la consultation de sites Internet, attaqués par des pirates avant votre visite. Les vers de réseau peuvent s'introduire sur votre machine virtuelle avant l'ouverture des pages Internet ou le téléchargement d'un fichier, directement au moment de la connexion à Internet.

L'Antivirus Internet protège les informations qui arrivent sur votre machine virtuelle et qui sont envoyées depuis celle-ci via les protocoles HTTP et FTP. Il permet également de déterminer s'il s'agit d'une adresse Internet malveillante ou de phishing.

Chaque page Internet ou fichier auquel vous ou une application accédez via le protocole HTTP ou FTP sont interceptés et analysés par l'Antivirus Internet pour détecter la présence éventuelle de virus et d'autres applications présentant une menace. Ensuite, l'application procède ainsi :

- Si aucun code malveillant n'a été détecté sur la page Internet ou dans le fichier, vous pouvez y accéder immédiatement.
- Si la page Internet ou le fichier contient un code malveillant, l'application exécute l'action définie dans les paramètres de l'Antivirus Internet (cf. section “Modifications de l'action à effectuer sur les objets malveillants du trafic Internet” à la page 74).

L'Antivirus Internet ne prend pas en compte les protocoles offrant un transfert des données sécurisé.

Activation et désactivation de l'Antivirus Internet

Par défaut, l'Antivirus Internet est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Internet le cas échéant.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver l'Antivirus Internet sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne **Antivirus Internet** avec les informations sur le module Antivirus Internet.

   Le menu de sélection des actions avec le module.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Internet**, sera modifiée sur l'icône .

   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Internet**, sera modifiée sur l'icône .

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver l'Antivirus Internet depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.

   Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer l'Antivirus Internet** pour activer l'Antivirus Internet.
   - Décochez la case **Activer l'Antivirus Internet** pour désactiver l'Antivirus Internet.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'Antivirus Internet

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Internet :

- Modifier le niveau de sécurité du trafic Internet.

  Vous pouvez sélectionner un des niveaux prédéfinis de sécurité du trafic Internet reçus ou envoyés via les protocoles HTTP et FTP, ou personnaliser le niveau de sécurité du trafic Internet.

  Après avoir modifié les paramètres du niveau de sécurité du trafic Internet, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du trafic Internet.

- Modifier l'action que Kaspersky Security exécutera sur les objets malveillants du trafic Internet.

  Si l'analyse d'un objet du trafic Internet par l'Antivirus Internet détermine la présence d'un code malveillant, la suite des opérations de l'Antivirus Internet dépendra de l'action que vous aurez spécifiée.

- Configurer l'Analyse par l'Antivirus Internet des liens par rapport aux bases d'adresses Internet de phishing ou malveillantes.

- Configurer l'utilisation de l'analyse heuristique pour rechercher la présence éventuelle de virus et d'autres applications dangereuses dans le trafic Internet.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases Kaspersky Security.

- Configurer l'utilisation de l'analyse heuristique lors de la recherche d'éventuels liens de phishing sur les pages Internet.
- Optimiser l'analyse du trafic Internet par l'Antivirus Internet.

  Pour optimiser l'analyse du trafic Internet vous pouvez configurer la durée de la mise en cache par l'Antivirus Internet du trafic Internet sortant et entrant via les protocoles HTTP et FTP.
- Composer la liste des adresses de confiance.

  Vous pouvez composer une liste d'adresses Internet dont vous faites confiance au contenu. Antivirus Internet ne recherche pas la présence éventuelle des virus et d'autres applications présentant une menace dans les informations en provenance des adresses Internet de confiance. Cette fonctionnalité peut être utilisée, par exemple, si l'Antivirus Internet empêche le téléchargement d'un fichier depuis un site Internet que vous connaissez.

  > Le terme URL signifie à la fois l'URL d'une page Internet et celle d'un site Internet.

Dans cette section

Modification du niveau de protection du trafic Internet

Pour protéger les données reçues ou envoyées via les protocoles HTTP et FTP, l'Antivirus Internet utilise différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de sécurité du trafic Internet*. Trois niveaux de sécurité du trafic Internet sont prévus : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité du trafic Internet **Recommandé** sont considérés comme optimaux et sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité du trafic Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :
   - Pour définir un des niveaux prédéfinis de protection du trafic Internet (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité du trafic Internet, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Internet** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité du trafic Internet, le nom du niveau de sécurité du trafic Internet dans le groupe **Niveau de sécurité** devient **Autre**.
   - Pour sélectionner le niveau de sécurité du trafic Internet **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modifications de l'action à effectuer sur les objets malveillants du trafic Internet

► *Pour modifier l'action sur les objets malveillants du trafic Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Security exécutera sur les objets malveillants du trafic Internet :

   - **Sélectionner l'action automatiquement**.
   - **Bloquer le chargement**.
   - **Autoriser le chargement**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des liens par l'Antivirus Internet à partir des bases d'adresses Internet de phishing ou malveillantes

La vérification des liens pour voir s'ils appartiennent aux adresses Internet de phishing permet d'éviter les *attaques de phishing*. L'exemple type d'attaque de phishing est le message électronique soi-disant envoyé par la banque dont vous êtes client et qui contient un lien vers un site Internet officiel de la banque. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque dont l'adresse, à première vue, ne diffère aucunement de l'adresse du véritable site Internet. Toutefois, vous vous trouvez sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site Internet de phishing peut figurer non seulement dans un message électronique, mais également dans un message ICQ par exemple, l'Antivirus Internet contrôle les tentatives d'accès à un site Internet de phishing pendant la durée d'analyse du trafic Internet et bloque l'accès à ces sites Internet. Les listes des adresses Internet de phishing sont reprises dans la distribution de Kaspersky Security et sont actualisées quand une mise à jour des listes figure dans la base de l'application.

► *Pour configurer l'analyse par l'Antivirus Internet des liens en fonction des bases d'adresses Internet malveillantes ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet**, sélectionnez l'onglet **Général**.
5. Procédez comme suit :

   - Dans le groupe **Méthodes d'analyse**, cochez la case **Vérifier si les liens se trouvent dans la base de données des URL malveillantes** si vous souhaitez que l'Antivirus Internet analyse les liens selon la base des adresses Internet malveillantes.
   - Dans le groupe **Paramètres d'Anti-Phishing**, cochez la case **Vérifier si les liens se trouvent dans la base de données des URL de phishing** si vous souhaitez que l'Antivirus Internet analyse les liens selon la base des adresses Internet de phishing.

   Pour comparer les liens aux bases d'adresses Internet malveillantes et de phishing, vous pouvez également utiliser les bases de données de réputation de Kaspersky Security Network.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de l'analyse heuristique dans l'Antivirus Internet

► *Pour configurer l'utilisation de l'analyse heuristique, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet**, sélectionnez l'onglet **Général**.
5. Procédez comme suit :

   - Si vous souhaitez que l'Antivirus Internet utilise l'analyse heuristique lors de l'analyse du trafic Internet à la recherche de virus et d'autres applications qui constituent une menace, dans le groupe **Méthodes d'analyse**, cochez la case **Analyse heuristique pour détecter les virus** et définissez le niveau de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.
   - Si vous souhaitez que l'Antivirus Internet utilise l'analyse heuristique lors de l'analyse des pages Internet à la recherche de liens de phishing, dans le groupe **Paramètres d'Anti-Phishing**, cochez la case **Analyse heuristique pour détecter les liens de phishing** et définissez le niveau de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la durée de mise en cache du trafic Internet

Afin d'augmenter l'efficacité de la détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. En utilisant la mise en cache, l'Antivirus Internet analyse les objets uniquement après qu'ils ont été entièrement reçus sur la machine virtuelle protégée.

Le recours à la mise en cache augmente la durée de traitement des objets et retarde leur arrivée jusqu'à vous. De plus, la mise en cache peut entraîner des problèmes lors du téléchargement et du traitement de grands objets en raison de l'expiration du délai d'attente de la connexion du client HTTP.

Pour résoudre ce problème, la possibilité de limiter la durée de la mise en cache des fragments des objets envoyés via Internet est prévue. Une fois le délai écoulé, chaque partie de l'objet reçue vous sera transmise sans vérification et l'objet sera analysé complètement une fois qu'il aura été copié. Ceci permet de vous transférer l'objet plus rapidement et de résoudre le problème de la déconnexion. Le niveau de sécurité de l'utilisation d'Internet ne sera pas réduit pour la cause.

La levée de la restriction sur la durée de la mise en cache du trafic Internet améliore l'efficacité de la recherche de virus mais retarde en même temps l'accès aux objets.

► *Pour configurer la durée de la mise en cache du trafic Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet,** sélectionnez l'onglet **Général**.

5. Dans le groupe **Actions**, exécutez une des actions suivantes :

   - Cochez la case **Limiter le temps de mise en cache du trafic Internet** pour limiter la durée de mise en cache du trafic Internet et pour accélérer l'analyse.
   - Décochez la case **Limiter le temps de mise en cache du trafic Internet** pour supprimer la limite de la durée de mise en cache du trafic Internet.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Constitution d'une liste d'adresses Internet de confiance

► *Pour composer une liste d'adresses Internet de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Sélectionnez l'onglet **URL de confiance**.

5. Cochez la case **Ne pas analyser le trafic Internet en provenance des adresses URL de confiance**.

6. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable. Pour ce faire, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter**.

      La fenêtre **Adresse/Masque d'adresse** s'ouvre.

b. Saisissez l'adresse du site Internet/de la page Internet ou le masque d'adresse du site Internet/de la page Internet.

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

   Un nouvel enregistrement apparaîtra dans la liste des adresses Internet de confiance.

d. Répétez les paragraphes a–c de l'instruction si nécessaire.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection du trafic des clients IM. Antivirus IM

Ce module est disponible si vous avez installé Kaspersky Security sur une machine virtuelle sous système d'exploitation Windows pour poste de travail.

Cette section contient des informations sur l'Antivirus IM et les instructions sur la configuration des paramètres du module.

Dans cette section

À propos de l'Antivirus IM

L'Antivirus IM est destiné à l'analyse du trafic transmis par les clients IM.

Les messages transmis via les clients IM peuvent contenir les types suivants de menaces contre la sécurité de la machine virtuelle :

- Des liens dont l'activation déclenche le téléchargement d'une application malveillante votre machine virtuelle.
- Des liens sur les applications et les pages Internet malveillantes que les individus malintentionnés utilisent pour les attaques de phishing.

  Le but des attaques de phishing est de voler les informations personnelles des utilisateurs, notamment les numéros des cartes bancaires, les informations sur leurs passeports, les mots de passe pour les systèmes de payement des établissements bancaires ou pour d'autres services en ligne (par exemple, les réseaux sociaux ou les services de messagerie en ligne).

Les clients IM permettent la transmission des fichiers. Pendant la tentative d'enregistrement de ces fichiers, ils sont analysés par le module Antivirus Fichiers (cf. section “A propos de l'Antivirus Fichiers” à la page 38).

L'Antivirus IM intercepte chaque message que vous recevez ou envoyez via un client IM et recherche dans ceux-ci la présence éventuelle de liens dangereux pour la machine virtuelle.

Ensuite, l'application procède ainsi :

- En l'absence de liens présentant une menace, vous pouvez accéder au message.
- Si le message contient des liens dangereux, l'Antivirus IM remplace le message par les informations sur la menace détectée dans la fenêtre des messages du client IM utilisé.

Activation et désactivation de l'Antivirus IM (“Chat”)

Par défaut, l'Antivirus IM est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus IM le cas échéant.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection** de la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver l'Antivirus IM sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.

4. Cliquez sur le bouton droit de la souris sur la ligne **Antivirus IM** pour ouvrir le menu contextuel des actions du module.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu contextuel l'option **Activer** si vous voulez activer l'Antivirus IM.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus IM**, sera modifiée sur l'icône .

   - Sélectionnez l'option **Désactiver** dans le menu contextuel si vous voulez désactiver l'Antivirus IM.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus IM**, sera modifiée sur l'icône .

   > Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver l'Antivirus IM depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.

   > Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer l'Antivirus IM** pour activer l'Antivirus IM.
   - Décochez la case **Activer l'Antivirus IM** pour désactiver l'Antivirus IM.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'Antivirus IM

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus IM :

- Constituer la zone de protection.

  Vous pouvez élargir ou restreindre la zone de protection en modifiant le type de messages à analyser reçus par les clients IM.

- Configurer l'analyse par l'Antivirus IM des liens dans les messages des clients IM sur les bases d'adresses Internet malveillantes ou de phishing.

- Configurer l'utilisation de l'analyse heuristique.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier dans les messages des clients IM de nouvelles menaces qui ne figurent pas encore dans les bases de Kaspersky Security.

Dans cette section

Formation de la zone de protection de l'Antivirus IM (“Chat”)

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. La propriété de la zone de protection de l'Antivirus IM est le type des messages analysés reçus et envoyés via les clients IM. L'Antivirus IM analyse par défaut les messages entrants et les messages sortants. Vous pouvez vous passer de l'analyse des messages sortants.

► *Pour former la zone de protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :
   - Sélectionnez l'option **Messages entrants et sortants**, si vous souhaitez que l'Antivirus IM analyse tous les messages entrants et sortants des clients IM.
   - Sélectionnez l'option **Analyser uniquement les messages entrants**, si vous souhaitez que l'Antivirus IM analyse uniquement les messages entrants des clients IM.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse par l'Antivirus IM des liens par rapport aux bases d'adresses Internet de phishing ou malveillantes

► *Pour configurer l'analyse des liens par l'Antivirus IM en fonction des bases d'adresses Internet malveillantes ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Méthodes d'analyse** cochez les cases à côté des noms des méthodes que vous souhaitez utiliser lors du fonctionnement de l'Antivirus IM :

   - Cochez la case **Vérifier si les liens se trouvent dans la base de données des URL malveillantes**, si vous voulez analyser les liens dans les messages des clients IM par rapport à la base des adresses Internet malveillantes.

   - Cochez la case **Vérifier si les liens se trouvent dans la base de données des URL de phishing**, si vous voulez analyser les liens dans les messages des clients IM par rapport à la base des adresses Internet de phishing.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de l'analyse heuristique dans l'Antivirus IM (“Chat”)

► *Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus IM, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Méthodes d'analyse**, procédez comme suit :

   a. Cochez la case **Analyse heuristique**.

   b. Sélectionnez à l'aide du curseur le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection réseau

Cette section contient les informations sur les principes de fonctionnement et sur la configuration des modules Pare-feu, Prévention des intrusions et Surveillance du réseau, ainsi que sur le contrôle du trafic réseau.

Dans cette section

Pare-feu

Cette section contient des informations sur le Pare-feu et les instructions sur la configuration des paramètres du module.

Dans cette section

A propos du Pare-feu

Lorsque votre machine virtuelle est connectée aux réseaux locaux et à Internet, elle risque non seulement une infection par des virus et d'autres applications présentant une menace, mais elle est aussi exposée aux différentes attaques qui exploitent les vulnérabilités des systèmes d'exploitation et du logiciel.

Le Pare-feu garantit la protection des données personnelles stockées sur votre machine virtuelle protégée car il bloque toutes les menaces réseau lorsque celle-ci est connectée à Internet ou au réseau local. Le Pare-feu permet de détecter toutes les connexions réseau sur votre machine virtuelle et d'afficher une liste de leurs adresses IP en indiquant l'état de la connexion réseau par défaut.

Lors d'une connexion à distance à la machine virtuelle protégée après l'installation de l'application, le Pare-feu est activé par défaut et il bloque la session RDP. Afin d'éviter ce blocage, configurez l'action du Pare-feu (cf. section “ Modification de l'action du Pare-feu pour la règle pour les paquets réseau “ à la page 99) pour la règle pour les paquets réseau “ Activité réseau pour le fonctionnement du bureau à distance “ sur **Autoriser**.

Le module Pare-feu filtre toute activité réseau conformément aux règles réseau (cf. section “A propos des règles réseau” à la page 90). La configuration des règles réseau permet de définir le niveau de la protection de la machine virtuelle, qui peut varier entre un blocage complet de l'accès Internet et l'autorisation de l'accès illimité.

Lorsque vous utilisez le Pare-feu, prêtez attention aux particularités suivantes :

- L'activité réseau au niveau appliqué selon les protocoles TCP et UDP ne se bloque pas si l'adresse IP de l'expéditeur et l'adresse du destinataire coïncident, à condition que le paquet soit expédié par le socket RAW.
- Le pare-feu n'effectue pas l'analyse des règles des applications et permet l'activité réseau si l'adresse IP de l'ordinateur distant présente la valeur :
  - Pour IPv4 : 127.0.0.1
  - Pour IPv6 : ::1

  Ceci à condition que le package soit expédié par le biais du socket RAW.

- Dans les cas suivants l'adresse locale, depuis/vers laquelle l'envoi des données est exécuté peut ne pas être définie :
  - L'application initiant l'activité réseau selon les protocoles TCP ou UDP, n'a pas indiqué l'adresse IP locale ;
  - L'application a initié l'activité réseau selon le protocole ICMP ;
  - L'application reçoit le paquet entrant via le protocole UDP.
- Le pare-feu n'exécute pas le filtrage du trafic loopback au niveau de réseau. La prise de décision sur les paquets loopback se produit au niveau appliqué.
- Lors du filtrage de l'activité réseau au niveau appliqué selon le protocole ICMP, le pare-feu appuie uniquement la demande sortante ICMP Echo-Request.
- Le filtrage des paquets ICMP entrants au niveau appliqué n'est pas exécuté.
- Pour l'activité réseau sortante via le socket RAW, le filtrage selon les règles des paquets au niveau appliqué n'est pas exécuté.
- Les paquets filtrés par le module Prévention des intrusions ne sont pas analysés par le pare-feu.
- Si la machine virtuelle comporte des interfaces de réseau tunnels, le filtrage du trafic des tunnels selon les règles de paquets se répète pour le même paquet au fur et à mesure de la progression de ce paquet entre les interfaces.

Activation et désactivation du Pare-feu

Par défaut, le Pare-feu est activé et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver le Pare-feu.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver le Pare-feu sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.
4. Cliquez-droit sur la ligne **Pare-feu et** ouvrez le menu contextuel des actions du Pare-feu.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu contextuel l'option **Activer** si vous voulez activer le Pare-Feu.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Pare-feu**, sera modifiée sur l'icône .

   - Sélectionnez l'option **Désactiver** dans le menu contextuel si vous voulez désactiver le Pare-feu.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Pare-feu**, sera modifiée sur l'icône .

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver le Pare-feu depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

> Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :
   - Cochez la case **Activer le Pare-feu** pour activer le Pare-feu.
   - Décochez la case **Activer le Pare-feu** pour désactiver le Pare-feu.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées

A propos des règles réseau

La règle réseau est une action d'autorisation ou d'interdiction que le Pare-feu exécute lorsqu'il détecte une tentative de connexion réseau.

Le Pare-feu réalise la protection contre les différents types d'attaques réseau sur deux niveaux : niveau de réseau et niveau appliqué. La protection au niveau de réseau est assurée par l'application des règles pour les paquets réseau. La protection au niveau appliqué est garantie grâce au respect de règles d'utilisation des ressources de réseau pour les applications installées sur votre machine virtuelle.

Les deux niveaux de sécurité du Pare-feu vous permettent de créer :

- *Règles pour les paquets réseau*. Elles sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Le Pare-feu définit certaines règles pour les paquets réseau par défaut.
- *Règles réseau des applications*. Elles sont utilisées pour limiter l'activité réseau d'une application spécifique. Elles tiennent ensuite compte non seulement des caractéristiques du paquet réseau, mais aussi de l'application spécifique destinataire ou expéditeur de ce paquet réseau. Ces règles permettent de configurer en détail le filtrage de l'activité réseau lorsque, par exemple, un type déterminé des connexions réseau est interdit pour certaines applications mais autorisé pour d'autres.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau des applications. Si des règles pour les paquets réseau et des règles réseau des applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Les règles de contrôle de l'activité réseau des applications ne prennent pas en considération les paramètres suivants du filtrage définis au niveau du réseau :

- l'identificateur de l'adaptateur réseau ;
- la liste des adresses MAC de l'adaptateur local ;
- la liste des adresses MAC locales ;
- la liste des adresses MAC distantes ;
- le type de cadre Ethernet (IP, IPv6, ARP) ;
- la durée de vie (TTL) du paquet IP.

Ainsi, l'utilisation partagée des règles des niveaux réseau et appliqué du trafic réseau peut être bloquée au niveau appliqué, malgré le fait qu'elle soit permise au niveau du réseau.

Vous pouvez configurer vos propres priorités d'application de chaque règle pour les paquets réseau (cf. section “Modification de la priorité de la règle pour les paquets réseau” à la page 100) et de chaque règle réseau de l'application (cf. section “Modification de la priorité de la règle réseau de l'application” à la page 119).

A propos des états de la connexion réseau

Le Pare-feu contrôle toutes les connexions réseau sur votre machine virtuelle et attribue automatiquement un état à toutes les connexions détectées.

Il existe les états suivant de la connexion réseau :

- **Réseau public**. Cet état a été développé pour les réseaux non protégés par des applications antivirus quelconques, des pare-feu, des filtres (ex : pour les réseaux des café Internet). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur de la machine virtuelle d'accéder aux fichiers et aux imprimantes de celle-ci. Les autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et d'accéder à distance au bureau de cette machine virtuelle. Le Pare-Feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.

  Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.

- **Réseau local**. Cet état a été développé pour les réseaux d'utilisateurs auxquels vous faites suffisamment confiance pour autoriser l'accès aux fichiers et aux imprimantes de votre machine virtuelle (par exemple, réseau local d'entreprise ou réseau domestique).

- **Réseau de confiance**. Cet état a été développé pour un réseau sûr dont l'utilisation n'expose pas la machine virtuelle au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état n'importe quelle activité réseau dans le cadre de ce réseau.

Modification de l'état de la connexion réseau

► *Pour modifier l'état d'une connexion réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Réseaux disponibles**.

   La fenêtre **Pare-feu** s'ouvre.

4. Choisissez l'onglet **Réseaux**.

5. Sélectionnez la connexion réseau dont vous souhaitez modifier l'état.

6. Ouvrez le menu contextuel de la connexion réseau en cliquant avec le bouton droit de la souris.

7. Dans le menu contextuel, choisissez l'option état de la connexion réseau (cf. section “A propos des états de la connexion réseau” à la page 91) :

   - **Réseau public**.
   - **Réseau local**.
   - **Réseau de confiance**.

8. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des règles pour les paquets réseau

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles pour les paquets réseau :

- Créer une nouvelle règle pour les paquets réseau.

  Vous pouvez une nouvelle règle pour les paquets réseau en sélectionnant un ensemble des conditions et des actions relatives aux paquets réseau et aux flux de données.

- Activer et désactiver la règle pour les paquets réseau.

  Toutes les règles pour les paquets réseau créés par défaut par le Pare-feu possèdent l'état *Activé(e)*. Si la règle pour les paquets réseau est activée, le Pare-feu applique cette règle.

  Vous pouvez activer toute règle pour les paquets réseau, sélectionnée dans la liste des règles pour les paquets réseau. Si la règle pour les paquets réseau est désactivée, le Pare-feu suspend temporairement l'application de la règle.

La nouvelle règle pour les paquets réseau créée par l'utilisateur est par défaut ajoutée à la liste des règles pour les paquets réseau avec l'état *Activé(e)*.

- Modifier les paramètres de la règle pour les paquets réseau.

  Après avoir créé une nouvelle règle pour les paquets réseau, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle pour les paquets réseau.

  Dans la liste des règles pour les paquets réseau, vous pouvez modifier l'action que le Pare-feu exécute en cas de détection d'une activité réseau de la règle pour les paquets réseau indiquée.

- Modifier la priorité de la règle pour les paquets réseau.

  Vous pouvez augmenter ou diminuer la priorité de la règle pour les paquets réseau sélectionnée dans la liste.

- Supprimer la règle pour les paquets réseau.

  Vous pouvez supprimer la règle pour les paquets réseau si vous ne souhaitez pas que le Pare-feu applique cette règle en cas de détection d'une activité réseau et qu'elle soit affichée dans la liste des règles pour les paquets réseau avec l'état *Désactivé(e)*.

Dans cette section

Création et modification d'une règle pour les paquets réseau

Au moment de créer des règles pour les paquets réseau, il ne faut pas oublier qu'elles ont priorité sur les règles réseau des applications.

► *Pour créer ou modifier une règle pour les paquets réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

   Cet onglet contient la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.
4. Exécutez une des actions suivantes :

   - Si vous voulez créer une nouvelle règle pour les paquets réseau, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle pour les paquets réseau, sélectionnez-la dans la liste des règles pour les paquets réseau et cliquez sur le bouton **Modifier**.
5. La fenêtre **Règle réseau** s'ouvre.
6. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :

   - **Autoriser**.
   - **Interdire**.
   - **Selon les règles de l'application**.

7. Indiquez dans le champ **Nom** le nom du service réseau d'une des manières suivantes :

   - Cliquez sur l'icône  qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service réseau.

     Kaspersky Security contient des services réseau qui décrivent les connexions réseau les plus souvent utilisées.

   - Dans le champ **Nom**, saisissez manuellement le nom du service réseau.

     > *Service réseau* est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle.

8. Indiquez le protocole de transfert des données :

   a. Cochez la case **Protocole**.

   b. Sélectionnez dans la liste déroulante le type de protocole selon lequel le Pare-feu doit contrôler l'activité réseau.

      Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

      La case **Protocole** est décochée par défaut.

      Si le service réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service réseau sélectionné.

9. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

   Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

   - **Entrant (paquet)**.
   - **Entrant**.
   - **Entrant/Sortant**.
   - **Sortant (paquet)**.
   - **Sortant**.

10. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type ICMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code ICMP** et sélectionnez dans la liste déroulante le code ICMP.

11. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de votre machine virtuelle et de l'ordinateur distant dont la connexion sera contrôlée :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de votre machine virtuelle.

12. Dans le tableau **Adaptateurs réseau**, indiquez les paramètres d'adaptateurs réseau à partir desquels des paquets réseau peuvent être envoyés ou qui peuvent recevoir ces derniers. Pour cela, utilisez les boutons **Ajouter**, **Modifier** et **Supprimer**.

13. Dans le champ **Valeur maximale de la durée de vie du paquet**, indiquez une plage de valeurs de durée de vie des paquets réseau transmis et/ou reçus. La règle réseau contrôle le transfert des paquets réseau dont la valeur pour la durée de vie est située dans une plage allant du chiffre un à la valeur indiquée.

14. Indiquez les adresses réseau des ordinateurs supprimés qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses distantes**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec une adresse IP quelconque.

    - **Adresses du sous-réseau**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP liées au type de réseau choisi : **Réseaux de confiance**, **Réseaux locaux** ou **Réseaux publics**.

    - **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

15. Indiquez les adresses réseau des machines virtuelles avec l'application Kaspersky Security installée qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses locales**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et une adresse IP quelconque.
    - **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

    > Il n'est pas toujours possible d'obtenir l'adresse locale des applications. Le cas échéant, le paramètre de la règle **Adresses locales** est ignoré.

16. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle de paquet réseau soit consignée dans le rapport.
17. Cliquez sur le bouton **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle pour les paquets réseau, elle apparaît sous l'onglet **Règles pour les paquets réseau** de la fenêtre **Pare-feu**. Par défaut, la nouvelle règle réseau est placée en fin de liste.
18. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.
19. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle pour les paquets réseau

► *Pour activer ou désactiver la règle pour les paquets réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle requise pour les paquets réseau.

5. Exécutez une des actions suivantes :

   - Cochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez activer la règle.

   - Décochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez désactiver la règle.

6. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action du Pare-feu pour la règle pour les paquets réseau

► *Pour modifier l'action du Pare-feu pour la règle pour les paquets réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle pour les paquets réseau dont vous souhaitez modifier l'action.

5. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Selon la règle de l'application**.
   - **Consigner dans le rapport**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées

Modification de la priorité de la règle pour les paquets réseau

La priorité d'exécution de la règle pour les paquets réseau est définie par l'emplacement de la règle dans la liste des règles pour les paquets réseau. La première règle pour les paquets réseau dans la liste des règles pour les paquets réseau possède la priorité la plus élevée.

Chaque règle pour les paquets réseau que vous avez créée est ajoutée à la fin de la liste des règles pour les paquets réseau et possède la priorité la plus faible.

Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles pour les paquets réseau haut/bas. Suivant chacune des règles pour les paquets réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

► *Pour modifier la priorité de la règle pour les paquets réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle pour les paquets réseau dont vous souhaitez modifier la priorité.

5. A l'aide des boutons **Haut** et **Bas**, déplacez la règle pour les paquets réseau vers la position requise dans la liste des règles pour les paquets réseau.

6. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des règles réseau du groupe d'applications

L'application Kaspersky Security regroupe par défaut toutes les applications installées dans le système d'exploitation de la machine virtuelle protégée selon le nom de l'éditeur de l'application dont elle contrôle l'activité de réseau ou de fichiers. Les groupes d'applications sont à leur tour regroupés en *groupes de confiance*. Toutes les applications et tous les groupes d'applications héritent des propriétés de leur groupe parent : règles du contrôle des applications, règles réseau de l'application, ainsi que la priorité de leur exécution.

A l'instar du module Contrôle de l'activité des applications (cf. section “A propos du contrôle de l'activité des applications” à la page 152), le module Pare-feu applique par défaut les règles réseau du groupe d'applications afin de filtrer l'activité réseau de toutes les applications appartenant à ce groupe. Les règles réseau du groupe d'applications définissent les droits d'accès aux différentes connexions réseau attribués aux applications qui font partie du groupe.

Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Security a identifié sur la machine virtuelle. Vous avez deux options pour modifier l'action du Pare-feu pour les règles réseau du groupe d'applications créées par défaut. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau du groupe d'applications créées par défaut, ni modifier leur priorité.

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles réseau du groupe d'applications :

- Créer une nouvelle règle réseau du groupe d'applications.

  Vous pouvez créer une règle réseau du groupe d'applications selon laquelle le Pare-feu va régir l'activité réseau des applications qui font partie du groupe sélectionné.

- Activer et désactiver la règle réseau du groupe d'applications.

  Toutes les règles réseau du groupe d'application sont ajoutées à la liste des règles réseau du groupe d'applications avec l'état *Activé(e)*. Si la règle réseau du groupe d'applications est activée, le Pare-feu applique cette règle.

  Vous pouvez désactiver toute règle réseau d'un groupe d'application que vous avez créée manuellement. Si la règle réseau du groupe d'applications est désactivée, le Pare-feu suspend temporairement l'application de la règle.

- Modifier les paramètres de la règle réseau du groupe d'applications.

  Après avoir créé une nouvelle règle réseau du groupe d'applications, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle réseau du groupe d'applications.

  Dans la liste des règles réseau du groupe d'applications, vous pouvez modifier l'action pour la règle réseau du groupe d'applications que le Pare-feu exécute lors de la détection de l'activité réseau de ce groupe d'applications.

- Modifier la priorité de la règle réseau du groupe d'applications.

  Vous pouvez augmenter ou diminuer la priorité de la règle réseau du groupe d'applications que vous avez créée manuellement.

- Supprimer la règle réseau du groupe d'applications.

  Vous pouvez supprimer la règle réseau du groupe d'applications que vous avez créée manuellement si vous ne souhaitez pas que le Pare-feu applique cette règle réseau au groupe sélectionné d'applications lors de la détection de l'activité réseau et qu'elle soit affichée sur la liste des règles réseau du groupe d'applications.

Dans cette section

Création et modification d'une règle réseau du groupe d'applications

► *Pour créer ou modifier la règle réseau du groupe d'applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications pour lequel vous souhaitez créer ou modifier une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Exécutez une des actions suivantes :

   - Si vous voulez créer une nouvelle règle réseau du groupe des applications, cliquez sur le bouton **Ajouter**.

- Si vous voulez modifier la règle réseau du groupe des applications, sélectionnez-la dans la liste des règles réseau et cliquez sur le bouton **Modifier**.

8. La fenêtre **Règle réseau** s'ouvre.
9. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**.
   - **Interdire**.
10. Indiquez dans le champ **Nom** le nom du service réseau d'une des manières suivantes :
    - Cliquez sur l'icône qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service réseau.

      Kaspersky Security contient des services réseau qui décrivent les connexions réseau les plus souvent utilisées.
    - Dans le champ **Nom**, saisissez manuellement le nom du service réseau.

      > *Service réseau* est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle réseau.

11. Indiquez le protocole de transfert des données :
    a. Cochez la case **Protocole**.
    b. Sélectionnez dans la liste déroulante le type de protocole selon lequel le Pare-feu doit contrôler l'activité réseau.

       Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

       La case **Protocole** est décochée par défaut.

       Si le service réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service réseau sélectionné.

12. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

    Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

    - **Entrant**.
    - **Entrant/Sortant**.
    - **Sortant**.

13. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type ICMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code ICMP** et sélectionnez dans la liste déroulante le code ICMP.

14. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de votre machine virtuelle et de l'ordinateur distant dont la connexion doit être contrôlée :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de votre machine virtuelle.

15. Dans le champ **Valeur maximale de la durée de vie du paquet**, indiquez une plage de valeurs de durée de vie des paquets réseau transmis et/ou reçus. La règle réseau contrôle le transfert des paquets réseau dont la valeur pour la durée de vie est située dans une plage allant du chiffre un à la valeur indiquée.

16. Indiquez les adresses réseau des ordinateurs supprimés qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses distantes**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec une adresse IP quelconque.
    - **Adresses du sous-réseau**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP liées au type de réseau choisi : **Réseaux de confiance**, **Réseaux locaux** ou **Réseaux publics**.

- **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

17. Indiquez les adresses réseau des machines virtuelles avec l'application Kaspersky Security installée qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses locales**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et une adresse IP quelconque.

    - **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

    > Il n'est pas toujours possible d'obtenir l'adresse locale des applications. Le cas échéant, le paramètre de la règle **Adresses locales** est ignoré.

18. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau d'un groupe d'applications soit consignée dans le rapport.

19. Cliquez sur le bouton **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau pour un groupe d'applications, elle apparaît sous l'onglet **Règles réseau** de la fenêtre **Règles de contrôle du groupe d'applications**.

20. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.

21. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

22. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle réseau du groupe d'applications

► *Pour activer ou désactiver la règle réseau du groupe d'applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications requis.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau du groupe d'applications la règle réseau du groupe d'applications requise.
8. Exécutez une des actions suivantes :

   - Cochez la case à côté du nom de la règle réseau du groupe d'applications si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle réseau du groupe d'applications si vous souhaitez désactiver la règle.

   > Vous ne pouvez pas désactiver la règle réseau du groupe d'applications si elle a été créée par le Pare-feu par défaut.

9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modifier les actions du Pare-feu pour la règle réseau du groupe d'applications

Vous pouvez modifier l'action du Pare-feu pour les règles réseau de tout le groupe des applications qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle spécifique du groupe d'applications qui a été créée manuellement.

► *Pour modifier l'action du Pare-feu pour les règles réseau de tout le groupe des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.

4. Sélectionnez dans la liste des applications le groupe d'applications si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau du groupe créées par défaut. Les règles réseau du groupe des applications, créées manuellement, resteront sans modification.

5. Dans la colonne **Réseau**, cliquez avec le bouton gauche de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Hériter**.
   - **Autoriser**.
   - **Interdire**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

► *Pour modifier l'action du Pare-feu pour une règle réseau du groupe des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.

4. Sélectionnez dans la liste des applications le groupe d'applications requis.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.

6. Sélectionnez l'onglet **Règles réseau**.

7. Sélectionnez dans la liste des règles réseau du groupe d'applications, sélectionnez la règle réseau du groupe d'applications pour lequel vous souhaitez modifier l'action du Pare-feu.

8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Consigner dans le rapport**.

9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la priorité de la règle réseau du groupe d'applications

La priorité d'exécution de la règle réseau pour le groupe d'applications est définie par l'emplacement de la règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Suivant chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau du groupe d'application créées manuellement ont une priorité plus élevée que les règles réseau du groupe d'application créées par défaut.

Vous ne pouvez pas modifier la priorité des règles réseau d'un groupe d'applications créées par défaut.

► *Pour modifier la priorité de la règle réseau du groupe d'applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications requis.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau du groupe d'applications, sélectionnez la règle réseau du groupe d'applications pour lequel vous souhaitez modifier la priorité.

8. A l'aide des boutons **Haut** et **Bas**, déplacez la règle réseau du groupe d'applications vers la position requise dans la liste des règles réseau du groupe d'applications.
9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des règles réseau de l'application

Conformément aux règles réseau de l'application, le Pare-feu réglementer l'accès de l'application aux différentes connexions réseau.

> Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Security a identifié sur la machine virtuelle. Les applications qui appartiennent à ce groupe héritent de ces règles réseau. Vous pouvez modifier les actions du Pare-feu pour les règles réseau des applications héritées. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau des applications héritées du groupe parent, ni modifier leur priorité.

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles réseau de l'application :

- Créer une nouvelle règle réseau de l'application.

  Vous pouvez créer une nouvelle règle réseau de l'application que le Pare-feu utilise pour réglementer l'activité réseau de cette application.

- Activer et désactiver la règle réseau de l'application.

  Toutes les règles réseau de l'application sont ajoutées à la liste des règles réseau de l'application avec l'état *Activé(e)*. Si la règle de l'application est activée, le Pare-feu applique cette règle.

  Vous pouvez désactiver toute règle réseau de l'application que vous avez créée manuellement. Si la règle de l'application est désactivée, le Pare-feu suspend temporairement l'application de la règle.

- Modifier les paramètres de la règle réseau de l'application.

  Après avoir créé une nouvelle règle de l'application, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle réseau de l'application.

  Dans la liste des règles de l'application, vous pouvez modifier l'action pour la règle réseau de l'application que le Pare-feu exécute lors de la détection de l'activité réseau de cette application.

- Modifier la priorité de la règle réseau de l'application.

  Vous pouvez augmenter ou diminuer la priorité de la règle réseau de l'application que vous avez créée manuellement.

- Supprimer la règle réseau de l'application.

  Vous pouvez supprimer la règle réseau de l'application que vous avez créée manuellement si vous ne souhaitez pas que le Pare-feu applique cette règle réseau à l'application sélectionnée lors de la détection de l'activité réseau et qu'elle soit affichée sur la liste des règles réseau de l'application.

Dans cette section

Création et modification d'une règle réseau de l'application

► *Pour créer ou modifier une règle réseau de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications celle pour laquelle vous souhaitez créer ou modifier une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Exécutez une des actions suivantes :
   - Si vous voulez créer une nouvelle règle réseau de l'application, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle réseau de l'application, sélectionnez-la dans la liste des règles réseau de l'application et cliquez sur le bouton **Modifier**.
8. La fenêtre **Règle réseau** s'ouvre.
9. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**.
   - **Interdire**.

10. Indiquez dans le champ **Nom** le nom du service réseau d'une des manières suivantes :

    - Cliquez sur l'icône  qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service réseau.

      Kaspersky Security contient des services réseau qui décrivent les connexions réseau les plus souvent utilisées.

    - Dans le champ **Nom**, saisissez manuellement le nom du service réseau.

      > *Service réseau* est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle.

11. Indiquez le protocole de transfert des données :

    a. Cochez la case **Protocole**.

    b. Sélectionnez dans la liste déroulante le type de protocole selon lequel le Pare-feu doit contrôler l'activité réseau.

       Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

       La case **Protocole** est décochée par défaut.

       Si le service réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service réseau sélectionné.

12. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

    Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

    - **Entrant**.
    - **Entrant/Sortant**.
    - **Sortant**.

13. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type ICMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code ICMP** et sélectionnez dans la liste déroulante le code ICMP.

14. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de la machine virtuelle et de l'ordinateur distant dont la connexion sera contrôlée :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de la machine virtuelle.

15. Dans le champ **Valeur maximale de la durée de vie du paquet**, indiquez une plage de valeurs de durée de vie des paquets réseau transmis et/ou reçus. La règle réseau contrôle le transfert des paquets réseau dont la valeur pour la durée de vie est située dans une plage allant du chiffre un à la valeur indiquée.

16. Indiquez les adresses réseau des ordinateurs supprimés qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses distantes**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec une adresse IP quelconque.
    - **Adresses du sous-réseau**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP liées au type de réseau choisi : **Réseaux de confiance**, **Réseaux locaux** ou **Réseaux publics**.
    - **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les ordinateurs distants avec des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

17. Indiquez les adresses réseau des machines virtuelles avec l'application Kaspersky Security installée qui peuvent transmettre et/ou recevoir des paquets réseau. Pour cela, dans la liste déroulante **Adresses locales**, sélectionnez une des valeurs suivantes :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et une adresse IP quelconque.

- **Adresse de la liste**. La règle réseau contrôle l'envoi et/ou la réception des paquets réseau par les machines virtuelles avec l'application Kaspersky Security installée et des adresses IP qui peuvent être indiquées dans la liste ci-dessous à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

> Il n'est pas toujours possible d'obtenir l'adresse locale des applications. Le cas échéant, le paramètre de la règle **Adresses locales** est ignoré.

18. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau de l'application soit consignée dans le rapport.
19. Cliquez sur le bouton **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau pour une application, elle apparaît sous l'onglet **Règles réseau de** la fenêtre **Règles pour l'application**.
20. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.
21. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.
22. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle réseau de l'application

► *Pour activer ou désactiver la règle réseau de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.

4. Sélectionnez l'application requise dans la liste des applications.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau de l'application la règle réseau de l'application requise.
8. Exécutez une des actions suivantes :
   - Cochez la case à côté du nom de la règle réseau de l'application si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle réseau de l'application si vous souhaitez désactiver la règle.

     > Vous ne pouvez pas désactiver la règle réseau de l'application si elle a été créée par le Pare-feu par défaut.
9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action du Pare-feu pour la règle réseau de l'application

Vous pouvez modifier l'action du Pare-feu pour toutes les règles réseau de l'application qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle spécifique de l'application qui a été créée manuellement.

► *Pour modifier l'action du Pare-feu pour toutes les règles réseau de l'application d'une application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.

4. Sélectionnez dans la liste des applications l'application si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau de l'application créées par défaut.

   Les règles réseau de l'application définies manuellement, resteront inchangées.

5. Dans la colonne **Réseau**, cliquez avec le bouton gauche de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Hériter**.
   - **Autoriser**.
   - **Interdire**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

► *Pour modifier l'action du Pare-feu pour une règle réseau de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres des modules du Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.

4. Sélectionnez l'application requise dans la liste des applications.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.

6. Sélectionnez l'onglet **Règles réseau**.

7. Sélectionnez dans la liste des règles réseau de l'application, sélectionnez la règle réseau de l'application pour lequel vous souhaitez modifier l'action du Pare-feu.

8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Consigner dans le rapport**.

9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la priorité de la règle réseau de l'application

La priorité d'exécution de la règle réseau de l'application est définie par l'emplacement de cette règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Suivant chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau de l'application (qu'elles soient héritées ou crées manuellement) ont la priorité sur les règles réseau héritées du groupe d'applications parent. Autrement dit, toutes les applications du groupe héritent automatiquement des règles réseau de ce groupe, mais si une règle pour une application en particulier est modifiée ou créée, elle est appliquée avant toutes les autres règles héritées.

Vous ne pouvez pas modifier la priorité des règles réseau héritées de l'application.

► *Pour modifier la priorité de la règle réseau de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles de contrôle des applications** s'ouvre.
4. Sélectionnez l'application requise dans la liste des applications.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau de l'application la règle de l'application dont vous souhaitez modifier la priorité.
8. A l'aide des boutons **Haut** et **Bas**, déplacez la règle réseau de l'application vers la position requise dans la liste des règles réseau de l'application.
9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Prévention des intrusions

Cette section contient des informations sur la Prévention des intrusions et les instructions sur la configuration du module.

Dans cette section

A propos de la Prévention des intrusions

Le module Prévention des intrusions recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre la machine virtuelle protégée, Kaspersky Security bloque l'activité réseau de l'ordinateur attaquant. Un message vous avertit après qu'une tentative d'attaque réseau a été effectuée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

L'activité réseau de l'ordinateur à l'origine de l'attaque est bloquée pendant une heure.
Vous pouvez modifier les paramètres de blocage de l'ordinateur à l'origine de l'attaque (cf. section “Modification des paramètres de blocage de l'ordinateur à l'origine de l'attaque” à la page 123).

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Security. La liste des attaques réseau que le module Prévention des intrusions détecte est enrichie lors de la mise à jour des bases de l'application (cf. section “A propos de la mise à jour des bases et des modules de l'application” à la page 235).

Activation et désactivation de la Prévention des intrusions

Par défaut, le module Prévention des intrusions est activé et fonctionne en mode optimal. En cas de nécessité, vous pouvez désactiver la Prévention des intrusions.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver le module Prévention des intrusions sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel des actions du module Prévention des intrusions sur la ligne **Prévention des intrusions**.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu contextuel l'option **Activer** pour activer la Prévention des intrusions.

     L'icône de l'état du fonctionnement du module qui s'affiche à gauche dans la ligne **Prévention des intrusions** sera remplacée par l'icône .
   - Choisissez dans le menu contextuel l'option **Désactiver** pour désactiver la Prévention des intrusions.

     L'icône de l'état du fonctionnement du module qui s'affiche à gauche dans la ligne **Prévention des intrusions** sera remplacée par l'icône .

> Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver la Prévention des intrusions depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Prévention des intrusions**.

   La partie droite de la fenêtre affiche les paramètres du module Prévention des intrusions.

   > Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Procédez comme suit :
   - Cochez la case **Activer la Prévention des intrusions** pour activer la Prévention des intrusions.
   - Décochez la case **Activer la Prévention des intrusions** pour désactiver la Prévention des intrusions.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification des paramètres de blocage de l'ordinateur à l'origine de l'attaque

► *Pour modifier les paramètres du blocage de l'ordinateur attaquant, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Prévention des intrusions**.

   La partie droite de la fenêtre affiche les paramètres du module Prévention des intrusions.

3. Cochez la case **Ajouter l'ordinateur attaquant à la liste des ordinateurs bloqués pendant**.

Si cette case est cochée, en cas de détection d'une tentative d'attaque réseau la Prévention des intrusions bloque l'activité réseau de l'ordinateur attaquant pendant la durée définie pour protéger automatiquement la machine virtuelle contre les futures attaques réseau possibles depuis cette adresse.

Si cette case est décochée, en cas de détection d'une tentative d'attaque réseau, la Prévention des intrusions n'active pas la protection automatique contre les futures attaques réseau possibles depuis cette adresse.

4. Modifiez la durée du blocage de l'ordinateur attaquant dans le champ qui se trouve à droite de la case **Ajouter l'ordinateur attaquant à la liste des ordinateurs bloqués pendant**.

   Par défaut, l'activité réseau de l'ordinateur à l'origine de l'attaque est bloquée pendant une heure.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle du trafic réseau

Cette section contient des informations sur le contrôle du trafic réseau et les instructions sur la configuration des paramètres des ports réseau contrôlés.

Dans cette section

A propos du contrôle du trafic réseau

Lors du fonctionnement de Kaspersky Security, les modules Antivirus Courrier (cf. section “A propos de l'Antivirus Courrier” à la page 54), Antivirus Internet (cf. section “A propos de l'Antivirus Internet” à la page 68) et Antivirus IM (cf. section “A propos de l'Antivirus IM” à la page 80) contrôlent les flux de données transmis selon les protocoles définis et transitant par les ports TCP et UDP ouverts définis de la machine virtuelle. Ainsi par exemple, Antivirus Courrier analyse les informations transmises via le protocole SMTP et Antivirus Internet, les informations transmises via les protocoles HTTP et FTP.

Kaspersky Security répartit les ports TCP et UDP du système d'exploitation en plusieurs groupes en fonction de la probabilité d'une attaque réussie contre ceux-ci. Les ports réseaux associés à des services vulnérables doivent être soumis à un contrôle plus strict car ceux-ci courent un risque plus élevé d'être pris pour cible par une attaque réseau. Si vous utilisez des services non standard quelconque affectés à des ports réseau inhabituels, sachez que ces ports peuvent être eux-aussi soumis à une attaque. Vous pouvez créer une liste de ports réseau et une liste d'applications qui sollicitent un accès au réseau et qui doivent faire l'objet d'une attention particulière des modules Antivirus Courrier, Antivirus Internet et Antivirus IM dans le cadre de la surveillance du trafic réseau.

Configuration des paramètres de contrôle du trafic réseau

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres du contrôle du trafic réseau :

- Activer le contrôle de tous les ports réseau.
- Composer la liste des ports réseau contrôlés.
- Composer la liste des applications dont tous les ports réseau sont contrôlés.

Dans cette section

Activation du contrôle de tous les ports réseau

► *Pour activer le contrôle de tous les ports réseau, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler tous les ports réseau**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Constitution de la liste des ports réseau contrôlés

► *Pour créer la liste des ports réseau contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**.

4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre. La fenêtre **Ports réseau** contient la liste des ports réseau utilisés habituellement pour le transfert des emails et du trafic réseau. Cette liste est livrée avec Kaspersky Security.

5. Dans la liste des ports réseau, procédez comme suit :

   - Cochez les cases en regard des ports réseau que vous souhaitez ajouter à la liste des ports réseau contrôlés.

     Par défaut, les cases sont cochées pour tous les ports réseau présentés dans la fenêtre **Ports réseau**.

   - Décochez les cases en regard des ports réseau que vous souhaitez exclure de la liste des ports réseau contrôlés.

6. Si le port réseau contrôlé ne figure pas sur la liste des ports réseau, ajoutez-la de la manière suivante :

   a. Le lien **Ajouter** situé sous la liste des ports réseau permet d'ouvrir la fenêtre **Port réseau**.

   b. Saisissez le numéro du port réseau dans le champ **Port**.

c. Dans le champ **Description**, saisissez le nom du port réseau.

d. Cliquez sur le bouton **OK**.

La fenêtre **Port réseau** se ferme. Le port réseau que vous ajoutez apparaît en fin de liste.

7. Cliquez sur le bouton **OK** dans la fenêtre **Ports réseau**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lors de l'utilisation du protocole FTP en mode passif, la connexion peut être établie via un port réseau aléatoire qui n'a pas été ajouté dans la liste des ports réseau contrôlés. Pour protéger ces connexions, vous devez activer le contrôle de tous les ports réseau (cf. section “Activation du contrôle de tous les ports réseau” à la page 125) ou configurer le contrôle de tous les ports réseau pour les applications (cf. section “Constitution de la liste des applications dont tous les ports réseau sont contrôlés” à la page 127) à l'aide desquelles la connexion FTP est établie.

Constitution de la liste des applications dont tous les ports réseau sont contrôlés.

Vous pouvez composer une liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Security.

Il est conseillé d'ajouter à cette liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Security les applications qui reçoivent ou envoient les données via le protocole FTP.

► *Pour composer la liste des applications dont tous les ports réseau seront contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection antivirus**.

Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**.

4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre.

5. Cochez la case **Contrôler tous les ports pour les applications indiquées**.

6. Dans la liste des applications situé sous la case **Contrôler tous les ports pour les applications indiquées**, procédez comme suit :

   - Cochez les cases en regard des noms des applications dont tous les ports réseau vous souhaitez contrôler.

     Par défaut, les cases sont cochées pour toutes les applications présentées dans la fenêtre **Ports réseau**.

   - Décochez les cases en regard des noms des applications dont tous les ports réseau vous ne souhaitez pas contrôler.

7. Si l'application ne figure pas dans la liste des applications, ajoutez-la d'une des manières suivantes :

   a. A l'aide du lien **Ajouter** situé sous la liste des applications ouvrez le menu contextuel.

   b. Sélectionnez dans le menu contextuel le mode d'ajout d'une application à la liste des applications :

      - Sélectionnez l'option **Applications** pour sélectionner l'application dans la liste des applications installées sur la machine virtuelle protégée. La fenêtre **Sélection de l'application** s'ouvre. Elle vous permet d'indiquer le nom de l'application.
      - Sélectionnez l'option **Parcourir** pour désigner l'emplacement du fichier exécutable de l'application. La fenêtre standard Microsoft Windows **Ouvrir** s'ouvre, à l'aide de laquelle vous pourrez indiquer le nom du fichier exécutable de l'application.

   c. Après avoir sélectionné l'application, la fenêtre **Application** s'ouvre.

d. Saisissez dans le champ **Nom** le nom pour l'application sélectionnée.

e. Cliquez sur le bouton **OK**.

La fenêtre **Application** se ferme. L'application que vous avez ajoutée apparaît dans la liste des applications.

8. Cliquez sur le bouton **OK** dans la fenêtre **Ports réseau**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Surveillance du réseau

Cette section contient des informations sur la surveillance du réseau et explique comment la démarrer.

Dans cette section

A propos de la surveillance du réseau

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de la machine virtuelle en temps réel.

Lancement de la surveillance du réseau

► *Pour lancer la Surveillance du réseau, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Choisissez l'onglet **Statut de la protection**.

3. Déployez le groupe **Administration de la protection**.

4. Cliquez-droit sur la ligne **Pare-feu et** ouvrez le menu contextuel des actions du Pare-feu.

5. Sélectionnez dans le menu contextuel l'option **Surveillance du réseau**.

   La fenêtre **Surveillance du réseau** s'ouvre. Cette fenêtre affiche les informations sur l'activité réseau de la machine virtuelle protégée sur quatre onglets :

   - L'onglet **Activité réseau** affiche toutes les connexions réseau actives de votre machine virtuelle protégée. Il affiche non seulement les connexions réseau ouvertes par la machine virtuelle protégée, mais aussi les connexions réseau entrantes.
   - L'onglet **Ports ouverts** reprend tous les ports réseau ouverts sur la machine virtuelle protégée.
   - L'onglet **Trafic réseau** affiche le volume du trafic réseau entrant et sortant entre la machine virtuelle protégée et les autres ordinateurs du réseau auquel vous êtes connecté au moment présent.
   - L'onglet **Ordinateurs bloqués** affiche la liste des adresses IP dont l'activité réseau a été bloquée par le module Prévention des intrusions après une tentative d'attaque réseau effectuée depuis cette adresse IP.

Surveillance du système

Ce module est disponible si vous avez installé Kaspersky Security sur une machine virtuelle sous système d'exploitation Windows pour poste de travail.

Cette section contient des informations sur la Surveillance du système et les instructions sur la configuration des paramètres du module.

Dans cette section

A propos de la surveillance du système

La Surveillance du système récolte des données sur l'activité des applications sur votre machine virtuelle et transmet ces informations aux autres modules afin qu'ils puissent offrir une protection plus efficace.

Modèles de comportement dangereux

Les modèles de comportement dangereux des applications BSS (Behavior Stream Signatures) (ci-après, modèles de comportement dangereux et modèles de comportement dangereux des applications) contiennent les séquences d'actions des applications que Kaspersky Security juge dangereuses. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Security exécute l'action définie. La fonction de Kaspersky Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de la machine virtuelle.

Annulation des actions exécutées par des programmes malveillants

Sur la base des informations recueillies par la Surveillance du système, Kaspersky Security peut annuler les actions exécutées par les programmes malveillants dans le système d'exploitation lors de la réparation des programmes malveillants.

L'annulation des actions des applications malveillantes peut être initiée par la défense proactive, l'Antivirus Fichiers (cf. section “Protection du système de fichiers de la machine virtuelle. Antivirus Fichiers” à la page 38) et l'application Kaspersky Security lors de la recherche de virus.

La remise à l'état antérieur aux actions du programme malveillant n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur votre machine virtuelle.

Activation et désactivation de la Surveillance du système

Par défaut, la Surveillance du système est activée et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Le cas échéant, vous pouvez désactiver la Surveillance du système.

Il est déconseillé de désactiver la Surveillance du système sans raison valable, parce que cela entraîne une baisse d'efficacité des modules de protection qui peuvent avoir besoin des informations recueillies par la Surveillance du système pour identifier avec une plus grande précision toute menace détectée.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver la Surveillance du système, sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Administration de la protection**.
4. Cliquez-droit pour ouvrir le menu contextuel de la ligne avec les informations sur le module Surveillance du système.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer la Surveillance du système.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Surveillance du système**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver la Surveillance du système.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Surveillance du système**, sera modifiée sur l'icône .

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver la Surveillance du système depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.

Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer la Surveillance du système** si vous souhaitez activer la Surveillance du système.
   - Décochez la case **Activer la Surveillance du système** si vous souhaitez désactiver la Surveillance du système.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des modèles de comportement dangereux

► *Pour utiliser les modèles de comportement dangereux, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Défense proactive**, cochez la case **Actualiser les modèles des comportements dangereux (BSS)**.
4. Sélectionnez l'action requise dans la liste déroulante **En cas de détection de l'activité d'une application malveillante** :

   - **Sélectionner l'action automatiquement**. Si cet élément est sélectionné, Kaspersky Security exécute l'action définie comme action par défaut par les experts de Kaspersky Lab. en cas de détection d'une activité malveillante de l'application.

- **Arrêter le programme malveillant**. Si cet élément est sélectionné, Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.
- **Ignorer**. Si cet élément est sélectionné, Kaspersky Security n'exécute aucune action sur le fichier exécutable de cette application en cas de détection d'une activité malveillante de l'application.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Annulation des actions des programmes malveillants lors de la réparation

► *Pour activer ou désactiver l'annulation des actions des programmes malveillants, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Annuler les actions des applications malveillantes lors de la réparation**, si vous souhaitez que l'application Kaspersky Security annule les actions exécutées par les programmes malveillants dans votre système d'exploitation lors de leur réparation.
   - Décochez la case **Annuler les actions des applications malveillantes lors de la réparation**, si vous souhaitez que l'application Kaspersky Security n'annule pas les actions exécutées par les programmes malveillants dans votre système d'exploitation lors de leur réparation.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle du lancement des applications

Ce module est disponible si vous avez installé l'application Kaspersky Security sur une machine virtuelle tournant sous le système d'exploitation Windows et que vous aviez choisi le type d'installation standard.

Cette section contient des informations sur le Contrôle du lancement des applications et les instructions sur la configuration du module.

Dans cette section

A propos du Contrôle du lancement des applications

Le module Contrôle du lancement des applications surveille les tentatives de lancement d'applications sur la machine virtuelle et utilise pour ce faire les *règles de contrôle du lancement des applications* (cf. section “*A propos des règles de contrôle du lancement des applications*” à la page 139).

Le lancement des applications dont aucun paramètre ne respecte les règles de contrôle du lancement des applications est régi par la règle par défaut “Tout autoriser”. La règle “Tout autoriser” permet à n'importe quel utilisateur de lancer n'importe quelle application.

Toutes les tentatives de lancement des applications sur la machine virtuelle sont consignées dans des rapports.

Activation et désactivation du Contrôle du lancement des applications

Le Contrôle du lancement des applications est activé par défaut. Le cas échéant, vous pouvez désactiver le Contrôle du lancement des applications.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver Contrôle du lancement des applications sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Protection Endpoint**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle du lancement des applications.

   Le menu de sélection des actions avec le module.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle du lancement des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle du lancement des applications**, sera modifiée sur l'icône .

   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle du lancement des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle du lancement des applications**, sera modifiée sur l'icône .

   > Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver le Contrôle du lancement des applications depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section Contrôle du lancement des applications.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

   > Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Contrôle des applications**, exécutez une des actions suivantes :

    - Cochez la case **Activer le Contrôle du lancement des applications** pour activer le Contrôle du lancement des applications.

    - Décochez la case **Activer le Contrôle du lancement des applications** pour désactiver le Contrôle du lancement des applications.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles de contrôle du lancement des applications

La règle de contrôle du lancement des applications est un ensemble de paramètres qui déterminent les fonctions suivantes du module Contrôle du lancement des applications :

- Classification des applications à l'aide des *conditions de déclenchement de la règle* (ci-après, les “conditions”). La condition de déclenchement de la règle est une équivalence : critères de la condition – valeur de la condition – type de condition.

  Le critère de déclenchement de la règle peut être :

  - Le chemin d'accès au dossier contenant le fichier exécutable de l'application ou le chemin d'accès au fichier exécutable de l'application.

  - Des métadonnées telles que le nom d'origine du fichier exécutable de l'application, le nom du fichier exécutable de l'application sur le disque, la version du fichier exécutable de l'application, le nom de l'application et l'éditeur de l'application.

  - Le hash (MD5) du fichier exécutable de l'application.

  - L'appartenance de l'application à une catégorie KL. La liste Catégorie KL est une liste composée par les experts de Kaspersky Lab. Elle regroupe les applications qui partagent des traits communs.

    Par exemple, la catégorie KL “Applications de bureautique” reprend les applications de la suite Microsoft Office, Adobe® Acrobat® et d'autres.

Le type de condition du déclenchement de la règle détermine le rapport de l'application à la règle :

- *Conditions d'inclusion*. L'application respecte la règle si ces paramètres répondent au moins à une condition d'inclusion de déclenchement de la règle.
- *Conditions d'exception*. L'application ne satisfait pas à la règle si ces paramètres répondent à au moins une condition d'exception de déclenchement de la règle ou ne répondent à aucune des conditions d'inclusion de déclenchement de la règle. La règle ne contrôle pas le lancement de telles applications.

- L'autorisation octroyée aux utilisateurs ou groupes d'utilisateurs sélectionnés pour démarrer l'application.

  Vous pouvez sélectionner l'utilisateur et/ou le groupe d'utilisateurs autorisé à démarrer l'application qui satisfait à la règle.

  Une règle qui ne désigne aucun utilisateur autorisé à lancer les applications qui satisfont à la règle est une règle de *refus*.

- L'interdiction pour les utilisateurs ou groupes d'utilisateurs sélectionnés de démarrer l'application.

  Vous pouvez sélectionner l'utilisateur et/ou le groupe d'utilisateurs qui n'est pas autorisé à démarrer l'application qui satisfait aux règles de contrôle du lancement des applications.

  Une règle qui ne désigne aucun utilisateur non autorisé à lancer les applications qui satisfont à la règle est une règle *d'autorisation*.

  > Une règle de refus a une priorité supérieure à une règle d'autorisation. Par exemple, si une règle d'autorisation du contrôle du lancement des applications a été définie pour un groupe d'utilisateurs et qu'un des membres de ce groupe est soumis à une règle de refus du contrôle du lancement des applications, il ne sera pas autorisé à exécuter l'application.

État de fonctionnement de la règle de contrôle du lancement des applications

Les règles de contrôle du lancement des applications peuvent avoir un des trois états suivants :

- *Actif* Cet état indique que la règle est activée.
- *Inactif*. Cet état indique que la règle est désactivée.

- *Test*. L'état de fonctionnement de la règle signifie que Kaspersky Security ne limite pas le lancement des applications conformément aux paramètres de la règle mais qu'il se contente de consigner dans les rapports les informations relatives au lancement des applications.

  L'état de la règle *Test* est utile pour vérifier le fonctionnement d'une nouvelle règle de contrôle du lancement des applications. L'utilisateur ne sera soumis à aucune restriction au niveau du lancement des applications répondant à la règle portant l'état *Test*. L'autorisation ou l'interdiction du lancement d'une application sont définis séparément pour les règles test et les autres règles.

Règles de contrôle du lancement des applications par défaut

Les règles suivantes de contrôle du lancement des applications par défaut sont créées :

- **Tout autoriser**. La règle permet à tous les utilisateurs de lancer n'importe quelle application. Cette règle est la base du fonctionnement du Contrôle du lancement des applications en mode “Liste noire” (cf. section “A propos des modes de fonctionnement du contrôle du lancement des applications” à la page 142). La règle est activée par défaut.

- **Programmes de mise à jour de confiance**. La règle autorise l'exécution des applications qui sont installés ou mis à jour par les applications de la catégorie KL “Programmes de mise à jour de confiance” et pour lesquelles aucune règle de refus n'a été définie. La catégorie KL “Programmes de mise à jour de confiance” reprend les programmes de mise à jour des éditeurs de logiciels les plus connus. La règle est créée par défaut uniquement à partir du plug-in d'administration Kaspersky Security. La règle est désactivée par défaut.

- **Système d'exploitation et ses modules**. La règle permet à tous les utilisateurs de lancer les applications de la catégorie KL “Catégorie principale”. La catégorie KL “Catégorie principale” reprend les applications indispensables au lancement et au fonctionnement du système d'exploitation. L'autorisation de lancement d'une application de cette catégorie KL est requise pour le fonctionnement du contrôle du lancement des applications en mode “Liste blanche” (cf. section “A propos des modes de fonctionnement du contrôle du lancement des applications” à la page 142). La règle est créée par défaut uniquement à partir du plug-in d'administration Kaspersky Security. La règle est désactivée par défaut.

A propos des modes de fonctionnement du Contrôle du lancement des applications

Le module Contrôle du lancement des applications peut fonctionner selon deux modes :

- **Liste noire**. Mode avec lequel le contrôle du lancement des applications autorise tous les utilisateurs à lancer n'importe quelle application, à l'exception de celles qui figurent dans les règles d'interdiction du contrôle du lancement des applications (cf. section “A propos des règles de contrôle du lancement des applications” à la page 139).

  Il s'agit du mode de fonctionnement du Contrôle du lancement des applications par défaut. L'autorisation du lancement de toutes les applications repose sur la règle du Contrôle du lancement des applications “Tout autoriser” créée par défaut.

- **Liste blanche**. Mode avec lequel le Contrôle du lancement des applications interdit à tous les utilisateurs de lancer n'importe quelle application, à l'exception de celles qui figurent dans les règles d'autorisation du Contrôle du lancement des applications. Si les règles d'autorisation du Contrôle du lancement des applications sont rédigées complètement, le Contrôle du lancement des applications interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

La configuration du Contrôle du lancement des applications pour le fonctionnement dans ces modes est possible à partir de l'interface locale de Kaspersky Security ou dans Kaspersky Security Center. Etant donné que Kaspersky Security Center dispose d'outils qui ne sont pas disponibles dans Kaspersky Security, il est recommandé d'effectuer la configuration du mode de fonctionnement du module Contrôle du lancement des applications à partir de Kaspersky Security Center (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

Actions impliquant les Règles de contrôle du lancement des applications

Vous pouvez réaliser les opérations suivantes au niveau des règles de contrôle du lancement des applications :

- Ajouter une nouvelle règle.
- Modifier la règle.
- Modifier l'état de fonctionnement de la règle.

  La règle de contrôle du lancement des applications peut être activée (état de fonctionnement *Actif.*), désactivée (état de fonctionnement *Inactif*) ou fonctionner en mode test (état de fonctionnement *Test*). Par défaut, les règles de contrôle du lancement des applications sont activées après la création (état *Actif.)*. Vous pouvez désactiver la règle de contrôle du lancement des applications ou activer son fonctionnement en mode test.
- Supprimer la règle.

Dans cette section

Ajout et modification d'une règle de contrôle du lancement des applications

► *Pour ajouter ou modifier une règle de contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Pour modifier la règle, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

4. Définissez ou modifiez les paramètres de la règle. Pour ce faire, procédez comme suit :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom**.

   b. Dans le tableau **Conditions d'inclusion**, composez ou modifiez la liste des conditions d'inclusion du déclenchement de la règle de contrôle du lancement des applications (cf. section “Ajout d'une condition de déclenchement de la règle de contrôle du lancement des applications” à la page 146). Utilisez pour ce faire les boutons **Ajouter**, **Modifier**, **Supprimer** et **Convertir en exception**.

   c. Dans le tableau **Conditions d'exception**, composez ou modifiez la liste des conditions d'exception du déclenchement de la règle de contrôle du lancement des applications. Utilisez pour ce faire les boutons **Ajouter**, **Modifier**, **Supprimer** et **Convertir en inclusion**.

d. Vous pouvez modifier le type de condition de déclenchement de la règle. Pour ce faire, procédez comme suit :

   - Pour faire passer une condition du type inclusion en type exception, sélectionnez la condition dans le tableau **Conditions d'inclusion**, puis cliquez sur **Convertir en exception**.
   - Pour faire passer une condition du type exception au type inclusion, sélectionnez la condition dans le tableau **Conditions d'exception**, puis cliquez sur le bouton **Convertir en inclusion**.

e. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés à exécuter les applications qui répondent aux conditions d'inclusion de déclenchement de la règle. Pour ce faire, dans le champ **Utilisateurs et/ou groupes autorisés**, saisissez les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**.

   La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

f. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs qui ne sont pas autorisés à exécuter les applications qui répondent aux conditions d'inclusion de déclenchement de la règle. Pour ce faire, dans le champ **Utilisateurs et/ou groupes interdits**, saisissez les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**.

   La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

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

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Ajout d'une condition de déclenchement de la règle de contrôle du lancement des applications

► *Pour ajouter une condition de déclenchement de la règle de contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** si vous souhaitez ajouter une condition de déclenchement d'une nouvelle règle de contrôle du lancement des applications.

   - Dans la liste **Règles du contrôle du lancement des applications**, sélectionnez la règle requise, puis cliquez sur le bouton **Modifier** si vous souhaitez ajouter une condition de déclenchement d'une règle de contrôle du lancement des applications qui existe déjà.

   La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

4. Exécutez une des actions suivantes :

   - Si vous souhaitez ajouter une condition d'inclusion, cliquez sur le bouton **Ajouter** dans le tableau **Conditions d'inclusion**.

   - Si vous souhaitez ajouter une condition d'exception, cliquez sur le bouton **Ajouter** dans le tableau **Conditions d'exception**.

   Le menu contextuel du bouton **Ajouter** s'ouvre.

5. Procédez comme suit :

   - Choisissez l'option **Condition à partir des propriétés du fichier** afin de créer une condition de déclenchement de la règle de contrôle du lancement des applications sur la base des propriétés du fichier exécutable de l'application. Pour ce faire, procédez comme suit :

     a. Dans la fenêtre standard **Ouvrir** de Microsoft Windows, choisissez le fichier exécutable de l'application dont les propriétés serviront de base à la composition de la condition de déclenchement de la règle de contrôle du lancement des applications.

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

        La fenêtre **Condition à partir des propriétés du fichier** s'ouvre. Les valeurs des paramètres de la fenêtre **Condition à partir des propriétés du fichier** sont extraites des propriétés du fichier exécutable de l'application.

     c. Dans la fenêtre **Condition à partir des propriétés du fichier**, sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin d'accès au fichier ou au dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application. Sélectionnez pour ce faire le paramètre correspondant.

     d. Au besoin, modifiez les valeurs des paramètres du critère de condition sélectionné.

     e. Cliquez sur le bouton **OK**.

   - Choisissez l'option **Condition à partir des propriétés du fichier du dossier indiqué** afin de composer une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications à partir des propriétés des fichiers du dossier indiqué. Pour ce faire, procédez comme suit :

     a. Dans la fenêtre **Sélection d'un dossier**, sélectionnez le dossier contenant les fichiers exécutables des applications sur la base des propriétés desquels vous souhaitez composer une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications.

     b. Cliquez sur le bouton **OK**.

        La fenêtre **Ajout des conditions** s'ouvre.

c. Dans le champ **Dossier**, modifiez si nécessaire le chemin d'accès au dossier contenant les fichiers exécutables des applications. Pour ce faire, cliquez sur le bouton **Sélectionner**. La fenêtre **Sélection d'un dossier** s'ouvre. Cette fenêtre permet de sélectionner le dossier souhaité.

d. Dans la liste déroulante **Ajouter selon le critère**, sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application.

   Si vous choisissez l'élément **Métadonnées** dans la liste **Ajouter selon le critère**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom du fichier**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Editeur**.

e. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

f. Cliquez sur le bouton **Suivant**.

   La liste des conditions de déclenchement de la règle définies s'affiche.

g. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de contrôle du lancement des applications.

h. Cliquez sur le bouton **Terminer**.

- Choisissez l'option **Condition(s) à partir des propriétés des applications lancées** pour définir une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications depuis les propriétés des applications lancées sur la machine virtuelle. Pour ce faire, procédez comme suit :

  a. Dans la fenêtre **Ajout des conditions**, dans la liste déroulante **Ajouter selon le critère**, sélectionnez le critère sur la base duquel vous souhaitez définir une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application.

Si vous choisissez l'élément **Métadonnées** dans la liste **Ajouter selon le critère**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom du fichier**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Editeur**.

b. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

c. Cliquez sur le bouton **Suivant**.

La liste des conditions de déclenchement de la règle définies s'affiche.

d. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de contrôle du lancement des applications.

e. Cliquez sur le bouton **Terminer**.

- Choisissez l'option **Condition(s) "Catégorie KL"** afin de définir une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications selon le critère catégorie KL. Pour ce faire, procédez comme suit :

  a. Dans la fenêtre **Condition(s) "Catégorie KL"**, cochez les cases en regard des noms de catégories KL qui vont servir de base à la création de la condition de déclenchement de la règle.

  b. Cliquez sur le bouton **OK**.

- Choisissez l'option **Condition manuelle** pour définir manuellement une condition de déclenchement de la règle de contrôle du lancement des applications. Pour ce faire, procédez comme suit :

  a. Saisissez le chemin d'accès au fichier exécutable de l'application dans la fenêtre **Condition personnalisée**. Pour ce faire, cliquez sur le bouton **Sélectionner**. La fenêtre de Microsoft Windows **Ouvrir** s'ouvre. Cette fenêtre permet de sélectionner le fichier exécutable de l'application.

  b. Sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin d'accès au fichier ou au dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application. Sélectionnez pour ce faire le paramètre correspondant.

c. Au besoin, modifiez les valeurs des paramètres du critère de condition sélectionné.

d. Cliquez sur le bouton **OK**.

- Sélectionnez l'option **Condition d'après le support du fichier** pour définir la condition de déclenchement de la règle de contrôle du lancement des applications sur la base des informations relatives au support du fichier exécutable de l'application. Pour ce faire, procédez comme suit :

  a. Dans la fenêtre **Condition d'après le support du fichier**, sélectionnez le type de support dont les applications sont soumises au contrôle de la règle de contrôle du lancement des applications dans la liste déroulante **Support**.

  b. Cliquez sur le bouton **OK**.

Modification de l'état de la règle de contrôle du lancement des applications

► *Pour modifier l'état de fonctionnement de la règle de contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez dans la liste de règles celle dont vous souhaitez modifier l'état.
4. Dans la colonne **Etat** ouvrez le menu contextuel de la colonne à l'aide du bouton gauche de la souris et sélectionnez l'état de la règle souhaité :

   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Actif*.
   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Inactif*.
   - Si vous souhaitez que la règle fonctionne en mode test, sélectionnez la valeur *Test*.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification des modèles de messages du Contrôle du lancement des applications

Quand vous tentez de lancer une application interdite par la règle de contrôle du lancement des applications, Kaspersky Security affiche un message sur le blocage du lancement. Si vous estimez que le blocage du lancement de l'application n'a pas lieu d'être, vous pouvez cliquer sur le lien dans le message afin d'envoyer une réclamation à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage du lancement de l'application et pour les messages de réclamation. Vous pouvez modifier les modèles de messages.

► *Pour modifier le modèle de message, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.
4. Exécutez une des actions suivantes :
   - Si vous souhaitez modifier le modèle de la notification relative au blocage du lancement de l'application, choisissez l'onglet **Blocage**.
   - Pour modifier le modèle de message de réclamation à l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Requête**.
5. Modifiez le modèle de message de blocage ou de réclamation. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle de l'activité des applications

> Ce module est disponible si vous avez installé l'application Kaspersky Security sur une machine virtuelle tournant sous le système d'exploitation Windows et que vous aviez choisi le type d'installation standard.

Cette section contient des informations sur le Contrôle de l'activité des applications et les instructions sur la configuration des paramètres du module.

Dans cette section

A propos du Contrôle de l'activité des applications

Le module Contrôle de l'activité des applications empêche l'exécution des actions dangereuses pour le système d'exploitation, et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles.

Le module contrôle les applications sur la machine virtuelle protégée, y compris l'accès des applications aux ressources protégées (fichiers et dossiers, clés du registre), à l'aide des *règles du contrôle des applications*. Les règles de contrôle des applications représentent un ensemble de restrictions pour différentes actions des applications dans le système d'exploitation et de droits d'accès aux ressources de la machine virtuelle protégée.

L'activité réseau des applications est contrôlée par le module Pare-feu (cf. section “A propos du Pare-feu” à la page 87).

Au premier lancement de l'application sur la machine virtuelle protégée, le module Contrôle de l'activité des applications vérifie le niveau de danger de l'application et la place dans un des *groupes de confiance*. Le groupe de confiance définit les règles du contrôle des applications que Kaspersky Security applique pour contrôler les applications.

Pour un fonctionnement plus efficace du Contrôle de l'activité des applications, il est conseillé de participer au Kaspersky Security Network (cf. section *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Les données obtenues à l'aide de Kaspersky Security Network permettent de référer plus précisément les applications à un groupe de confiance ou à un autre, et aussi appliquer les règles optimales du contrôle des applications.

Lors du prochain lancement de l'application, le Contrôle de l'activité des applications analyse l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les règles de contrôle des applications existantes. En cas de modification de l'application, le Contrôle de l'activité des applications l'analyse comme s'il s'agissait de sa première exécution.

Activation et désactivation du Contrôle de l'activité des applications

Par défaut, le Contrôle de l'activité des applications est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Le cas échéant, vous pouvez désactiver le Contrôle de l'activité des applications.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver Contrôle de l'activité des applications sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Protection Endpoint**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle de l'activité des applications.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle de l'activité des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne Contrôle de l'activité des applications, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle de l'activité des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne Contrôle de l'activité des applications, sera modifiée sur l'icône .

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver le Contrôle de l'activité des applications depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section Contrôle de l'activité des applications.

Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

> Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :

   - Cochez la case **Activer le Contrôle de l'activité des applications** pour activer le Contrôle de l'activité des applications.
   - Décochez la case **Activer le Contrôle de l'activité des applications** pour désactiver le Contrôle de l'activité des applications.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Répartition des applications selon les groupes de confiance

Au premier lancement de l'application sur la machine virtuelle protégée, le module Contrôle de l'activité des applications vérifie le niveau de danger de l'application et la place dans un des groupes de confiance.

A la première étape de l'analyse de l'application, Kaspersky Security cherche l'enregistrement sur l'application dans la base interne des applications connues, puis envoie une demande à la base Kaspersky Security Network (s'il existe une connexion à Internet). Si l'enregistrement a été trouvé dans la base de Kaspersky Security Network, l'application se place dans le groupe de confiance enregistré dans la base de Kaspersky Security Network.

Afin de placer les applications inconnues (n'étant pas présentes dans la base de Kaspersky Security Network et ne possédant pas la signature numérique d'un éditeur fiable) dans des groupes de confiance, Kaspersky Security effectue, par défaut, une analyse heuristique. Pendant l'analyse heuristique, Kaspersky Security définit le degré de menace de l'application.

En fonction du degré de menace de l'application, Kaspersky Security place l'application dans un groupe de confiance approprié. Au lieu d'utiliser l'analyse heuristique, vous pouvez définir le groupe de confiance dans lequel Kaspersky Security doit mettre automatiquement les applications inconnues.

Par défaut, Kaspersky Security analyse l'application pendant 30 secondes. Si à l'issue de ce temps, le degré de menace de l'application n'a pas été défini, Kaspersky Security place l'application dans le groupe de confiance Restrictions faibles et continue le processus de définition du degré de menace de l'application en arrière-plan. Ensuite, Kaspersky Security place l'application dans un groupe de confiance définitif. Vous pouvez modifier la durée consacrée à l'analyse du degré de menace des applications exécutées. Si vous êtes convaincu qu'aucune des applications exécutées sur la machine virtuelle protégée ne menace sa sécurité, vous pouvez réduire la durée d'évaluation du niveau de menace de l'application. Si, au contraire, vous installez sur la machine virtuelle protégée des applications dont vous ne pouvez pas garantir la fiabilité en matière de sécurité, il est conseillé d'augmenter la durée d'évaluation du niveau de menace des applications.

Si le degré de menace de l'application est élevé, Kaspersky Security vous en avertit et vous invite à sélectionner le groupe de confiance pour y placer cette application. La notification contient les statistiques d'utilisation de cette application par les participants de Kaspersky Security Network. En vous basant sur ces statistiques et l'historique de l'apparition de l'application sur la machine virtuelle, vous pouvez prendre une décision plus réfléchie sur le groupe de confiance correspondant à cette application.

► *Pour configurer la répartition des applications dans les groupes de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Si vous voulez placer automatiquement les applications avec une signature numérique dans le groupe “De confiance”, cochez la case **Faire confiance aux applications dotées d'une signature numérique**.

4. Sélectionner le mode de répartition des applications inconnues selon les groupes de confiance :

   - Si vous souhaitez utiliser l'analyse heuristique pour la répartition des applications inconnues dans les groupes de confiance, sélectionnez l'option **Déterminer le groupe à l'aide de l'analyse heuristique** et indiquez le temps à consacrer à l'analyse de l'application exécutée dans le champ **Durée maximale pour déterminer le groupe**.

   - Si vous voulez placer toutes les applications inconnues dans le groupe de confiance indiqué, sélectionnez l'option **Placer automatiquement dans le groupe** et sélectionnez le groupe de confiance requis dans la liste déroulante.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Transfert d'une application vers un autre groupe de confiance

Lors de la première exécution d'une application, Kaspersky Security place automatiquement cette application dans un groupe de confiance. En cas de nécessité, vous pouvez manuellement déplacer l'application vers un autre groupe de confiance.

> Les experts de Kaspersky Lab déconseillent de déplacer les applications du groupe de confiance défini automatiquement vers un autre groupe de confiance. Si nécessaire, il est plutôt conseillé de modifier les règles de contrôle de l'application en question (cf. section “Modification des règles de contrôle de l'application” à la page 161).

► *Pour déplacer une application vers un groupe de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Applications**.

   La fenêtre **Applications** s'ouvre.

4. Sélectionnez l'onglet **Règles de contrôle des applications**.
5. Sélectionnez l'application requise dans la liste des applications.
6. Exécutez une des actions suivantes :
    - Cliquez-droit pour ouvrir le menu contextuel de l'application. Dans le menu contextuel de l'application, choisissez l'option **Déplacer dans le groupe** → **<nom du groupe>**.
    - Ouvrez le menu contextuel à l'aide des liens de **confiance** / **Restrictions faibles** / **Restrictions élevées** / **Douteuses** dans l'angle inférieur gauche de l'onglet **Règles de contrôle des applications**. Sélectionnez le groupe de confiance requis dans le menu contextuel.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des règles du Contrôle des applications

Par défaut, le contrôle de l'application est régi par les règles de contrôle des applications définies pour le groupe de confiance dans lequel Kaspersky Security a placé l'application lors de son premier lancement. En cas de nécessité, vous pouvez modifier les règles de contrôle des applications pour tout le groupe de confiance, pour une application spécifique ou pour un groupe d'applications faisant partie du groupe de confiance.

Les règles de contrôle des applications définies pour une application spécifique ou pour un groupe d'applications faisant partie du groupe de confiance ont une priorité plus élevée que les règles de contrôle des applications définies pour le groupe de confiance. Cela veut dire que si les paramètres des règles de contrôle des applications définis pour une application spécifique ou un groupe d'applications faisant partie du groupe de confiance sont différents des paramètres des règles de contrôle des applications définies pour le groupe de confiance, le Contrôle de l'activité des applications analyse l'application ou le groupe d'applications faisant partie du groupe de confiance conformément aux règles de contrôle des applications définies pour l'application ou le groupe d'applications.

Dans cette section

Modification des règles de contrôle des groupes de confiance et des règles de contrôle des groupes d'applications

Par défaut, les règles optimales de contrôle des applications ont été créées pour différents groupes de confiance. Les paramètres des règles de contrôle de groupes d'applications qui font partie du groupe de confiance héritent les valeurs des paramètres des règles de contrôle de groupes de confiance. Vous pouvez modifier les règles de contrôle de groupes de confiance préinstallées et les règles de contrôle de groupes d'applications.

► *Pour modifier les règles de contrôle du groupe de confiance ou les règles de contrôle du groupe d'applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Applications**.

   La fenêtre **Applications** s'ouvre.

4. Sélectionnez l'onglet **Règles de contrôle des applications**.

5. Sélectionnez dans la liste des applications le groupe de confiance ou le groupe d'applications requis.

6. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du groupe de confiance ou du groupe d'applications, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.

7. Exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et base de registre** pour modifier les règles de contrôle du groupe de confiance et les règles de contrôle du groupe d'applications qui régissent les privilèges du groupe de confiance ou du groupe d'applications relatives aux opérations avec le registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.

   - Sélectionnez l'onglet **Privilèges** pour modifier les règles de contrôle du groupe de confiance ou les règles de contrôle du groupe d'applications qui régissent les Privilèges du groupe de confiance ou du groupe d'applications relatifs à l'accès aux processus et aux objets du système d'exploitation.

8. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.

9. Sélectionnez l'option souhaitée dans le menu contextuel.

   - **Hériter**.

   - **Autoriser**.

   - **Interdire**.

   - **Consigner dans le rapport**.

> Si vous modifiez les règles de contrôle du groupe de confiance, l'option **Hériter** est inaccessible.

10. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle du groupe d'applications**.
11. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.
12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification des règles de contrôle de l'application

Par défaut, les paramètres des règles de contrôle des applications qui font partie du groupe d'application ou de groupe de confiance héritent les valeurs des paramètres des règles de contrôle du groupe de confiance. Vous pouvez modifier les paramètres des règles de contrôle des applications.

► *Pour modifier une règle du contrôle de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   La fenêtre **Applications** s'ouvre.
4. Sélectionnez l'onglet **Règles de contrôle des applications**.
5. Sélectionnez l'application requise dans la liste des applications.
6. Exécutez une des actions suivantes :

   - Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'application, puis sélectionnez l'option **Règles pour l'application**.

- Cliquez sur le bouton **Avancé** dans le coin inférieur droit de l'onglet **Règles de contrôle des applications**.

La fenêtre **Règles de contrôle de l'application** s'ouvre.

7. Exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et base de registre** pour modifier les règles de contrôle de l'application qui régissent les Privilèges de l'application relatifs aux opérations avec le registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.

   - Sélectionnez l'onglet **Privilèges** pour modifier les règles de contrôle de l'application qui régissent les Privilèges de l'application relatifs à l'accès aux processus et à d'autres objets du système d'exploitation.

8. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.

9. Sélectionnez l'option souhaitée dans le menu contextuel.

   - **Hériter**.

   - **Autoriser**.

   - **Interdire**.

   - **Consigner dans le rapport**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.

11. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.

12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Désactivation du téléchargement et de la mise à jour des règles de contrôle des applications depuis la base de Kaspersky Security Network

Par défaut, les règles du contrôle des applications téléchargées depuis la base de Kaspersky Security Network sont appliquées pour les applications détectées dans cette base.

Si l'application ne figurait pas dans la base de Kaspersky Security Network au moment de la première exécution de l'application, mais que les informations la concernant ont été ajoutées par la suite à la base de Kaspersky Security Network, Kaspersky Security met à jour automatiquement par défaut les règles de contrôle de cette application.

Vous pouvez désactiver le téléchargement des règles de contrôle des applications depuis les bases de Kaspersky Security Network et la mise à jour automatique des règles de contrôle pour les applications jusqu'alors inconnues.

► *Pour désactiver le téléchargement et la mise à jour des règles de contrôle des applications depuis la base de Kaspersky Security Network, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Décochez la case **Actualiser les règles de contrôle des applications inconnues depuis la base KSN**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Désactivation de l'héritage des restrictions du processus parent

L'utilisateur ou une autre application en cours d'exécution peut être à l'origine du lancement d'une application. Si l'application a été lancée par une autre, alors la séquence de lancement est composée des processus parent et fils.

Lorsque l'application tente d'accéder à la ressource contrôlée, le Contrôle de l'activité des applications analyse les privilèges de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource. Dans ce cas, c'est la règle de la priorité minimale qui est appliquée : lorsque les privilèges d'accès de l'application et du processus parent sont comparés, les privilèges d'accès avec la priorité minimale sont appliqués à l'activité de l'application.

Priorité des privilèges d'accès :

1. **Autoriser**. Ce droit d'accès a une priorité élevée.
2. **Interdire**. Ce privilège d'accès a une priorité faible.

Ce mécanisme empêche l'utilisation d'applications de confiance par des applications douteuses ou dont les privilèges sont réduits pour exécuter des actions avec des privilèges.

Si l'activité de l'application est bloquée en raison de privilèges insuffisants au niveau d'un des processus parents, vous pouvez modifier ces privilèges (cf. section “Modification des règles de contrôle de l'application” à la page 161) ou désactiver l'héritage des restrictions du processus parent.

► *Pour désactiver l'héritage des restrictions du processus parent, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   La fenêtre **Applications** s'ouvre.

4. Sélectionnez l'onglet **Règles de contrôle des applications**.
5. Sélectionnez l'application requise dans la liste des applications.
6. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'application, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.
7. Sélectionnez l'onglet **Exclusions**.
8. Cochez la case **Ne pas hériter des restrictions du processus parent (application)**.
9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Exclusion de certaines actions de l'application des règles de contrôle de l'application

► *Pour exclure certaines actions des applications des règles du contrôle des applications, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   La fenêtre **Applications** s'ouvre.
4. Sélectionnez l'onglet **Règles de contrôle des applications**.

5. Sélectionnez l'application requise dans la liste des applications.
6. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'application, puis sélectionnez l'option **Règles pour l'application**.

   La fenêtre **Règles de contrôle de l'application** s'ouvre.
7. Sélectionnez l'onglet **Exclusions**.
8. Cochez les cases en regard des actions de l'application à ne pas contrôler :
   - **Ne pas analyser les fichiers ouverts**.
   - **Ne pas surveiller l'activité de l'application**.
   - **Ne pas hériter des restrictions du processus parent (application)**.
   - **Ne pas surveiller l'activité des applications enfants**.
   - **Autoriser l'interaction avec l'interface de l'application**.
   - **Ne pas analyser le trafic réseau**.
9. Cliquez sur le bouton **OK** dans la fenêtre **Règles de contrôle de l'application**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration des paramètres de stockage des règles de contrôle des applications non utilisées

Les règles du contrôle des applications qui n'ont pas été utilisées depuis 60 jours sont supprimées automatiquement par défaut. Vous pouvez modifier la durée de stockage des règles du contrôle des applications non utilisées ou désactiver la suppression automatique.

► *Pour configurer les paramètres de stockage des règles du contrôle des applications non utilisées, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cochez la case **Supprimer les règles de contrôle des applications qui n'ont plus été lancées depuis** et indiquez le nombre de jours requis si vous voulez que Kaspersky Security supprime les règles du contrôle des applications non utilisées.

   - Décochez la case **Supprimer les règles de contrôle des applications qui n'ont plus été lancées depuis** pour désactiver la suppression automatique des règles du contrôle des applications non utilisées.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection des ressources du système d'exploitation et des données personnelles

Le module Contrôle de l'activité des applications gère les privilèges des applications relatifs aux opérations sur différentes catégories de ressources du système d'exploitation et de données personnelles.

Les experts de Kaspersky Lab ont sélectionné des catégories de ressources à protéger. Vous ne pouvez pas modifier ou supprimer les catégories préinstallées de ressources à protéger et des ressources protégées connexes.

Vous pouvez exécuter les opérations suivantes :

- ajouter une nouvelle catégorie de ressources protégées ;
- ajouter une nouvelle ressource protégée ;
- désactiver la protection de la ressource.

Dans cette section

Ajout de la catégorie de ressources protégées

► *Pour ajouter une catégorie des ressources protégées, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Ressources**.

   La fenêtre **Applications** s'ouvre.
4. Sélectionnez l'onglet **Ressources protégées**.
5. Sélectionnez dans la partie gauche de l'onglet **Ressources protégées** la section ou la catégorie des ressources protégées dans laquelle vous souhaitez ajouter une nouvelle catégorie des ressources protégées.

6. Cliquez-gauche dans la partie supérieure gauche de l'onglet **Ressources protégées** afin d'ouvrir le menu contextuel du bouton **Ajouter**.

7. Sélectionnez **Catégorie** dans le menu contextuel.

   La fenêtre **Catégorie des ressources protégées** s'ouvre.

8. Indiquer le nom de la nouvelle catégorie de ressources protégées.

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

   Un élément nouveau apparaît dans la liste des catégories des ressources protégées.

10. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Ajout de la ressource protégée

► *Pour ajouter une ressource protégée, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Ressources**.

   La fenêtre **Applications** s'ouvre.

4. Sélectionnez l'onglet **Ressources protégées**.

5. Sélectionnez dans la partie gauche de l'onglet **Ressources protégées** la catégorie des ressources protégées à laquelle vous souhaitez ajouter une nouvelle ressource protégée.

6. Cliquez-gauche dans la partie supérieure gauche de l'onglet **Ressources protégées** afin d'ouvrir le menu contextuel du bouton **Ajouter**.

7. Dans le menu contextuel, sélectionnez le type de ressource que vous souhaitez ajouter :

   - **Fichier ou dossier**.
   - **Clé de registre**.

   La fenêtre **Ressource protégée** s'ouvre.

8. Dans le champ **Nom**, saisissez le nom pour l'application sélectionnée.
9. Cliquez sur le bouton **Parcourir**.
10. Définissez dans la fenêtre qui s'ouvre les paramètres requis en fonction du type de la ressource protégée ajoutée et cliquez sur **OK**.
11. Dans la fenêtre **Ressource protégée**, cliquez sur **OK**.

    Sous l'onglet **Ressources protégées** un élément nouveau apparaît dans la liste des ressources protégées.

12. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.
13. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Désactivation de la protection de la ressource

► *Pour désactiver la protection de la ressource, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Ressources**.0

   La fenêtre **Applications** s'ouvre.

4. Sélectionnez l'onglet **Ressources protégées**.

5. Exécutez une des actions suivantes :

   - Sélectionnez la ressource dans la liste des ressources protégées de la partie gauche de l'onglet dont vous souhaitez désactiver la protection et décochez la case en regarde de son nom.

   - Ajouter la ressource à la liste des exclusions de la protection du module Contrôle de l'activité des applications. Pour ce faire, procédez comme suit :

     a. Dans la partie supérieure droite de l'onglet **Ressources protégées** cliquez sur le bouton **Exclusions**.

     b. Cliquez-gauche dans la fenêtre **Exclusions** qui s'ouvre afin d'ouvrir le menu contextuel du bouton **Ajouter**.

     c. Dans le menu contextuel, sélectionnez le type de ressource que vous souhaitez ajouter à la liste des exclusions de la protection du module Contrôle de l'activité des applications : **Fichier ou dossier** ou **Clé de registre**.

        La fenêtre **Ressource protégée** s'ouvre.

     d. Dans le champ **Nom**, saisissez le nom pour l'application sélectionnée.

     e. Cliquez sur le bouton **Parcourir**.

     f. Définissez dans la fenêtre qui s'ouvre les paramètres requis en fonction du type de la ressource protégée que vous souhaitez ajouter à la liste des exclusions de la protection du module Contrôle de l'activité des applications.

     g. Cliquez sur le bouton **OK**.

     h. Cliquez sur le bouton **OK** dans la fenêtre **Ressource protégée**.

        Dans la liste des ressources exclues de la protection du module Contrôle de l'activité des applications, un élément nouveau apparaît.

     i. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Applications**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle des périphériques

Ce module est disponible si vous avez installé l'application Kaspersky Security sur une machine virtuelle tournant sous le système d'exploitation Windows et que vous aviez choisi le type d'installation standard.

Cette section contient des informations sur le Contrôle des périphériques et les instructions sur la configuration du module.

Dans cette section

A propos du contrôle des périphériques

Le Contrôle des périphériques garantit la sécurité des données confidentielles en limitant l'accès utilisateur aux périphériques installés ou connectés à la machine virtuelle protégée :

- périphériques de stockage de données (disques durs, disques amovibles, CD/DVD) ;
- périphériques réseau (modems, carte de réseau externe) ;
- périphériques d'impression (imprimantes) ;
- bus de connexion (ci-après, bus) : interfaces qui permettent de connecter les périphériques à la machine virtuelle protégée (USB, FireWire, etc.).

Le contrôle des périphériques gère l'accès utilisateur aux périphériques à l'aide des *règles d'accès aux périphériques* (ci-après, règles d'accès) (cf. rubrique “*A propos des règles d'accès aux périphériques et aux bus de connexion*” à la page 175) et des *règles d'accès aux bus de connexion* (ci-après, règles d'accès aux bus).

Par défaut, l'accès à tous les types de périphériques et bus de connexion est autorisé pour tous les utilisateurs et à tout moment. L'inscription dans les rapports de l'application des tentatives d'accès aux périphériques et bus de connexion refusées est aussi activée.

Activation et désactivation du Contrôle des périphériques

Le Contrôle des périphériques est activé par défaut. Le cas échéant, vous pouvez activer le Contrôle des périphériques.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;
- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver le Contrôle des périphériques, sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Protection Endpoint**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle des périphériques.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle des périphériques.
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle des périphériques.

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver le Contrôle des périphériques depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

> Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer le Contrôle des périphériques** pour activer le Contrôle des périphériques.
   - Décochez la case **Activer le Contrôle des périphériques** pour désactiver le Contrôle des périphériques.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles d'accès aux périphériques et aux bus de connexion

La règle d'accès aux périphériques est un ensemble des paramètres qui définit les fonctions suivantes du module Contrôle des périphériques :

- L'autorisation aux utilisateurs et/ou aux groupes d'utilisateurs sélectionnés d'accéder les types des périphériques pour les périodes définies.

  Vous pouvez sélectionner les utilisateurs et/ou les groupes d'utilisateurs et leur créer une programmation de l'accès aux périphériques.

- Définition de privilèges de lecture du contenu des périphériques de mémoire.
- Définition de privilèges de modification du contenu des périphériques de mémoire.

Par défaut, pour tous les types de périphériques de la classification du module Contrôle des périphériques sont créées les règles d'accès qui autorisent l'accès libre aux périphériques à tous les utilisateurs à tout moment si l'accès aux bus de connexion pour les types appropriés de périphériques est autorisé.

La règle d'accès au bus de connexion représente une extension ou une interdiction d'accès au bus de connexion.

Par défaut, les règles qui autorisent l'accès à tous les bus ont été créées pour les bus de connexion de la classification du module Contrôle des périphériques.

Vous ne pouvez pas créer et supprimer les règles d'accès aux périphériques et les règles d'accès aux bus de connexion, mais vous pouvez les modifier.

A propos des périphériques de confiance

Les *Périphériques de confiance* sont les périphériques que les utilisateurs définis dans les paramètres du périphérique de confiance peuvent accéder librement à tout moment.

> Si le périphérique est ajouté à la liste des périphériques de confiance et une règle d'accès qui interdit ou limite l'accès est créée pour ce type de périphérique, lors de la prise de la décision sur l'accès au périphérique la présence du périphérique sur la liste des périphériques de confiance a une priorité plus élevée que la règle d'accès.

Décisions types sur l'accès aux périphériques

Kaspersky Security décide d'autoriser ou non l'accès à un périphérique une fois que vous avez connecté ce périphérique à la machine virtuelle protégée.

Tableau 2. Décisions types sur l'accès aux périphériques

Conditions d'origine	Etapes intermédiaires avant la prise de décision sur l'accès au périphérique			Décision sur l'accès au périphérique
	Vérification de la présence du périphérique dans la liste des périphériques de confiance	Vérification de l'accès au périphérique sur la base de la règle d'accès	Vérification de l'accès au bus sur la base de la règle d'accès au bus	
Le périphérique ne figure pas dans le classement du module Contrôle des périphériques.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Ignoré	Accès autorisé
Le périphérique est un périphérique de confiance.	Figure sur la liste des périphériques de confiance.	Ignoré	Ignoré	Accès autorisé
L'accès au périphérique est autorisé.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé	Ignoré	Accès autorisé
Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès autorisé	Accès autorisé
Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès interdit.	Accès interdit.
L'accès au périphérique est autorisé. Règle d'accès au bus absente.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé	Règle d'accès au bus inexistante.	Accès autorisé

Conditions d'origine	Etapes intermédiaires avant la prise de décision sur l'accès au périphérique			Décision sur l'accès au périphérique
	Vérification de la présence du périphérique dans la liste des périphériques de confiance	Vérification de l'accès au périphérique sur la base de la règle d'accès	Vérification de l'accès au bus sur la base de la règle d'accès au bus	
Accès au périphérique interdit.	Ne figure pas sur la liste des périphériques de confiance.	Accès interdit.	Ignoré	Accès interdit.
Règle d'accès au périphérique et règle d'accès au bus inexistantes.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Règle d'accès au bus inexistante.	Accès autorisé
Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Accès autorisé	Accès autorisé
Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Accès interdit.	Accès interdit.

Vous pouvez modifier la règle d'accès au périphérique après sa connexion. Si le périphérique a été connecté et la règle d'accès a autorisé l'accès au périphérique, mais que vous avez ensuite modifié la règle d'accès pour interdire l'accès au périphérique, toute tentative d'accès au périphérique pour une opération de fichiers (consultation de l'arborescence des catalogues, lecture, enregistrement) sera d'ores et déjà bloquée par Kaspersky Security. Le blocage du périphérique sans système de fichiers aura lieu uniquement lors de la connexion suivante du périphérique.

Modification d'une règle d'accès aux périphériques

► *Pour modifier le privilège d'accès aux périphériques, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez l'onglet **Types de périphériques**.

   Sous l'onglet **Types de périphériques** se trouvent les règles d'accès pour tous les périphériques qui figurent dans le classement du module Contrôle des périphériques.
4. Sélectionnez la règle d'accès que vous souhaitez modifier.
5. Cliquez sur le bouton **Modifier**. Le bouton est accessible uniquement pour les types de périphériques avec un système de fichiers.

   La fenêtre **Configuration de la règle d'accès aux périphériques** s'ouvre.

   Par défaut, la règle d'accès aux périphériques autorise un accès libre au type de périphériques à tout moment pour tous les utilisateurs. Cette règle d'accès dans la liste **Utilisateurs et/ou groupes d'utilisateurs** contient le groupe **Tous** et contient dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès** la planification de l'accès aux périphériques tout le temps avec des privilèges définis pour toutes les opérations possibles avec les périphériques.
6. Modifiez les paramètres de la règle d'accès aux périphériques :

   a. Pour modifier la liste **Utilisateurs et/ou groupes d'utilisateurs**, utilisez les boutons **Ajouter**, **Modifier**, **Supprimer**.

   b. Pour modifier la liste de programmations d'accès aux périphériques, utilisez les boutons **Créer**, **Modifier**, **Copier**, **Supprimer** dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès**.

c. Sélectionnez l'utilisateur et/ou le groupe d'utilisateurs dans la liste **Utilisateurs et/ou groupes d'utilisateurs**.

d. Dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès**, configurez la programmation de l'accès aux périphériques pour l'utilisateur et/ou le groupe sélectionné d'utilisateurs. Pour ce faire, cochez les cases à côté des noms des programmations de l'accès aux périphériques que vous souhaitez utiliser dans la règle modifiable d'accès aux périphériques.

e. Pour chaque programmation de l'accès aux périphériques utilisée pour l'utilisateur ou le groupe d'utilisateurs sélectionnés, définissez les opérations autorisées lors de l'utilisation des périphériques. Pour ce faire, dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès** cochez les cases dans les colonnes avec les noms des opérations requises.

f. Répétez les étapes c à e pour les autres éléments de la liste **Utilisateurs et/ou groupes d'utilisateurs**.

g. Cliquez sur le bouton **OK**.

Une fois que vous avez modifié les valeurs d'origine des paramètres de la règle d'accès aux périphériques, le paramètre d'accès au type de périphérique prend la valeur *Limiter à l'aide de règles*.

7. En cas de nécessité, vous pouvez modifier la valeur du paramètre d'accès dans l'onglet **Types de périphériques** de la fenêtre de configuration du module Contrôle des périphériques :

   - si vous souhaitez autoriser l'accès à un type de périphérique, cliquez sur le bouton gauche de la souris dans la colonne **Accès** pour ouvrir le menu contextuel et choisissez l'option **Autoriser** ;

   - si vous souhaitez interdire l'accès à un type de périphérique, cliquez sur le bouton gauche de la souris dans la colonne **Accès** pour ouvrir le menu contextuel et choisissez l'option **Interdire**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la règle d'accès au bus de connexion

► *Pour modifier la règle d'accès au bus de connexion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez l'onglet **Bus de connexion**.

   Sous l'onglet **Bus de connexion** se trouvent les règles d'accès pour tous les bus de connexion qui existent dans la classification du module Contrôle des périphériques.
4. Sélectionnez la règle d'accès au bus que vous souhaitez modifier.
5. Modifiez la valeur du paramètre d'accès :
   - si vous souhaitez autoriser l'accès à un bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Autoriser** ;
   - si vous souhaitez interdire l'accès à un bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Interdire**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Actions avec les périphériques de confiance

Les actions suivantes peuvent être exécutées sur les périphériques de confiance :

- ajout du périphérique à la liste des périphériques de confiance ;
- modification de l'utilisateur et/ou groupe d'utilisateurs qui ont l'accès au périphérique de confiance ;
- suppression du périphérique de la liste des périphériques de confiance.

Dans cette section

Ajout du périphérique à la liste des périphériques de confiance

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

► *Pour ajouter un périphérique à la liste des périphériques de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez l'onglet **Périph. De confiance**.
4. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des périphériques de confiance** s'ouvre.
5. Cochez la case en regard du nom du périphérique que vous souhaitez ajouter à la liste des périphériques de confiance.

   La liste des périphériques dans la colonne **Périphériques** dépend de la valeur sélectionnée dans la liste déroulante **Afficher les périphériques connectés**.
6. Cliquez sur le bouton **Sélectionner**.

   La fenêtre de Microsoft Windows **Sélectionnez utilisateurs ou groupes** s'ouvre.

7. Indiquez les utilisateurs et/ou groupes d'utilisateurs pour lesquels Kaspersky Security doit considérer les périphériques sélectionnés comme périphériques de confiance.

   Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélectionnez utilisateurs ou groupes** s'affichent dans le champ **Autoriser les utilisateurs et/ou groupes d'utilisateurs**.

8. Cliquez sur le bouton **OK** dans la fenêtre **Sélection des périphériques de confiance**.

   La ligne des paramètres du périphérique de confiance ajouté s'affichera dans le tableau sous l'onglet **Périph. De confiance** de la fenêtre des paramètres du module **Contrôle des périphériques**.

9. Répétez les étapes 4 à 8 pour chacun des périphériques que vous souhaitez ajouter à la liste des périphériques de confiance pour des utilisateurs et/ou des groupes d'utilisateurs spécifiques.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du paramètre Utilisateurs du périphérique de confiance

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder. Vous pouvez modifier le paramètre **Utilisateurs** du périphérique de confiance.

► *Pour modifier le paramètre Utilisateurs du périphérique de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Sélectionnez l'onglet **Périph. De confiance**.

4. Dans la liste des périphériques de confiance, sélectionnez celui dont vous souhaitez modifier les paramètres.
5. Cliquez sur le bouton **Modifier**.

   La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.
6. Modifier la liste des utilisateurs et/ou des groupes d'utilisateurs pour lesquels ce périphérique est un périphérique de confiance.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression du périphérique de la liste des périphériques de confiance

► *Pour supprimer le périphérique de la liste des périphériques de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. De confiance**.
4. Sélectionnez le périphérique que vous souhaitez supprimer de la liste des périphériques de confiance.
5. Cliquez sur le bouton **Supprimer**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

La décision sur l'accès au périphérique que vous avez supprimé de la liste des périphériques de confiance est prise par Kaspersky Security sur la base des règles d'accès aux périphériques et sur la base des règles d'accès aux bus de connexion.

Modification des modèles de messages du Contrôle des périphériques

Quand vous tentez de vous adresser au périphérique bloqué, Kaspersky Security affiche le message sur le blocage d'accès au périphérique ou sur l'interdiction de l'opération sur le contenu du périphérique. Si vous estimez que le blocage d'accès au périphérique ou l'interdiction de l'opération sur le contenu du périphérique sont intervenus par erreur, vous pouvez cliquer sur le lien dans le message de blocage pour envoyer une réclamation à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message de blocage d'accès au périphérique et de message d'interdiction de l'opération avec le contenu du périphérique. Vous pouvez modifier les modèles de messages.

► *Pour modifier le modèle de message du Contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.
4. Exécutez une des actions suivantes :

   - Pour modifier le modèle de message de blocage d'accès au périphérique ou d'interdiction de l'opération avec le contenu du périphérique, sélectionnez l'onglet **Blocage**.
   - Pour modifier le modèle de message de réclamation à l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Requête**.

5. Modifiez le modèle de message de blocage ou de réclamation. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Obtention de l'accès au périphérique bloqué

Vous pouvez accéder au périphérique bloqué. Pour ce faire, il faut envoyer la demande depuis la fenêtre de configuration du module Contrôle des périphériques ou en passant par le lien dans le message de blocage de périphérique.

> Les fonctions de Kaspersky Security pour recevoir l'accès temporaire au périphérique sont disponibles uniquement dans le cas où Kaspersky Security fonctionne sous une stratégie de Kaspersky Security Center et que cette fonctionnalité a été activée dans les paramètres de la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

► *Pour accéder au périphérique bloqué depuis la fenêtre de configuration du module Contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Choisissez l'onglet **Statut de la protection**.

3. Déployez le groupe **Protection Endpoint**.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle des périphériques.

   Le menu de sélection des actions avec le module.

5. Choisissez l'option **Accès au périphérique** dans le menu.

   La fenêtre **Demande d'accès au périphérique** s'ouvre.

6. Sélectionnez dans la liste des périphériques connectés celui auquel vous souhaitez accéder.
7. Cliquez sur le bouton **Recevoir la clé d'accès**.

   La fenêtre **Obtenir la clé d'accès au périphérique** s'ouvre.
8. Indiquez dans le champ **Durée de l'accès** la durée pendant laquelle vous souhaitez avoir accès au périphérique.
9. Cliquez sur le bouton **Enregistrer**.

   Une fenêtre standard Microsoft Windows intitulée **Enregistrement de la clé d'accès** s'ouvre.
10. Sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès au périphérique, puis cliquez sur **Enregistrer**.
11. Transmettez le fichier contenant la clé d'accès au périphérique à l'administrateur du réseau local de l'organisation.
12. Il vous remettra le code d'accès au périphérique.
13. Dans la fenêtre **Demande d'accès au périphérique**, cliquez sur le bouton **Activer le code d'accès**.

    La fenêtre standard Microsoft Windows **Chargement du code d'accès** s'ouvre.
14. Sélectionnez le fichier contenant le code d'accès au périphérique remis par l'administrateur du réseau local, puis cliquez sur **Ouvrir**.

    La fenêtre **Activation du code d'accès au périphérique** qui fournit des informations sur l'accès octroyé s'ouvre.
15. Dans la fenêtre **Activation du code d'accès au périphérique**, cliquez sur **OK**.

► *Pour accéder au périphérique bloqué via le lien dans le message de blocage de l'appareil, procédez comme suit :*

1. Depuis la fenêtre de message de blocage du périphérique ou du bus de connexion, cliquez sur le lien **Demander l'accès**.

   La fenêtre **Obtenir la clé d'accès au périphérique** s'ouvre.

2. Indiquez dans le champ **Durée de l'accès** la durée pendant laquelle vous souhaitez avoir accès au périphérique.

3. Cliquez sur le bouton **Enregistrer**.

   Une fenêtre standard Microsoft Windows intitulée **Enregistrement de la clé d'accès** s'ouvre.

4. Sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès au périphérique, puis cliquez sur **Enregistrer**.

5. Transmettez le fichier contenant la clé d'accès au périphérique à l'administrateur du réseau local de l'organisation.

6. Il vous remettra le code d'accès au périphérique.

7. Dans la fenêtre **Demande d'accès au périphérique**, cliquez sur le bouton **Activer le code d'accès**.

   La fenêtre standard Microsoft Windows **Chargement du code d'accès** s'ouvre.

8. Sélectionnez le fichier contenant le code d'accès au périphérique remis par l'administrateur du réseau local, puis cliquez sur **Ouvrir**.

   La fenêtre **Activation du code d'accès au périphérique** qui fournit des informations sur l'accès octroyé s'ouvre.

9. Dans la fenêtre **Activation du code d'accès au périphérique**, cliquez sur **OK**.

La durée d'accès au périphérique octroyée peut varier de celle que vous avez demandée. L'accès au périphérique est octroyé pour une durée que l'administrateur du réseau local indique lors de la création du code d'accès au périphérique.

Contrôle Internet

Ce module est disponible si vous avez installé l'application Kaspersky Security sur une machine virtuelle tournant sous le système d'exploitation Windows et que vous aviez choisi le type d'installation standard.

Cette section contient des informations sur le Contrôle Internet et les instructions sur la configuration du module.

Dans cette section

À propos du Contrôle Internet

Le module Contrôle Internet permet de contrôler l'activité utilisateur du réseau local d'entreprise : limiter ou autoriser l'accès aux ressources Web. Une ressource Web désigne aussi bien une page Internet individuelle ou plusieurs pages ainsi qu'un site Internet ou plusieurs sites regroupés selon des traits communs.

Le Contrôle Internet offre les possibilités suivantes :

- Economie du trafic.

  Pour contrôler le trafic le module offre la possibilité de limiter ou interdire le téléchargement des fichiers multimédia et de limiter ou interdire l'accès aux sites Internet sans rapport avec l'activité professionnelle.

- Délimitation de l'accès selon les catégories de contenu des ressources Web.

  Pour minimiser le trafic et les pertes éventuelles dues à l'abus d'accès, vous pouvez limiter ou interdire l'accès aux ressources Web de catégories spécifiques (par exemple, interdire l'accès aux ressources Web appartenant à la catégorie “Médias d'actualités”). Pour plus d'informations sur les catégories de contenu, consultez la Base de connaissances (http://support.kaspersky.com/fr/13175).

- Une gestion centralisée d'accès aux ressources Web.

  Dans le cadre de l'utilisation de Kaspersky Security Center, il est possible de configurer l'accès aux ressources Web tant pour des individus que pour des groupes.

Toutes les restrictions et les interdictions d'accès aux sites Internet sont effectuées sous forme de règles d'accès aux sites Internet (cf. section “ a propos des règles d'accès aux ressources Web” à la page 192).

Activation et désactivation du Contrôle Internet

Le Filtrage du contenu est activé par défaut. Vous pouvez désactiver le Filtrage du contenu le cas échéant.

Vous pouvez activer et désactiver le module de deux manières :

- sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23) ;

- à partir de la fenêtre de configuration de l'application (cf. section “Fenêtre de configuration des paramètres de l'application” à la page 25).

► *Pour activer ou désactiver le Contrôle Internet, sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Protection Endpoint**.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle Internet.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle Internet.
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle Internet.

   Si l'option du menu n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

► *Pour activer ou désactiver le Contrôle Internet depuis la fenêtre de configuration de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

   Si les paramètres du module ne sont pas accessibles, cela signifie que vous ne pouvez pas activer ou désactiver ce module car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer le Contrôle Internet** pour activer le Contrôle Internet.
   - Décochez la case **Activer le Contrôle Internet** pour désactiver le Contrôle Internet.

   Si le Contrôle Internet est désactivé, Kaspersky Security ne contrôle pas l'accès aux ressources Web.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles d'accès aux ressources Web

La règle d'accès aux ressources Web est un ensemble de filtres et d'actions que Kaspersky Security exécute lorsque les utilisateurs consultent les ressources Web définies dans la règle à l'heure planifiée indiquée du fonctionnement de la règle. Les filtres permettent de préciser les ressources Web dont l'accès est contrôlé par le Contrôle Internet.

Les filtres suivants sont accessibles :

- **Filtrage selon le contenu**. Le Contrôle Internet organise les ressources Web en catégories de contenu et en catégories de type de données. Vous pouvez contrôler l'accès des utilisateurs aux ressources Web des catégories de contenu et/ou des catégories de types de données spécifiques. Lorsque les utilisateurs consultent les ressources Web qui appartiennent à la catégorie de contenu sélectionnée et/ou à la catégorie de type de données sélectionnée, Kaspersky Security exécute l'action indiquée dans la règle.
- **Filtrage selon les URL des ressources Web**. Vous pouvez contrôler l'accès des utilisateurs à toutes les adresses des ressources Web ou à certaines adresses de ressources Web/ou à certains groupes d'adresses de ressources Web.

  Si le filtrage selon le contenu et le filtrage selon les URL des ressources Web sont activés et les adresses des ressources Web définies et/ou les groupes d'adresses des ressources Web définis appartiennent aux catégories de contenu ou aux catégories de types de données sélectionnées, Kaspersky Security ne contrôle pas l'accès à toutes les ressources Web des catégories de contenu sélectionnées et/ou des catégories de types de données sélectionnées, mais uniquement aux adresses des ressources Web définies et/ou aux groupes d'adresses des ressources Web.

- **Filtrer par nom d'utilisateur et de groupe d'utilisateurs**. Vous pouvez définir les utilisateurs et/ou les groupes d'utilisateurs pour lesquels l'accès aux ressources Web est contrôlé conformément à la règle.

- **Planification de l'application de la règle**. Vous pouvez planifier l'application de la règle. La planification de l'application de la règle définit le moment où Kaspersky Security contrôle l'accès aux ressources Web indiquées dans la règle.

Après l'installation de l'application Kaspersky Security, le module Contrôle Internet dispose de deux règles pré-installées :

- La règle **Scripts et tables de styles** qui autorise tous les utilisateurs à accéder à tout moment à tous les sites dont l'URL contient des fichiers portant l'extension css, js, vbs. Par exemple, http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- La **Règle par défaut** qui autorise tous les utilisateurs à accéder à tous les sites Internet à tout moment.

Actions avec les règles d'accès aux ressources Web

Vous pouvez exécuter les actions suivantes avec les règles d'accès aux ressources Web :

- Ajouter une nouvelle règle.

- Exporter ou importer la liste d'URL des ressources Web de la règle.

  Si vous avez créé dans la règle d'accès aux ressources Web une liste des adresses des ressources Web, vous pouvez l'exporter dans un fichier au format TXT. Vous pouvez ensuite importer la liste depuis ce fichier pour ne pas créer manuellement la liste des adresses des ressources Web lors de la configuration de la règle. La fonction de l'exportation et de l'importation de la liste des adresses des ressources Web peut vous être utile si vous créez par exemple les règles aux paramètres similaires.

- Modifier la règle.

- Modifier la priorité de la règle.

  La priorité d'une règle dépend de la position de la ligne avec une brève description de la règle dans le tableau les **règles d'accès par ordre de priorité** de la fenêtre des paramètres du module Contrôle Internet. En d'autres termes, la règle qui se trouve au-dessus des autres règles dans le tableau les **règles d'accès par ordre de priorité** a une priorité supérieure.

  Si le site Internet auquel l'utilisateur essaie d'accéder correspond aux paramètres de plusieurs règles, l'action de Kaspersky Security sera définie par la règle avec la priorité la plus élevée.

- Vérifier le fonctionnement de la règle.

  Vous pouvez vérifier la cohérence de l'application des règles à l'aide du “Diagnostic des règles”.

- Activer et désactiver la règle.

  La règle d'accès aux ressources Web peut être activée (état *Actif*) ou désactivée (état *Inactif*). Par défaut, toute règle nouvellement créée est activée (état *Actif*). Vous pouvez désactiver la règle.

- Supprimer la règle.

Dans cette section

Ajout et modification de la règle d'accès aux ressources Web

► *Pour ajouter ou modifier la règle d'accès aux ressources Web, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Pour modifier la règle, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
4. Définissez ou modifiez les paramètres de la règle. Pour ce faire, procédez comme suit :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom**.

   b. Sélectionnez l'option requise dans la liste déroulante **Filtrer le contenu** :

      - **Tout contenu**.
      - **Par catégories**.
      - **Par types de données**.
      - **Par catégories et types de données**.

      Si un élément autre que **Tout contenu** est sélectionné, s'ouvre le groupe de sélection des catégories de contenu et/ou des catégories de type de données. Cochez les cases en regard des noms voulus des catégories de contenu et/ou des catégories de type de données.

      Si la case en regard du nom de la catégorie de contenu et/ou de la catégorie de type de données est cochée, Kaspersky Security, conformément à la règle, contrôle l'accès aux ressources Web qui appartiennent aux catégories de contenu et/ou aux catégories de type de données sélectionnées.

c. Choisissez l'option requise dans la liste déroulante **Appliquer aux adresses** :

- **A toutes les adresses**.
- **A certaines adresses**.

Si l'élément **A certaines adresses** est sélectionné, le groupe pour créer la liste des adresses des ressources Web s'ouvre. Vous pouvez créer ou modifier la liste des adresses des ressources Web à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**. Pour créer une liste d'adresses de sites Internet, vous pouvez également utiliser les *masques d'adresse d'un site Internet* (ci-après, masques d'adresse) (cf. section “Règles de création de masques d'adresse d'une ressource Web” à la page 198).

Une fois la liste d'adresses de ressources Web créée vous pouvez l'exporter vers un fichier afin de pouvoir par la suite importer cette liste depuis le fichier (cf. section “Exportation et importation de la liste des adresses de ressources Web” à la page 201).

d. Cochez la case **Indiquez les utilisateurs et/ou groupes** et cliquez sur le bouton **Sélectionner**.

La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

e. Définissez ou modifier la liste des utilisateurs et/ou des groupes d'utilisateurs qui interdit ou limite leur accès aux ressources Web prévus dans la règle.

f. Choisissez l'option requise dans la liste déroulante **Action** :

- **Autoriser**. Si cette valeur est sélectionnée, Kaspersky Security autorise l'accès aux ressources Web conformes aux paramètres de la règle.
- **Interdire**. Si cette valeur est sélectionnée, Kaspersky Security interdit l'accès aux ressources Web conformes aux paramètres de la règle.
- **Avertir**. Si cette valeur est sélectionnée, Kaspersky Security affiche un message d'avertissement sur le caractère éventuellement indésirable de la ressource Web lorsque l'utilisateur essaie d'accéder aux ressources Web conformes aux paramètres de la règle. Les liens du message d'avertissement permettent à l'utilisateur d'accéder à la ressource Web demandée.

g. Dans la liste déroulante **Planification de l'application de la règle**, sélectionnez le nom de la planification requise ou créez une autre planification sur la base de votre sélection. Pour ce faire, procédez comme suit :

   1. Cliquez sur le bouton **Configuration** en regard de la liste déroulante **Planification de l'application de la règle**.

      La fenêtre **Planification de l'application de la règle** s'ouvre.

   2. Pour ajouter à la planification de l'application de la règle un intervalle au cours duquel la règle n'est pas appliquée, cliquez-gauche sur les cellules correspondant aux heures et aux jours voulus de la semaine dans le tableau représentant la planification de l'application de la règle.

      La couleur des cellules deviendra grise.

   3. Pour modifier, dans la planification de l'application de la règle, l'intervalle au cours duquel la règle est appliquée en intervalle au cours duquel la règle n'est pas appliquée, cliquez-gauche sur les cellules grises du tableau correspondant aux heures et aux jours voulus de la semaine.

      La couleur des cellules deviendra verte.

   4. Cliquez sur le bouton **OK** ou sur **Enregistrer sous** si vous planifiez l'application de la règle sur la base de la règle “Toujours”, composée par défaut. Cliquez sur le bouton **Enregistrer sous** si vous planifiez l'application de la règle sur la base d'une planification autre qu'une planification par défaut.

      La fenêtre **Nom de la planification de l'application de la règle** s'ouvre.

   5. Saisissez le nom de la planification de l'application de la règle ou gardez le nom proposé par défaut.

   6. Cliquez sur le bouton **OK**.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règle d'accès aux sites Internet**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Règles de création de masques d'adresse d'une ressource Web

Le masque d'adresse de la ressource Web peut vous être utile lorsque vous devez saisir une multitude d'adresses de ressources Web similaires au moment de la création d'une règle d'accès aux ressources Web. Un seul masque correct peut se substituer à une multitude d'adresses de ressources Web.

Pour créer un masque d'adresse, il faut prendre en considération les règles suivantes :

1. Le caractère `*` remplace n'importe quelle séquence de caractères dont le nombre de caractères est zéro ou plus.

   Par exemple, lors de la saisie du masque d'adresse *abc* la règle d'accès aux ressources Web s'applique à toutes les adresses de ressources Web qui contiennent la séquence abc. Exemple : http://www.example.com/page_0-9abcdef.html.

   Le caractère `?` est l'équivalent au point d'interrogation et pas à n'importe quel caractère, ce qui est en général le cas pour les règles de création des masques d'adresse dans le module Antivirus Internet.

   Pour ajouter le caractère `*` au masque d'adresse, vous devez saisir deux caractères `*`, et non pas la séquence `\*`, comme c'est le cas d'habitude dans les règles de création des masques d'adresses du module Antivirus Internet.

2. La suite de caractère `www.` au début du masque d'adresse est remplacée par `*.`

   Exemple : le masque d'adresse www.example.com est équivalent à *.example.com.

3. Si le masque d'adresse commence par un caractère autre que `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `*.`

4. La séquence des caractères `*.` au début du masque d'adresse est traitée comme `*.` ou comme la ligne vide.

   Exemple : le masque d'adresse http://www.*.example.com couvre l'adresse http://www2.example.com.

5. Si le masque d'adresses se termine par le caractère différent de / ou *, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe /*.

   Exemple : le masque d'adresse http://www.example.com couvre les adresses du type http://www.example.com/abc, où a, b, c représentent n'importe quels caractères.

6. Si le masque d'adresse se termine par le caractère /, le contenu du masque d'adresse est équivalent au même contenu avec le suffixe *.

7. La séquence des caractères /* à la fin du masque d'adresse est traitée comme /* ou comme la ligne vide.

8. La vérification des adresses des ressources Web par masque d'adresse est effectuée compte tenu du schéma (http ou https) :

   - S'il n'y a pas de protocole réseau dans le masque d'adresse, ce masque d'adresse couvre les adresses de ressources Web avec n'importe quel protocole réseau.

     Exemple : le masque d'adresse example.com couvre les adresses de ressource Web http://example.com et https://example.com.

   - S'il y a un protocole réseau dans le masque d'adresse, ce masque d'adresse couvre uniquement les adresses de ressources Web avec un protocole réseau identique à celui du masque d'adresse.

     Exemple : le masque d'adresse http://*.example.com couvre l'adresse http://www.example.com et ne couvre pas l'adresse https://www.example.com.

9. Le masque d'adresse dans les guillemets doubles est interprété sans aucune permutation supplémentaire, sauf le caractère * s'il faisait partie du masque d'adresse d'origine. Cela veut dire que pour ces masques d'adresses les règles 5 et 7 ne sont pas appliquées.

10. Lors de la comparaison au masque d'adresse de la ressource Web ne sont pas pris en compte le nom d'utilisateur et le mot de passe, le port de connexion et le registre de caractères.

Tableau 3. Exemples d'application des règles de création de masques d'adresses

N°	Masque d'adresse	Adresse de la ressource Web analysée	Est-ce que l'adresse analysée satisfait au masque d'adresse	Commentaires
1	*.example.com	http://www.123example.com	Non	Cf. règle 1.
2	*.example.com	http://www.123.example.com	Oui	Cf. règle 1.
3	*example.com	http://www.123example.com	Oui	Cf. règle 1.
4	*example.com	http://www.123.example.com	Oui	Cf. règle 1.
5	http://www.*.example.com	http://www.123example.com	Non	Cf. règle 1.
6	www.example.com	http://www.example.com	Oui	Cf. règle 2, 1.
7	www.example.com	https://www.example.com	Oui	Cf. règle 2, 1.
8	http://www.*.example.com	http://123.example.com	Oui	Cf. règles 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Oui	Cf. règles 2, 5, 1.
10	example.com	http://www.example.com	Oui	Cf. règle 3, 1.
11	http://example.com/	http://example.com/abc	Oui	Cf. règles 6.
12	http://example.com/*	http://example.com	Oui	Cf. règle 7.
13	http://example.com	https://example.com	Non	Cf. règle 8.
14	“example.com”	http://www.example.com	Non	Cf. règle 9.
15	“http://www.example.com”	http://www.example.com/abc	Non	Cf. règle 9.
16	“*.example.com”	http://www.example.com	Oui	Cf. règle 1, 9.
17	“http://www.example.com/*”	http://www.example.com/abc	Oui	Cf. règle 1, 9.

N°	Masque d'adresse	Adresse de la ressource Web analysée	Est-ce que l'adresse analysée satisfait au masque d'adresse	Commentaires
18	“www.example.com”	http://www.example.com ; https://www.example.com	Oui	Cf. règle 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Non	Le masque d'adresse contient plus d'informations que l'adresse de la ressource Web

Exportation et importation de la liste des adresses de ressources Web

Si vous avez créé dans la règle d'accès aux ressources Web une liste des adresses des ressources Web, vous pouvez l'exporter dans un fichier au format TXT. Vous pouvez ensuite importer la liste depuis ce fichier pour ne pas créer manuellement la liste des adresses des ressources Web lors de la configuration de la règle. La fonction de l'exportation et de l'importation de la liste des adresses des ressources Web peut vous être utile si vous créez par exemple les règles aux paramètres similaires.

► *Pour exporter la liste des adresses des ressources Web dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Sélectionnez la règle dont la liste des adresses des ressources Web que vous souhaitez exporter dans un fichier.

4. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.

   Sous la liste déroulante **Appliquer aux adresses** apparaîtra la liste des adresses de ressources Web auxquelles s'applique la règle.

5. Pour exporter uniquement une partie de la liste des adresses des ressources Web, sélectionnez les adresses requises des ressources Web.

6. Cliquez sur le bouton  à droite du champ avec la liste des adresses des ressources Web.

   La fenêtre de confirmation de l'action s'ouvre.

7. Exécutez une des actions suivantes :

   - Pour exporter uniquement les éléments sélectionnés dans liste des adresses des ressources Web, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Oui**.
   - Pour exporter tous les éléments sélectionnés dans liste des adresses des ressources Web, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Non**.

   La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvre.

8. Sélectionnez le fichier où vous souhaitez exporter la liste des adresses des ressources Web, puis cliquez sur le bouton **Enregistrer**.

► *Pour importer dans la règle la liste des adresses des ressources Web depuis un fichier, procédez comme suit :*

1. Ouvrez la fenetre de configuration des parametres de l'application.
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Si vous voulez créer une nouvelle règle, cliquez sur le bouton **Ajouter**.
   - Pour modifier la règle, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.

4. Exécutez une des actions suivantes :

   - Pour créer une nouvelle règle d'accès aux ressources Web, sélectionnez dans la liste déroulante **Appliquer aux adresses** l'élément **A certaines adresses**.
   - Si vous modifiez la règle d'accès aux ressources Web, passez au paragraphe 5 de l'instruction.

5. Cliquez sur le bouton  à droite du champ avec la liste des adresses des ressources Web.

   Si vous créez une nouvelle règle la fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

   Si vous modifiez la règle, la fenêtre de confirmation de l'action s'ouvre.

6. Exécutez une des actions suivantes :

   - Si vous créez une nouvelle règle d'accès aux ressources Web, passez au paragraphe 7 de l'instruction.
   - Si vous modifiez la règle d'accès aux ressources Web, dans la fenêtre de confirmation de l'action exécutez une des actions suivantes :
     - Pour ajouter aux éléments existants les éléments importés de la liste des adresses des ressources Web, cliquez sur le bouton **Oui**.
     - Pour supprimer les éléments existants de la liste des adresses des ressources Web et ajouter les éléments importés, cliquez sur le bouton **Non**.

   La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

7. Sélectionnez dans la fenêtre de Microsoft Windows **Ouvrir le fichier** le fichier avec la liste des adresses des ressources Web à importer.

8. Cliquez sur le bouton **Ouvrir**.

9. Cliquez sur le bouton **OK** dans la fenêtre **Règle d'accès aux sites Internet**.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Vérification du fonctionnement des règles d'accès aux ressources Web

Vous pouvez vérifier le fonctionnement des règles d'accès aux ressources Web. Pour ce faire, le module Contrôle Internet prévoit le “Diagnostic des règles”. A l'issue de l'analyse de fonctionnement des règles, un message sur l'action de Kaspersky Security conformément à la première règle appliquée au moment de l'accès à la/aux ressource(s) Web définie(s) (autorisation, interdiction, avertissement) sera affiché. Toutes les autres règles appliquées sont ensuite vérifiées.

► *Pour vérifier le fonctionnement des règles d'accès aux ressources Web, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Diagnostic**.

   La fenêtre **Diagnostic des règles** s'ouvre.
4. Remplissez les champs dans le groupe **Conditions** :

   a. Cochez la case **Indiquez l'adresse** pour vérifier le fonctionnement des règles que Kaspersky Security utilise pour contrôler l'accès à une ressource Web spécifique. Saisissez l'adresse de la ressource Web dans le champ ci-dessous.

   b. Définissez la liste des utilisateurs et/ou des groupes d'utilisateurs si vous voulez vérifier le fonctionnement des règles que Kaspersky Security utilise pour contrôler l'accès à des ressources Web pour des utilisateurs et/ou des groupes d'utilisateurs spécifiques. Pour ce faire, procédez comme suit :

      1. Cochez la case **Indiquez les utilisateurs et/ou groupes** et cliquez sur le bouton **Sélectionner**.

         La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

2. Indiquez les utilisateurs et/ou groupes d'utilisateurs nécessaires dans la fenêtre Microsoft Windows **Sélectionnez Utilisateurs ou Groupes**, puis cliquez sur le bouton **OK**.

c. Sélectionnez dans la liste déroulante **Filtrer le contenu** l'élément requis (**Par catégories**, **Par types de données** ou **Par catégories et types de données**) pour vérifier le fonctionnement des règles que Kaspersky Security utilise pour contrôler l'accès à des ressources Web avec des catégories de contenu et/ou des catégories de type de données, puis cochez les cases correspondant aux catégories de contenu et/ou aux catégories de type de données nécessaires.

d. Cochez la case **Tenir compte de l'heure de la tentative d'accès** si vous voulez vérifier le fonctionnement des règles en tenant compte du jour de la semaine et de l'heure des tentatives d'accès aux ressources Web indiquées dans les conditions du diagnostic des règles. Indiquez sur la droite le jour de la semaine et l'heure.

5. Cliquez sur le bouton **Analyser**.

A droite du bouton **Analyser**, un message sur l'action de Kaspersky Security conformément à la première règle appliquée au moment de l'accès à la/aux ressources Web définie(s)sera affiché. La première règle appliquée est celle qui se trouve dans la liste des règles de Contrôle Internet au-dessus des autres règles conformes aux conditions du diagnostic. Le tableau dans la partie inférieure de la fenêtre **Diagnostic des règles** affiche la liste des autres règles qui se sont déclenchées et le nom de l'action exécutée par Kaspersky Security. Les règles sont classées par ordre de priorité décroissante.

Modification de la priorité des règles d'accès aux ressources Web

Vous pouvez modifier la priorité de chaque règle d'accès aux ressources Web dans la liste des règles en les structurant dans un ordre spécifique.

> Vous ne pouvez pas modifier la priorité de la règle “Règle par défaut”. Elle possède toujours la priorité la plus basse et se trouve au bas de la liste de règles.

► *Pour modifier la priorité des règles d'accès aux ressources Web, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez dans la liste de règles celle dont vous souhaitez modifier la priorité.
4. Déplacez la règle en position souhaitée dans la liste des règles à l'aide des boutons **Haut** et **Bas**.
5. Répétez les paragraphes 3 et 4 de l'instruction pour les règles dont la priorité vous souhaitez modifier.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle d'accès aux ressources Web

► *Pour activer ou désactiver la règle d'accès aux ressources Web, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la liste de règles, sélectionnez celle que vous souhaitez activer ou désactiver.
4. Dans la colonne **Etat**, procédez comme suit :
   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Actif*.
   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Inactif*.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des messages du Contrôle Internet

En fonction de l'action définie dans les propriétés des règles d'accès aux ressources Web, lorsque vous essayez d'accéder aux ressources Web, Kaspersky Security affiche un message (en remplaçant la réponse du serveur HTTP par une page HTML avec le message) d'un des types suivants :

- **Message d'avertissement**. Ce message signale un danger éventuel au niveau du site Internet et/ou un non-respect de la stratégie d'entreprise. Kaspersky Security affiche le message d'avertissement si, dans les propriétés de la règle qui décrit ce site Internet, dans la liste déroulante **Action**, l'élément **Avertir** est sélectionné.

  Si vous croyez recevoir ce message d'avertissement par erreur, en cliquant sur le lien dans le corps du message d'avertissement vous pouvez ouvrir un message de réclamation destiné à l'administrateur du réseau local d'entreprise.

- **Message de blocage de la ressource Web**. Kaspersky Security affiche le message de blocage de la ressource Web, si dans les propriétés de la règle qui décrit cette ressource dans la liste déroulante **Action** l'élément **Interdire** est sélectionné.

  Si vous croyez que l'accès à la ressource Web a été bloqué par erreur, cliquez sur le lien dans le corps du message de blocage de la ressource Web pour ouvrir un message de réclamation destiné à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message d'avertissement et de message de réclamation destinés à l'administrateur du réseau local d'entreprise. Vous pouvez modifier leur contenu (cf. section “Modification des modèles de messages du contrôle Internet” à la page 208).

Modification des modèles de messages du Contrôle Internet

► *Pour modifier le modèle de message du Contrôle Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.
4. Exécutez une des actions suivantes :

   - Si vous souhaitez modifier le modèle du message d'avertissement sur le danger éventuel du site Internet, sélectionnez l'onglet **Avertissement**.
   - Si vous souhaitez modifier le modèle du message de blocage d'accès au site Internet, sélectionnez l'onglet **Blocage**.
   - Si vous souhaitez modifier le modèle du message de réclamation, sélectionnez l'onglet **Requête**.
5. Modifier le modèle de message. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse de la machine virtuelle

Cette section présente les particularités et la configuration des tâches d'analyse, les niveaux de sécurité ainsi que les méthodes et technologies d'analyse. Elle explique également comment manipuler les fichiers non traités par Kaspersky Security lors de la recherche sur la machine virtuelle d'éventuels virus et autres programmes présentant une menace potentielle.

Dans cette section

A propos des tâches d'analyse

La recherche de virus est un élément important dans la protection de la machine virtuelle. Il est indispensable d'effectuer la recherche de virus et d'autres applications présentant une menace pour la machine virtuelle à intervalle régulier afin d'éviter la propagation de programmes malveillants qui n'auraient pas été détectés par les modules de protection, par exemple en raison d'un niveau de sécurité trop faible ou pour toute autre raison.

Kaspersky Security propose les tâches d'analyse suivantes pour la recherche de virus et d'autres applications malveillantes :

- **Analyse complète**. Analyse approfondie de l'ensemble du système d'exploitation invité installé sur la machine virtuelle protégée. Kaspersky Security analyse par défaut les objets suivants :
  - mémoire vive ;
  - objets chargés au démarrage du système d'exploitation ;

- sauvegarde du système d'exploitation ;
- tous les disques durs ou amovibles connectés à la machine virtuelle protégée.

- **Analyse des zones critiques**. Kaspersky Security analyse par défaut les objets chargés au démarrage du système d'exploitation.
- **Analyse personnalisée**. Kaspersky Security analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :
  - mémoire vive ;
  - objets chargés au démarrage du système d'exploitation ;
  - sauvegarde du système d'exploitation ;
  - bases de messagerie ;
  - tous les disques durs, amovibles ou réseau connectés à la machine virtuelle protégée ;
  - n'importe quel fichier sélectionné.

> La tâche d'analyse complète et la tâche d'analyse des zones critiques sont des tâches spécifiques. Pour ces tâches, il est déconseillé de modifier la zone d'analyse.

Après le lancement des tâches d'analyse, la progression de l'analyse est affichée dans le champ en face du nom de la tâche d'analyse exécutée dans le groupe **Gestion des tâches** sous l'onglet **Statut de la protection de** la fenêtre principale de l'application (cf. section “Fenêtre principale de l'application” à la page 23).

Les informations relatives aux résultats de l'analyse et à tous les événements survenus pendant l'exécution des tâches d'analyse sont consignées dans le rapport de Kaspersky Security.

Lancement et arrêt de la tâche d'analyse

Vous pouvez lancer ou arrêter la tâche d'analyse à tout moment, et ce indépendamment du mode de lancement de la tâche d'analyse sélectionné (cf. section “Sélection du mode d'exécution de la tâche d'analyse” à la page 225).

► *Pour lancer ou arrêter la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Gestion des tâches**.
4. Cliquez sur la ligne affichant le nom de la tâche d'analyse.

   Le menu de sélection des actions pour la tâche d'analyse s'ouvre.

   > Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que l'administration de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Lancer l'analyse** pour lancer la tâche d'analyse.

     L'état de l'exécution de la tâche d'analyse affiché à droite du nom de la tâche d'analyse passera à *En cours*.

   - Sélectionnez dans le menu l'option **Arrêter l'analyse** pour arrêter la tâche d'analyse.

     L'état de l'exécution de la tâche d'analyse affiché à droite du nom de la tâche d'analyse passera à *Arrêté*.

Vous pouvez également lancer une analyse personnalisée de n'importe quel fichier après avoir appelé le menu contextuel de Windows et sélectionné l'élément **Rechercher des virus**.

Configuration des paramètres des tâches d'analyse

Pour configurer les paramètres des tâches d'analyse, vous pouvez exécuter les opérations suivantes :

- Modifier le niveau de sécurité.

  Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

- Modifier l'action que Kaspersky Security exécute en cas de détection d'un fichier infecté.

- Créer la zone d'analyse.

  Vous pouvez élargir ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets d'analyse ou en modifiant le type de fichiers à analyser.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. Vous pouvez également réduire la période d'analyse d'un fichier. A l'issue du temps défini, Kaspersky Security exclut le fichier de l'analyse en cours (sauf les archives et les objets qui incluent plusieurs fichiers).

- Configurer l'analyse des fichiers composés.

- Configurer l'utilisation de l'analyse heuristique.

  Kaspersky Security utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Security analyse l'activité des objets dans le système d'exploitation. L'Analyse heuristique permet de détecter de nouveaux objets malveillants dont les enregistrements n'ont pas encore été ajoutés aux bases de l'application.

- Configurer l'utilisation de la technologie d'analyse iSwift.

  Vous pouvez activer la technologie iSwift qui permet d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse. L'activation de la technologie iSwift implique l'utilisation de la technologie SharedCache qui permet d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers ayant déjà été analysés sur une autre machine virtuelle.

- Sélectionner le mode d'exécution des tâches d'analyse.

  Si l'exécution de la tâche d'analyse est impossible pour une raison quelconque (par exemple, la machine virtuelle protégée était éteinte à ce moment), vous pouvez configurer le lancement automatique de la tâche d'analyse ignorée dès que cela est possible.

  Vous pouvez reporter le lancement de la tâche d'analyse par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche d'analyse **Selon la planification** et l'heure de lancement de Kaspersky Security est le même que l'heure programmée pour le lancement de la tâche d'analyse. La tâche d'analyse ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Security.

- Configurer le lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur.

- Indiquer les paramètres de l'analyse des disques amovibles lors de leur connexion à la machine virtuelle protégée.

Dans cette section

Modification du niveau de sécurité

Kaspersky Security utilise différents ensembles de paramètres pour exécuter les tâches d'analyse. Ces ensembles de paramètres sont appelés *niveaux de sécurité*. Trois niveaux sont prévus pour la protection : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont considérés comme optimaux et sont recommandés par les experts de Kaspersky Lab.

► *Afin de modifier le niveau de sécurité, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :
   - **Analyse complète**.
   - **Analyse des zones critiques**.
   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

   Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre avec le nom de la tâche d'analyse qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité, le nom du niveau de sécurité dans le groupe **Niveau de sécurité** devient **Autre**.
   - Si vous souhaitez revenir au niveau **Recommandé**, cliquez sur le bouton **Par défaut**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action sur les fichiers infectés

► *Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :

   - **Analyse complète**.
   - **Analyse des zones critiques**.
   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

   > Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :

   - **Sélectionner l'action automatiquement**.

     Cette option est sélectionnée par défaut. Suite à la détection d'une menace, l'application exécute l'action **Réparer. Supprimer si la réparation est impossible**.

   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible**.

   - **Exécuter l'action : Réparer**.

     > Pour les fichiers qui font partie d'une application Windows Store, Kaspersky Security exécute l'action **Supprimer** quelle que soit l'option sélectionnée.

   - **Exécuter l'action : Supprimer**.

   - **Exécuter l'action : Informer**.

   > Lors de la suppression ou de la réparation, des copies des fichiers sont conservées dans la sauvegarde.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Constitution de la zone d'analyse

La *zone d'analyse* fait référence à l'emplacement et au type de fichiers (par exemple, tous les disques durs, objets de démarrage, bases de messagerie), analysés par l'application pendant l'exécution de la tâche d'analyse.

Pour former la zone d'analyse, vous devez procéder comme suit :

- Créer la liste des objets analysés par Kaspersky Security.
- Sélectionnez le type de fichiers à analyser.

► *Pour former la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Choisissez l'onglet **Statut de la protection**.
3. Déployez le groupe **Gestion des tâches**.
4. Cliquez sur la ligne affichant le nom de la tâche d'analyse souhaitée :
   - **Analyse complète**.
   - **Analyse des zones critiques**.
   - **Analyse personnalisée**.

   Le menu de sélection des actions pour la tâche d'analyse s'ouvre.

   > Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

5. Dans le menu, sélectionnez l'option **Zone d'analyse**.

   La fenêtre **Zone d'analyse** va s'ouvrir.

6. Dans le groupe **Zone d'analyse**, exécutez une des actions suivantes :
   - Si vous souhaitez ajouter un nouvel objet à la liste des objets analysés, cliquez sur le bouton **Ajouter**.

     La fenêtre **Sélection de l'objet** s'ouvre.
   - Pour modifier le chemin de l'objet, sélectionnez-le dans la liste des objets et cliquez sur le bouton **Modifier**.

     La fenêtre **Sélection de l'objet** s'ouvre.

- Pour supprimer un objet de la zone d'analyse, sélectionnez l'objet dans la liste des objets et cliquez sur **Supprimer**.

  La fenêtre de confirmation de suppression s'ouvre.

  > Vous ne pouvez pas supprimer ou modifier les objets ajoutés à la zone d'analyse par défaut.

7. Exécutez une des actions suivantes dans la fenêtre **Sélection de l'objet** :

   - Pour ajouter un nouvel objet, sélectionnez-le dans la fenêtre **Sélection de l'objet** et cliquez sur le bouton **Ajouter**.

     Tous les objets sélectionnés dans la fenêtre **Sélection de l'objet** seront affichés dans la liste des objets de la fenêtre **Zone d'analyse**.

     Cliquez sur le bouton **OK**.

   - Si vous souhaitez modifier le chemin vers un objet de la liste des objets, indiquez un autre chemin dans le champ **Objet et** cliquez sur le bouton **OK**.

   - Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

8. Le cas échéant, répétez les points 6 et 7 pour ajouter des objets, modifier leur chemin ou les supprimer de la zone d'analyse.

9. Si vous souhaitez exclure un objet de la zone d'analyse décochez la case à côté de cet objet dans la liste des objets de la fenêtre **Zone d'analyse**. Cet objet reste dans la liste des objets analysés mais n'est pas analysé pendant l'exécution de la tâche d'analyse.

10. Cliquez sur le bouton **OK** dans la fenêtre **Zone d'analyse**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

► *Pour sélectionner le type de fichiers à analyser, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :
   - **Analyse complète**.
   - **Analyse des zones critiques**.
   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

   > Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.
4. Dans la fenêtre avec le nom de la tâche d'analyse sélectionnée, sélectionnez l'onglet **Zone d'action**.
5. Sélectionnez dans le groupe **Types de fichiers** le type de fichiers que vous souhaitez analyser pendant l'exécution de la tâche d'analyse :
   - Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
   - Sélectionnez **Fichiers analysés selon le format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
   - Sélectionnez **Fichiers analysés selon l'extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

Au moment de choisir le type d'objet à analyser, il convient de ne pas oublier les éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, les formats EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- L'individu malintentionné peut envoyer un virus ou une autre application malveillante sur votre machine virtuelle dans un fichier exécutable renommé avec une extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors Kaspersky Security analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Ce fichier est scrupuleusement analysé pour la recherche de virus et d'autres applications malveillantes.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Optimisation de l'analyse des fichiers

► *Pour optimiser l'analyse des fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :

   - **Analyse complète**.

   - **Analyse des zones critiques**.

   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Zone d'action**.
5. Dans le groupe **Optimisation de l'analyse**, procédez comme suit :
   - Cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.
   - Cochez la case **Ignorer les fichiers si l'analyse dure plus de et** définissez la durée d'analyse d'un fichier (en secondes).
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés

L'insertion de virus et d'autres applications malveillantes dans des fichiers composés tels que des archives ou les bases de données est une pratique de dissimulation très répandue. Pour détecter les virus dissimulés et les autres applications malveillantes, vous devez décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limites le cercle des fichiers composés analysés pour accélérer l'analyse.

► *Pour configurer l'analyse des fichiers composés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :
   - **Analyse complète**.

- **Analyse des zones critiques**.
- **Analyse personnalisée**.

Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

> Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action**, dans le groupe **Analyse des fichiers composés**, indiquez les fichiers composés à analyser : archives, paquets d'installation ou objets OLE incorporés, fichiers au format de messagerie ou fichiers protégés par un mot de passe en cochant les cases correspondantes.

5. Si dans le groupe **Optimisation de l'analyse** la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est décochée, vous pouvez indiquer pour chaque type de fichier composé s'il faut analyser tous les fichiers de ce type ou uniquement les nouveaux fichiers. Pour réaliser la sélection, cliquez sur le lien **tous/nouveaux**, situé à côté du nom de type du fichier composé. Le lien change de valeur lorsque vous cliquez sur le bouton gauche de la souris.

   Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée, l'application analyse uniquement les nouveaux fichiers.

6. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

7. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Si vous ne souhaitez pas que l'application décompresse les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

- Si vous souhaitez que l'application décompresse les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

  Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

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

8. Cliquez sur le bouton **OK** dans la fenêtre **Fichiers composés**.
9. Cliquez sur le bouton **OK** dans la fenêtre avec le nom de la tâche d'analyse.
10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'utilisation de l'analyse heuristique

► *Pour configurer l'utilisation de l'analyse heuristique, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :
   - **Analyse complète**.
   - **Analyse des zones critiques**.
   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

> Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

5. Dans le groupe **Méthodes d'analyse**, procédez comme suit :

   - Si vous souhaitez que l'application utilise l'analyse heuristique au cours de la tâche d'analyse, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

   - Si vous souhaitez que l'application n'utilise pas l'analyse heuristique au cours de la tâche d'analyse, décochez la case **Analyse heuristique**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'utilisation de la technologie iSwift

► *Pour configurer l'utilisation de la technologie iSwift, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :

   - **Analyse complète**.

   - **Analyse des zones critiques**.

   - **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
5. Dans le groupe **Technologie d'analyse**, exécutez une des actions suivantes :

   - Cochez la case **Technologie iSwift** si vous souhaitez utiliser cette technologie pendant l'analyse.
   - Décochez la case **Technologie iSwift** si vous souhaitez utiliser cette technologie pendant l'analyse.

   L'activation de la technologie iSwift entraîne également l'activation de la technologie SharedCache.

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection du mode de lancement de la tâche d'analyse

► *Pour sélectionner le mode d'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise :

   - **Analyse complète**.

- **Analyse des zones critiques**.
- **Analyse personnalisée**.

Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

> Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre avec le nom de la tâche sélectionnée s'ouvre.

4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche d'analyse :

   - Sélectionnez l'option **Manuel** pour lancer la tâche d'analyse manuellement.
   - Sélectionnez l'option **Selon la planification**, pour programmer l'exécution de la tâche d'analyse.

5. Exécutez une des actions suivantes :

   - Si vous avez sélectionné l'option **Manuel**, passez au paragraphe 6 de l'instruction.
   - Si vous avez sélectionné l'option **Selon la planification**, définissez les paramètres de planification du lancement de la tâche d'analyse. Pour ce faire, procédez comme suit :

     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche d'analyse. Sélectionnez une des options suivantes : **Jours**, **Chaque semaine**, **A l'heure indiquée**, **Tous les mois**, **Après le lancement de l'application**, **Après chaque mise à jour**.

     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche d'analyse.

c. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que l'application Kaspersky Security lance à la première occasion les tâches d'analyse non exécutées en temps opportun.

> Si dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application** ou **Après chaque mise à jour** est sélectionné, la case **Lancer les tâches non exécutées** est inaccessible.

d. Cochez la case **Suspendre l'analyse programmée lorsque l'écran de veille est inactif et si la machine virtuelle protégée n'est pas verrouillée** si vous souhaitez que l'application Kaspersky Security suspende l'analyse lorsque les ressources de la machine virtuelle sont occupées. Cette option de planification de la tâche d'analyse permet d'économiser les ressources pendant l'utilisation de la machine virtuelle.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration du lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur

Par défaut, la tâche d'analyse est lancée sous le compte que vous avez utilisé pour ouvrir la session dans le système d'exploitation invité de la machine virtuelle protégée. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche d'analyse sous les privilèges d'un autre utilisateur. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de la tâche d'analyse et lancer la tâche d'analyse au nom de cet utilisateur.

► *Pour configurer le lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise :

   - **Analyse complète**.

- **Analyse des zones critiques**.
- **Analyse personnalisée**.

Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

> Si des tâches d'analyse n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de ces tâches d'analyse est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**.
5. Saisissez dans le champ **Nom** le nom du compte utilisateur dont les privilèges sont exigés pour lancer la tâche d'analyse.
6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur dont vous souhaitez utiliser les privilèges pour lancer la tâche d'analyse.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des disques amovibles lors de leur connexion à la machine virtuelle

Ces derniers temps, les programmes malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles sont largement répandus. Kaspersky Security permet d'analyser les disques amovibles pour y rechercher des virus et d'autres applications malveillantes lors de la connexion des disques amovibles à la machine virtuelle.

► *Pour configurer l'analyse des disques amovibles lors de leur connexion à la machine virtuelle, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Sélectionnez le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre.

   La partie droite de la fenêtre affichera les paramètres généraux des tâches planifiées.
3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez l'action requise dans la liste déroulante **Action à exécuter lors de la connexion d'un disque amovible** :

   - **Ne pas analyser**.
   - **Analyse complète**.
   - **Analyse rapide**.

   Si le groupe n'est pas disponible, cela signifie que la configuration des paramètres de l'analyse des disques amovibles est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.
4. Cochez la case **Taille maximale du disque amovible** du disque amovible et indiquez dans le champ à côté la valeur en mégaoctets si vous souhaitez que l'application Kaspersky Security analyse les disques amovibles dont la taille est inférieure ou égale à la valeur définie.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Manipulation des fichiers non traités

Cette section explique comment manipuler les fichiers infectés que l'application Kaspersky Security n'a pas traité lors de la recherche d'éventuels virus et autres programmes dangereux sur la machine virtuelle.

Dans cette section

A propos des fichiers non traités

L'application Kaspersky Security consigne les informations sur les fichiers dans lesquels elle a détecté une menace mais qu'elle n'a pas traités. Ces informations se présentent sous la forme d'événements dans la liste des fichiers non traités.

Un fichier infecté est considéré comme *traité* si l'application Kaspersky Security, lors de la recherche de la présence éventuelle de virus et autres applications malveillantes sur la machine virtuelle, a réalisé une des opérations suivantes sur ce fichier conformément aux paramètres définis :

- Réparer.
- Supprimer.
- Supprimer si la désinfection est impossible.

Un fichier infecté est considéré comme *non traité* si l'application Kaspersky Security, lors de la recherche de la présence éventuelle de virus et autres applications malveillantes sur la machine virtuelle, n'a réalisé, pour quelque raison que ce soit, aucune action sur le fichier infecté conformément aux paramètres définis de l'application.

Cette situation peut se présenter dans les cas suivants :

- Le fichier à analyser n'est pas accessible (par exemple, il se trouve sur un disque réseau ou sur un périphérique externe sans droit en écriture).
- Dans le groupe **Action en cas de détection d'une menace** des paramètres de l'application pour les tâches d'analyse, l'action **Informer** a été sélectionnée, puis lorsque le message relatif au fichier infecté s'est affiché, vous avez choisi l'option **Ignorer**.

Vous pouvez lancer manuellement la tâche d'analyse personnalisée de fichiers depuis la liste des fichiers non traités après la mise à jour des bases de l'application. L'état des fichiers peut changer après l'analyse. En fonction de l'état, vous pouvez réaliser vous-même les actions requises sur les fichiers.

Par exemple, vous pouvez exécuter les opérations suivantes :

- supprimer les fichiers dont l'état est *Infecté* (cf. section “*Suppression de fichiers dans la liste des fichiers non traités*” à la page 234) ;
- restaurer les fichiers infectés qui contiennent des informations importantes et restaurer des fichiers dont l'état est *Réparé* et *Sain* (cf. section “*Restauration de fichiers à partir de la liste des fichiers non traités*” à la page 233).

Manipulation de la liste des fichiers non traités

La liste des fichiers non traités se présente sous la forme d'un tableau.

Vous pouvez réaliser les opérations suivantes sur les fichiers non traités à partir de la liste des fichiers non traités :

- consulter la liste des fichiers non traités ;
- analyser les fichiers non traités à l'aide de la version actuelle des bases de l'application ;
- restaurer des fichiers de la liste des fichiers non traités vers leurs dossiers d'origine ou vers n'importe quel autre dossier (si le dossier d'origine du fichier n'est pas accessible en écriture) ;
- supprimer des fichiers de la liste des fichiers non traités ;
- ouvrir le dossier d'origine du fichier non traité.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer la liste des fichiers non traités selon les valeurs d'une colonne ou selon un filtre complexe ;
- utiliser la fonction de recherche de fichiers non traités ;
- trier les fichiers non traités ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des fichiers non traités ;
- regrouper les fichiers non traités ;
- copier les entrées sélectionnées sur les fichiers non traités dans le presse-papier.

Dans cette section

Lancement de la tâche d'analyse personnalisée pour les fichiers non traités

Vous pouvez lancer manuellement la tâche d'analyse personnalisée de fichiers non traités, par exemple si l'analyse avait été interrompue pour une raison quelconque ou si vous souhaitez que l'application Kaspersky Security analyse les fichiers après une nouvelle mise à jour des bases de l'application.

► *Pour lancer la tâche d'analyse personnalisée pour les fichiers non traités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Sélectionnez l'onglet **Fichiers non traités**.
4. Dans le tableau sous l'onglet **Fichiers non traités**, sélectionnez un ou plusieurs fichiers que vous souhaitez analyser. Pour sélectionner plusieurs fichiers, sélectionnez-les en maintenant la touche **CTRL** enfoncée.
5. Lancez la tâche d'analyse personnalisée des fichiers d'une des manières suivantes :
   - Cliquez sur le bouton **Nouvelle analyse**.
   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Nouvelle analyse**.

A l'issue de l'analyse, un message indique le nombre de fichiers analysés et le nombre de menaces détectées.

Restauration de fichiers à partir de la liste des fichiers non traités

Le cas échéant, vous pouvez restaurer des fichiers à partir de la liste des fichiers non traités.

> Les experts de Kaspersky Lab conseillent de restaurer les fichiers à partir de la liste des fichiers non traités uniquement s'ils possèdent l'état *Sain*.

► *Pour restaurer des fichiers depuis la liste des fichiers non traités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Sélectionnez l'onglet **Fichiers non traités**.
4. Si vous souhaitez restaurer tous les fichiers, procédez comme suit :
   a. Cliquez-droit n'importe où dans le tableau de l'onglet **Fichiers non traités** et ouvrez le menu contextuel.
   b. Choisissez l'option **Restaurer tout**.

      Kaspersky Security déplace tous les fichiers de la liste des fichiers non traités vers leurs dossiers d'origine, si ces dossiers sont accessibles en écriture.
   c. Si un des dossiers d'origine des fichiers de la liste n'est pas accessible en écriture, une fenêtre standard **Enregistrer sous** de Microsoft Windows s'ouvre. Dans cette fenêtre, vous pouvez désigner le dossier dans lequel il convient d'enregistrer le fichier.
5. Si vous souhaitez restaurer un ou plusieurs fichiers, procédez comme suit :
   a. Dans le tableau de l'onglet **Fichiers non traités**, sélectionnez un ou plusieurs fichiers que vous souhaitez restaurer. Pour sélectionner plusieurs fichiers, sélectionnez-les en maintenant la touche **CTRL** enfoncée.
   b. Choisissez une des méthodes suivantes pour restaurer les fichiers :
      - Cliquez sur le bouton **Restaurer**.
      - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Restaurer**.

Kaspersky Security déplace les fichiers sélectionnés vers leurs dossiers d'origine, à condition que ces dossiers soient accessibles en écriture.

c. Si un des dossiers d'origine des fichiers de la liste n'est pas accessible en écriture, une fenêtre standard **Enregistrer sous** de Microsoft Windows s'ouvre. Dans cette fenêtre, vous pouvez désigner le dossier dans lequel il convient d'enregistrer le fichier.

Suppression de fichiers dans la liste des fichiers non traités

Vous pouvez supprimer un fichier infecté de la liste des fichiers non traités. Avant de supprimer le fichier, Kaspersky Security crée une copie de sauvegarde de celui-ci et la place dans le dossier de sauvegarde au cas où il faudrait restaurer le fichier plus tard (cf. section “Restauration des fichiers depuis la sauvegarde” à la page 257).

► *Pour supprimer des fichiers de la liste des fichiers non traités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Sélectionnez l'onglet **Fichiers non traités**.
4. Dans le tableau de l'onglet **Fichiers non traités**, sélectionnez un ou plusieurs fichiers que vous souhaitez supprimer. Pour sélectionner plusieurs fichiers, sélectionnez-les en maintenant la touche **CTRL** enfoncée.
5. Supprimez les fichiers à l'aide d'un des moyens suivants :

   - Cliquez sur le bouton **Supprimer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Supprimer**.

   Kaspersky Security crée une copie de sauvegarde de chaque fichier et la place dans le dossier de sauvegarde (cf. section “ A propos de la sauvegarde “ à la page 253). Ensuite, Kaspersky Security supprime les fichiers sélectionnés de la liste des fichiers non traités.

Mise à jour des bases de données et des modules de l'application

Cette section contient des informations sur la mise à jour des bases et des modules de l'application (ci-après mises à jour) et les instructions sur la configuration de la mise à jour.

Dans cette section

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

La mise à jour des bases et des modules de l'application permet de maintenir à jour la protection de votre machine virtuelle. Chaque jour, de nouveaux virus, et autres applications présentant une menace apparaissent dans le monde. Les bases de Kaspersky Security contiennent les données relatives aux menaces et aux méthodes de neutralisation. Les bases de l'application sont enrichies régulièrement avec les définitions des nouvelles menaces et les moyens de lutter contre celles-ci. Ces informations sont utilisées par les modules de protection pour rechercher les fichiers infecter sur votre machine virtuelle protégées et les neutraliser. Pour que Kaspersky Security puisse détecter à temps les nouvelles menaces, il vous faut actualiser les bases et les modules de l'application à intervalle régulier.

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

Kaspersky Security contrôle régulièrement la présence de paquets de mises à jour dans le dossier de la SVM à laquelle est connectée la machine virtuelle protégée (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). En cas de présence d'un paquet

de mises à jour, l'application installe sur la machine virtuelle protégée les mises à jour des bases et des modules nécessaires au fonctionnement de l'application.

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

La mise à jour des bases et des modules s'effectue via la tâche de mise à jour. La tâche de mise à jour s'exécute automatiquement. En cas de nécessité, vous pouvez lancer la tâche de mise à jour manuellement (cf. section “ Lancement et arrêt de la tâche de mise à jour “ à la page 236) ou configurer la planification du lancement de la tâche de mise à jour.

> Si les bases et les modules de l'application n'ont pas été mises à jour depuis un certain temps, un message d'avertissement apparaîtra dans le groupe **Gestion des tâches** sous l'onglet **Statut de la protection** de la fenêtre principale de l'application (cf. rubrique “ Fenêtre principale de l'application “ à la page 23).

Si l'exécution de la tâche de mise à jour est impossible pour une raison quelconque (par exemple, la machine virtuelle était désactivée à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que possible.

Vous pouvez reporter le lancement de la tâche de mise à jour par rapport au démarrage de l'application si vous avez configuré son exécution selon la planification et que l'heure de lancement de Kaspersky Security correspond à l'heure programmée pour le lancement de la tâche de mise à jour. La tâche de mise à jour ne sera lancée qu'à l'issue de la période définie après le démarrage de Kaspersky Security.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches de mise à jour sont consignées dans le rapport de Kaspersky Security.

Lancement et arrêt des tâches

Quel que soit le mode d'exécution de la tâche de mise à jour sélectionné, vous pouvez lancer ou arrêter la tâche de mise à jour de Kaspersky Security à tout moment.

► *Pour lancer ou arrêter la tâche de recherche de mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Choisissez l'onglet **Statut de la protection**.

3. Déployez le groupe **Gestion des tâches**.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec le nom de la tâche de **Mise à jour**.

   Le menu de sélection des actions avec la tâche de mise à jour.

   > Si les tâches de mise à jour n'apparaissent pas dans le groupe, cela signifie que la configuration des paramètres de la mise à jour des bases de données et des modules de l'application est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Lancer la mise à jour** pour lancer la tâche de mise à jour.

     L'état de l'exécution de la tâche de mise à jour affiché à droite du nom de la tâche de **Mise à jour** passera à *En cours*.

   - Sélectionnez dans le menu l'option **Arrêter la mise à jour** pour arrêter la tâche de mise à jour.

     L'état de l'exécution de la tâche de mise à jour affiché à droite du nom de la tâche de **Mise à jour** passera à *Arrêté*.

Une fois que la tâche de mise à jour a été lancée, vous pouvez suivre sa progression dans le champ en regard du nom de la tâche de **Mise à jour** du groupe **Gestion des tâches** sous l'onglet **Statut de la protection** de la fenêtre principale de l'application Kaspersky Security.

Sélection du mode d'exécution de la tâche de mise à jour

► *Pour programmer l'exécution de la tâche de mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases de l'application.

   > Si la section **Mise à jour** n'apparaît pas dans le groupe, cela signifie que la configuration des paramètres de la mise à jour des bases de données et des modules de l'application est interdite par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

3. Cliquez sur le bouton **Mode d'exécution**.

   La fenêtre **Mise à jour** s'ouvre.

4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche de mise à jour :

   - Sélectionnez l'option **Automatique**, si vous souhaitez que l'application Kaspersky Security lance la tâche de mise à jour en fonction de la présence de paquets de mises à jour sur la SVM à laquelle est connectée la machine virtuelle protégée (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). L'intervalle de vérification par l'application de la présence du paquet des mises à jour est augmenté en cas d'épidémie et réduit en situation normale.

     > En l'absence de nouvelles mises à jour sur la SVM, la tâche de mise à jour n'est pas lancée.

- Sélectionnez l'option **Manuel** pour lancer la tâche de mise à jour manuellement.
- Sélectionnez l'option **Selon la planification** pour programmer l'exécution de la tâche de mise à jour.

5. Exécutez une des actions suivantes :
   - Si vous avez sélectionné l'option **Automatique** ou **Manuel**, passez au paragraphe 6 de l'instruction.
   - Si vous avez sélectionné l'option **Selon la planification**, définissez les paramètres de planification du lancement de la tâche de mise à jour. Pour ce faire, procédez comme suit :
     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche de mise à jour. Sélectionnez une des options suivantes : **Minutes**, **Heures**, **Jours**, **Chaque semaine**, **A l'heure indiquée**, **Tous les mois**, **Après le lancement de l'application**.
     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche de mise à jour.

        Lors de la configuration de la fréquence de lancement de la tâche de mise à jour, il est conseillé de prendre en compte la fréquence de mise à jour des bases de l'application sur la SVM de laquelle est connectée la machine virtuelle protégée (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

     c. Indiquez dans le champ **Reporter le lancement après le démarrage de l'application de** le temps qui doit s'écouler avant l'exécution de la tâche de mise à jour après le lancement de Kaspersky Security.

        Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application**, le champ **Reporter le lancement après le démarrage de l'application de** est inaccessible.

d. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que l'application Kaspersky Security lance à la première occasion les tâches de mise à jour non exécutées en temps opportun.

> Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Heures**, **Minutes** ou **Après le lancement de l'application**, la case **Lancer les tâches non exécutées** est inaccessible.

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Zone de confiance

Cette section présente des informations sur la zone de confiance et explique comment configurer les exclusions de l'analyse et composer une liste d'applications de confiance.

Dans cette section

A propos de la zone de confiance

La *zone de confiance* est une liste composée par l'utilisateur d'objets et d'applications non contrôlés par l'application Kaspersky Security au cours de l'opération. En d'autres termes, il s'agit d'un ensemble d'exclusions de l'analyse et de la protection.

L'utilisateur forme la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées dans le système d'exploitation invité de la machine virtuelle protégée. Il sera peut-être nécessaire d'inclure des objets et des applications dans la zone de confiance si Kaspersky Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Vous pouvez exclure de l'analyse les objets des types suivants :

- les fichiers d'un format déterminé ;
- fichiers selon un masque ;
- dossiers ;
- applications ;
- les processus des applications ;
- objets selon la classification de l'Encyclopédie des virus de Kaspersky Lab.

Exclusions de l'analyse et de la protection

L'*exclusion* est un ensemble de conditions décrivant l'objet ou l'application. Si l'objet satisfait ces conditions, Kaspersky Security ne l'analyse pas à la recherche de virus ou d'autres programmes présentant une menace.

Certaines applications légitimes peuvent être exploitées par des individus malintentionnés pour nuire à la machine virtuelle protégée ou à vos données. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, ou les numéroteurs automatiques. Ce genre d'application n'est pas considéré comme un virus. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'Encyclopédie de virus de Kaspersky Lab en cliquant sur le lien http://securelist.com/threats/riskware/.

Kaspersky Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de configurer des exclusions de l'analyse et de la protection de Kaspersky Security pour les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque du nom de la menace conformément au classement de l'Encyclopédie des virus de Kaspersky Lab. Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'un système d'accès à distance qui permet de travailler sur un ordinateur distant. Pour éviter le blocage de cette application, vous devez créer une exclusion dans laquelle vous indiquerez le nom ou le masque du nom selon la classification de l'Encyclopédie des virus de “Kaspersky Lab”.

Les exclusions peuvent être utilisées au cours du fonctionnement des modules suivants et des tâches de l'application :

- Antivirus Fichiers.
- Antivirus Courrier.
- Antivirus Internet.
- Surveillance du système.
- Contrôle de l'activité des applications.
- Tâches d'analyse.

Liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Security ne contrôle pas l'activité de fichier et de réseau (y compris l'activité suspecte), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Kaspersky Security exclut de l'analyse toute application ajoutée à la liste des applications de confiance (cf. section “Composition de la liste des applications de confiance” à la page 249).

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), vous pouvez ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance pour ne pas analyser les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Security considère comme dangereuses peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic réseau d'un ordinateur par l'application Kaspersky Security et un autre logiciel antivirus) et d'améliorer les performances de la machine virtuelle, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre programmes malveillants. Pour exclure complètement une application de l'analyse et de la protection de Kaspersky Security, une exclusion doit être créée pour cette application.

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

Configuration de la zone de confiance

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres de la zone de confiance :

- Créer une exclusion.

  Vous pouvez créer une exclusion dans le cadre de laquelle Kaspersky Security n'analysera pas les fichiers, les dossiers et/ou les objets indiqués.

- Suspendre l'utilisation d'une exclusion.

  Vous pouvez suspendre temporairement l'utilisation d'une exclusion sans devoir la supprimer de la liste des exclusions.

- Modifier les paramètres d'une exclusion existante.

  Après avoir créé une exclusion, vous pouvez toujours revenir à la configuration des paramètres de cette exclusion et modifier les paramètres requis.

- Supprimer une exclusion.

  Vous pouvez supprimer une exclusion si vous ne souhaitez pas que Kaspersky Security l'applique pendant la durée de protection et d'analyse de la machine virtuelle.

- Composer la liste des applications de confiance.

  Vous pouvez composer la liste des applications de confiance pour lesquelles Kaspersky Security ne contrôlera pas les activités de fichier et de réseau (y compris les activités malveillantes), ni les requêtes de ces applications adressées à la base de registre.

- Suspendre l'exclusion de l'analyse par Kaspersky Security d'une application de confiance.

  Vous pouvez suspendre temporairement l'exclusion d'une application de confiance de l'analyse de l'application Kaspersky Security sans devoir la supprimer de la liste des applications de confiance.

Dans cette section

Création d'une exclusion

Kaspersky Security n'analyse pas l'objet exclu si, au lancement d'une des tâches d'analyse, le disque dur ou le dossier d'emplacement de cet objet a été indiqué. Cependant, si vous avez lancé une tâche d'analyse personnalisée, Kaspersky Security analyse l'objet même si celui-ci a fait l'objet d'une exclusion.

► *Pour créer une exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et zone de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.
4. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion** s'ouvre.

5. Si vous souhaitez exclure de l'analyse et de la protection un fichier ou un dossier, procédez comme suit :

   a. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.

   b. Le lien **sélectionnez un fichier ou un dossier** situé dans le groupe **Description de l'exclusion** permet d'ouvrir la fenêtre **Nom du fichier ou du dossier**. Cette fenêtre permet de saisir le nom du fichier ou du dossier, le masque du nom de fichier ou de dossier ou de sélectionner un fichier ou un dossier dans l'arborescence des dossiers.

   c. Après avoir sélectionné l'objet, cliquez sur le bouton **OK** dans la fenêtre **Nom du fichier ou du dossier**.

      Le lien vers l'objet ajouté apparaîtra dans le groupe **Description de l'exclusion** de la fenêtre **Exclusions**.

6. Si vous souhaitez exclure de l'analyse et de la protection les objets portant un nom défini sur la base de la classification des programmes malveillants et autres applications répertoriés dans l'Encyclopédie des virus de Kaspersky Lab, procédez comme suit :

   a. Dans le groupe **Propriétés**, cochez la case **Nom de l'objet**.

   b. Le lien **saisissez le nom de l'objet** situé dans le groupe **Description de l'exclusion** permet d'ouvrir la fenêtre **Nom de l'objet**. Cette fenêtre permet de saisir le nom ou le masque de l'objet conformément au classement de l'Encyclopédie de virus de Kaspersky Lab.

   c. Cliquez sur le bouton **OK** dans la fenêtre **Nom de l'objet**.

7. Saisissez un bref commentaire sur l'exclusion à créer dans le champ **Commentaires**.

8. Définissez les modules de Kaspersky Security qui doivent appliquer l'exclusion :

   a. Cliquez sur le lien **quelconque** situé dans le groupe **Description de l'exclusion** pour le transformer en **sélectionnez les modules**.

   b. Cliquez sur le lien **sélectionnez les modules** pour ouvrir la fenêtre **Modules de la protection**.

c. Sélectionnez les modules requis.

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

Si les modules sont indiqués dans les paramètres de l'exclusion, l'objet sera exclu de l'analyse effectuée par ces modules de Kaspersky Security uniquement.

Si les modules ne sont pas indiqués dans les paramètres de l'exclusion, l'objet sera exclu de l'analyse effectuée par tous les modules de Kaspersky Security.

9. Cliquez sur le bouton **OK** dans la fenêtre **Exclusion**.

   L'exclusion ajoutée apparaît dans la liste des exclusions de l'onglet **Exclusions** dans la fenêtre **Zone de confiance**. Le groupe **Description de l'exclusion** affiche les paramètres de cette exclusion.

10. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification d'une exclusion

► *Pour modifier une exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

4. Sélectionnez l'exclusion requise dans la liste des exclusions.

5. Cliquez sur le bouton **Modifier**.

   La fenêtre **Exclusion** s'ouvre.

6. Modifiez les paramètres de l'exclusion.

7. Cliquez sur le bouton **OK** dans la fenêtre **Exclusion**.

   Le groupe **Description de l'exclusion** affiche les modifications des paramètres de cette exclusion.

8. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression d'une exclusion

► *Pour supprimer une exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.

4. Sélectionnez l'exclusion requise dans la liste des exclusions.

5. Cliquez sur le bouton **Supprimer**.

   L'exclusion supprimée disparaît de la liste des exclusions de l'onglet **Exclusions** dans la fenêtre **Zone de confiance**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement et suspension de l'utilisation d'une exclusion

► *Pour lancer ou arrêter une exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions**.
4. Sélectionnez l'exclusion requise dans la liste des exclusions.
5. Exécutez une des actions suivantes :
   - Cochez la case en regard du nom de l'exclusion si vous voulez utiliser cette exclusion.
   - Décochez la case en regard du nom de l'exclusion si vous souhaitez suspendre temporairement l'application de cette exclusion.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition de la liste des applications de confiance

► *Pour composer une liste des applications de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.

4. Sélectionnez l'onglet **Applications de confiance**.

5. Si vous voulez ajouter une application à la liste des applications de confiance, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter**.

   b. Dans le menu déroulant ouvert, exécutez une des actions suivantes :

      - Sélectionnez l'option **Applications** si vous voulez trouver l'application dans la liste des applications installées sur la machine virtuelle. La fenêtre **Sélection de l'application** s'ouvre.
      - Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin au fichier exécutable de l'application nécessaire. La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

   c. Sélectionnez l'application que vous souhaitez ajouter à la liste des applications de confiance.

      La fenêtre **Exclusions pour l'application** s'ouvre.

   d. Cochez les cases pour les types d'activité à ne pas analyser de l'application :

      - **Ne pas analyser les fichiers ouverts**.
      - **Ne pas surveiller l'activité de l'application**.
      - **Ne pas hériter des restrictions du processus parent (application)**.
      - **Ne pas surveiller l'activité des applications enfants**.
      - **Autoriser l'interaction avec l'interface de l'application**.
      - **Ne pas analyser le trafic réseau**.

   e. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions pour l'application**.

      L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.

6. Si vous voulez modifier les paramètres de l'application de confiance, procédez comme suit :

   a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

   b. Cliquez sur le bouton **Modifier**.

   c. La fenêtre **Exclusions pour l'application** s'ouvre.

   d. Modifiez les statuts des cases pour les types requis de l'activité de l'application.

   > Si aucun type d'activité de l'application n'a été sélectionné dans la fenêtre **Exclusions pour l'application**, l'inclusion de l'application de confiance dans l'analyse se produit (cf. section “Inclusion et exclusion de l'application de confiance de l'analyse” à la page 251). L'application de confiance n'est pas supprimée de la liste des applications de confiance, seule sa case est décochée.

   e. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions pour l'application**.

7. Si vous voulez supprimer l'application de confiance de la liste des applications de confiance, procédez comme suit :

   a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

   b. Cliquez sur le bouton **Supprimer**.

8. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Inclusion et exclusion de l'application de confiance de l'analyse

► *Pour inclure une application de confiance dans l'analyse ou l'en exclure, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.

4. Sélectionnez l'onglet **Applications de confiance**.

5. Sélectionnez l'application de confiance requise dans la liste des applications de confiance.

6. Exécutez une des actions suivantes :

   - Cochez la case en regard du nom de l'application de confiance si vous souhaitez l'exclure de l'analyse de l'application Kaspersky Security.

   - Décochez la case en regard du nom de l'application de confiance si vous souhaitez l'inclure dans l'analyse de l'application Kaspersky Security.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sauvegarde

Cette section contient les instructions sur l'utilisation de la sauvegarde.

Dans cette section

A propos de la sauvegarde

La *Sauvegarde* est une liste des copies de sauvegarde des fichiers supprimés ou modifiés pendant la réparation. La *copie de sauvegarde* est une copie de fichier créée lors de la première réparation ou suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la réparation. Si le fichier réparé contenait des informations critiques partiellement ou complètement perdues suite à la réparation, vous pouvez tenter de restaurer le fichier depuis sa copie réparée dans son dossier d'origine.

Lors de la suppression de l'application, les fichiers de la sauvegarde sont supprimés de la machine virtuelle protégée.

Configuration des paramètres de la sauvegarde

Vous pouvez réaliser les opérations suivantes au niveau de la configuration de la sauvegarde :

- Configurer la durée maximale de conservation des copies de sauvegarde de fichiers dans le dossier de sauvegarde.

  Par défaut, les copies de sauvegarde des fichiers sont conservées 30 jours maximum. Une fois ce délai maximal écoulé, Kaspersky Security supprime les fichiers les plus anciens de la sauvegarde. Vous pouvez annuler la restriction sur la durée de conservation des fichiers ou la modifier.

- Configurer la taille maximale de la sauvegarde.

  Par défaut, la taille maximale de la sauvegarde est de 100 Mo. Quand le stockage des données atteint la taille maximale configurée, Kaspersky Security supprime automatiquement les fichiers les plus anciens de la sauvegarde afin de ne plus dépasser la limite. Vous pouvez lever la restriction sur la taille maximale de la sauvegarde ou modifier la taille maximale.

Dans cette section

Configuration de la durée de conservation maximale des fichiers dans la sauvegarde

► *Pour configurer la durée de conservation maximale des fichiers dans la sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Dans la partie droite de la fenêtre dans le groupe **Paramètres de la sauvegarde** exécutez une des actions suivantes :

   - Cochez la case **Ne pas conserver les fichiers plus de**, si vous souhaitez limiter la durée de conservation des copies de sauvegarde des fichiers dans la sauvegarde. Dans le champ situé à droite de la case, saisissez la durée de conservation maximale des copies de sauvegarde de fichiers dans la sauvegarde. Par défaut, les copies de sauvegarde des fichiers sont conservées 30 jours maximum.

   - Décochez la case **Ne pas conserver les fichiers plus de**, si vous souhaitez supprimer la limite de la durée de conservation des copies de sauvegarde des fichiers dans la sauvegarde.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la taille maximale de la sauvegarde

► *Pour configurer la taille maximale de la sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Exécutez une des actions suivantes :

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la sauvegarde**, cochez la case **Taille maximale du stockage** si vous souhaitez définir une taille limite pour la sauvegarde. Dans le champ à droite de la case, indiquez la taille maximale de la sauvegarde. Par défaut, la taille maximale est limitée à 100 Mo.

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la sauvegarde**, décochez la case **Taille maximale du stockage** si vous ne souhaitez pas définir une taille limite pour la sauvegarde.

   Par défaut, il n'y a pas de limite sur la taille de la sauvegarde.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de la sauvegarde

Si Kaspersky Security détecte un code malveillant dans un fichier, il bloque celui-ci, le supprime de son dossier d'origine et place une copie dans le dossier de sauvegarde avant de tenter de le réparer. Si le fichier est réparé, l'état de la copie de sauvegarde devient *Réparé*. Ensuite, vous pouvez restaurer le fichier à partir de sa copie de sauvegarde réparée dans son dossier d'origine.

> En cas de détection d'un code malveillant dans un fichier qui appartient à une application de Windows Store, Kaspersky Security ne place pas le fichier dans la sauvegarde, mais le supprime directement. Vous pouvez restaurer l'intégrité de l'application Windows Store via le système d'exploitation Microsoft Windows.

Kaspersky Security supprime automatiquement les copies de sauvegarde des fichiers dans le dossier de sauvegarde après expiration de la durée définie dans les paramètres de l'application (cf. section “ Configuration de la durée maximale de conservation des fichiers dans la sauvegarde “ à la page 254).

Vous pouvez supprimer vous-même une copie de sauvegarde d'un fichier restauré ou non.

La liste des copies de sauvegarde des fichiers se présente sous la forme d'un tableau.

Vous pouvez réaliser les opérations suivantes sur les copies de sauvegarde des fichiers du dossier de sauvegarde :

- consulter la liste des copies de sauvegarde des fichiers ;
- restaurer les fichiers à partir des copies de sauvegarde dans leurs dossiers d'origine ;
- supprimer des copies de sauvegarde de fichiers du dossier de sauvegarde.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer la liste des copies de sauvegarde selon les valeurs d'une colonne ou selon un filtre complexe ;
- utiliser une fonction de recherche des copies de sauvegarde des fichiers ;
- trier les copies de sauvegarde des fichiers ;

- regrouper les copies de sauvegarde des fichiers ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des copies de sauvegarde des fichiers ;
- copier les copies de sauvegarde des fichiers sélectionnées dans le presse-papier.

Dans cette section

Restauration des fichiers depuis la sauvegarde

Il est conseillé de restaurer les fichiers à partir des copies de sauvegarde uniquement si ceux-ci ont l'état *Réparé*.

► *Pour restaurer des fichiers depuis le dossier de sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Sélectionnez l'onglet **Sauvegarde**.
4. Si vous souhaitez restaurer tous les fichiers du dossier de sauvegarde, procédez comme suit :
   a. Cliquez-droit n'importe où dans le tableau de l'onglet **Sauvegarde** et ouvrez le menu contextuel.
   b. Choisissez l'option **Restaurer tout**.

   Kaspersky Security restaurera tous les fichiers depuis leurs copies de sauvegarde dans le dossier de sauvegarde vers leurs dossiers d'origine.

5. Si vous souhaitez restaurer un ou plusieurs fichiers depuis le dossier de sauvegarde, procédez comme suit :

   a. Dans le tableau de l'onglet **Sauvegarde**, sélectionnez une ou plusieurs copies de sauvegarde des fichiers. Pour sélectionner plusieurs copies de sauvegarde, sélectionnez-les en maintenant la touche **CTRL** enfoncée.

   b. Choisissez une des méthodes suivantes pour restaurer les fichiers :

      - Cliquez sur le bouton **Restaurer**.
      - Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Restaurer**.

   Kaspersky Security restaurera les fichiers depuis les copies de sauvegarde sélectionnées dans le dossier de sauvegarde vers leurs dossiers d'origine.

Suppression des copies de sauvegarde des fichiers depuis le dossier de sauvegarde

► *Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Sélectionnez l'onglet **Sauvegarde**.
4. Si vous souhaitez supprimer toutes les copies de sauvegarde des fichiers du dossier de sauvegarde, optez pour l'une des actions suivantes :

   - Cliquez-droit n'importe où dans le tableau de l'onglet **Sauvegarde** pour ouvrir le menu contextuel et sélectionner l'option **Purger le stockage**.
   - Cliquez sur le bouton **Purger le stockage**.

5. Si vous souhaitez supprimer une ou plusieurs copies de sauvegarde de fichiers depuis le dossier de sauvegarde, procédez comme suit :

    a. Dans le tableau de l'onglet **Sauvegarde**, sélectionnez une ou plusieurs copies de sauvegarde des fichiers. Pour sélectionner plusieurs copies de sauvegarde, sélectionnez-les en maintenant la touche **CTRL** enfoncée.

    b. Supprimez les copies de sauvegarde des fichiers à l'aide d'un des moyens suivants :

        - Cliquez sur le bouton **Supprimer**.
        - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer**.

Utilisation des rapports

Cette section explique comment utiliser les rapports et en configurer les paramètres.

Dans cette section

Principes d'utilisation des rapports

Les informations relatives au fonctionnement de chaque module de Kaspersky Security, à l'exécution de chaque tâche d'analyse et de mise à jour, et au fonctionnement de l'application dans son ensemble sont consignées dans un rapport.

Les données du rapport se présentent sous la forme d'un tableau qui reprend la liste des événements. Chaque ligne du tableau contient des informations sur un événement en particulier. Les attributs de l'événement sont repris dans les colonnes du tableau. Certaines colonnes sont complexes et contiennent des sous-colonnes avec des attributs complémentaires. Les attributs varient en fonction des événements enregistrés lors du fonctionnement de divers modules ou tâches.

Il est possible de composer les types de rapports suivants :

- Rapport “Audit système”. Ce rapport contient les informations relatives aux événements survenus pendant votre interaction avec l'application, ainsi que pendant le fonctionnement de l'application dans son ensemble sans rapport avec un module ou une tâche particuliers de Kaspersky Security.
- Rapport “Tous les modules de la protection”. Ce rapport contient des informations sur les événements survenus pendant le fonctionnement des modules suivants de Kaspersky Security :
  - Antivirus Fichiers.
  - Antivirus Courrier.
  - Antivirus Internet.
  - Antivirus IM.
  - Surveillance du système.
  - Pare-feu.
  - Prévention des intrusions.
- Rapport sur le fonctionnement d'un module ou d'une tâche de Kaspersky Security. Ce rapport contient des informations sur les événements survenus pendant le fonctionnement du module ou de la tâche sélectionné de Kaspersky Security.

Les niveaux d'importance suivants sont utilisés pour les événements :

- Icône . **Evénements d'informations**. Evénement à caractère informatif qui en général ne contient aucune information importante.
- Icône . **Evénements importants**. Evénements qui doivent être examinés car ils désignent des situations importantes dans le fonctionnement de Kaspersky Security.
- Icône . **Evénements critiques**. Evénements critiques et dysfonctionnements de l'application entraînant des problèmes dans le fonctionnement de Kaspersky Security.

Vous pouvez exécuter les actions suivantes sur les données des rapports :

- filtrer la liste des événements selon les valeurs d'une colonne ou selon un filtre complexe ;
- utiliser la fonction de recherche d'un événement en particulier ;
- consulter l'événement sélectionné dans un groupe distinct ;
- trier la liste des événements selon chaque colonne ;
- afficher ou masquer les données groupées ;
- modifier l'ordre et la sélection des colonnes affichées dans le rapport ;
- sauvegarder le rapport dans un fichier texte.

Vous pouvez également supprimer des informations des rapports selon les modules ou les tâches de Kaspersky Security regroupés dans le rapport. Kaspersky Security supprime toutes les entrées des rapports sélectionnés depuis la plus ancienne jusqu'au début de la suppression.

Configuration des paramètres des rapports

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres des rapports :

- Configurer la durée maximale de conservation des rapports.

  Par défaut, la durée maximale de conservation des rapports sur les événements détectés par Kaspersky Security est de 30 jours. A l'issue de cette période, Kaspersky Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport. Vous pouvez annuler la restriction sur la durée de conservation des rapports ou la modifier.

- Configurer la taille maximale du fichier de rapport.

  Vous pouvez définir la taille maximale du fichier contenant le rapport. Par défaut, la taille maximum du fichier du rapport est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille repasse au-dessous de la taille maximale autorisée. Vous pouvez lever la restriction sur la taille du fichier du rapport ou définir une autre valeur.

Dans cette section

Configuration de la durée maximale de conservation des rapports

► *Pour configurer la durée maximale de conservation des rapports, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre dans le groupe **Paramètres des rapports** exécutez une des actions suivantes :

   - Cochez la case **Conserver les rapports au maximum** si vous voulez établir des restrictions sur la conservation des rapports. Dans le champ à droite de la case **Conserver les rapports au maximum**, indiquez la durée maximale d'enregistrement des rapports. La durée maximale de conservation par défaut des rapports est de 30 jours.
   - Décochez la case **Conserver les rapports au maximum** si vous voulez annuler les restrictions sur l'enregistrement des rapports.

   Par défaut, la restriction de la durée d'enregistrement des rapports est activée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la taille maximale du fichier de rapport

► *Pour configurer la taille maximale du fichier de rapport, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Dans la partie droite de la fenêtre dans le groupe **Paramètres des rapports**, exécutez une des actions suivantes :

   - Cochez la case **Taille maximale du fichier** si vous souhaitez établir une limite sur la taille du fichier du rapport. Dans le champ situé à droite de la case **Taille maximale du fichier**, saisissez la taille maximale du fichier du rapport. Par défaut, la limite sur la taille du fichier du rapport est de 1024 Mo.

   - Décochez la case **Taille maximale du fichier** si vous souhaitez lever la restriction sur la taille du fichier du rapport.

   Par défaut, la limite sur la taille du fichier du rapport est activée.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition des rapports

► *Pour composer des rapports, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport “Audit système” s'affiche par défaut sous l'onglet **Rapports**.

3. Si vous souhaitez composer le rapport “Tous les modules de la protection”, dans la partie gauche de la fenêtre **Rapports et stockages**, dans la liste des modules et des tâches de la section **Protection antivirus**, choisissez l'option **Tous les modules de la protection**.

   La partie droite de la fenêtre affichera le rapport “Tous les modules de la protection” qui contient la liste des événements sur le fonctionnement de tous les modules de protection de Kaspersky Security.

4. Si vous souhaitez composer un rapport sur le fonctionnement d'un module ou d'une tâche, sélectionnez le module concerné dans la liste des modules et des tâches située dans la partie gauche de la fenêtre **Rapports et stockages**.

   La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche de Kaspersky Security.

   Par défaut, les événements dans le rapport sont classés selon l'ordre croissant des valeurs de la colonne **Date de l'événement**.

Consultation des informations sur les événements du rapport dans un groupe particulier

Vous pouvez consulter des informations détaillées sur l'événement du rapport présenté dans le groupe distinct.

► *Pour consulter les informations relatives à un événement du rapport dans un groupe distinct, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport “Audit système” s'affiche par défaut sous l'onglet **Rapports**.

3. Exécutez une des actions suivantes :

   - Si vous voulez composer le rapport “Tous les modules de la protection”, sélectionnez l'option **Tous les modules de la protection** dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport “Tous les modules de la protection” qui contient la liste des événements sur le fonctionnement de tous les modules de protection.

   - Si vous voulez composer le rapport sur le fonctionnement du module particulier ou de la tâche, sélectionnez ce module ou cette tâche dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche.

4. Le cas échéant, utilisez les filtres, la recherche et le tri pour trouver l'événement requis dans le rapport.

5. Sélectionnez l'événement trouvé dans le rapport.

   Un groupe contenant les attributs de cet événement et les informations relatives à son niveau d'importance apparaît dans la partie inférieure de la fenêtre.

Enregistrement du rapport dans un fichier

Vous pouvez sauvegarder le rapport composé dans un fichier texte au format TXT ou CSV.

> Kaspersky Security enregistre l'événement dans un rapport de la même manière qu'il est présenté à l'écran, c'est-à-dire avec la même composition et avec la même séquence d'attributs de l'événement.

► *Pour enregistrer le rapport dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport “Audit système” s'affiche par défaut sous l'onglet **Rapports**.

3. Exécutez une des actions suivantes :

   - Si vous voulez composer le rapport “Tous les modules de la protection”, sélectionnez l'option **Tous les modules de la protection** dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport “Tous les modules de la protection” qui contient la liste des événements sur le fonctionnement de tous les modules de protection.

   - Si vous voulez composer le rapport sur le fonctionnement du module particulier ou de la tâche, sélectionnez ce module ou cette tâche dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche.

4. S'il faut, modifiez la présentation des données dans le rapport à l'aide des moyens suivants :

   - filtrage des événements ;
   - recherche d'événements ;
   - modification de l'emplacement des colonnes ;
   - classement des événements.

5. Cliquez sur le bouton **Enregistrer le rapport** situé dans la partie supérieure droite de la fenêtre.

   Un menu contextuel s'ouvre.

6. Dans le menu contextuel, sélectionnez l'encodage requis pour l'enregistrement du fichier : **Enregistrer au format ANSI** ou **Enregistrer au format Unicode**.

   La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvre.

7. Dans la fenêtre ouverte **Enregistrer sous**, saisissez le champ dans lequel vous voulez enregistrer le fichier de rapport.

8. Saisissez le nom du fichier du rapport dans le champ **Nom du fichier**.

9. Dans le champ **Type de fichier**, sélectionnez le format requis du fichier de rapport : TXT ou CSV.

10. Cliquez sur le bouton **Enregistrer**.

Suppression des informations des rapports

► *Pour supprimer les informations des rapports, procédez comme suit* :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Dans la partie droite de la fenêtre, dans le groupe **Paramètres des rapports**, cliquez sur le bouton **Supprimer les rapports**.

   La fenêtre **Suppression des informations des rapports** s'ouvre.

4. Cochez les cases pour les rapports depuis lesquels vous voulez supprimer les informations :

   - **Tous les rapports**.
   - **Rapport de protection général**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Security :
     - Antivirus Fichiers.
     - Antivirus Courrier.

- Antivirus Internet.
- Antivirus IM.
- Pare-feu.
- Prévention des intrusions.

- **Rapport des tâches d'analyse**. Contient les informations sur les tâches exécutées de l'analyse :
  - Analyse complète.
  - Analyse des zones critiques.
  - Analyse personnalisée.
- **Rapport des tâches de mise à jour**. Contient les informations sur les tâches de mise à jour exécutées :
- **Rapport de traitement des règles du Pare-feu**. Contient les informations sur le fonctionnement du Pare-feu.
- **Rapport des modules de contrôle**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Security :
  - Contrôle du lancement des applications.
  - Contrôle de l'activité des applications.
  - Contrôle des périphériques.
  - Contrôle Internet.
- **Données de la surveillance du système**. Contient les informations sur le fonctionnement de la Surveillance du système.

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

Notifications

Cette section contient des informations sur les notifications qui signalent les événements dans le fonctionnement de Kaspersky Security, ainsi que des instructions sur la configuration des notifications relatives aux événements.

Dans cette section

A propos des notifications de Kaspersky Security

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Security. Il peut s'agir d'événements simplement informatifs ou d'événements importants. Par exemple, l'événement permet à l'application de signaler la réussite de la mise à jour des bases et des modules de l'application ou de signaler une erreur dans le fonctionnement d'un module qu'il faudra rectifier.

Kaspersky Security peut émettre les notifications sur les événements d'une des manières suivantes :

- à l'aide de pop-ups de notification dans la zone de notification de la barre des tâches de Microsoft Windows ;
- par email.

Vous pouvez configurer les modes de notification sur les événements. Le mode de notification est défini pour chaque type d'événement.

Kaspersky Security permet également de consigner les informations relatives aux événements survenus lors du fonctionnement de l'application dans le journal des événements Microsoft Windows et/ou dans les rapports de l'application (cf. page 260).

Configuration des notifications

Vous pouvez exécuter les opérations suivantes pour configurer les notifications :

- configurer l'enregistrement des événements sur le fonctionnement de Kaspersky Security (cf. section “Configuration de l'enregistrement des événements” à la page 271) ;
- configurer l'affichage des notifications à l'écran (cf. section “Configuration de l'affichage des notifications à l'écran” à la page 272) ;
- configurer les notifications sur les événements par courrier électronique (cf. section “Configuration des notifications sur les événements par courrier électronique” à la page 273).

En utilisant le tableau des événements, vous pouvez exécuter les opérations suivantes :

- utiliser la fonction de recherche d'événements ;
- trier les événements par ordre chronologique ou inversement ;
- modifier la sélection des colonnes affichées dans la liste des événements.

Dans cette section

Configuration de l'enregistrement des événements

► *Pour configurer l'enregistrement des événements, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Paramètres complémentaires** de la partie gauche de la fenêtre, sélectionnez la section **Interface**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Notifications** cliquez sur le bouton **Configuration**.

4. La fenêtre **Notifications** s'ouvre.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

5. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer l'enregistrement des événements.

6. Dans la colonne, cochez les cases en regard des types d'événements requis :

   - **Enregistrer dans le journal de l'application** si vous souhaitez enregistrer les événements dans les rapports de l'application (cf. page 260).

   - **Enregistrer dans le journal d'événements Windows** si vous souhaitez enregistrer les événements dans le journal des événements Microsoft Windows.

7. Cliquez sur le bouton **OK** dans la fenêtre **Notifications**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'affichage des notifications à l'écran

► *Pour configurer l'affichage des notifications à l'écran, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** de la partie gauche de la fenêtre, sélectionnez la section **Interface**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Notifications** cliquez sur le bouton **Configuration**.

4. La fenêtre **Notifications** s'ouvre.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

5. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous souhaitez configurer les notifications sur les événements à l'écran.

6. Dans la colonne **Notifier sur écran**, cochez les cases en regard des types d'événements requis.

Les informations relatives aux événements sélectionnés s'afficheront dans des pop-ups de notification situés dans la zone de notification de la barre des tâches de Microsoft Windows.

Configuration des notifications sur les événements par messagerie électronique

► *Pour configurer les notifications sur les événements par email, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

2. Dans le groupe **Paramètres complémentaires** de la partie gauche de la fenêtre, sélectionnez la section **Interface**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Notifications** cliquez sur le bouton **Configuration**.

4. La fenêtre **Notifications** s'ouvre.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

5. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous souhaitez configurer les notifications sur les événements par email.

6. Dans la colonne **Notifier par courrier électronique**, cochez les cases en regard des types d'événements requis.
7. Cliquez sur le bouton **Configuration des notifications par courrier**.

   La fenêtre **Configuration des notifications par courrier** s'ouvre.
8. Cochez la case **Envoyer des notifications sur les événements** pour activer l'envoi des informations sur les événements du fonctionnement de Kaspersky Security, sélectionnés dans la colonne **Notifier par courrier électronique**.
9. Définissez les paramètres d'envoi des messages électroniques.
10. Cliquez sur le bouton **OK** dans la fenêtre **Configuration des notifications par courrier**.
11. Cliquez sur le bouton **OK** dans la fenêtre **Notifications**.
12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Performances de Kaspersky Security

Cette section contient les informations sur les performances de l'application Kaspersky Security et sur la compatibilité avec d'autres applications, ainsi que les instructions sur la sélection des types d'objets à détecter et le mode de fonctionnement de Kaspersky Security.

Dans cette section

A propos des performances de Kaspersky Security

Les performances de Kaspersky Security comprennent la quantité de types d'objets à détecter et la consommation en ressources de la machine virtuelle protégée.

Sélection des types d'objets à détecter

Kaspersky Security permet de configurer en souplesse la protection de la machine virtuelle et de sélectionner les types d'objets (cf. section “Sélection des types d'objets à détecter” à la page 277) que l'application va détecter durant son fonctionnement. Kaspersky Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans le système d'exploitation. Vous ne pouvez pas désactiver l'analyse pour ces types d'objets. Ces programmes peuvent infliger des dégâts considérables à la machine virtuelle protégée. Pour élargir la protection offerte à la machine virtuelle, vous pouvez enrichir la liste des types d'objets à détecter en activant le contrôle de l'activité des applications légitimes qui pourraient être utilisées par des individus malintentionnés pour nuire à votre machine virtuelle ou à vos données.

Application de la technologie de réparation de l'infection active

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer.
Quand Kaspersky Security a détecté une activité malveillante dans le système d'exploitation, il exécute une procédure de réparation étendue en appliquant la technologie spéciale de réparation de l'infection active (cf. section “Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour ordinateur personnel” à la page 278).
La *technologie de réparation de l'infection active* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui empêchent l'application Kaspersky Security de les supprimer à l'aide d'autres méthodes. La menace est supprimée suite à l'application de la technologie de réparation de l'infection active. Pendant la réparation de l'infection active, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registre du système d'exploitation. La technologie de réparation de l'infection active est gourmande en ressources du système d'exploitation et peut ralentir d'autres applications.

Au terme du processus de réparation de l'infection active sur la machine virtuelle sous système d'exploitation pour poste de travail Windows, Kaspersky Security vous demande l'autorisation de redémarrer la machine virtuelle. Après le redémarrage de la machine virtuelle, Kaspersky Security supprime les fichiers de l'application malveillante et lance un analyse complète simplifiée de la machine virtuelle.

> Si Kaspersky Security est exécuté sur une machine virtuelle temporaire, en cas d'infection active de cette machine virtuelle temporaire, il est nécessaire de s'assurer de l'absence de virus et d'autres applications dangereuses sur le modèle de machine virtuelle puis de procéder au redémarrage de la machine virtuelle temporaire.

La demande de redémarrage de la machine virtuelle sous système d'exploitation pour serveur Windows est indisponible en raison des particularités de l'application Kaspersky Security pour systèmes d'exploitation pour serveur. Le redémarrage non prévu du système d'exploitation pour serveur peut entraîner des problèmes liés à l'accès temporairement refusé aux données du système d'exploitation pour serveur ou à la perte des données non enregistrées. Il est conseillé de redémarrer le système d'exploitation pour serveur en respectant scrupuleusement la planification prévue.
Pour cette raison, la technologie de réparation de l'infection active sur une machine virtuelle protégée sous système d'exploitation pour serveur Windows est désactivée par défaut.

En cas de détection d'une infection active sur une machine virtuelle protégée sous système d'exploitation pour serveur Windows, un événement relatif à la nécessité de réparer l'infection active est envoyé au Kaspersky Security Center. Afin de réparer une infection active sur une machine virtuelle protégée sous système d'exploitation pour serveur Windows, il est nécessaire d'activer la technologie de réparation d'une infection active pour système d'exploitation pour serveur et de lancer une tâche de groupe pour la recherche de virus au moment jugé opportun par les utilisateurs du système d'exploitation pour serveur (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

Sélection des types d'objets à détecter

► *Pour sélectionner les types d'objets à identifier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Objets**, cliquez sur le bouton **Configuration**.

   La fenêtre **Objets à détecter** s'ouvre.
4. Cochez les cases pour les types d'objets que l'application Kaspersky Security doit détecter :
   - **Outils malveillants**.
   - **Logiciels publicitaires (adwares, ...)**.
   - **Dialer**.
   - **Autres**.
   - **Fichiers compressés**.
   - **Fichiers compressés à plusieurs reprises**.

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

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

   La fenêtre **Objets à détecter** se ferme. Le groupe **Objets** sous l'inscription **Activation de la détection des objets des types suivants** affichera les types d'objets que vous avez sélectionnés.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la technologie de réparation de l'infection active pour les systèmes d'exploitation pour poste de travail

► *Pour activer ou désactiver la technologie de réparation de l'infection active pour les systèmes d'exploitation pour poste de travail, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :

   - Cochez la case **Appliquer la technologie de réparation de l'infection active** si vous souhaitez activer la technologie de réparation de l'infection active.
   - Décochez la case **Appliquer la technologie de réparation de l'infection active** si vous souhaitez désactiver la technologie de réparation de l'infection active.

   Si la case n'est pas disponible, cela signifie que vous ne pouvez pas activer ou désactiver la technologie de réparation de l'infection active pour les systèmes d'exploitation pour poste de travail car cela est interdit par une stratégie pour toutes les machines virtuelles protégées du groupe d'administration (cf. *Manuel de l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Autodéfense de Kaspersky Security

Cette section contient des informations sur les mécanismes de l'autodéfense de l'application Kaspersky Security et de la protection contre l'administration externe de l'application, ainsi que les instructions sur la configuration de ces mécanismes.

Dans cette section

A propos de l'autodéfense de Kaspersky Security

Kaspersky Security protège les machines virtuelles protégées contre les programmes malveillants, y compris ceux qui tentent de bloquer le fonctionnement de Kaspersky Security ou de supprimer l'application de la machine virtuelle.

La stabilité du système de protection de la machine virtuelle est garantie par les mécanismes d'autodéfense et de protection contre l'administration externe intégrés à Kaspersky Security.

Le mécanisme d'autodéfense empêche la modification et la suppression des fichiers de l'application sur le disque dur, des processus dans la mémoire et des clés de la base de registre système.

Le mécanisme de protection contre l'administration externe permet de bloquer toutes les tentatives d'administration par les services de l'application depuis un poste distant.

Activation et désactivation du mécanisme d'autodéfense

Par défaut, le mécanisme d'autodéfense de Kaspersky Security est activé. S'il faut, vous pouvez désactiver le mécanisme d'autodéfense.

La désactivation de l'autodéfense réduit le niveau de sécurité de la machine virtuelle conte les programmes malveillants.

► *Pour activer ou désactiver le mécanisme d'autodéfense procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'autodéfense** si vous voulez activer le mécanisme d'autodéfense de l'application.
   - Décochez la case **Activer l'autodéfense** si vous voulez désactiver le mécanisme d'autodéfense de l'application.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation du mécanisme d'autodéfense contre l'administration externe

Par défaut, le mécanisme d'autodéfense contre l'administration externe est activé. Le cas échéant, vous pouvez désactiver le mécanisme d'autodéfense contre l'administration externe.

► *Pour activer ou désactiver le mécanisme de l'autodéfense contre l'administration externe, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Désactiver la gestion externe du service système** si vous voulez activer le mécanisme de protection contre l'administration externe.
   - Décochez la case **Désactiver la gestion externe du service système** si vous voulez désactiver le mécanisme de protection contre l'administration externe.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Assurance de fonctionnement des applications de l'administration à distance

Il arrive souvent que lors de l'utilisation de mécanismes de protection contre l'administration externe il soit nécessaire d'appliquer une application d'administration externe.

► *Pour garantir le fonctionnement des applications d'administration à distance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.

4. Sélectionnez l'onglet **Applications de confiance**.
5. Cliquez sur le bouton **Ajouter**.
6. Dans le menu déroulant ouvert, exécutez une des actions suivantes :
   - Sélectionnez l'option **Applications** si vous voulez trouver l'application d'administration à distance dans la liste des applications installées sur la machine virtuelle protégée. La fenêtre **Sélection de l'application** s'ouvre.
   - Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin d'accès au fichier exécutable de l'application d'administration à distance. La fenêtre standard de Microsoft Windows **Sélection du fichier ou du dossier** s'ouvre.
7. Sélectionnez l'application.

   La fenêtre **Exclusions pour l'application** s'ouvre.
8. Cochez la case **Ne pas surveiller l'activité de l'application**.
9. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions pour l'application**.

   L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.
10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection par mot de passe

Cette section contient des informations sur les restrictions d'accès à Kaspersky Security à l'aide d'un mot de passe.

Dans cette section

A propos de la restriction de l'accès à l'application

La machine virtuelle peut être utilisée par plusieurs personnes dont les connaissances informatiques varient. L'accès illimité des utilisateurs à l'application Kaspersky Security et à ses paramètres peut entraîner une réduction du niveau de sécurité de la machine virtuelle dans son ensemble.

Pour limiter l'accès à l'application Kaspersky Security, vous devez définir un mot de passe et désigner les opérations qui ne pourront être exécutées qu'après la saisie du mot de passe en question :

- toutes les opérations (sauf les notifications de danger) ;
- configuration de l'application ;
- arrêt de l'application ;
- désactivation des modules de protection et arrêt des tâches d'analyse ;
- désactivation des modules du contrôle ;
- suppression/modification/restauration de l'application.

Activation et désactivation de la protection par mot de passe

► *Pour activer ou désactiver la protection par mot de passe, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).
2. Dans le groupe **Paramètres complémentaires** de la partie gauche de la fenêtre, sélectionnez la section **Interface**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.
3. Si vous souhaitez limiter l'accès à l'application Kaspersky Security via un mot de passe, procédez comme suit :

   a. Dans le groupe **Protection par mot de passe**, cochez la case **Activer la protection par mot de passe**.

   > Si la case n'est pas accessible, cela signifie que vous ne pouvez pas activer ou désactiver la protection par mot de passe car la valeur appliquée à l'ensemble des machines virtuelles protégées du groupe d'administration est celle définie par la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Contactez l'administrateur système.

   b. Dans le groupe **Protection par mot de passe**, cliquez sur le bouton **Configuration**.

      La fenêtre **Protection par mot de passe** s'ouvre.

   c. Dans le champ **Nouveau nom d'utilisateur**, saisissez le nom d'utilisateur qui aura accès à l'application.

   d. Dans le champ **Nouveau mot de passe**, saisissez le mot de passe d'accès à l'application.

   e. Dans le champ **Confirmation du mot de passe**, saisissez à nouveau le mot de passe.

f. Dans le groupe **Zone d'action du mot de passe**, indiquez les opérations de l'application que l'utilisateur pourra exécuter uniquement après avoir saisi le mot de passe :

- Choisissez l'option **Toutes les opérations (sauf notifications d'événements dangereux)** si vous souhaitez limiter l'accès à toutes les opérations de l'application.
- Choisissez l'option **Opérations sélectionnées** si vous souhaitez désigner les opérations manuellement.

g. Si vous avez choisi l'option **Opérations sélectionnées**, cochez les cases en regard des noms des opérations concernées :

- **Configuration de l'application**.
- **Arrêt de l'application**.
- **Désactivation des modules de protection et arrêt des tâches d'analyse**.
- **Désactivation des modules du contrôle**.
- **Suppression/modification/restauration de l'application**.
- **Consultation des rapports**.

h. Cliquez sur le bouton **OK**.

> Il est conseillé d'être prudent au moment de décider de limiter l'accès à l'application par mot de passe. Si vous avez oublié le mot de passe, vous devez contacter le Support Technique de Kaspersky Lab afin d'obtenir les instructions sur l'annulation de la protection par mot de passe (http://support.kaspersky.com/fr).

4. Si vous souhaitez lever la restriction d'accès à l'application Kaspersky Security par mot de passe, procédez comme suit :

a. Décochez la case **Activer la protection par mot de passe**.

b. Cliquez sur le bouton **Enregistrer**.

   L'application vérifie si l'opération d'annulation de la restriction d'accès est protégée.

   - Si l'annulation de la restriction de l'accès aux applications n'est pas protégée par un mot de passe, alors la restriction de l'accès à l'application est levée.
   - Si l'opération d'annulation de la restriction de l'accès à l'application est protégée par un mot de passe, la fenêtre **Vérification du mot de passe** s'ouvre. Cette fenêtre apparaît chaque fois que l'utilisateur exécute une opération protégée par un mot de passe.

c. Saisissez le mot de passe dans le champ **Mot de passe** de la fenêtre **Vérification du mot de passe**.

d. Cochez la case **Mémoriser le mot de passe pour la session actuelle du fonctionnement de l'application** si vous ne souhaitez pas avoir à saisir le mot de passe pour exécuter cette opération au cours de la même session. La restriction de l'accès à l'application sera levée après le prochain lancement de l'application.

   Si la case **Mémoriser le mot de passe pour la session actuelle du fonctionnement de l'application** est décochée, cela signifie que l'application demande le mot de passe à chaque tentative d'exécution de cette opération.

e. Cliquez sur le bouton **OK**.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Administration des paramètres de Kaspersky Security

Cette section contient les instructions pour le transfert des paramètres de Kaspersky Security vers l'application installée sur une autre machine virtuelle, ainsi que pour la réinitialisation des paramètres par défaut.

Dans cette section

Transfert des paramètres de Kaspersky Security vers l'application installée sur une autre machine virtuelle

Une fois les paramètres de Kaspersky Security configurés, vous pouvez les transférer vers la même application installée sur une autre machine virtuelle. Ainsi, Kaspersky Security sera configuré à l'identique sur les deux machines virtuelles.

Vous pouvez enregistrer les paramètres de l'application dans un fichier de configuration spécial au format CFG, puis transférer le fichier de configuration d'une machine virtuelle à l'autre.

Le fichier CFG de configuration est aussi utilisé pour importer les paramètres lors de l'installation à distance de l'application et lors de la création de la stratégie pour le Light Agent (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Le fichier de configuration utilisé pour l'importation des paramètres lors de l'installation à distance de l'application doit être nommé install.cfg.

► *Afin de transférer les paramètres de Kaspersky Security vers la même application installée sur une autre machine virtuelle, procédez comme suit :*

1. Sauvegardez les paramètres actuels de l'application Kaspersky Security dans le fichier de configuration de la manière suivante :

   a. Ouvrez la fenêtre de configuration des paramètres de l'application (à la page 25).

   b. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

      Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.

   c. Dans le groupe **Administration des paramètres**, cliquez sur le bouton **Enregistrer**.

      La fenêtre standard de Microsoft Windows **Sélection du fichier de configuration** s'ouvre.

   d. Saisissez le nom du fichier de configuration puis sélectionnez l'emplacement où il sera enregistré.

   e. Cliquez sur le bouton **Enregistrer**.

2. Transférez le fichier de configuration sauvegardé vers une autre machine virtuelle (envoyez-le par email ou placez-le sur un disque amovible, par exemple).

3. Sur l'autre machine virtuelle, téléchargez les paramètres de fonctionnement de l'application dans Kaspersky Security depuis le fichier de configuration ; ceci de la manière suivante :

   a. Ouvrez la fenêtre de configuration des paramètres de l'application.

   b. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

      Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.

   c. Dans le groupe **Administration des paramètres**, cliquez sur le bouton **Télécharger**.

      La fenêtre standard de Microsoft Windows **Sélection du fichier de configuration** s'ouvre.

d. Sélectionnez le fichier à partir duquel vous souhaitez importer les paramètres de Kaspersky Security.

e. Cliquez sur le bouton **Ouvrir**.

f. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Restauration des paramètres par défaut de l'application

Sur la base des informations relatives au système d'exploitation et aux programmes installés sur la machine virtuelle protégée, les experts de Kaspersky Lab vous recommandent des paramètres optimaux de protection. Tout au long de votre utilisation de Kaspersky Security, vous avez la possibilité de restaurer les paramètres par défaut de l'application. La restauration des paramètres s'effectue à l'aide de l'Assistant de configuration initiale de l'application.

► *Pour restaurer les paramètres par défaut de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de l'application.
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Administration des paramètres**, cliquez sur le bouton **Restaurer.**

   L'Assistant de configuration initiale de l'application s'ouvre.
4. Dans la fenêtre **Bienvenue**, Cliquez sur le bouton **Suivant** afin de lancer l'Assistant de configuration initiale de l'application.
5. Dans la fenêtre **Restauration des paramètres**, vous trouverez une liste des modules et tâches de Kaspersky Security dont les paramètres ont été modifiés.

   Si des paramètres uniques ont été créés pour l'un des modules lors du fonctionnement de l'application, ils seront aussi affichés dans cette fenêtre. Ces paramètres uniques comprennent, par exemple, les listes d'adresses Internet de confiance, les exclusions créées, les règles réseau du Pare-feu, les règles de contrôle des programmes, etc.

Ces paramètres uniques sont définis pendant l'utilisation de l'application Kaspersky Security, en tenant compte des tâches individuelles et des exigences de sécurité. Il faut souvent beaucoup de temps pour créer des paramètres uniques, c'est pourquoi les experts de Kaspersky Lab recommandent de les conserver, faute de quoi, tous les paramètres créés au cours du fonctionnement de l'application seront perdus.

Cochez les cases correspondant aux modules et tâches dont vous souhaitez rétablir les paramètres par défaut.

6. Cliquez sur le bouton **Suivant**.

7. Lors de l'étape suivante, l'Assistant de configuration initiale analyse les informations sur les programmes contenus dans Microsoft Windows. Ces applications sont intégrées à la liste des applications de confiance (cf. section “Composition de la liste des applications de confiance” à la page 249), pour lesquelles aucune restriction d'activité dans le système d'exploitation n'est appliquée. La progression de l'analyse des informations s'affiche dans la fenêtre **Analyse du système**.

   Une fois l'analyse du système d'exploitation terminée, l'Assistant de configuration initiale de l'application passe automatiquement à l'étape suivante.

8. Dans la fenêtre **Fin de la configuration initiale de l'application**, cliquez sur le bouton **Terminer**.

   L'Assistant de configuration initiale de l'application se ferme et les paramètres par défaut de l'application sont rétablis.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Participer au Kaspersky Security Network

Cette section contient des informations relatives à la participation au Kaspersky Security Network et les instructions pour la vérification de la connexion au Kaspersky Security Network.

Dans cette section

A propos de la participation au Kaspersky Security Network

Pour renforcer l'efficacité de la protection de la machine virtuelle, Kaspersky Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet de collecter ces données.

Kaspersky Security Network (KSN) est une infrastructure de services de cloud qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Web et des logiciels. Grâce aux données de Kaspersky Security Network, Kaspersky Security peut réagir plus rapidement face aux menaces inconnues. L'efficacité de certains modules est améliorée.

La participation des utilisateurs au Kaspersky Security Network permet à Kaspersky Lab d'obtenir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des outils de neutralisation et de réduire le nombre de faux positifs.

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

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

La configuration de l'utilisation du KSN privé s'effectue dans les propriétés du Serveur d'administration de Kaspersky Security Center, dans la section **Serveur proxy KSN**. Pour plus d'informations, consultez la documentation de Kaspersky Security Center.

Pour continuer à utiliser le KSN privé après la modification de la clé, il faut fournir les informations relatives à la clé au prestataire de service. Dans le cas contraire, l'échange d'informations avec KSN est impossible.

Pendant l'utilisation de KSN, l'application envoie automatiquement Kaspersky Security Network les statistiques reçues suite à son exécution (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*). Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi et aux politiques de Kaspersky Lab.

Kaspersky Lab utilise les informations obtenues uniquement de manière impersonnelle et sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas de données personnelles ou d'autres données confidentielles. Les informations obtenues sont supprimées au fur et à mesure de leur accumulation (une fois par an). Les données des statistiques générales sont conservées de manière illimitée. Pour plus d'informations sur l'envoi à Kaspersky Lab, la conservation et la destruction des statistiques obtenues pendant l'utilisation du KSN, vous pouvez consulter le règlement du KSN et le site Web de Kaspersky Lab http://www.kaspersky.fr/privacy.

La participation à Kaspersky Security Network est volontaire. C'est l'administrateur de l'application qui décide d'activer ou non l'utilisation de KSN via les paramètres de la stratégie (cf. *Manuel* de *l'administrateur de Kaspersky Security for Virtualization 4.0 Light Agent*).

Vérification de la connexion à Kaspersky Security Network

► *Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 23).
2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Kaspersky Security Network**.

   La fenêtre **Kaspersky Security Network** s'ouvrira.

Le bouton **KSN** rond dans la partie gauche de la fenêtre désigne le mode de connexion de l'application au Kaspersky Security Network :

- Si l'application Kaspersky Security est connectée à Kaspersky Security Network, le bouton **KSN** est vert. Le bouton **KSN** donne accès à l'état *Activé(e)*, au type de KSN utilisé, KSN privé (KPSN) ou KSN global, et aux données de la dernière synchronisation avec les serveurs KSN*. Les* statistiques relatives à la réputation des fichiers et des ressources Web apparaissent dans la partie droite de la fenêtre.

  > L'application Kaspersky Security reçoit les statistiques d'utilisation des services Kaspersky Security Network lors de l'ouverture de la fenêtre **Kaspersky Security Network**. Les statistiques ne sont pas mises à jour en temps réel.

- Si l'application Kaspersky Security n'est pas connectée à Kaspersky Security Network, le bouton **KSN** est gris. L'état *Désactivé(e)* s'affiche sous le bouton **KSN**.

  La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

  - L'application n'est pas activée ou la licence a expiré ;
  - Vous ne participez pas au Kaspersky Security Network.
  - Le service KSN Proxy est désactivé dans Kaspersky Security Center (consultez la documentation du Kaspersky Security Center).

Glossaire

A

Analyse heuristique

Technologie de détection des menaces dont les données n'ont pas encore été ajoutées aux bases de l'application Kaspersky Lab. Permet de détecter des fichiers pouvant contenir un programme malveillant absent des bases ou une forme modifiée d'un virus connu.

Analyse sur la base de signatures

Technologie d'identification des menaces qui utilise les bases de l'application Kaspersky Lab contenant les descriptions des menaces connues et les méthodes de leur élimination.
La protection selon cette méthode offre le niveau minimum de sécurité. Conformément aux recommandations des experts de Kaspersky Lab, cette méthode d’analyse est toujours activée.

Archive

Un ou plusieurs fichiers regroupés dans un même fichier compressé. Pour la compression ou la décompression de telles données, une application spécifique appelée compresseur est indispensable.

B

Base des adresses Internet de phishing

Liste des adresses Internet de ressources Web identifiées par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Base des adresses Internet malveillantes

Liste des d'adresses des ressources Web dont le contenu pourrait constituer une menace. La liste est composée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

Bases de l'application

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les bases de l'application sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

C

Copie de sauvegarde du fichier

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

E

Enregistreur de frappes

Application conçue pour enregistrer de façon masquée les touches sur lesquelles l'utilisateur appuie pendant l'utilisation de l'ordinateur. Les enregistreurs de frappe sont parfois désignés sous le terme keylogger.

F

Faux positif

Situation où un fichier sain est considéré comme infecté par l'application de Kaspersky Lab car son code évoque celui d'un virus.

Fichier composé

Un fichier composé comprend plusieurs fichiers séparés qui se trouvent dans un fichier physique et auxquels il est possible d'accéder individuellement. Les exemples des fichiers composés sont les archives, les paquets d'installation, les objets OLE joints et les fichiers aux formats de messagerie. Une pratique répandue de dissimulation des virus est de les intégrer aux fichiers composés. Pour détecter les virus dissimulés ainsi, il est nécessaire de décompresser le fichier composé.

K

Kaspersky Private Security Network

Solution permettant aux utilisateurs des applications antivirus de Kaspersky Lab d'accéder aux données de Kaspersky Security Network sans envoyer d'informations aux serveurs Kaspersky Security Network de Kaspersky Lab de leur côté.

Kaspersky Security Network (KSN)

Infrastructure des services de cloud qui offre l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Web et du logiciel L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

M

Machine virtuelle protégée

Machine virtuelle sur laquelle le module Light Agent est installé.

O

Objet infecté

Objet dont une partie du code correspond parfaitement à une partie du code d'un programme connu présentant une menace. Les experts de Kaspersky Lab déconseillent de manipuler ce type d'objets.

Objet OLE

Objet rattaché à un autre fichier ou intégré à un autre fichier à l'aide de 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.

Objets de démarrage

Ensemble d'applications indispensables au lancement et au fonctionnement du système d'exploitation et des applications installés sur votre machine virtuelle. Le système d'exploitation lance ces objets à chaque démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

Phishing

Type d'escroquerie sur Internet dont le but est d'obtenir un accès non autorisé aux données confidentielles des utilisateurs.

S

Sauvegarde

Dossier de sauvegarde spécifique pour les fichiers qui ont été supprimés ou modifiés durant la réparation.

SVM

Secure virtual machine, SVM. Machine virtuelle sur l'hyperviseur où est installé le module Serveur de protection Kaspersky Security.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection des ordinateurs contre différents types de menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top quatre des leaders mondiaux du marché des solutions de sécurité informatique des utilisateurs finaux (classement “IDC Worldwide Endpoint Security Revenue by Vendor”). En Russie, d'après les données IDC, Kaspersky Lab est l'éditeur favori de systèmes de protection des ordinateurs pour les particuliers (“IDC Endpoint Tracker 2014”).

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est un groupe international de sociétés avec 34 bureaux dans 31 pays du monde. La société emploie plus de 3000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers inclut des applications de protection des données pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des tablettes, des smartphones et d'autres appareils nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail et des appareils nomades, des machines virtuelles, des serveurs de fichiers et des serveurs Web, des passerelles de messagerie et des pare-feu. Le portefeuille de la société comprend également des produits spécialisés de protection contre les attaques DDoS, de protection des environnements grâce à un système automatisé de contrôle de processus et de prévention des escroqueries. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée des organisations de toutes tailles contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et ajoutent les signatures de celles-ci aux bases utilisées par les applications de Kaspersky Lab.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est pas le fruit du hasard si le noyau logiciel de Kaspersky Antivirus est utilisé dans les produits de nombreux autres éditeurs de logiciels, tels que : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu et ZyXEL. De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Par exemple, en 2014, selon les résultats des expériences et des recherches effectuées par le laboratoire antivirus autrichien qui fait autorité AV-Comparatives, Kaspersky Lab est devenu un des deux leaders pour la quantité de certificats Advanced+ reçus. Par conséquent, la société a été récompensée du certificat Top Rated. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 400 millions d'utilisateurs. Elle compte plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie Virus :	http://www.securelist.fr/
Laboratoire antivirus :	http://newvirus.kaspersky.com/fr (pour l'analyse des fichiers et sites suspects)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

Avis de marques déposées

Les marques et marques de service déposées appartiennent à leurs propriétaires respectifs.

Adobe et Acrobat sont des marques commerciales ou des marques déposées d'Adobe Systems Incorporated enregistrées aux Etats-Unis et/ou dans d'autres pays.

Citrix et XenServer sont des marques commerciales de Citrix Systems, Inc. et/ou des filiales déposées à l'office des brevets des Etats-Unis et d'autres pays.

FireWire est une marque d'Apple déposée aux Etats-Unis et dans d'autres pays.

ICQ est une marque et/ou une marque de service d'ICQ LLC.

Microsoft, Excel, Hyper-V, Outlook, Windows et Windows Server sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Mozilla et Thunderbird sont des marques de Mozilla Foundation.

VMware ESXi est une marque commerciale de VMware, Inc. ou une marque déposée de VMware, Inc. aux Etats-Unis ou dans d'autres juridictions.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Index

A

B

C

D

E

F

I

K

M

N

P

R

S

T

Z