KASPERSKY lab

Kaspersky Security 10 for Windows Server

Manuel de l'administrateur

Version de l'application : 10

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

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

Date d'édition : 12/02/2016

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

Table des matières

A propos de ce document

Le manuel de l'administrateur de Kaspersky Security 10 for Windows Server® (ci-après Kaspersky Security, distribué antérieurement sous le nom Kaspersky Anti-Virus for Windows Servers Enterprise Edition) est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Security et aux spécialistes du support technique au sein des organisations qui utilisent Kaspersky Security.

Ce guide reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security.

Il renseigne également les sources d'informations sur l'application et explique la marche à suivre pour bénéficier du Support Technique.

Dans cette section

Dans ce document

Le Manuel de l'administrateur de Kaspersky Security contient les sections suivantes :

Sources d'informations sur Kaspersky Security

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

Kaspersky Security

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Security. Elle reprend la configuration matérielle et logicielle requise pour l'application.

Licence de l'application

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

Interface de Kaspersky Security et accès aux fonctions de l'application

Cette section aborde la console de Kaspersky Security et l'administration de Kaspersky Security via la console installée sur le serveur à protéger ou sur un autre ordinateur.

Autorisations d'accès aux fonctions de Kaspersky Security

Cette section contient les informations relatives au lancement et à l'arrêt du service de Kaspersky Security.

Zone de confiance

Cette section contient des informations sur la zone de confiance de Kaspersky Security, sur les instructions pour ajouter des objets à la zone de confiance et sur l'application de la zone de confiance aux tâches de Kaspersky Security.

Gestion des tâches de Kaspersky Security

Cette section contient les informations relatives aux tâches de Kaspersky Security, à leur création, à la configuration des paramètres d'exécution, au lancement et à l'arrêt des tâches et à la configuration du lancement et de l'arrêt automatiques des tâches planifiées.

Protection en temps réel

Cette section présente les tâches de protection en temps réel : la tâche Protection des fichiers en temps réel, la tâche Analyse des scripts et la tâche Utilisation du KSN. La section contient également les instructions relatives à la configuration des paramètres des tâches de protection en temps réel et des paramètres de la sécurité du serveur protégé.

Contrôle du serveur

Cette section contient des informations sur la fonctionnalité de Kaspersky Security relative au contrôle de l'accès aux fichiers réseau et au contrôle des applications exécutées sur le serveur.

Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande. La section contient également les instructions relatives à la configuration des paramètres des tâches d'analyse à la demande et des paramètres de la sécurité du serveur protégé.

Mise à jour des bases de données et des modules de Kaspersky Security

Cette section présente les tâches de mises à jour des bases et des modules logiciels de Kaspersky Security, la copie des mises à jour et le retour à l'état antérieur aux mises à jour. Elle explique également comment configurer les paramètres des tâches de mise à jour des bases et des modules de l'application.

Sauvegardes de Kaspersky Security

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur réparation ou leur suppression. Elle fournit également des instructions sur l'isolement des fichiers probablement infectés.

Consignation des événements. Journaux de Kaspersky Security

Cette section contient des informations sur l'utilisation des journaux de Kaspersky Security : journal d'audit système, journaux d'exécution des tâches de Kaspersky Security et journal des événements de Kaspersky Security.

Configuration des notifications

Cette section contient des informations sur les différentes méthodes de notification des utilisateurs et des administrateurs de Kaspersky Security sur les événements de l'application et l'état de la protection du serveur, ainsi que les instructions relatives à la configuration des notifications.

Administration du stockage hiérarchique

Cette section contient des informations sur l'analyse antivirus des fichiers qui se trouvent dans des stockages hiérarchiques et dans des systèmes de sauvegarde.

Administration de Kaspersky Security via la ligne de commande

Cette section contient des informations et des instructions sur la gestion du fonctionnement de Kaspersky Security via la ligne de commande.

Administration de Kaspersky Security via Kaspersky Security Center

Cette section contient les informations et les instructions relatives à l'administration de Kaspersky Security et à la configuration de ses paramètres via la console d'administration Kaspersky Security Center.

Compteurs de Kaspersky Security

Cette section contient des informations sur les compteurs de Kaspersky Security : compteurs de performances pour l'application Moniteur système et compteurs et interruptions SNMP.

Contacter le Support Technique

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

Glossaire

Cette section reprend les termes utilisés dans ce document et leur définition.

AO KASPERSKY LAB

Cette section contient des informations sur AO Kaspersky Lab.

Informations sur le code tiers

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

Avis de marques déposées

Cette section reprend les marques de commerce citées dans le document et leurs détenteurs respectifs.

Index

Cette section permet de trouver rapidement les informations que vous cherchez dans le document.

Conventions

Ce document utilise des conventions de style (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui pourraient avoir des conséquences fâcheuses.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires et des conseils.
Exemple :	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments suivants sont en italique dans le texte : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
► *Pour programmer une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et possèdent l'icône "flèche".

Exemple de texte	Description de la convention
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : Indiquez la date au format `JJ:MM:AA`.	Les types de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir via le clavier.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les chevrons sont omis.

Sources d'informations sur Kaspersky Security

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

Vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

Dans cette section

Sources de données pour des consultations indépendantes

Vous pouvez utiliser les sources suivantes pour rechercher vous-même des informations sur Kaspersky Security 10 for Windows Server :

- La page de l'application sur le site de Kaspersky Lab ;
- La page de l'application sur le site du support technique (la Base de connaissances).
- aide électronique ;
- documentation.

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab (cf. section « Contacter le Support Technique » à la page 467).

L'utilisation des sources d'informations sur le site Internet de Kaspersky Lab requiert une connexion à Internet.

Page de Kaspersky Security sur le site Web de Kaspersky Lab

La page de Kaspersky Security (http://www.kaspersky.fr/business-security/windows-server-security) fournit des informations générales sur l'application, sur ses fonctionnalités et ses particularités.

La page de Kaspersky Security for Windows Server affiche un lien vers le magasin en ligne. Dans la boutique, vous pourrez acheter l'application ou prolonger vos droits d'utilisation.

Page de Kaspersky Security dans la base de connaissances

La *base de connaissances* est une rubrique du site du Support technique.

La page de Kaspersky Security 10 for Windows Server dans la Base des connaissances (http://support.kaspersky.com/fr/ksws10) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la Base de connaissances peuvent répondre à des questions qui concernent non seulement Kaspersky Security mais également d'autres logiciels de Kaspersky Lab. Ces articles peuvent également contenir des actualités du Support technique.

Sauvegardes de Kaspersky Security

Le Manuel d'installation de Kaspersky Security 10 for Windows Server reprend les informations relatives à l'exécution des tâches suivantes :

- préparatifs pour l'installation, installation et activation de Kaspersky Security ;
- préparatifs pour l'utilisation de Kaspersky Security ;
- réparation ou suppression de Kaspersky Security.

Le manuel de l'administrateur de Kaspersky Security 10 for Windows Server reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security.

Le manuel d’implantation pour la protection des référentiels réseau reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security dans le cadre de la protection des stockages réseau.

Discussion sur les logiciels de Kaspersky Lab sur le forum

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs sur notre forum (http://forum.kaspersky.fr).

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

Kaspersky Security

Kaspersky Security 10 for Windows Server (commercialisé antérieurement sous le nom Kaspersky Anti-Virus for Windows Servers Enterprise Edition) protège les serveurs tournant sous les systèmes d'exploitation Microsoft® Windows® et les stockages réseau contre les virus et autres menaces informatiques qui se propagent via l'échange de fichiers. Kaspersky Security a été développé pour les intranets des grandes et des moyennes entreprises. Les utilisateurs de Kaspersky Security sont les administrateurs du réseau de l'organisation et les personnes chargées de la protection antivirus de ce réseau.

Vous pouvez installer Kaspersky Security les serveurs suivants :

- serveurs de terminaux ;
- serveurs d'impression ;
- serveurs d'applications ;
- contrôleurs de domaine ;
- serveurs de protection de stockages réseau ;
- serveurs de fichiers ; ceux-ci sont plus exposés aux infections car ils interviennent dans l'échange des fichiers avec les postes de travail des utilisateurs.

Vous pouvez administrer Kaspersky Security d'une des manières suivantes :

- via la console de Kaspersky Security installée sur un serveur doté de Kaspersky Security ou sur un autre ordinateur ;
- via la ligne de commande ;
- via la console d'administration Kaspersky Security Center.

Vous pouvez utiliser l'application Kaspersky Security Center pour l'administration centralisée de la protection de nombreux serveurs doté chacun de Kaspersky Security.

Il est possible de consulter les compteurs de performance de Kaspersky Security pour l'application « Moniteur système » ainsi que les compteurs et les interruptions SNMP.

Modules et fonctions de Kaspersky Security

L'application intègre les modules suivants :

- Protection en temps réel.

  Kaspersky Security analyse les objets lorsqu'ils sont sollicités. Kaspersky Security analyse les objets suivants :

  - les fichiers ;
  - les scripts ;
  - les flux alternatifs des systèmes de fichiers (flux NTFS) ;
  - l'enregistrement principal de démarrage et les secteurs d'amorçage des disques durs locaux ou des périphériques externes.

- Contrôle du serveur.

  Kaspersky Security surveille toutes les requêtes adressées aux ressources fichier réseau, contrôle le lancement des applications et bloque l'accès des ordinateurs distants au serveur si ceux-ci manifestent une activité malveillante ou de chiffrement.

- Protection des stockages réseau connectés via le protocole RPC ou Protection des stockages réseau connectés via le protocole ICAP.

  Kaspersky Security installé sur un serveur tournant sous un système d'exploitation Microsoft Windows protège les stockages réseau contre les virus et autres menaces informatiques qui se propagent via l'échange de fichiers.

- Analyse à la demande.

  Kaspersky Security recherche une fois des virus et autres menaces informatique dans la zone indiquée. Kaspersky Security analyse les fichiers, la mémoire vive du serveur et les objets de démarrage.

L'application peut remplir les fonctions suivantes :

- Mise à jour des bases et des modules de l'application.

  Kaspersky Security télécharge la mise à jour des bases et des modules de l'application depuis des serveurs FTP ou HTTP de mises à jour de Kaspersky Lab, depuis le serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.

- Quarantaine.

  Kaspersky Security place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers la *quarantaine*. Pour des raisons de sécurité, une fois en quarantaine, les objets sont chiffrés.

- Sauvegarde.

  Kaspersky Security enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Potentiellement infecté* dans la *sauvegarde* avant de procéder à la réparation ou à la suppression de ces objets.

- Notifications de l'administrateur et des utilisateurs.

  Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Security et à l'état de la protection antivirus du serveur.

- Importation et exportation des paramètres.

  Vous pouvez exporter les paramètres de Kaspersky Security dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.

- Application des modèles.

  Vous pouvez configurer manuellement les paramètres de sécurité de l'entrée dans l'arborescence des ressources fichier du serveur et enregistrer les valeurs définies dans un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Security.

- Consignation des événements.

  Kaspersky Security consigne dans les journaux les informations relatives aux paramètres des modules de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution de celles-ci, ainsi que les renseignements sur les événements liés à l'administration de Kaspersky Security et les informations indispensables au diagnostic des échecs dans le fonctionnement de l'application.

- Stockage hiérarchique.

  Kaspersky Security peut fonctionner en mode d'utilisation de systèmes de gestion de stockage hiérarchique (système HSM). Le recours aux systèmes HSM permet de transférer des données entre des disques locaux rapides et des périphériques lents de stockage d'informations de longue durée.

- Zone de confiance.

  Vous pouvez composer la liste des exclusions de la zone de protection ou d'analyse que Kaspersky Security exploite dans les tâches d'analyse à la demande, de protection des fichiers en temps réel, d'analyse des scripts et de protection des stockages réseau via le protocole RCP.

- Administration des autorisations.

  Vous pouvez configurer les autorisations d'administration de Kaspersky Security et des services Windows que l'application enregistre pour des utilisateurs ou des groupes d'utilisateurs.

Dans cette section

Nouveautés

Kaspersky Security 10 introduit les modules et les possibilités suivants :

- Fonctionnalité d'intégration avec les services Kaspersky Security Network (dans le cadre de la tâche Utilisation du KSN). Vous pouvez utiliser les services KSN pour accélérer la vitesse de réaction de Kaspersky Security face aux nouvelles menaces, augmenter l'efficacité de certains modules de la protection et réduire la possibilité de faux positifs.

- Fonctionnalité de contrôle du lancement des applications (dans le cadre de la tâche Contrôle du lancement des applications). Vous pouvez autoriser ou interdire le lancement de fichiers exécutables, de scripts et de paquets MSI, ainsi que le téléchargement de modules DLL à l'aide des règles indiquées. Les règles de contrôle du lancement des applications sont créées manuellement, à l'aide de la tâche de génération automatique des règles d'autorisation ou à l'aide du traitement des événements de la tâche Contrôle du lancement des applications dans la console de Kaspersky Security ou à partir du rapport sur les applications bloquées dans le Kaspersky Security Center.

- Fonctionnalité de blocage de l'accès des ordinateurs aux dossiers réseau partagés d'un serveur protégé (dans le cadre de la tâche de blocage de l'accès aux fichiers réseau). Vous pouvez configurer les paramètres du blocage de l'accès des ordinateurs distants aux fichiers réseau. L'application bloque l'accès aux fichiers réseau quand une activité malveillante est détectée sur ces ordinateurs lors de l'exécution des tâches Protection des fichiers en temps réel ou Protection contre le chiffrement.

- Fonctionnalité de protection des dossiers réseau partagés d'un serveur contre le chiffrement (dans le cadre de la tâche Protection contre le chiffrement). Vous pouvez configurer le blocage de l'accès aux fichiers réseau pour les ordinateurs distants à l'origine d'une activité de chiffrement. Si une activité de chiffrement des fichiers est détectée, l'application inscrit les informations concernant l'événement dans le journal d'exécution de la tâche et bloque l'accès aux ressources réseau pour l'ordinateur sur lequel l'activité de chiffrement a été identifiée. Vous pouvez exclure de la zone de protection tout dossier dont l'activité de chiffrement des données n'est pas malveillante.

- Possibilité d'envoi des objets de la quarantaine à Kaspersky Lab pour analyse via le Kaspersky Security Center.

- Possibilité de configurer les autorisations de gestion de certaines fonctions de l'application pour les utilisateurs depuis le Kaspersky Security Center.
- Possibilité de configurer les autorisations d'administration du service Kaspersky Security pour les utilisateurs. Vous pouvez limiter l'accès au service dans la Console de Kaspersky Security ou dans la Console d'administration de Kaspersky Security Center pour les utilisateurs sélectionnés ou pour des groupes d'utilisateurs.

Distribution

La distribution contient une page de bienvenue au départ de laquelle vous pouvez réaliser les opérations suivantes :

- lancer l'Assistant d'installation de Kaspersky Security ;
- lancer l'Assistant d'installation de la console de Kaspersky Security ;
- lancer l'Assistant d'installation du plug-in d'administration de Kaspersky Security via Kaspersky Security Center ;
- lire le Manuel d'installation, le Manuel de l'administrateur, le Manuel d'implantation pour la protection des stockages réseau ;
- ouvrir la page de Kaspersky Security sur le site Web de Kaspersky Lab ;
- accéder au site Internet du Support technique ;
- lire les informations sur la version actuelle de Kaspersky Security.

Le dossier \server contient :

- les fichiers d'installation des modules de protection de Kaspersky Security sur un ordinateur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows ;
- le fichier d'installation du plug-in d'administration de Kaspersky Security via Kaspersky Security Center ;
- une archive contenant les bases antivirus d'actualité au moment de l'édition de l'application ;
- un fichier contenant le texte du contrat de licence utilisateur final.

Le dossier \client contient les fichiers d'installation de la console de Kaspersky Security (ensemble des composants "Outils d'administration").

Le dossier \setup contient les fichiers indispensables au lancement de l'application de bienvenue.

La fonction des fichiers de la distribution de Kaspersky Security est décrite dans le tableau ci-dessous.

Tableau 2. Fichiers de la distribution de Kaspersky Security

Fichier	Fonction
\setup\setup.hta	Fichier de lancement de l'application d'accueil.
ks4ws_install_guide_fr.pdf	Manuel d'installation et de déploiement.
ks4ws_netstorage_guide_fr.pdf	Manuel d'implantation pour les stockages réseau.
ks4ws_admin_guide_fr.pdf	Manuel de l'administrateur.
autorun.inf	Fichier de démarrage automatique de l'Assistant d'installation de Kaspersky Security pour l'installation de l'application depuis un support amovible.
server\bases.cab	Archive contenant les bases antivirus d'actualité au moment de l'édition de l'application.
server\license.txt	Texte du contrat de licence utilisateur final.
release_notes.txt	Ce fichier contient les informations relatives à la version.
\server\setup.exe	Fichier de lancement de l'Assistant d'installation de Kaspersky Security sur le serveur protégé ; lance le fichier du paquet d'installation ks4ws.msi selon les paramètres d'installation définis dans l'Assistant.
\server\ks4ws_x86(x64).msi	Paquet d'installation du service Windows Installer ; installe Kaspersky Security sur le serveur protégé.

Fichier	Fonction
\server\ks4ws.kpd	Fichier reprenant la description du paquet d'installation pour l'installation à distance de Kaspersky Security via Kaspersky Security Center ; porte l'extension kpd (Kaspersky Package Definition). Ce fichier contient le nom du paquet d'installation, des informations générales sur Kaspersky Security (numéro de la version et date d'édition) et une description des codes de retour du programme d'installation. Ce fichier contient également les arguments de la ligne de commande qui définissent les paramètres d'installation via Kaspersky Security Center.
\server\ks4ws.kud	Fichier contenant une description du paquet d'installation pour l'installation à distance de Kaspersky Security via Kaspersky Security Center au format Kaspersky Unicode Definition. Utilise le fichier ks4ws.kpd.
\client\setup.exe	Fichier de lancement de l'Assistant d'installation de l'ensemble des composants "Outils d'administration" (contient la console de Kaspersky Security) ; lance le fichier du paquet d'installation ks4wstools.msi selon les paramètres d'installation définis dans l'Assistant.
client\ks4wstools_x86(x64).msi	Paquet d'installation du service Windows Installer ; installe la console de Kaspersky Security.
server\klcfginst.exe	Programme d'installation du plug-in d'administration de Kaspersky Security via Kaspersky Security Center. Installez le plug-in sur chacun des ordinateurs doté de la console d'administration Kaspersky Security Center si vous avez l'intention de l'utiliser pour administrer Kaspersky Security.

Vous pouvez lancer les fichiers de la distribution depuis le cd. Si vous avez d'abord copié les fichiers sur le disque local, assurez-vous que la structure des fichiers de la distribution a été préservée.

Configurations logicielle et matérielle requises

Cette section reprend la configuration logicielle et matérielle requise pour Kaspersky Security.

Dans cette section

Configuration requise pour le serveur sur lequel Kaspersky Security est installé

Avant d'installer Kaspersky Security, il convient de supprimer du serveur tout autre logiciel antivirus qui serait installé.

Vous pouvez installer Kaspersky Security sans supprimer la version de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition qui serait déjà installée.

Configuration matérielle requise pour le serveur

Recommandations d'ordre général :

- systèmes compatibles x86-64 avec un ou plusieurs processeurs ;
- Espace disque requis :
  - pour l'installation de tous les modules de l'application : 70 Mo ;
  - pour le téléchargement et le stockage des bases antivirus de l'application : 2 Go (recommandé) ;

- pour l'enregistrement des fichiers en quarantaine et dans la sauvegarde : 400 Mo (recommandé) ;
- pour l'enregistrement des journaux : 1 Go (recommandé).

Configuration minimale :

- Processeur monocoeur 1,4 GHz
- Mémoire vive : 1 Go
- Disque : 4 Go d'espace disponible

Configuration recommandée :

- Processeur quadricoeur 2,4 GHz
- Mémoire vive : 2 Go
- Disque : 4 Go d'espace disponible

Configuration logicielle requise pour le serveur

Vous pouvez installer Kaspersky Security sur un serveur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows.

L'installation et l'utilisation de Kaspersky Security sur le serveur requièrent Microsoft Windows Installer 3.1.

Vous pouvez installer Kaspersky Security sur un serveur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 ou suivant

Vous pouvez installer Kaspersky Security sur un serveur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 ou suivant

- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Hyper-V® Server 2008 R2 SP1 ou suivant
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

Vous pouvez installer Kaspersky Security sur un des serveurs de terminaux suivants :

- Microsoft Remote Desktop Services sur la base de Windows 2008 Server
- Microsoft Remote Desktop Services sur la base de Windows 2012 Server
- Microsoft Remote Desktop Services sur la base de Windows 2012 Server R2
- Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6 ;
- Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6.

Configuration requise pour le stockage réseau protégé

Kaspersky Security peut être utilisé pour la protection des stockages réseau suivants :

- NetApp® sous un des systèmes d'exploitation suivants :
  - Data ONTAP® 7.x et Data ONTAP 8.x en mode 7-mode
  - Data ONTAP 8.2.1 ou suivant en mode cluster-mode
- EMC™ Celerra™ / VNX™ avec la configuration logicielle suivante :
  - Système d'exploitation EMC DART 6.0.36 ou suivant
  - Agent antivirus Celerra (CAVA) 4.5.2.3 ou suivant
- EMC Isilon™ sous le système d'exploitation OneFS™ 7.0 ou suivant.
- Hitachi NAS sur une des plateformes suivantes :
  - HNAS 4100
  - HNAS 4080

- HNAS 4060
- HNAS 4040
- HNAS 3090
- HNAS 3080

- IBM® NAS série IBM System Storage® N series.
- Oracle® NAS Systems de la série Oracle ZFS Storage Appliance.
- Dell™ NAS sur la plateforme Dell Compellent™ FS8600.

Configuration requise pour l'ordinateur sur lequel la console de Kaspersky Security est installée

Configuration matérielle requise pour l'ordinateur

Mémoire vive recommandée : 128 Mo minimum.

Espace disque disponible : 30 Mo.

Configuration logicielle requise pour l'ordinateur

Vous pouvez installer la console de Kaspersky Security sur un ordinateur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows.

L'installation et l'utilisation de la console de Kaspersky Security sur l'ordinateur requièrent Microsoft Windows Installer 3.1.

Vous pouvez installer la console de Kaspersky Security sur un ordinateur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions

- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional ;
- Microsoft Windows 10 Enterprise / Professional.

Vous pouvez installer la console de Kaspersky Security sur un ordinateur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 ou suivant
- Windows Hyper-V Server 2008 R2 SP1 ou suivant
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 ou suivant
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional ;
- Microsoft Windows 10 Enterprise / Professional.

Licence de l'application

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

Dans cette section

A propos du Contrat de licence utilisateur final

Le *Contrat de Licence Utilisateur Final* est un accord juridique conclu entre vous et AO Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

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

Vous pouvez prendre connaissances des conditions du contrat de licence Utilisateur final, en utilisant les moyens suivants :

- pendant l'installation de Kaspersky Security.
- en lisant le document license.txt. Ce document est inclus dans la distribution de l'application.

Vous acceptez les conditions du contrat de licence, en confirmant votre accord avec le texte du contrat de licence Utilisateur final lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence Utilisateur final, vous devez interrompre l'installation de l'application et vous ne pouvez pas utiliser l'application.

A propos du certificat de licence

Le *certificat de licence* est un document qui vous est remis avec le fichier clé ou le code d'activation.

Le certificat de licence reprend les informations suivantes relatives à la licence octroyée :

- numéro de la commande ;
- informations sur l'utilisateur qui bénéficie de la licence ;
- informations sur l'application qui peut être activée à l'aide de la licence octroyée ;
- restrictions sur le nombre de postes sous licence (par exemple, les périphériques sur lesquels l'utilisation de l'application est autorisée) ;
- date de début de validité de la licence ;
- date de fin de validité de la licence ou durée de validité de la licence ;
- type de licence.

A propos de la licence

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

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application dans le respect des dispositions du contrat de licence utilisateur final ;
- Obtention du Support Technique.

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

Il existe les types de licence suivants :

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

  La durée de validité de la licence d'évaluation est courte. Une fois que la licence d'évaluation de Kaspersky Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, il vous faudra acheter une licence commerciale.

  Vous pouvez activer l'application à l'aide d'une licence d'évaluation une seule fois uniquement.

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

  A l'expiration de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases de Kaspersky Security n'est plus disponible). Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky Security, il faut renouveler la validité de la licence de la licence commerciale.

Il est conseillé de renouveler la validité de la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre toutes les menaces.

A propos de l'abonnement

L'abonnement à Kaspersky Security est une commande pour l'utilisation de l'application selon des paramètres définis (date d'expiration de l'abonnement, nombre de périphériques protégés). Il est possible d'enregistrer un abonnement à Kaspersky Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur d'accès Internet). Vous pouvez renouveler l'abonnement manuellement ou automatiquement ou décider de ne pas le renouveler. Un abonnement peut également être suspendu et rétabli. La gestion de l'abonnement est confiée au prestataire du service. Vous ne pouvez pas gérer l'abonnement vous-même.

Le choix des possibilités de gestion de l'abonnement diffère selon les prestataires de services. Le prestataire de services peut accorder une *période de grâce* pour renouveler l'abonnement.

La période de grâce est un intervalle entre l'expiration de l'abonnement et son renouvellement au cours duquel les fonctions de l'application sont conservées.

L'abonnement peut être *limité* ou *illimité*.

L'abonnement limité correspond au type de licence indiquée qui possède une durée de validité définie et pour laquelle le renouvellement automatique n'est pas prévu.

L'abonnement illimité correspond au type de licence indiquée qui est renouvelée automatiquement sans votre intervention après avoir réalisé le paiement en temps opportuns et qui ne possède pas de date d'échéance fixe.

L'état de l'abonnement actif apparaît dans le panneau des résultats de l'entrée **Kaspersky Security** et il est actualisé toutes les heures. Il est impossible d'actualiser l'état de l'abonnement manuellement.

La sélection des modules de l'application disponible sur abonnement correspond aux fonctions de l'application pour la solution Kaspersky Security Basic (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41).

> Les codes d'activation achetés par abonnement ne peuvent pas être utilisés pour l'activation de versions antérieures de l'application.

A propos de la clé

La *clé* est une séquence d'octets qui permet d'activer l'application en vue de son utilisation dans le respect des dispositions du contrat de licence Utilisateur final. La clé est générée par les experts de Kaspersky Lab.

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

La clé peut être bloquée par Kaspersky Lab en cas de non-respect du Contrat de licence. Si la clé est bloquée, il faudra en ajouter une autre pour pouvoir utiliser l'application.

Une clé peut être active ou complémentaire.

Clé active est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour une licence d'évaluation ou une licence commerciale peut être ajoutée en tant que clé active. L'application ne peut pas contenir plus d'une clé active.

La *Clé additionnelle* est une clé qui confirme le droit d'utilisation de l'application, non utilisée au moment actuel. Une clé additionnelle devient automatiquement une clé active à l'expiration de la validité de la licence associée à la clé active en cours. Une clé additionnelle ne peut être ajoutée que si une clé active existe.

Une clé pour une licence d'évaluation ne peut être qu'une clé active. Il est impossible d'ajouter une clé pour licence d'évaluation en tant que clé additionnelle.

A propos du fichier clé

Le *fichier clé* est un fichier portant l'extension .key qui vous est remis par Kaspersky Lab. Le fichier clé permet d'ajouter une clé pour activer l'application.

Le fichier clé est envoyé à l'adresse email que vous avez indiquée après avoir acheté Kaspersky Security ou après avoir sollicité une version d’essai de Kaspersky Security.

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

En cas de suppression accidentelle du fichier clé, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer un fichier clé, réalisez une des actions suivantes :

- Contacter le Support Technique (http://support.kaspersky.com/fr).
- Récupérer le fichier clé sur le site de Kaspersky Lab (https://activation.kaspersky.com/fr/) à l'aide du code d'activation en votre possession.

A propos du code d'activation

Le *code d'activation* est une séquence unique de 20 caractères alphanumériques latins. Vous saisissez le code d'activation afin d'ajouter la clé qui va activer Kaspersky Security. Le code d'activation à l'adresse email que vous avez indiquée après avoir acheté Kaspersky Security ou après avoir sollicité une version d'essai de Kaspersky Security.

Pour activer l'application à l'aide du code d'activation, il faut un accès Internet afin de pouvoir contacter le serveur d'activation de Kaspersky Lab.

Si vous perdez le code d'activation après l'activation de l'application, vous pourrez le récupérer. Vous aurez besoin du code d'activation pour ouvrir un Kaspersky CompanyAccount par exemple. Pour récupérer un code d'activation, il faut contacter le Support Technique de Kaspersky Lab (cf. section "Modes d'obtention du Support Technique" à la page 467).

A propos des solutions accessibles de Kaspersky Security

Kaspersky Security for Windows Server se retrouve dans différentes solutions de protection des organisations. La disponibilité de la fonction de Kaspersky Security dépend de la solution choisie. Le tableau ci-dessous reprend les types de solutions proposées et les fonctions de l'application disponibles pour chacune d'entre elles.

Tableau 3. Solutions Kaspersky Security

Solution de protection	Fonction de Kaspersky Security for Windows Server				
	Protection de base	Protection des stockages réseau	Contrôle du lancement des applications	Protection contre le chiffrement	Blocage de l'accès aux fichiers réseau
Kaspersky Security Standard	Oui	Non	Non	Non	Non
Kaspersky Security Basic (sur abonnement)	Oui	Non	Non	Non	Non
Kaspersky Security Etendu	Oui	Non	Oui	Oui	Oui
Kaspersky Security Total	Oui	Non	Oui	Oui	Oui
Kaspersky Security pour serveurs de fichiers	Oui	Non	Oui	Oui	Oui
Kaspersky Security pour systèmes de stockage de données	Oui	Oui	Oui	Oui	Oui

A propos de l'approvisionnement des données

L'acceptation des dispositions du contrat de licence utilisateur final ou la Déclaration de Kaspersky Security Network, vous acceptez de transmettre automatiquement à Kaspersky Lab les informations suivantes dans le cadre du fonctionnement de Kaspersky Security sur votre ordinateur :

- les informations sur les sommes de contrôle des fichiers traités (MD5) ;
- les informations relatives aux programmes, y compris la version et le nom de l'application ;
- l'identifiant unique de l'installation de l'application.

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. Ces statistiques générales se créent automatiquement à partir des informations reçues et ne contiennent aucune donnée personnelle, ni autres données confidentielles. Les informations obtenues sont supprimées au fur et à mesure de leur accumulation (une fois par an). Les statistiques générales sont conservées pendant une durée indéterminée.

Méthodes d'activation de l'application

Vous pouvez activer Kaspersky Security à l'aide d'une des méthodes suivantes :

- activation à l'aide d'un code d'activation ;
- activation à l'aide d'un fichier clé ;
- activation via la ligne de commande.

Dans cette section

Ajout d'un code d'activation

L'activation de l'application à l'aide d'un code d'activation requiert la connexion de l'ordinateur à Internet.

Il est possible d'activer Kaspersky Security à l'aide d'un code d'activation.

Lors de l'activation de l'application à l'aide de cette méthode, Kaspersky Security envoie des données au serveur d'activation afin de vérifier le code saisi :

- Si la validité du code d'activation est confirmée, l'application reçoit un fichier clé qui sera installé automatiquement.
- Dans le cas contraire, un message de circonstance s'affiche à l'écran. Dans ce cas, il faut contacter la société où vous avez acheté la licence de Kaspersky Security afin d'obtenir des informations.
- Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. La procédure d'activation de l'application est interrompue et un message vous invite à contacter le Support Technique de Kaspersky Lab.

► *Pour obtenir une clé pour l'activation de Kaspersky Security à l'aide d'un code d'activation, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Licence**.
2. Dans le panneau des résultats de l'entrée **Licence**, cliquez sur le lien **Ajouter un code d'activation**.
3. Saisissez la clé d'activation dans la fenêtre qui s'ouvre.
4. Cliquez sur **OK**.

Kaspersky Security envoie les données relatives au code d'activation à appliquer au serveur d'activation.

Ajout d'un fichier clé

Il est possible d'activer Kaspersky Security en appliquant un fichier clé.

Si Kaspersky Security possède déjà une clé active et si vous ajoutez une autre clé en tant que clé active, la nouvelle clé remplacera l'ancienne. L'ancienne clé active sera supprimée.

Si Kaspersky Security possède déjà une clé additionnelle et si vous ajoutez une autre clé en tant que clé additionnelle, la nouvelle clé remplacera l'ancienne. L'ancienne clé additionnelle sera supprimée.

Si une clé additionnelle et une clé active avaient déjà été ajoutées à Kaspersky Security et que vous ajoutez une nouvelle clé en tant que clé active, cette nouvelle clé remplacera la clé active antérieure et la clé additionnelle ne sera pas supprimée.

► *Pour activer Kaspersky Security à l'aide d'un fichier clé, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Licence**.
2. Dans le panneau des résultats de l'entrée **Licence**, cliquez sur le lien **Ajouter une clé**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir** et sélectionnez le fichier clé portant l'extension key.
4. Cliquez sur **OK**.

Le fichier clé sera appliqué et l'application sera activée.

Activation via la ligne de commande

Il est possible d'activer Kaspersky Security via la ligne de commande.

Activez l'application à l'aide de la commande suivante :

```
kavshell.exe license /add: <code d'activation ou numéro de la clé>
```

Pour renouveler la licence, saisissez la commande :

```
kavshell.exe license /add: <code d'activation ou clé> /r
```

Consultation des informations sur la licence active

Consultation de l'état de la licence

Les informations relatives à l'état de la licence ou de la clé active s'affichent dans le panneau des résultats de l'entrée **Kaspersky Security** de la console de Kaspersky Security. L'état de la licence ou de la clé peut prendre une des valeurs suivantes :

- **Vérification de l'état de la licence en cours** : Kaspersky Security analyse le fichier clé ajouté et le code d'activation appliqué, puis attend une réponse concernant l'état actuel de la licence.
- **Licence active : jusqu'au <date de fin de validité de la licence>** : Kaspersky Security est actif jusqu'à la date indiquée. L'état est mis en évidence en jaune dans les cas suivants :
  - Il reste 14 jours avant l'expiration de la licence et aucun fichier clé additionnel n'a été ajouté.
  - La clé ajoutée est inscrite sur la liste noire et va bientôt être bloquée.
- **L'application n'a pas été activée** : Kaspersky Security n'est pas actif car aucun fichier clé n'a été ajouté ou aucun code d'activation n'a été appliqué. L'état est mis en évidence en rouge.
- **Durée de validité de la licence écoulée**: Kaspersky Security n'est pas actif car la durée de validité de la licence est arrivée à échéance. L'état est mis en évidence en rouge.
- **Le Contrat de Licence Utilisateur Final a été violé** : Kaspersky Security n'est pas actif en raison d'une violation des conditions du Contrat de Licence Utilisateur Final (cf. section « A propos du Contrat de Licence Utilisateur Final » à la page 37). L'état est mis en évidence en rouge.
- **La clé es inscrite sur la liste noire** : le fichier clé ajouté a été bloqué et inscrit sur la liste noire par les experts de Kaspersky Lab, par exemple, en cas d'utilisation du fichier clé par des tiers pour l'activation illicite d'une application. L'état est mis en évidence en rouge.
- **L'abonnement est suspendu** : l'abonnement est temporairement suspendu, l'état est mis en évidence en rouge. Vous pouvez rétablir l'abonnement à tout moment.

Consultation des informations sur la licence

Vous pouvez consulter des informations générales et détaillées sur la licence active.

► *Pour consulter les informations générales ou détaillées sur la licence, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, sélectionnez l'entrée **Licence**.

   Les informations générales relatives à la licence active apparaissent dans le panneau des résultats du noeud **Licence** (cf. tableau ci-dessous).

2. Ouvrez le menu contextuel de la ligne contenant les informations relatives à la clé dont vous souhaitez consulter les informations.

3. Choisissez l'option **Propriétés**.

La fenêtre **Propriétés : <Numéro de la licence>** s'ouvre. L'onglet **Général** reprend les détails relatifs à la licence active, l'onglet **Avancé** contient les informations relatives au client et les coordonnées de Kaspersky Lab ou du partenaire chez qui vous avez acheté Kaspersky Security (cf. tableau ci-dessous).

*Tableau 4. Informations générales sur la licence dans l'entrée **Licence***

Champ	Description
Code d'activation	Numéro du code d'activation. Le champ se remplit si vous activez l'application à l'aide d'un code d'activation.
Etat de l'activation	Informations sur l'état de l'activation de l'application.
Clé	Numéro de la clé que vous avez utilisée pour activer l'application.
Type de licence	Type de licence : commerciale, abonnement.
Fin de validité de la licence	Date de fin de validité de la licence associée à la clé.
Etat du code d'activation ou de la clé	Etat du code d'activation ou de la clé : actif ou complémentaire.

*Tableau 5. Détails sur la licence dans la fenêtre **Propriétés <numéro de clé>***

Champ	Description
Onglet Général	
Clé	Numéro de la clé que vous avez utilisée pour activer l'application.
Date d'ajout de la clé	Date d'ajout de la clé dans l'application.
Type de licence	Type de licence : commerciale, abonnement.
Expire dans (jours)	Nombre de jours restants avant la date de fin de validité de la licence associée à la clé active.
Fin de validité de la licence	Date de fin de validité de la licence associée à une clé active. Si vous activez l'application selon un abonnement illimité, la valeur *Illimité* apparaît dans le champ. Si Kaspersky Security ne parvient pas à déterminer la date de fin de validité de la licence, la valeur *Inconnue* apparaît dans le champ.
Application	Nom de l'application pour laquelle une clé a été ajoutée.
Restrictions d'utilisation de la clé	Restriction prévue sur l'utilisation de la clé (le cas échéant).
Accès au Support Technique	Indique si la licence prévoit une assistance technique offerte par Kaspersky Lab ou par ses partenaires.
Onglet Avancé	
Informations relatives à la licence	Numéro et type de la licence active.
Informations relatives au support	Coordonnées de Kaspersky Lab ou du partenaire qui offre le Support Technique. Le champ peut être vide en l'absence de Support Technique.
Informations relatives au détenteur	Informations relatives à la personne qui a commandé la licence : nom du client ou de l'organisation pour laquelle une licence active a été achetée.

Les informations de la colonne **Etat de l'activation** dans le panneau d'administration du noeud **Licence** peuvent prendre une des valeurs suivantes :

- **Appliqué** : si vous avez activé l'application à l'aide d'un code d'activation ou d'une clé.
- **Activation** : si vous avez appliqué un code d'activation pour activer l'abonnement et que le processus est toujours en cours. L'état prend la valeur **Appliqué** à l'issue de l'activation de l'application et après l'actualisation du contenu du panneau des résultats de l'entrée.
- **Echec de l'activation** : apparaît en cas d'échec de l'activation de l'application. Vous pouvez voir la cause de l'échec de l'activation dans le journal d'exécution des tâches.

Renouvellement de la licence

Quand il reste 14 jours avant l'expiration de la licence, Kaspersky Security vous prévient : l'état **Licence : Date de fin de validité <date de fin de validité de la licence>** dans le panneau des résultats du noeud **Kaspersky Security** est mis en évidence en jaune.

Vous pouvez renouveler la licence avant son expiration. Ainsi, la protection du serveur ne sera pas interrompue entre la fin de la validité de la licence active et l'activation de l'application à l'aide d'une nouvelle licence.

► *Pour renouveler la licence, procédez comme suit :*

1. Achetez un nouveau code d'activation de l'application ou un nouveau fichier clé.
2. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Licence**.
3. Dans le panneau des résultats de l'entrée **Licence**, exécutez une des actions suivantes :

   Si vous souhaitez renouveler la licence à l'aide d'une clé additionnelle :

   a. Cliquez sur le lien **Ajouter une clé**.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**, puis sélectionnez le nouveau fichier clé portant l'extension key.

   Si vous souhaitez renouveler la licence à l'aide d'un code d'activation :

   c. Cliquez sur le lien **Ajouter un code d'activation**.

d. Dans la fenêtre qui s'ouvre, saisissez le code d'activation.

> L'application d'un code d'activation requiert une connexion à Internet.

4. Cochez la case **Utiliser en tant que clé complémentaire**.
5. Cliquez sur **OK**.

La clé additionnelle ou le code d'activation sera ajouté et il entrera automatiquement en vigueur à l'expiration de la licence de Kaspersky Security en cours d'utilisation.

Activation et renouvellement de l'abonnement

► *Pour utiliser Kaspersky Security selon un abonnement,*

appliquez à l'application le code d'activation fourni par le prestataire de service.

Quand le code d'activation a été saisi dans l'application, la clé active est installée. Celle-ci définit la licence d'utilisation de l'application selon un abonnement.

Vous ne pouvez pas renouveler l'abonnement à l'aide d'une clé additionnelle ou d'un autre code d'activation.

Renouvellement d'un abonnement limité

Pour prolonger l'action de Kaspersky Security à l'expiration d'un abonnement limité, il est nécessaire de renouveler ce dernier auprès du prestataire de service. Au cours de la période comprise entre l'expiration de l'abonnement et son renouvellement, l'application fonction avec certaines restrictions : toutes les tâches existantes sont exécutées, à l'exception des tâches de mise à jour ; vous ne pouvez pas non plus lancer de nouvelles tâches.

> Une fois que l'abonnement limité a expiré, Kaspersky Security cesse de fonctionner complètement après le redémarrage de l'application.

Si l'abonnement est limité, une période de grâce de renouvellement vous est proposée après sa date d'expiration. Pendant cette période, l'application continue à fonctionner. L'offre d'une période de grâce et, le cas échéant, sa durée, dépendent du fournisseur de services.

Renouvellement d'un abonnement illimité

L'abonnement illimité se renouvelle automatiquement si le montant dû au prestataire de service est versé dans les délais.

Si vous utilisez l'application sous un abonnement illimité, Kaspersky Security vérifie automatiquement en arrière-plan la présence éventuelle d'une clé mise à jour sur le serveur d'activation. Si l'application trouve une clé mise à jour sur le serveur d'activation, il l'ajoute et remplace la clé antérieure.

Suppression d'une clé

Vous pouvez supprimer une clé que vous avez ajoutée.

Si Kaspersky Security possède une clé additionnelle et que vous supprimez la clé active, la clé additionnelle deviendra automatiquement la clé active.

Si vous supprimez la clé qui avait été ajoutée, vous pourrez la restaurer uniquement après avoir appliqué à nouveau le fichier clé.

► *Pour supprimer la clé ajoutée, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, sélectionnez l'entrée **Licence**.
2. Dans le tableau contenant les informations relatives aux clés ajoutées qui figure dans le panneau des résultats de l'entrée **Licence**, sélectionnez la clé que vous souhaitez supprimer.
3. Dans le menu contextuel de la ligne contenant les informations sur la clé sélectionnée, choisissez l'option **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

La clé sélectionnée sera supprimée.

Interface de Kaspersky Security et accès aux fonctions de l'application

Cette section présente les principaux éléments de l'interface de l'application.

Dans cette section

Utilisation de la console de Kaspersky Security

Cette section aborde la console de Kaspersky Security et l'administration de Kaspersky Security via la console installée sur le serveur à protéger ou sur un autre ordinateur.

Dans cette section

Présentation de la console de Kaspersky Security

La console de Kaspersky Security est un composant logiciel enfichable isolé qui est ajouté à la console Microsoft Management Console.

Il est possible d'administrer Kaspersky Security via la console de Kaspersky Security installée sur le serveur protégé ou sur tout autre ordinateur du réseau de l'organisation. Une fois que la Console de Kaspersky Security a été installée sur un autre ordinateur, vous devez effectuer la configuration avancée (cf. section « Administration de Kaspersky Security via une Console sur un autre ordinateur » à la page 74).

Si la console de Kaspersky Security et Kaspersky Security sont installés sur différents ordinateurs appartenant à différents domaines, il se peut qu'il y ait des restrictions au niveau de la remise des informations de Kaspersky Security à la console de Kaspersky Security. Par exemple, après le démarrage d'une tâche quelconque de Kaspersky Security, il se peut que l'état de cette tâche ne soit pas actualisé dans la console.

Une fois l'installation de la console de Kaspersky Security terminée, le programme d'installation conserve le fichier kavfs.msc dans le répertoire d'installation et ajoute le composant logiciel enfichable à la liste des composants isolés de Microsoft Windows.

Vous pouvez ouvrir la console de Kaspersky Security depuis le menu **Démarrer.** Vous pouvez également ouvrir la Console de Kaspersky Security sur le serveur protégé à l'aide de l'icône de Kaspersky Security (cf. section « Icône de Kaspersky Security dans la zone de notification de la barre des tâches » à la page 75) dans la zone de notification de la barre des tâches.

Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Security ou ajouter ce composant logiciel enfichable à la console Microsoft Management Console existante en tant que nouvel élément de son arborescence (cf. section "Interface de la fenêtre de la Console de Kaspersky Security" à la page 54).

Sous la version 64 bits de Microsoft Windows, vous pouvez ajouter le composant logiciel enfichable de Kaspersky Security uniquement dans la console Microsoft Management Console de la version 32 bits (MMC32). Pour ce faire, tapez la commande mmc.exe/32 dans la ligne de commande pour ouvrir la Microsoft Management Console.

Dans une des copies de la console Microsoft Management Console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants enfichables Kaspersky Security afin de pouvoir administrer ainsi la protection de plusieurs serveurs sur lesquels Kaspersky Security est installé.

Interface de la fenêtre de la console de Kaspersky Security

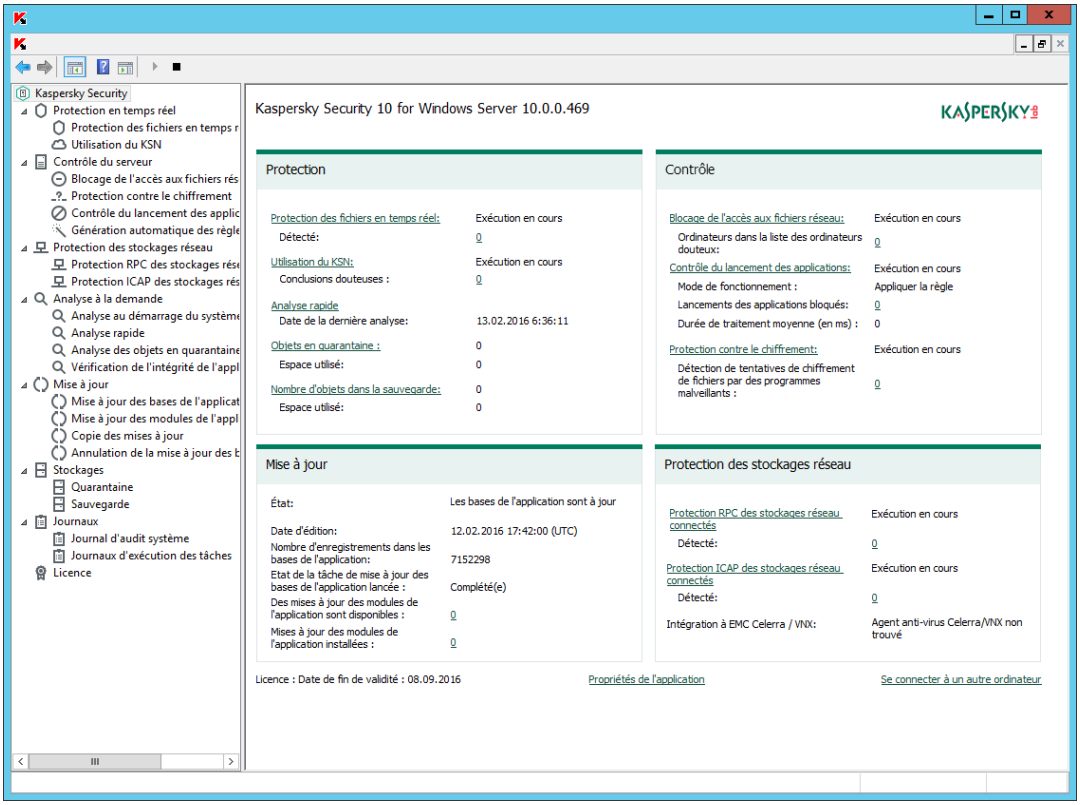
La console de Kaspersky Security s'affiche dans l'arborescence de Microsoft Management Console sous l'entrée **Kaspersky Security**.

Après la connexion à la copie de Kaspersky Security installée sur un autre ordinateur, le nom du noeud reprend le nom de l'ordinateur sur lequel Kaspersky Security est installé ainsi que le nom du compte utilisateur sous les privilèges duquel la connexion a été réalisée : **Kaspersky Security <Nom de l'ordinateur> sous <nom du compte utilisateur>**. En cas de connexion à une copie de Kaspersky Security installée sur le même ordinateur que la Console, le nom de l'entrée prend la forme : **Kaspersky Security**.

Par défaut, la fenêtre de la console de Kaspersky Security contient les éléments suivants :

- arborescence de la Console ;
- panneau des résultats ;
- Panneau de tâche ;
- Barre d'outils.

Vous pouvez également activer l'affichage de la zone de description et du panneau des actions dans la console de Kaspersky Security.



Arborescence de la Console

L'arborescence de la Console affiche l'entrée Kaspersky Security et ses sous-entrées correspondant aux modules opérationnels de l'application.

Dans le cas de **Kaspersky Security**, il s'agit des nœuds enfants suivants :

- **Protection en temps réel** : administration de la protection des fichiers en temps réel et de l'analyse des scripts, ainsi que des paramètres d'utilisation des services du KSN. Chaque zone fonctionnelle dispose de son propre élément d'administration :
  - **Protection des fichiers en temps réel**.
  - **Analyse des scripts**.
  - **Utilisation du KSN**.
- **Contrôle du serveur** : contrôle de l'accès aux fichiers réseau appliqué aux ordinateurs distants et contrôle du lancement des applications. Chaque zone fonctionnelle dispose de son propre élément d'administration :
  - **Blocage de l'accès aux fichiers réseau**.
  - **Protection contre le chiffrement**.
  - **Contrôle du lancement des applications**.
  - **Génération automatique des règles d'autorisation**.
  - Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).
- **Protection des stockages réseau** : gestion de la protection des stockages réseau.
  - **Protection des stockages réseau connectés via le protocole RPC**.
  - **Protection des stockages réseau connectés via le protocole ICAP**.

- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Une entrée séparée existe pour chacune des tâches prédéfinie :
  - **Analyse au démarrage du système d'exploitation**.
  - **Analyse rapide**.
  - **Analyse des objets en quarantaine**.
  - **Vérification de l'intégrité de l'application**.
  - Tâches définies par l’utilisateur **<Nom des tâches>** (le cas échéant).

  Une entrée séparée existe pour chaque tâche définie par l’utilisateur et pour chaque tâche de groupe créée pour l'analyse à la demande et transmise au serveur par la console d'administration de Kaspersky Security Center.
- **Mise à jour** : gère la mise à jour des bases et des modules de Kaspersky Security ainsi que la copie des mises à jour dans le dossier de la source locale de mises à jour. Le nœud contient des nœuds secondaires permettant d'administrer chacune des tâches prédéfinies de mise à jour ou d'annulation de la dernière mise à jour des bases de l'application :
  - **Mise à jour des bases de l'application**.
  - **Mise à jour des modules de l'application**.
  - **Copie des mises à jour**.
  - **Annulation de la mise à jour des bases de l'application**.

  Une entrée séparée existe pour chaque tâche créée et transmise au serveur par la console d'administration de Kaspersky Security Center.
- **Stockages** : administration des paramètres de la quarantaine et de la sauvegarde :
  - **Quarantaine** ;
  - **Sauvegarde**.

- **Journaux** : gestion des journaux relatifs à la protection en temps réel, à la protection des stockages réseau, à l'analyse à la demande, au contrôle du serveur et aux tâches de mise à jour ; gestion du journal d'audit système de Kaspersky Security. Une entrée séparée existe pour chaque type de journal :
  - **Journal d'audit système**.
  - **Journaux d'exécution des tâches**.
- **Licence** : ajout et suppression de clés et de codes d'activation pour Kaspersky Security, consultation des informations relatives aux licences.

Panneau de résultats

Le panneau des résultats reprend les informations relatives au nœud sélectionné. Si vous avez choisi l'entrée **Kaspersky Security**, le panneau des résultats affichera des informations sur l'état actuel de la protection du serveur, sur Kaspersky Security, sur l'état de ses modules opérationnels ainsi que sur l'état de la licence ou de la clé.

Menu contextuel de l'entrée Kaspersky Security

A l'aide des options du menu contextuel de l'entrée **Kaspersky Security**, vous pouvez exécuter les opérations suivantes :

- **Se connecter à un autre ordinateur**. Se connecter à un autre serveur pour administrer la copie de Kaspersky Security installée sur ce serveur. Pour effectuer cette opération, vous pouvez également utiliser le lien situé dans le coin inférieur droit du panneau des résultats de l'entrée **Kaspersky Security**.
- **Lancer Kaspersky Security** / **Arrêter Kaspersky Security** (**Démarrer** / **Arrêter**). Lancer ou arrêter Kaspersky Security ou la tâche sélectionnée (cf. section Lancement / suspension / rétablissement / arrêt manuel d'une tâche" à la page 109). Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. L'exécution de ces opérations est également disponible dans les menus contextuels des tâches de l'application.
- **Configurer les paramètres de la zone de confiance**. Consulter et configurer les paramètres de la zone de confiance (cf. section « A propos de la zone de confiance de Kaspersky Security » à la page 97).

- **Modifier les permissions utilisateur pour l'administration de l'application**. Consulter et configurer les privilèges d'accès aux fonctions de Kaspersky Security (cf. section "A propos des autorisations d'administration de Kaspersky Security" à la page 86).

- **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service**. Consulter et configurer les autorisations d'accès à l'administration du service Kaspersky Security (cf. section "A propos des autorisations d'administration du service Kaspersky Security » à la page 89).

- **Configurer les paramètres des notifications**. Consulter et configurer les paramètres des notifications de l'administrateur et des utilisateurs de Kaspersky Security (cf. section "Configuration des notifications de l'administrateur et des utilisateurs" à la page 320).

- **Stockage hiérarchique**. Consulter et configurer les paramètres de fonctionnement du stockage hiérarchique de Kaspersky Security. (cf. section « A propos du stockage hiérarchique » à la page 324)

- **Exporter les paramètres**. Enregistrer les paramètres de l'application dans un fichier de configuration au format XML (cf. section « Exportation des paramètres » à la page 118). L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

- **Importer les paramètres**. Importer les paramètres de l'application depuis le fichier de configuration au format XML (cf. section « Importation des paramètres » à la page 119). L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

- **A propos du logiciel**. Accéder à la consultation des informations sur Kaspersky Security.

- **Nouvelle fenêtre**. Ouvrir une nouvelle fenêtre dans la Console de Kaspersky Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

- **Mettre à jour**. Actualiser le contenu de la fenêtre de la Console de Kaspersky Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

- **Propriétés**. Consulter et configurer les paramètres de fonctionnement de Kaspersky Security ou d'une tâche sélectionnée. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

  > Pour exécuter cette opération, vous pouvez également utiliser le lien **Propriétés de l'application** dans le panneau des résultats de l'entrée **Kaspersky Security** ou le bouton dans la barre d'outils.

- **Aide**. Accéder à la consultation de l'aide de Kaspersky Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Volet d'accès rapide et menu contextuel des tâches de Kaspersky Security

Vous pouvez administrer les tâches de Kaspersky Security à l'aide des options du menu contextuel de chaque tâche dans l'arborescence de la Console, ou à l'aide du volet d'accès rapide situé à droite du panneau des résultats de la tâche sélectionnée.

À l'aide des liens du volet d'accès rapide et des options du menu contextuel de la tâche sélectionnée, vous pouvez effectuer les actions suivantes :

- **Reprendre / Suspendre**. Rétablir ou suspendre l'exécution d'une tâche (cf. section "Lancement / suspension / rétablissement / arrêt manuel d'une tâche" à la page 109). Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches de protection des fichiers en temps réel et d'analyse à la demande.

- **Ajouter tâche**. Créer une tâche personnalisée (cf. section "Création d'une tâche d'analyse à la demande" à la page 251). L'opération est disponible pour les tâches d'analyse à la demande.

- **Ouvrir le journal d'exécution**. Accéder à la consultation et à l'utilisation du journal d'exécution de la tâche. (cf. section « A propos des journaux d'exécution des tâches » à la page 307) L'opération est disponible pour toutes les tâches.

- **Enregistrer la tâche**. Enregistrer et appliquer les modifications apportées aux paramètres de la tâche (cf. section « Enregistrement de la tâche après modification de ses paramètres » à la page 109). Cette action est disponible pour les tâches de protection des fichiers en temps réel, de protection des stockages réseau connectés via le protocole RPC et d'analyse à la demande.

- **Supprimer la tâche**. Supprimer une tâche prédéfinie (cf. section "Suppression d'une tâche" à la page 255). L'opération est disponible pour les tâches d'analyse à la demande.
- **Statistiques**. Accéder à la consultation des statistiques de la tâche. L'opération est disponible pour la tâche de vérification de l'intégrité de l'application.
- **Modèles des paramètres**. Accéder à l'utilisation des modèles. Cette action est disponible pour les tâches de protection des fichiers en temps réel, de protection des stockages réseau connectés via le protocole RPC et d'analyse à la demande.

Lancement de la console de Kaspersky Security depuis le menu Démarrer

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Assurez-vous que la console de Kaspersky Security est installée sur l'ordinateur.

► *Pour lancer la console de Kaspersky Security depuis le menu "Démarrer", procédez comme suit :*

Dans le menu **Démarrer**, choisissez **Programmes→ Kaspersky Security 10 for Windows Server → Outils d'administration → Console de Kaspersky Security**.

Si vous avez l'intention d'ajouter d'autres composants logiciels enfichables à la Console de Kaspersky Security, lancez la Console en mode auteur.

► *Pour lancer la Console de Kaspersky Security en mode auteur, procédez comme suit :*

1. Dans le menu **Démarrer,** sélectionnez **Programmes → Kaspersky Security 10 for Windows Server → Outils d'administration**.
2. Dans le menu contextuel de l'application **Console de Kaspersky Security**, choisissez la commande **Auteur**.

La Console de Kaspersky Security sera lancée en mode auteur.

Si vous avez lancé la console de Kaspersky Security sur le serveur à protéger, la fenêtre de la console s'ouvre (cf. section "Interface de la fenêtre de la console de Kaspersky Security" à la page 54).

Si vous aviez lancé la Console de Kaspersky Security non pas sur le serveur à protéger, mais sur un autre ordinateur, connectez-vous au serveur à protéger.

► *Pour vous connecter au serveur à protéger, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Sélectionnez la commande **Se connecter à un autre ordinateur**.

   La fenêtre **Sélection d'ordinateur** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez **Autre ordinateur**.
4. Dans le champ de saisie de droite, indiquez le nom réseau du serveur à protéger.
5. Cliquez sur **OK**.

La Console de Kaspersky Security sera connectée au serveur à protéger.

Si le compte que vous avez utilisé pour ouvrir une session dans Microsoft Windows ne possède pas les autorisations d'accès au service d'administration de Kaspersky Security sur le serveur, cochez la case **Se connecter sous le compte utilisateur** et désignez un autre compte disposant de ces privilèges (cf. section "A propos des autorisations d'accès au service Kaspersky Security Manager" à la page 92).

Paramètres de fonctionnement de Kaspersky Security dans la Console

Les paramètres généraux et les paramètres du diagnostic des pannes de Kaspersky Security définissent les conditions générales de fonctionnement de l'application. Ils déterminent le nombre de processus utilisés par Kaspersky Security, ils permettent d'activer la reprise des tâches de Kaspersky Security après un arrêt inopiné de leur fonctionnement, de tenir un journal de traçage, d'activer la création d'un fichier dump des processus de Kaspersky Security lorsqu'ils sont arrêtés en raison d'une erreur et de configurer d'autres paramètres généraux.

Dans cette section

Configuration des paramètres de fonctionnement de Kaspersky Security dans la Console

► *Pour configurer les paramètres de fonctionnement de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, sélectionnez l'entrée **Kaspersky Security** et réalisez l'une des actions suivantes :

   - Dans le panneau des résultats de l'entrée, suivez le lien **Propriétés de l'application**.
   - Dans le menu contextuel de l'entrée, sélectionnez l'option **Propriétés**.

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

2. Dans la fenêtre qui s'ouvre, configurez les paramètres de fonctionnement de Kaspersky Security en fonction de vos exigences :

   - L'onglet **Général** permet de configurer les paramètres suivants :

     Dans le groupe **Paramètres d'optimisation** :

     - nombre maximum de processus de travail actifs que Kaspersky Security peut lancer ;

Tableau 6. Quantité maximale de processus actifs

Paramètre	Quantité maximale de processus actifs.
Description	Ce paramètre appartient au groupe **Paramètres d'optimisation** de Kaspersky Security. Il définit le nombre maximum de processus de travail qui peuvent être exécutés simultanément par Kaspersky Security. L'augmentation du nombre de processus de travail exécutés en parallèle accélère la vitesse d'analyse des fichiers et la résistance de Kaspersky Security aux échecs. Toutefois, si cette valeur est trop élevée, les performances globales du serveur peuvent chuter et la mémoire vive requise peut augmenter. N'oubliez pas que la console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre **Quantité maximale de processus actifs** uniquement pour Kaspersky Security sur un serveur séparé (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.

<table>
<tr><td>Valeurs possibles</td><td>1 – 8</td></tr>
<tr><td>Valeur par défaut</td><td>Kaspersky Security réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :
<table>
<tr><th>Nombre de processeurs</th><th>Quantité maximale de processus actifs</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1< nbre de processeurs < 4</td><td>2</td></tr>
<tr><td>4 et plus</td><td>4</td></tr>
</table></td></tr>
</table>

- définition du nombre de processus pour les tâches de protection en temps réel ;

Tableau 7. Nombre de processus de protection en temps réel

Paramètre	Nombre de processus pour la protection en temps réel.
Description	Ce paramètre appartient au groupe **Paramètres d'optimisation** de Kaspersky Security. Grâce à ce paramètre, vous pouvez définir un nombre fixe de processus qui serviront à Kaspersky Security pour l'exécution de la protection en temps réel. La valeur plus élevée de ce paramètre accélère l'analyse des objets dans les tâches liées à la protection en temps réel. Toutefois, plus le nombre de processus de travail affectés à Kaspersky Security est élevé, plus grand sera l'impact sur les performances globales du serveur protégé et sur son utilisation de la mémoire vive. N'oubliez pas que la console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre **Nombre de processus de protection en temps réel** uniquement pour Kaspersky Security sur un serveur distinct (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.

<table>
<tr><td>Valeurs possibles</td><td>Valeurs possibles: 1-N, où N est la valeur définie par le paramètre Quantité maximale de processus actifs.

Si vous attribuez au paramètre Nombre de processus de protection en temps réel une valeur égale au nombre maximum de processus actifs, vous diminuez l’impact de Kaspersky Security sur la vitesse de l’échange de fichiers entre les postes de travail et le serveur, tout en augmentant sa vitesse de réaction pendant la protection en temps réel. Toutefois, les tâches de mise à jour et les tâches d’analyse à la demande avec la priorité de base Moyenne (Normal) seront exécutées dans les processus de Kaspersky Security déjà lancés. Les tâches d’analyse à la demande seront exécutées plus lentement. Si l’exécution de la tâche entraîne un échec, son redémarrage prendra plus de temps.

Les tâches d’analyse à la demande avec la priorité de base Bas (Low) seront toujours exécutées dans un processus ou dans des processus séparés.</td></tr>
<tr><td>Valeur par défaut</td><td>Kaspersky Security réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :

<table><tr><th>Nombre de processeurs</th><th>Nombre de processus pour la protection en temps réel</th></tr><tr><td>=1</td><td>1</td></tr><tr><td>>1</td><td>2</td></tr></table></td></tr>
</table>

- nombre de processus de travail pour les tâches d'analyse à la demande en arrière-plan ;

Tableau 8. Nombre de processus pour les tâches d'analyse à la demande en arrière-plan

Paramètre	Nombre de processus pour les tâches d'analyse à la demande en arrière-plan.
Description	Ce paramètre appartient au groupe **Paramètres d'optimisation** de Kaspersky Security. Grâce à ce paramètre, vous pouvez définir le nombre maximum de processus que Kaspersky Security utilisera pour l'exécution de l'analyse à la demande en arrière-plan. Le nombre de processus que vous définissez à l'aide de ce paramètre ne fait pas partie du total des processus de travail de Kaspersky Security défini à l'aide du paramètre **Quantité maximale de processus actifs**. Par exemple, si vous spécifiez les valeurs des paramètres comme ci-dessous : • Nombre maximum de processus actifs – 3 ; • Nombre de processus pour les tâches de protection en temps réel – 3 ; • Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan – 1 ; et puis que vous lancez la tâche de protection en temps réel et une tâche d'analyse à la demande en arrière-plan, le nombre total de processus de travail de kavfswp.exe de Kaspersky Security est de 4. Un processus de travail de faible priorité peut exécuter plusieurs tâches d'analyse à la demande. Vous pouvez augmenter le nombre de processus de travail, par exemple si vous lancez simultanément plusieurs tâches en arrière-plan, afin d'attribuer des processus distincts à chaque tâche. L'attribution de processus distincts aux tâches augmente la fiabilité de l'exécution de ces tâches ainsi que la vitesse.
Valeurs possibles	1-4
Valeur par défaut	1

Dans le groupe **Paramètres de restauration du logiciel** :

- nombre de tentatives de restauration des tâches d'analyse à la demande en cas d'échec suite à une erreur.

Tableau 9. Récupération automatique

Paramètre	Restauration des tâches (**Réaliser la restauration des tâches**).
Description	Ce paramètre appartient au groupe **Paramètres de restauration du logiciel** de Kaspersky Security. Il active la restauration des tâches lorsque celles-ci se solde par une erreur et définit le nombre de tentatives de restauration des tâches d'analyse à la demande. Lorsqu'une tâche se solde par un échec, le processus kavfs.exe de Kaspersky Security tente de relancer le processus dans lequel cette tâche était exécutée au moment de l'arrêt. Si la restauration des tâches est désactivée, Kaspersky Security ne restaure pas les tâches d'analyse à la demande et de protection en temps réel. Si la restauration des tâches est activée, Kaspersky Security tente de restaurer les tâches de protection en temps réel jusqu'à la réussite de l'opération et tente de restaurer les tâches d'analyse à la demande autant de fois que le précise le paramètre.
Valeurs possibles	Activée / désactivée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 1-10.
Valeur par défaut	La restauration des tâches est activée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 2

- L'onglet **Avancé** permet de configurer les paramètres suivants :

  Dans le groupe **Interaction avec l'utilisateur** :

  - affichage de l'icône de Kaspersky Security dans la zone de notification de la barre des tâches (cf. section "Icône de Kaspersky Security dans la zone de notification de la barre des tâches" à la page 75) à chaque lancement de l'application ;

  Dans le groupe **Actions lors du passage à une source d'alimentation sans interruption** :

  - actions de Kaspersky Security en cas d'alimentation via la source d'alimentation de secours ;

Tableau 10. Utilisation de la source d'alimentation de secours

Paramètre	Actions à exécuter en cas d'alimentation via la batterie
Description	Ce paramètre définit les actions exécutées par Kaspersky Security lorsque le serveur fonctionne sur l'alimentation électrique de secours.
Valeurs possibles	Lancer ou pas les tâches d'analyse à la demande qui ont été programmées ; Exécuter ou arrêter toutes les tâches d'analyse à la demande lancées.
Valeur par défaut	Par défaut, lorsque le serveur utilise une source d'alimentation de secours, Kaspersky Security fonctionne selon le mode suivant : • N'exécute pas les tâches d'analyse à la demande qui ont été programmées ; • Arrête automatiquement toutes les tâches d'analyse à la demande lancées.

  Dans le groupe **Seuil de déclenchement des événements** :

  - nombre de jours à l'issue desquels les événements *Les bases de l'application sont dépassées*, *Les bases de l'application sont fortement dépassées* et *L'analyse des zones critiques de l'ordinateur n'a pas été réalisée depuis longtemps* seront déclenchés.

Tableau 11. Actions dans le fonctionnement sur la source d'alimentation de secours

Paramètre	Seuils de déclenchement des événements.
Description	Vous pouvez définir le seuil de déclenchement des événements des trois types suivants : • *Les bases de l'application sont dépassées* et *Les bases de l'application sont fortement dépassées*. Cet événement se déclenche lorsque les bases de Kaspersky Security n'ont pas été actualisées durant une période (nombre de jours) définie depuis la création des dernières mises à jour des bases de données. Vous pouvez configurer la notification de l'administrateur lorsque ces événements surviennent. • *L'analyse rapide de l'ordinateur n'a pas été réalisée depuis longtemps*. L'événement se produit si aucune des tâches accompagnées de la case **Considérer l'exécution de la tâche comme une analyse rapide** (cf. section "**Attribution de l'état "Tâche d'analyse des zones critiques" à la tâche d'analyse**' à la page 435) n'est exécutée pendant le nombre de jours indiqué.
Valeurs possibles	Nombre de jours compris entre 1 et 365
Valeur par défaut	Les bases de l'application sont dépassées – 7 jours ; Les bases de l'application sont fortement dépassées – 14 jours ; L'analyse des zones critiques n'a pas été réalisée depuis longtemps – 30 jours.

Dans le groupe **Licence** :

- utilisation de Kaspersky Security Center en guise de serveur proxy pour l'activation de l'application.

- Sous l'onglet **Paramètres de connexion** :

  Dans le groupe **Paramètres du serveur proxy** :

  - activation et désactivation de l'utilisation du serveur proxy ;
  - définition automatique des paramètres du serveur proxy ;

- utilisation des paramètres du serveur proxy indiqués ;
- utilisation du serveur proxy pour les adresses locales.

Dans le groupe **Paramètres d'authentification du serveur proxy** :

- type d'authentification sur le serveur proxy et données nécessaires à celle-ci.

- Sur l'onglet **Diagnostic des échecs** :
  - Si vous souhaitez enregistrer les informations de débogage dans un fichier, cochez la case **Consigner les informations de débogage dans le fichier de traçage**.
    - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security enregistrera les fichiers de trace.
    - Configurez le niveau de détail des informations de débogage.

    La liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Security consigne dans le fichier de trace.

    Vous avez le choix parmi les niveaux de détail suivants :

    - **Evénements critiques** : Kaspersky Security enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.
    - **Erreurs** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
    - **Evénements importants** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.
    - **Evénements d'information** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs, aux événements importants et aux événements d'information.
    - **Toutes les informations de débogage** : Kaspersky Security enregistre dans le fichier de trace toutes les informations de débogage.

    Le niveau de détail à définir pour résoudre le problème qui se pose est déterminé par l'expert du Support Technique.

    Le niveau de détail sélectionné par défaut est **Toutes les informations de débogage**.

La liste déroulante est accessible si la case **Consigner les informations de débogage dans le fichier de traçage** est cochée.

- Taille maximale du fichier de trace
- Indiquez les modules à déboguer.

Liste des codes de sous-systèmes de Kaspersky Security dont les informations de débogage sont enregistrées dans le fichier de trace. Les codes des sous-systèmes doivent être séparés par une virgule et en respectant la distinction entre majuscules et minuscules (cf. tableau ci-dessous).

Tableau 12. Codes des sous-systèmes de Kaspersky Security

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Security dans MMC
ak_conn	Sous-système d'intégration à l'agent d'administration de Kaspersky Security Center
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Security.
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance de Kaspersky Security.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de protection des fichiers en temps réel.
netapp	Sous-système de protection des stockages réseau.
qb	Sous-système de la quarantaine et des sauvegardés.
scandll	Module auxiliaire d'analyse antivirus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.

Code de sous-système	Nom du sous-système
prague	Sous-système des fonctions de base.
scsrv	Sous-système d'affichage de messages sur les interceptions de scripts.
script	Intercepteur de scripts.
updater	Sous-système de mise à jour des bases et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant logiciel enfichable de Kaspersky Security (gui) et du plug-in d'administration de Kaspersky Security pour Kaspersky Security Center (ak_conn) sont appliqués après le redémarrage de ces composants. Les paramètres de traçage des sous-systèmes de prise en charge du protocole SNMP (snmp) sont appliqués après le redémarrage du service SNMP. Les paramètres de traçage du sous-système des compteurs de performances (perfcount) sont appliqués après le redémarrage de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Security sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Kaspersky Security enregistre par défaut les informations de débogage du fonctionnement de tous les sous-systèmes de Kaspersky Security (recommandé).

Le champ est accessible si la case **Consigner les informations de débogage dans le fichier de traçage** est cochée

- Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump sur incident**.
    - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security enregistrera le fichier dump.

Kaspersky Security consigne les informations dans les fichiers de trace et le fichier dump de mémoire en clair.

3. Cliquez sur **OK**.

Les paramètres de fonctionnement de Kaspersky Security seront enregistrés.

Autorisation des connexions réseau pour la console de Kaspersky Security

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

La console de Kaspersky Security sur l'ordinateur distant utilise le protocole DCOM pour obtenir les informations sur les événements de Kaspersky Security (objets analysés, tâches terminées, etc.) fournies par le service d'administration de Kaspersky Security sur le serveur à protéger. Il faut autoriser les connexions réseau dans le pare-feu Windows pour la console de Kaspersky Security afin d'établir une connexion entre la console et le service d'administration de Kaspersky Security.

Exécutez les actions suivantes :

- assurez-vous que l'accès à distance anonyme aux applications COM est autorisé (mais pas le lancement à distance et l'activation des applications COM) ;
- dans le pare-feu Windows, ouvrez le port TCP 135 et autorisez les connexions de réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Security kavfsrcn.exe.

  L'ordinateur sur lequel la console de Kaspersky Security est installée utilise le port TCP 135 pour échanger les informations avec le serveur protégé.

Si la console de Kaspersky Security était ouverte lorsque vous avez configuré la connexion entre le serveur à protéger et l'ordinateur sur lequel la console de Kaspersky Security est installée, il faudra fermer la console, attendre la fin du processus d'administration à distance de Kaspersky Security kavfsrcn.exe et lancer à nouveau la console. Les nouvelles valeurs des paramètres de connexion seront appliquées.

► *Pour autoriser l'accès à distance anonyme aux applications COM, procédez comme suit :*

1. Sur l'ordinateur accueillant la Console de Kaspersky Security, ouvrez la console du Service des composants : sélectionnez **Démarrer** → **Exécuter**, saisissez la commande dcomcnfg, puis cliquez sur **OK**.

2. Dans la console Services des composants de l'ordinateur, déployez le nœud **Ordinateurs**, ouvrez le menu contextuel du nœud **Poste de travail** et sélectionnez **Propriétés**.

3. Dans l'onglet **Sécurité COM** de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les restrictions** du groupe de paramètres **Privilèges d'accès**.

4. Dans la fenêtre **Autorisation d'accès**, vérifiez que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur ANONYMOUS LOGON.

5. Cliquez sur **OK**.

L'accès anonyme à distance aux applications COM sera autorisé.

► *Pour ouvrir le port TCP 135 du pare-feu Windows et autoriser les connexions de réseau pour le fichier exécutable du processus d'administration à distance de Kaspersky Security, procédez comme suit :*

1. Sur l'ordinateur distant, fermez la console de Kaspersky Security.

2. Exécutez une des actions suivantes :

   - Dans Microsoft Windows XP ou Microsoft Windows Vista :

     a. Dans Microsoft Windows XP Service Pack 2 ou supérieur, sélectionnez **Démarrer → Pare-feu Windows**.

     Dans Microsoft Windows Vista sélectionnez l'option **Démarrer → Panneau de configuration → Pare-feu Windows**.

     b. Dans la fenêtre **Pare-feu Windows**, cliquez sur **Modifier les paramètres**.

     c. Sur l'onglet **Exclusions** de la fenêtre **Pare-feu Windows** (**Paramètres du pare-feu Windows**), cliquez sur le bouton **Ajouter port**.

     d. Dans le champ **Nom**, indiquez le nom du port RPC (TCP/135) ou définissez un autre nom, par exemple DCOM Kaspersky Security.

     e. Dans le champ **Numéro de port**, indiquez le numéro du port : 135.

     f. Sélectionnez le protocole **TCP**.

     g. Cliquez sur **OK**.

     h. Sur l'onglet **Exclusions**, cliquez sur le bouton **Ajouter programme**.

- Dans Microsoft Windows 7 :

    a. Choisissez l'option **Démarrer → Panneau de configuration → Pare-feu Windows**.

    b. Dans la fenêtre **Pare-feu Windows** sélectionnez **Autoriser le lancement de l'application ou du module via le Pare-feu Windows**.

    c. Dans la fenêtre **Autoriser un programme via le Pare-feu Windows**, cliquez sur le bouton **Autoriser un autre programme**.

3. Dans la fenêtre **Ajout de programme**, désignez le fichier kavfsrcn.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de la console de Kaspersky Security.
4. Cliquez sur **OK**.
5. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu Windows** (**Paramètres du pare-feu Windows**).

Administration de Kaspersky Security via une Console sur un autre ordinateur

Il est possible d'administrer Kaspersky Security depuis une Console installée sur un ordinateur distant.

Pour administrer l'application via la console de Kaspersky Security sur un ordinateur distant, confirmez que :

- Les utilisateurs de la console de Kaspersky Security sur l'ordinateur distant sont ajoutés au groupe KAVWSEE Administrators sur le serveur à protéger.
- Les connexions réseau sont autorisées pour le processus du service Kaspersky Security Management kavfsgt.exe, si le Pare-feu Windows est activé sur le serveur à protéger (cf. section "Autorisation des connexions réseau pour le service Kaspersky Security Management" à la page 95).

    Le pare-feu Windows est activé par défaut dans toutes les versions du système d'exploitation Windows pour serveur à partir de Windows Server 2008.

- La case **Autoriser l'accès à distance** a été cochée dans la fenêtre de l'Assistant d'installation lors de l'installation de Kaspersky Security.

Icône de Kaspersky Security dans la zone de notification de la barre des tâches

Chaque fois que Kaspersky Security se lance automatiquement après le redémarrage du serveur, l'icône de Kaspersky Security apparaît dans la zone de notification de la barre des tâches. L'icône est affichée par défaut si vous avez installé le composant **Icône de Kaspersky Security** lors de l'installation de l'application.

L'apparence de l'icône de Kaspersky Security indique l'état actuel de la protection du serveur. L'icône de Kaspersky Security peut avoir un des états suivants :

- actif (en couleurs) si au moins une des tâches suivantes est actuellement en cours d'exécution : Protection des fichiers en temps réel, Analyse des scripts ou Contrôle du lancement des applications ;
- inactif (en noir et blanc) si aucune des tâches suivantes n'est actuellement en cours d'exécution : Protection des fichiers en temps réel, Analyse des scripts ou Contrôle du lancement des applications.

Le menu contextuel de l'icône de Kaspersky Security s'ouvre d'un clic droit de la souris.

Le menu contextuel contient plusieurs commandes d'affichage de fenêtre de l'application (cf. tableau ci-après).

Tableau 13. Commandes du menu contextuel de l'icône de Kaspersky Security

Instruction	Description
Ouvrir la console de Kaspersky Security	Ouvre la console de Kaspersky Security (si celle-ci est installée).
À propos du logiciel	Ouvre la fenêtre **À propos du logiciel** qui contient des informations sur Kaspersky Security. Si vous êtes un utilisateur enregistré de Kaspersky Security, alors la fenêtre **À propos du logiciel** contient des informations sur les mises à jour urgentes installées.
Fermer	Masque l'icône de Kaspersky Security dans la zone de notification de la barre des tâches.

Vous pouvez à tout moment restaurer l'icône de Kaspersky Security masquée.

► *Pour afficher à nouveau l'icône de l'application,*

dans le menu **Démarrer** de Microsoft Windows, sélectionnez **Programmes** → **Kaspersky Security 10 for Windows Server** → **Icône de Kaspersky Security**.

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Lors de la configuration des paramètres généraux de Kaspersky Security, vous pouvez activer ou désactiver l'affichage de l'icône de Kaspersky Security lors du lancement automatique de l'application après le redémarrage du serveur.

Lancement et arrêt du service Kaspersky Security

Le service Kaspersky Security est lancé automatiquement par défaut au démarrage du système d'exploitation. Le service Kaspersky Security gère les processus de travail chargés de la protection en temps réel, du contrôle du serveur, de la protection des stockages réseau, de l'analyse à la demande et de la mise à jour.

Le lancement du service Kaspersky Security marque par défaut le lancement des tâches Protection des fichiers en temps réel, Analyse des scripts (si ce module est installé), Analyse au démarrage du système d'exploitation, Vérification de l'intégrité de l'application ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Si vous arrêtez le service Kaspersky Security, l'ensemble des tâches en cours d'exécution sera interrompu. Après que vous avez lancé à nouveau le service Kaspersky Security, l'application lance automatiquement uniquement les tâches dont la planification reprend la fréquence **Au lancement de l'application**, les autres tâches sont lancées manuellement.

Vous pouvez lancer et arrêter le service Kaspersky Security à l'aide du menu contextuel de l'entrée **Kaspersky Security** ou via le composant logiciel enfichable **Services** de Microsoft Windows.

Vous pouvez lancer et arrêter Kaspersky Security uniquement si vous faites partie du groupe d'administrateurs sur le serveur protégé.

► *Pour arrêter ou lancer Kaspersky Security via la console de gestion, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.

2. Choisissez une des commandes suivantes :

   - **Arrêter Kaspersky Security** pour arrêter le service Kaspersky Security ;
   - **Lancer Kaspersky Security** pour lancer le service Kaspersky Security.

Le service Kaspersky Security sera lancé ou arrêté.

Consultation de l'état de la protection et des informations sur Kaspersky Security

► *Afin de consulter les informations relatives à l'état de la protection du serveur, des stockages réseau et les informations sur Kaspersky Security,*

ouvrez le nœud **Kaspersky Security** dans l'arborescence de la Console.

Par défaut, les informations du panneau des résultats de la Console de Kaspersky Security sont automatiquement actualisées :

- toutes les 10 secondes en cas de connexion locale ;
- toutes les 15 secondes en cas de connexion distante.

Vous pouvez actualiser les informations manuellement.

► *Pour actualiser manuellement les informations du nœud Kaspersky Security,*
choisissez l'option **Mettre à jour** dans le menu contextuel du nœud **Kaspersky Security**.

Le panneau des résultats de la console de Kaspersky Security affiche les informations suivantes sur l'application :

- état de la protection du serveur ;
- état de la protection des stockages réseau ;
- données sur la mise à jour des bases et des modules de l'application ;

- données relatives à la licence ;
- état de l'intégration à Kaspersky Security Center : données du serveur doté de Kaspersky Security Center auquel l'application est connectée ; données sur le contrôle des tâches de l'application par la stratégie active.

Les couleurs suivantes sont utilisées pour désigner l'état de la protection :

- *Vert*. La tâche est exécutée conformément aux paramètres définis. La protection est garantie.
- *Jaune*. La tâche n'a pas été lancée, a été suspendue ou est arrêtée. Des menaces pour la sécurité peuvent apparaître. Il est conseillé de lancer la tâche.
- *Rouge*. La tâche s'est soldée sur une erreur ou une menace pour la sécurité a été détectée pendant l'exécution de la tâche. Il est conseillé de lancer la tâche ou d'adopter les mesures d'élimination de la menace détectée.

Une partie des informations du groupe (par exemple, les noms des tâches ou le nombre de menaces détectées) se présente sous la forme de liens qui permettent d'accéder à l'entrée de la tâche correspondante ou d'ouvrir le journal de son exécution.

Tableau 14. Informations sur l'état de la protection du serveur

Groupe Protection	Conseil
Indicateur d'état de la protection du serveur	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que les tâches de protection en temps réel sont en cours d'exécution et que la tâche d'analyse rapide a été exécutée il y a moins de 30 jours (par défaut). • Volet de couleur jaune : une ou plusieurs tâches de protection en temps réel ne sont pas en cours d'exécution ou ont été arrêtées et la tâche d'analyse rapide n'a pas été exécutée depuis longtemps. • Volet de couleur rouge : la tâche de protection des fichiers en temps réel n'a pas pu être exécutée.

Groupe Protection	Conseil
Protection des fichiers en temps réel	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Détecté** : nombre d'objets détectés par Kaspersky Security. Par exemple, si Kaspersky Security a découvert un programme malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité. Si le nombre de programmes malveillants détectés dépasse 0, la valeur est mise en évidence en rouge.
Analyse des scripts	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Scripts dangereux** : nombre de scripts dangereux découverts par Kaspersky Security depuis le lancement de la tâche. Si le nombre de scripts dangereux détectés dépasse 0, la valeur est mise en évidence en rouge.
Utilisation du KSN	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Conclusions douteuses** : nombre d'objets identifiés comme douteux par les services du KSN. Par exemple, si au cours de l'analyse de cinq fichiers, le service du KSN renvoie un résultat établissant le caractère malveillant de l'un d'entre eux, la valeur de ce champ augmentera d'une unité. Si le nombre de conclusions douteuses dépasse 0, la valeur de la ligne est mise en évidence en rouge.
Analyse rapide	*N'a pas été réalisée :* événement qui survient quand la tâche d'analyse des zones critiques a été effectuée il y a 30 jours ou plus (par défaut). Vous pouvez modifier le seuil de déclenchement de l'événement. **Date de la dernière analyse** : date et heure de la dernière recherche de virus et autres menaces informatiques dans les zones critiques de l'ordinateur.

Groupe Protection	Conseil
Quarantaine	*Dépassement du seuil d'espace disponible dans la quarantaine* : événement qui se produit si le seuil d'espace disponible dans la quarantaine atteint la valeur indiquée. Kaspersky Security continue malgré tout à placer les objets en quarantaine. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en jaune. *Dépassement de la taille maximum de la quarantaine* : événement qui se produit si la taille de la quarantaine atteint la valeur indiquée. Kaspersky Security continue malgré tout à placer les objets en quarantaine. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en rouge. **Objets en quarantaine** : nombre d'objets qui se trouvent actuellement en quarantaine. **Espace utilisé** : volume occupé dans la quarantaine.
Sauvegarde	*Dépassement du seuil d'espace disponible dans la sauvegarde* : événement qui se produit si le seuil d'espace disponible dans la sauvegarde atteint la valeur indiquée. Kaspersky Security continue malgré tout à placer les objets en sauvegarde. Dans ce cas, la valeur du champ **Espace utilisé** est mis en évidence en jaune. *Dépassement de la taille maximum de la sauvegarde* : événement qui se produit si la taille de la sauvegarde atteint la valeur indiquée. Kaspersky Security continue malgré tout à placer les objets en sauvegarde. Dans ce cas, la valeur du champ **Espace utilisé** est mis en évidence en rouge. **Nombre d'objets dans la sauvegarde** : nombre d'objets présents actuellement dans la sauvegarde. **Espace utilisé** : volume d'espace occupé dans la sauvegarde.

Tableau 15. Informations sur l'état des bases et des modules de Kaspersky Security

Le bloc Mise à jour	Conseil
Témoin de l'état des bases et des modules de l'application	La couleur du volet portant le nom du groupe indique l'état des bases et des modules de l'application. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que les bases de l'application sont à jour et qu'aucune mise à jour critique des modules de l'application n'est disponible. • Volet de couleur jaune : un des événements suivants s'est produit : *Les bases de l'application sont dépassées* ; *Une mise à jour critique des modules de l'application est disponible* ; *Le rappel de la mise à jour critique des modules de l'application a été annoncé* ; *Afin de terminer la mise à jour des modules de l'application, l'ordinateur doit être redémarré.* • Volet de couleur rouge : l'événement *Les bases de l'application sont fortement dépassées* ou *Les bases de l'application sont endommagées* s'est produit.

Le bloc Mise à jour	Conseil
Mise à jour des bases et des modules de l'application	**Etat** : évaluation de l'actualité des bases de l'application. Le paramètre peut prendre les valeurs suivantes : • **Les bases de l'application sont à jour** : les bases de l'application ont été mises à jour il y a 7 jours maximum (par défaut). • **Les bases de l'application sont dépassées** : les bases de l'application ont été mises à jour il y a 7 à 14 jours. • **Les bases de l'application sont fortement dépassées** : les bases de l'application ont été mises à jour il y a plus de 14 jours (par défaut). Vous pouvez modifier les seuils de déclenchement des événements *Les bases de l'application sont dépassées* et *Les bases de l'application sont fortement dépassées*. **Date d'édition** : date et heure de la publication de la dernière mise à jour des bases de l'application installée. La date et l'heure sont exprimées en TU. **Nombre d'enregistrements dans les bases de l'application** : nombre d'enregistrements relatifs aux menaces dans les bases de données de l'application installées. **Etat de la dernière tâche de mise à jour des bases de l'application lancée** : date et heure de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées selon l'heure locale du serveur à protéger. La valeur du champ prend la couleur rouge si l'événement *Echec* s'est produit. **Des mises à jour des modules de l'application sont disponibles** : nombre de mises à jour des modules de Kaspersky Security prêtes à être téléchargées et installées. **Mises à jour des modules de l'application installées** : nombre de mises à jour des modules de Kaspersky Security installées.

Le groupe **Contrôle** (voir tableau ci-dessous) s'affiche si au moins l'un des composants suivants a été installé : Blocage de l'accès aux fichiers réseau, Protection contre le chiffrement ou Contrôle du lancement des applications.

Tableau 16. Informations sur l'état du contrôle du serveur

Groupe Contrôle	Conseil
Indicateur d'état du contrôle du serveur	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que toutes les tâches de contrôle du serveur sont en cours d'exécution. • Volet de couleur jaune : une ou plusieurs tâches de protection du serveur n'ont pas été exécutées ; l'événement *Non exécuté* se produit. • Volet de couleur rouge : échec du lancement des tâches de blocage de l'accès aux fichiers réseau, de contrôle du lancement des applications ou de protection contre le chiffrement ; l'événement *Soldée par un échec* se produit.
Blocage de l'accès aux fichiers réseau	**Ordinateurs dans la liste des ordinateurs douteux** : nombre d'ordinateurs distants placés dans la liste des ordinateurs douteux et/ou bloqués lors de l'exécution de la tâche de contrôle du serveur. Si le nombre d'ordinateurs suspects dépasse 0, la valeur du champ est mise en évidence en rouge.
Contrôle du lancement des applications	**Lancements des applications bloqués** : nombre de tentatives de lancement d'applications bloquées par Kaspersky Security au cours de l'exécution de la tâche de contrôle du lancement des applications. Si le nombre de lancements d'applications bloqués dépasse 0, la valeur du champ prend la couleur rouge. **Durée de traitement moyenne (en ms)** : temps qui a été nécessaire à Kaspersky Security pour le traitement des tentatives de lancement d'applications sur le serveur à protéger.
Protection contre le chiffrement	**Détection de tentatives de chiffrement de fichiers par des programmes malveillants** : nombre de tentatives de chiffrement de données du stockage réseau détectées par Kaspersky Security au cours de l'exécution de la tâche Protection contre le chiffrement. Si le nombre de tentatives de chiffrement de fichiers détectées dépasse 0, la valeur du champ prend la couleur rouge.

Le groupe **Protection des stockages réseau** (cf. tableau ci-dessous) contient des informations sur la protection des stockages réseau.

Tableau 17. Informations sur la protection des stockages réseau.

Groupe Protection des stockages réseau	Conseil

Indicateur de l'état de la protection des stockages réseau	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes :
	• Le volet vert apparaît dans les cas suivants :
	  • l'une des tâches suivantes est en cours d'exécution : Protection des stockages réseau connectés via le protocole RPC ou Protection des stockages réseau connectés via le protocole ICAP ;
	  • Kaspersky Security a ouvert une connexion avec l'application de la société EMC et Kaspersky Security assure la protection des fichiers en temps réel.
	• Le volet jaune s'affiche par défaut dans tous les autres cas.

Protection des stockages réseau connectés via le protocole RPC	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Détecté** : nombre d'objets détectés par Kaspersky Security depuis le lancement de la tâche. Si le nombre de programmes malveillants détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.
Protection des stockages réseau connectés via le protocole ICAP	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Détecté** : nombre d'objets détectés par Kaspersky Security depuis le lancement de la tâche. Si le nombre de programmes malveillants détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.

Groupe Protection des stockages réseau	Conseil
Intégration à EMC Celerra / VNX	Le paramètre peut prendre les valeurs suivantes : • **Agent anti-virus Celerra/VNX non trouvé** : Kaspersky Security n'a pas trouvé le logiciel de la société EMC ou une erreur s'est produite dans le code d'intégration. • **Protection désactivée** : Kaspersky Security a ouvert une connexion avec l'application de la société EMC, mais Kaspersky Security n'assure pas la protection des fichiers en temps réel. • **Protection activée** : Kaspersky Security a ouvert une connexion avec l'application de la société EMC, et Kaspersky Security assure la protection des fichiers en temps réel.

Pour obtenir des instructions détaillées sur la protection des stockages réseau à l'aide de Kaspersky Security, consultez le *Manuel d'implantation de Kaspersky Security 10 for Windows Server pour la protection des stockages réseau*.

Les informations sur l'état de la licence de Kaspersky Security sont affichées dans la ligne dans le coin inférieur gauche du panneau des résultats de l'entrée **Kaspersky Security**. (cf. section "Consultation des informations sur la licence active" à la page 45)

Autorisations d'accès aux fonctions de Kaspersky Security

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Security et des services Windows qui enregistrer l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

Dans cette section

A propos des autorisations d'administration de Kaspersky Security

Par défaut, les utilisateurs qui appartiennent au groupe "Administrateurs" sur le serveur à protéger ainsi que les membres du groupe KAVWSEE Administrators (cf. section "À propos des autorisations d'accès au service Kaspersky Security Management" à la page 92), créé sur le serveur à protéger lors de l'installation de Kaspersky Security, ont accès à toutes les fonctions de l'application, sans oublier le groupe SYSTEM.

Les utilisateurs qui ont accès à la fonction **Modifier les privilèges** de Kaspersky Security peuvent offrir l'accès aux fonctions de Kaspersky Security aux autres utilisateurs enregistrés sur le serveur protégé ou repris dans le domaine.

Si l'utilisateur ne figure pas dans la liste des utilisateurs de Kaspersky Security, il ne pourra pas ouvrir la console de Kaspersky Security.

Vous pouvez attribuer à l'utilisateur ou au groupe d'utilisateurs de Kaspersky Security un des niveaux prédéfinis d'accès aux fonctions de Kaspersky Security :

- **Contrôle complet** : accès à toutes les fonctions de l'application ; consultation et modifications des paramètres généraux de fonctionnement de Kaspersky Security, des paramètres de fonctionnement des modules de Kaspersky Security, des autorisations des utilisateurs de Kaspersky Security ainsi que la consultation des statistiques de fonctionnement de Kaspersky Security.

- **Modifier** : accès à toutes les fonctions de l'application, à l'exception de la modification des autorisations des utilisateurs ; consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security, des paramètres de fonctionnement des modules de Kaspersky Security ainsi que la consultation des statistiques de fonctionnement de Kaspersky Security et des autorisations des utilisateurs de l'application.

- **Lire** : lecture et modification des paramètres généraux de fonctionnement de Kaspersky Security, des paramètres de fonctionnement des modules de Kaspersky Security, des statistiques de fonctionnement de Kaspersky Security et des autorisations des utilisateurs de l'application.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès (cf. section "Configuration des autorisations d'accès aux fonctions de Kaspersky Security et à l'administration du service Kaspersky Security" à la page 92) : autoriser ou interdire l'accès aux fonctions individuelles de Kaspersky Security.

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

Tableau 18. Autorisations d'accès aux fonctions de Kaspersky Security

Autorisations d'accès	Description
Administration des tâches	Lancement/arrêt/suspension/reprise d'une tâche de Kaspersky Security.
Création et suppression de tâches	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilités : • consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security ; • importation des paramètres de fonctionnement de Kaspersky Security depuis un fichier de configuration et exportation de ceux-ci dans le fichier de configuration ; • consultation et modification des paramètres des tâches ; • consultation et modification des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Lire les paramètres	Possibilités : • consultation des paramètres généraux de fonctionnement de Kaspersky Security et des paramètres des tâches ; • exportation des paramètres de fonctionnement de Kaspersky Security dans un fichier de configuration ; • consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Gérer la quarantaine et les sauvegardes	Possibilités : • placement d'objets en quarantaine ; • suppression d'objets de la quarantaine et de la sauvegarde ; • restauration d'objets de la quarantaine et de la sauvegarde ;
Administration des journaux	Suppression des journaux d'exécution des tâches et purge du journal d'audit système.

Autorisations d'accès	Description
Lecture des journaux	Possibilité de consulter les événements dans les journaux d'exécution des tâches et le journal d'audit système.
Consultation des statistiques	Possibilité de consulter les statistiques de fonctionnement de chaque tâche de Kaspersky Security.
Licence de l'application	Possibilité d'activer ou de désactiver Kaspersky Security.
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Security et des privilèges d'accès de chacun d'entre eux.
Modification des privilèges	Possibilités : • modifier la liste des utilisateurs qui ont accès à l'administration de l'application ; • modification des autorisations d'accès des utilisateurs aux fonctions de Kaspersky Security.

A propos des autorisations d'administration du service Kaspersky Security

Le *Manuel d'installation de Kaspersky Security 10 for Windows Server* présente en détails les services Windows enregistrés par Kaspersky Security.

Lors de l'installation de Kaspersky Security, le service Kaspersky Security (KAVFS) est enregistré dans Windows car il contient les modules fonctionnels lancés au démarrage du système d'exploitation. Pour réduire le risque d'accès d'un tiers aux fonctions de l'application et aux paramètres de sécurité sur le serveur protégé via l'administration du service Kaspersky Security, vous pouvez limiter les autorisations d'administration du service Kaspersky Security depuis la Console de Kaspersky Security.

Par défaut, l'accès à l'administration du service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe "Administrateur" du serveur à protéger, ainsi qu'aux groupes système SERVICE et INTERACTIVE avec autorisation de lecture et au groupe système SYSTEM avec autorisation de lecture et d'exécution.

Les utilisateurs qui disposent d'un accès aux fonctions du niveau **Modifier les privilèges** (cf. section "**A propos des autorisations d'administration de Kaspersky Security**" à la page 86) peuvent octroyer l'accès à l'administration du service Kaspersky Security à d'autres utilisateurs enregistrés sur le serveur à protéger ou appartenant au domaine.

Vous pouvez attribuer à l'utilisateur ou à un groupe d'utilisateurs de Kaspersky Security un des niveaux prédéfinis d'administration du service Kaspersky Security :

- **Contrôle complet** : consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security Service et des autorisations des utilisateurs, ainsi lancement et arrêt du service Kaspersky Security.
- **Lire** : consultation des paramètres généraux de fonctionnement de Kaspersky Security Service et des autorisations des utilisateurs.
- **Modifier** : consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security Service et des autorisations des utilisateurs.
- **Exécution** : lancement et arrêt du fonctionnement de Kaspersky Security Service.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès (cf. section "Configuration des autorisations d'accès à l'administration de Kaspersky Security et du service Kaspersky Security" à la page 92) : octroyer ou limiter les autorisations d'administration du service Kaspersky Security (cf. tableau ci-dessous).

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

Tableau 19. Restriction des autorisations d'accès aux fonctions de Kaspersky Security

Fonction	Description
Lecture des paramètres du service	Consultation des paramètres généraux de fonctionnement de Kaspersky Security Service et des autorisations des utilisateurs.
Interrogation sur l'état du service et du gestionnaire de services	Interrogation sur l'état d'exécution de Kaspersky Security Service dans le gestionnaire de services de Microsoft Windows.
Interrogation du service sur son état	Interrogation de Kaspersky Security Service sur l'état de l'exécution du service.
Liste des services dépendants	Consultation de la liste des services dont dépend Kaspersky Security Service ainsi que des services qui dépendent de Kaspersky Security Service.
Modification des paramètres du service	Consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security Service et des autorisations des utilisateurs.
Lancement du service	Exécution de Kaspersky Security Service.
Arrêt du service	Arrêt de Kaspersky Security Service.
Suspension/reprise du service	Suspension et reprise de l'exécution de Kaspersky Security Service.
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Security et des privilèges d'accès de chacun d'entre eux.
Modification des privilèges	Possibilités : • ajout et suppression d'utilisateurs de Kaspersky Security Service ; • modification des autorisations d'accès des utilisateurs au Kaspersky Security Service.
Suppression du service	Annulation de l'enregistrement de Kaspersky Security Service dans le Gestionnaire de service de Microsoft Windows.
Interrogations personnalisées adressées au service	Création et envoi d'interrogations personnalisées adressées au Kaspersky Security Service.

À propos des autorisations d'accès au service Kaspersky Security Management

Le *Manuel d'installation de Kaspersky Security 10 for Windows Server* présente en détails les services enregistrés par Kaspersky Security.

Lors de l'installation de Kaspersky Security, l'utilisateur enregistre le service de gestion de l'application Kaspersky Security Management Service (KAVFSGT). Pour administrer l'application via la console de Kaspersky Security installée sur un autre ordinateur, il faut que le compte sous les autorisations duquel la connexion à Kaspersky Security s'opère possède un accès complet à Kaspersky Security Management Service sur le serveur protégé.

Par défaut, l'accès à l'administration de Kaspersky Security Management Service est octroyé aux utilisateurs du groupe Administrateurs sur le serveur protégé et aux utilisateurs du groupe KAVWSEE Administrators créé sur le serveur protégé lors de l'installation de Kaspersky Security.

Vous pouvez administrer Kaspersky Security Management Service uniquement via le composant logiciel enfichable **Services** de Microsoft Windows.

Vous ne pouvez pas octroyer ou interdire l'accès des utilisateurs au service Kaspersky Security Management Service en configurant les paramètres de Kaspersky Security.

Vous pouvez vous connecter à Kaspersky Security sous un compte utilisateur local si un compte utilisateur avec le même nom et le même mot de passe sont enregistrés sur le serveur protégé.

Configuration des autorisations d'accès à l'administration de Kaspersky Security et du service Kaspersky Security

Vous pouvez modifier la liste des utilisateurs et groupes d'utilisateurs ayant accès aux fonctions de Kaspersky Security et à l'administration du service Kaspersky Security, ainsi que modifier les privilèges d'accès des utilisateurs et groupes d'utilisateurs.

► *Pour ajouter un utilisateur ou un groupe à la liste ou pour l'en supprimer, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security** et réalisez une des actions suivantes :

   - Choisissez l'option **Modifier les permissions utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration des fonctions de Kaspersky Security.
   - Choisissez l'option **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration de l'application à l'aide du service Kaspersky Security.

   La fenêtre **Autorisations pour le groupe "Kaspersky Security"** s'ouvre.

2. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

   - Pour ajouter un utilisateur (un groupe) à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez octroyez des autorisations.
   - Pour supprimer un utilisateur (un groupe) de la liste, sélectionnez les utilisateurs (les groupes) pour lesquels vous souhaitez restreindre l'accès, puis cliquez sur le bouton **Supprimer**.

3. Cliquez sur le bouton **Appliquer**.

Les utilisateurs (ou groupes) sélectionnés seront ajoutés ou supprimés.

► *Pour modifier les autorisations d'administration de Kaspersky Security ou du service Kaspersky Security d'un utilisateur (ou d'un groupe d'utilisateurs), procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security** et réalisez une des actions suivantes :

   - Choisissez l'option **Modifier les permissions utilisateur pour l'administration de l'application** si vous souhaitez configurer les autorisations d'accès aux fonctions de Kaspersky Security.
   - Choisissez l'option **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service** si vous souhaitez configurer les autorisations d'accès au service Kaspersky Security.

   La fenêtre **Autorisations pour le groupe "Kaspersky Security"** s'ouvre.

2. Dans la fenêtre qui s'ouvre sélectionnez dans la liste **Groupes ou utilisateurs** l'utilisateur ou le groupe d'utilisateurs dont vous souhaitez modifier les autorisations.

3. Dans le groupe **Autorisation pour le groupe « <Utilisateur (Groupe)> »**, cochez les cases **Autoriser** ou **Interdire** pour les niveaux d'accès suivants :

   - **Contrôle complet** : sélection complète des autorisations d'administration de Kaspersky Security ou du service Kaspersky Security.

   - **Lire** :

     - autorisations suivantes sur l'administration de Kaspersky Security : **Lecture des statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lire les privilèges**;

     - autorisations suivantes pour l'administration du service Kaspersky Security : **Lecture des paramètres du service**, **Requête concernant le statut du service auprès du Gestionnaire d'administration des services**, **Requête concernant le statut auprès du service**, **Lecture de la liste des services dépendants, Lire les privilèges**.

   - **Modifier** :

     - toutes les autorisations d'administration de Kaspersky Security, sauf **Modifier les privilèges** ;

     - autorisations suivantes sur l'administration du service Kaspersky Security : **Modification des paramètres du service, Lire les privilèges**.

   - **Exécution** : autorisations suivantes sur l'administration du service Kaspersky Security : **Lancement du service**, **Arrêt du service**, **Suspension/reprise du service**, **Lire les privilèges**, **Requêtes de l'utilisateur au service**.

4. Si vous souhaitez réaliser une configuration étendu des autorisations pour un utilisateur ou un groupe d'utilisateurs (**Autorisations spéciales**), cliquez sur le bouton **Avancé**.

   a. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Security** qui s'ouvre, sélectionnez l'utilisateur ou le groupe requis.

   b. Cliquez sur le bouton **Modifier**.

   c. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Afficher les autorisations spéciales**.

d. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).

e. Cochez la case en regard des fonctions pour lesquelles vous souhaitez octroyer ou non un accès à un utilisateur ou un groupe d'utilisateurs sélectionnés.

f. Cliquez sur **OK**.

g. Dans la fenêtre **Paramètres de sécurité avancé pour Kaspersky Security**, cliquez sur **OK**.

5. Dans la fenêtre **Autorisations pour le groupe "Kaspersky Security"**, cliquez sur le bouton **Appliquer**.

Les autorisations d'administration de Kaspersky Security ou du service Kaspersky Security Service configurées seront enregistrées.

Autorisation des connexions réseau pour le service Kaspersky Security Management

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

► *Pour autoriser les connexions réseau pour le service Kaspersky Security Management sur le serveur à protéger, procédez comme suit :*

1. Sur le serveur à protéger sous Microsoft Windows Server, sélectionnez **Démarrer** → **Panneau de configuration** → **Sécurité** → **Pare-feu Windows**.

2. Dans la fenêtre **Paramètres du pare-feu Windows**, cliquez sur **Modifier les paramètres**.

3. Sur l'onglet **Exclusions** dans la liste des exclusions prédéfinies, cochez les cases **COM + Accès réseau**, **Windows Management Instrumentation (WMI)** et **Remote Administration**.

4. Cliquez sur **Ajouter programme**.

5. Dans la fenêtre **Ajout de programme**, sélectionnez le fichier kavfsgt.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de la console de Kaspersky Security.

6. Cliquez sur **OK**.

7. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du pare-feu Windows**.

Les connexions réseau pour le service Kaspersky Security Management sur le serveur à protéger seront autorisées.

Zone de confiance

Cette section contient des informations sur la zone de confiance de Kaspersky Security, sur les instructions pour ajouter des objets à la zone de confiance et sur l'application de la zone de confiance aux tâches de Kaspersky Security.

Dans cette section

Présentation de la zone de confiance de Kaspersky Security

La zone de confiance est la liste des exclusions de la zone de protection ou d'analyse que vous pouvez créer et utiliser dans les tâches d'analyse à la demande, de protection des fichiers en temps réel, d'analyse des scripts et de protection des stockages réseau via le protocole RCP.

Si lors de l'installation de Kaspersky Security, vous aviez coché la case **Ajouter les objets sous le masque not-a-virusRemoteAdmin* aux exclusions**, Kaspersky Security ajoute à la zone de confiance l'exclusion des objets selon le masque `not-a-virus:RemoteAdmin*` pour les tâches de protection des fichiers en temps réel, d'analyse des scripts, de protection des stockages réseau connectés via le protocole RCP et des tâches d'analyse à la demande.

Si lors de l'installation de Kaspersky Security, vous aviez cochez les cases **Ajouter les exclusions recommandées par Microsoft** et **Ajouter les exclusions recommandées par Kaspersky Lab**, Kaspersky Security ajoute à la zone de confiance les fichiers recommandés par Microsoft et Kaspersky Lab pour les tâches de protection des fichiers en temps réel.

Vous pouvez créer une zone de confiance de Kaspersky Security selon les règles suivantes :

- **Processus de confiance**. La zone de confiance contient les objets sollicités par les processus des applications sensibles aux interceptions de fichier.
- **Opérations de sauvegarde**. La zone de confiance reprend les objets sollicités lors des opérations des systèmes de sauvegarde des disques durs sur des périphériques externes.
- **Exclusions**. La zone de confiance reprend les objets, indiqués par leur emplacement et/ou l'objet détectés dans ceux-ci.

Vous pouvez utiliser la zone de confiance dans les tâches Protection des fichiers en temps réel, dans la protection des stockages réseau connectés via le protocole RPC et dans l'analyse des scripts, dans les tâches d'analyse à la demande définies par l'utilisateur nouvellement créées et dans toutes les tâches prédéfinies d'analyse à la demande, à l'exception de la tâche Analyse des objets en quarantaine.

Par défaut, la zone de confiance est appliquées dans les tâches de protection des fichiers en temps réel, d'analyse des scripts et dans les tâches d'analyse à la demande.

Vous pouvez exporter la liste des règles de composition de la zone de confiance dans un fichier de configuration au format XML afin de pouvoir l'importer par la suite dans une version de Kaspersky Security installée sur un autre serveur.

Processus de confiance

Applicable aux tâches de protection des fichiers en temps réel et de protection des stockages réseau connectés via le protocole RPC.

Certaines applications du serveur peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par l'application Kaspersky Security. Les contrôleurs de domaine sont un exemple d'applications appartenant à cette catégorie.

Afin de ne pas perturber la stabilité de telles applications, vous pouvez désactiver la protection en temps réel des objets sollicités par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Microsoft Corporation recommande d'exclure de la protection en temps réel certains fichiers du système d'exploitation Microsoft Windows et les fichiers des applications de Microsoft qui ne peuvent être infectés. Les noms de certains d'entre eux sont repris sur le site Internet de Microsoft http://www.microsoft.com/fr-fr (code de l'article : KB822158).

Vous pouvez activer ou désactiver l'application des processus de confiance dans la zone de confiance.

> Si le fichier exécutable du processus change, par exemple s'il est actualisé, Kaspersky Security l'exclura de la liste des processus de confiance.

Opérations de sauvegarde

Applicable aux tâches de protection en temps réel.

Pendant la sauvegarde des données des disques durs sur des périphériques externes, vous pouvez désactiver la fonction de protection en temps réel des objets sollicités durant les opérations de sauvegarde. Kaspersky Security n'analyse pas les objets que l'application de sauvegarde ouvre en lecture avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Exclusions

Applicable aux tâches de protection des fichiers en temps réel, de protection des stockages réseau connectés via le protocole RPC, d'Analyse des scripts et d'analyse à la demande.

Vous pouvez sélectionner les tâches dans lesquelles vous souhaitez appliquer chacune des exclusions ajoutée à la zone de confiance. Vous pouvez également exclure des objets de l'analyse séparément dans le cadre de la configuration des paramètres du niveau de sécurité de chaque tâche de Kaspersky Security.

Vous pouvez ajouter à la zone de confiance des objets en fonction de leur emplacement sur le serveur ou en fonction du nom ou du masque de nom de l'objet détecté dans ces objets. Vous pouvez également utiliser les deux paramètres.

Sur la base de l'exclusion, Kaspersky Security peut ignorer des objets dans les tâches indiquées en fonction des paramètres suivants :

- objets à détecter désignés selon le nom ou le masque du nom dans les zones désignées du serveur ou du stockage réseau ;
- tous les objets à détecter dans les zones désignées du serveur ou du stockage réseau ;
- objets à détecter désignés selon le nom ou le masque de nom dans toute la zone de protection ou d'analyse.

Activation et désactivation de l'application de la zone de confiance dans les tâches de Kaspersky Security

La zone de confiance est appliquée par défaut dans les tâches Protection des fichiers en temps réel, dans la protection des stockages réseau connectés via le protocole RPC et dans l'analyse des scripts, dans les tâches d'analyse à la demande définies par l'utilisateur nouvellement créées et dans toutes les tâches prédéfinies d'analyse à la demande, à l'exception de la tâche Analyse des objets en quarantaine.

Dès que la zone de confiance est activée/désactivée, les exclusions seront ou ne seront plus appliquées dans les tâches exécutées immédiatement.

► *Pour activer ou désactiver l'utilisation d'une zone de confiance dans les tâches de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer l'application de la zone de confiance.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et dans le groupe **Zone de confiance**, réalisez une des opérations suivantes :

   - Si vous souhaitez utiliser une zone de confiance dans la tâche, cochez la case **Appliquer la zone de confiance**.
   - Si vous ne souhaitez pas utiliser une zone de confiance, décochez la case **Appliquer la zone de confiance**.

4. Pour configurer les paramètres de la zone de confiance, cliquez sur le lien dans le nom de la case **Appliquer la zone de confiance**.
5. Cliquez sur **OK**.

Les modifications seront enregistrées.

Ajout d'exclusions à la zone de confiance

Cette section fournit des instructions sur l'ajout d'exclusions uniques à la zone de confiance de Kaspersky Security.

Dans cette section

Ajout de processus à la liste des processus de confiance

Vous pouvez ajouter un processus à la liste des processus de confiance d'une des manières suivantes :

- Sélectionner ce processus dans la liste des processus exécutés sur le serveur protégé.
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

  Si le fichier exécutable du processus change, Kaspersky Security l'exclut de la liste des processus de confiance.

► *Pour ajouter un processus à la liste des processus de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Processus de confiance** et cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés**.
4. Ajoutez un processus de confiance d'une des méthodes suivantes :
   - Pour ajouter un processus de la liste des processus exécutés, procédez comme suit :

     a. Cliquez sur **Ajouter**.

     La fenêtre **Ajout d'un processus de confiance** s'ouvre.

     b. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **Processus**.

     La fenêtre **Processus actifs** s'ouvre.

c. Dans la fenêtre **Processus actifs**, sélectionnez le processus souhaité dans la liste des processus en exécution et cliquez sur **OK**.

> Le compte utilisateur sous les privilèges duquel la tâche de protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur le serveur où Kaspersky Security est installé afin de pouvoir consulter la liste des processus actifs. Vous pouvez trier les processus dans la liste des processus actifs selon le nom du fichier, le PID ou le chemin d'accès au fichier exécutable du processus sur l'ordinateur local.

d. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **OK**.

Le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

- Si vous souhaitez indiquer le fichier exécutable du processus, procédez comme suit :

a. Cliquez sur **Ajouter**.

La fenêtre **Ajout d'un processus de confiance** s'ouvre.

b. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du processus, puis cliquez sur **OK**.

Le nom du fichier exécutable et son chemin d'accès apparaissent dans la fenêtre **Ajout d'un processus de confiance**.

> Kaspersky Security ne considèrera pas un processus comme un processus de confiance si le chemin d'accès au fichier exécutable du processus est différent du chemin d'accès que vous avez saisi dans le champ **Dossier contenant le fichier sur l'ordinateur protégé**.

c. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **OK**.

Le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

5. Cliquez sur **OK**.

La fenêtre **Zone de confiance** se ferme ; les processus sélectionnés seront ajoutés à la liste des processus de confiance.

Suppression d'un processus de la liste des processus de confiance

► *Pour désactiver l'application d'un processus de confiance dans la zone de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Dans la fenêtre **Zone de confiance**, choisissez l'onglet **Processus de confiance** et dans la liste des processus de confiance proposée, décochez la case en regard du nom du fichier exécutable que vous souhaitez exclure temporairement de la zone de confiance.
4. Cliquez sur **OK**.

La fenêtre **Zone de confiance** se ferme ; les processus sélectionnés seront supprimés de la liste des processus de confiance.

Désactivation de la protection des fichiers en temps réel pendant la copie de sauvegarde

► *Pour désactiver la protection des fichiers en temps réel pendant la copie de sauvegarde depuis les disques durs, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Processus de confiance** et cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.
4. Cliquez sur **OK**.

La fenêtre **Zone de confiance** se ferme ; la protection des fichiers en temps réel sera suspendue pendant la copie de sauvegarde.

Ajout d'une exclusion à la zone de confiance

► *Pour ajouter une exclusion à la zone de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion** s'ouvre.
4. Dans le groupe **L'objet ne sera pas analysé lorsque les conditions suivantes seront remplies**, indiquez les objets que vous souhaitez exclure de la zone de protection/d'analyse et les objets que vous souhaitez exclure de la liste des objets à détecter (par exemple, un utilitaire d'administration à distance) :

   - Si vous souhaitez exclure un objet de la zone de protection/d'analyse, procédez comme suit :

     a. Cochez la case **Objet à analyser**.

     Ajout d'un fichier, d'un dossier, d'un disque ou d'un fichier de script à l'exclusion.

     Quand la case est cochée, Kaspersky Security ignore la zone définie, le fichier, le dossier, le disque ou le fichier de script désigné lors de l'analyse à l'aide du composant de Kaspersky Security sélectionné dans le groupe **Zone d'application de la règle**.

     Cette case est cochée par défaut.

     b. Cliquez sur le bouton **Modifier**.

     La fenêtre **Sélection de l'objet** s'ouvre.

     c. Dans la fenêtre qui s'ouvre, indiquez l'objet que vous souhaitez exclure de la zone d'analyse.

     > Vous pouvez utiliser pour ce faire les caractères génériques ? et *.

- Si vous souhaitez indiquer le nom de l'objet à détecter, procédez comme suit :

    a. Cochez la case **Objets à détecter**.

    Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque de nom d'objet à détecter. Par exemple, vous pouvez exclure les utilitaires d'administration à distance à l'aide du masque `not-a-virus:RemoteAdmin*`. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

    Si la case est cochée, Kaspersky Security ignore les objets à détecter indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Security détecte tous les objets indiqués par défaut dans l'application.

    Cette case est décochée par défaut.

    b. Cliquez sur le bouton **Modifier**.

    La fenêtre **Liste des objets à détecter** s'ouvre.

    c. Dans la fenêtre qui s'ouvre, indiquez le nom ou le masque du nom de l'objet à détecter conformément à la classification de l'Encyclopédie des virus (http://www.securelist.fr), par exemple, `not-a-virus:RemoteAdmin*`.

- Dans le groupe **Zone d'application de l'exclusion**, cochez les cases en regard du nom des tâches qui appliqueront l'exclusion.

5. Cliquez sur **OK**.

L'exclusion ajoutée apparaît dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

Gestion des tâches de Kaspersky Security

Cette section contient les informations relatives aux tâches de Kaspersky Security, à leur création, à la configuration des paramètres d'exécution, au lancement et à l'arrêt des tâches et à la configuration du lancement et de l'arrêt automatiques des tâches planifiées.

Dans cette section

Catégories de tâches de Kaspersky Security

Les fonctions de la protection en temps réel, de la protection des stockages réseau, du contrôle du serveur, de l'analyse à la demande et de la mise à jour de Kaspersky Security sont réalisées à l'aide de tâches.

Ces tâches peuvent être administrées via les options du menu contextuel du nom de la tâche dans l'arborescence de la console, de la barre d'outils ou du volet d'accès rapide. Vous pouvez consulter les informations sur l'état d'une tâche dans le volet des résultats. Les opérations d'administration des tâches sont consignées dans le journal d'audit système.

Il existe deux types de tâches dans Kaspersky Security : *locales* et *de groupe*.

Tâches locales

Les tâches locales sont uniquement exécutées sur le serveur protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- **Tâches locales prédéfinies**. Ces tâches sont créées automatiquement lors de l'installation de Kaspersky Security. Vous pouvez modifier les paramètres de toutes les tâches prédéfinies à l'exception des tâches Analyse des objets en quarantaine et Remise des bases de l'application à l'état antérieur. Il est impossible de renommer ou de supprimer les tâches prédéfinies. Vous pouvez lancer les tâches d’analyse à la demande prédéfinies en même temps que les tâches définies par l'utilisateur.

- **Tâches locales définies par l'utilisateur**. Vous pouvez créer une tâche d'analyse à la demande dans la console de Kaspersky Security. La console d'administration de Kaspersky Security Center vous permet de créer des tâches d'analyse à la demande, de mise à jour des bases de l’application, de remise à l'état antérieur à la mise à jour et de copie des mises à jour. C'est ce qu'on appelle les tâches définies par l'utilisateur. Vous pouvez renommer, configurer et supprimer les tâches définies par l'utilisateur. Vous pouvez exécuter simultanément plusieurs tâches définies par l'utilisateur.

Tâches de groupe

Les tâches de groupe et les tâches pour les sélections d'ordinateurs créées dans la console d'administration de Kaspersky Security Center sont affichées dans la console de Kaspersky Security. Ces tâches sont les tâches de groupe. Vous pouvez administrer les tâches de groupe et les configurer au départ de Kaspersky Security Center. La console de Kaspersky Security permet uniquement de consulter l'état des tâches de groupe.

Enregistrement d'une tâche après modification de ses paramètres

Vous pouvez modifier les paramètres d'une tâche, qu'elle soit en cours d'exécution ou arrêtée (suspendue). Les nouvelles valeurs des paramètres seront appliquées si les conditions suivantes sont remplies :

- si vous avez modifié les paramètres d'une tâche à exécuter : les nouvelles valeurs des paramètres seront appliquées directement après l'enregistrement de la tâche ;
- si vous avez modifié les paramètres d'une tâche arrêtée (suspendue), les nouvelles valeurs seront appliquées à la prochaine exécution de la tâche.

► *Pour enregistrer les paramètres modifiés d'une tâche :*

Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Si, après la modification des paramètres de la tâche, vous sélectionnez un autre nœud dans l'arborescence de la console sans avoir sélectionné la commande **Enregistrer la tâche**, la fenêtre d'enregistrement des paramètres s'ouvre.

► *Pour enregistrer les paramètres modifiés au moment de passer à une autre entrée de la console :*

Dans la fenêtre d'enregistrement des paramètres, cliquez sur **Oui**.

Lancement / suspension / rétablissement / arrêt manuel d'une tâche

Vous ne pouvez suspendre et reprendre que les tâches de protection en temps réel et d'analyse à la demande.

► *Pour lancer/suspendre/reprendre/arrêter une tâche, procédez comme suit :*

1. Ouvrez le menu contextuel du nom de la tâche dans la console de Kaspersky Security.
2. Sélectionnez une des options : **Démarrer**, **Suspendre**, **Reprendre** ou **Arrêter**.

L'opération sera exécutée et enregistrée dans le journal d'audit système (cf. section "Journal d'audit système" à la page 303).

Quand vous suspendez, puis relancez une tâche d'analyse à la demande, Kaspersky Security reprend l'analyse à l'objet qui était traité au moment de l'interruption.

Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Security et configurer les paramètres de la planification.

Dans cette section

Configuration des paramètres de planification du lancement des tâches

La console de Kaspersky Security vous permet de planifier le lancement des tâches prédéfinies et des tâches définies par l'utilisateur locales (cf. page 107). Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement d'une tâche,* procédez comme suit *:*

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez configurer la planification du lancement.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, activez le lancement programmé de la tâche en cochant la case **Exécuter de manière planifiée**.

> Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée est interdite par une stratégie de Kaspersky Security Center (cf. section "Configuration de la planification de l'exécution programmée des tâches prédéfinies locales" à la page 404).

4. Configurez l'horaire en fonction de vos besoins. Pour ce faire, exécutez les actions suivantes *:*

   a. Choisissez une des options suivantes dans la liste **Fréquence** :

   - **Chaque heure** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Une fois toutes les <nombre> heures** ;
   - **Chaque jour** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Une fois tous les <nombre> jour**;
   - **Chaque semaine** si vous souhaitez que la tâche soit exécutée selon une fréquence hebdomadaire que vous aurez définie dans le champ **Une fois toutes les <nombre> semaines**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;
   - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security ;
   - **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de données de l'application.

   b. Indiquez, dans le champ **Heure de démarrage**, l'heure de la première exécution de la tâche.

   c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

Après avoir indiqué la fréquence d'exécution de la tâche, l'heure de la première exécution et la date d'entrée en vigueur de la planification, dans la partie supérieure dans la fenêtre, le champ **Prochain démarrage** affiche des informations relatives au temps restant avant la nouvelle exécution de la tâche. Des informations actualisées sur le temps restant seront proposées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** du champ **Prochain démarrage** s'affiche si le lancement programmé des tâches prédéfinies est interdit par la stratégie en vigueur de l'application Kaspersky Security Center (cf. section "Configuration de la planification de l'exécution programmée des tâches prédéfinies locales" à la page. 404).

5. Sous l'onglet **Avancé**, configurez le reste des paramètres en fonction de vos besoins.

   - Dans le groupe **Paramètres d'arrêt de la tâche** :

     a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la carte.

     b. Cochez la case **Suspendre entre … et …** , puis saisissez le début et la fin de l'intervalle de temps au cours de la journée pendant lequel l'exécution de la tâche sera suspendu.

   - Dans le groupe **Paramètres avancés** :

     a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.

     b. Cochez la case **Lancer les tâches non exécutées** pour activer l'exécution des tâches ignorées.

     c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.

6. Cliquez sur le bouton **Appliquer**.

Les paramètres de la planification de la tâche sélectionnée seront enregistrés.

Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver le lancement des tâches planifiées après ou avant la configuration de la planification.

► *Pour activer ou désactiver la planification du lancement d'une tâche, procédez comme suit :*

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez configurer la planification du lancement.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes sous l'onglet **Planification** :
   - Cochez la case **Exécuter de manière planifiée** si vous souhaitez activer l'exécution planifiée d'une tâche ;
   - Décochez la case **Exécuter de manière planifiée** si vous souhaitez désactiver l'exécution planifiée d'une tâche ;

   > Les paramètres de la planification du lancement de la tâche ne seront pas supprimés. Ils seront toujours valides à la prochaine activation de l'exécution planifiée de la tâche.
4. Cliquez sur le bouton **Appliquer**.

Les paramètres configurés de l'exécution planifiée de la tâche seront enregistrés.

Utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez lancer les tâches sous un compte utilisateur système ou sous un autre compte que vous désignerez.

Dans cette section

A propos de l'utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez indiquer le compte sous les autorisations duquel vous souhaitez exécuter la tâche sélectionnée pour les modules suivants de Kaspersky Security :

- tâches Génération automatique des règles d'autorisation ;
- tâches d'analyse à la demande ;
- tâches de mise à jour.

Par défaut, les tâches désignées sont exécutées avec les autorisations du compte système.

Il est conseillé de définir un autre compte avec les privilèges suffisants dans les cas suivants :

- Pour la tâche de mise à jour, si la source de mise à jour est un dossier partagé sur un autre ordinateur du réseau.
- Pour la mise à jour, si l'accès à la source des mises à jour s'opère via un serveur proxy doté de la vérification intégrée de l'authenticité Microsoft Windows (authentification NTLM).

- Pour les tâches d'analyse à la demande, si le compte système ne possède pas les autorisations d'accès à un des objets à analyser (par exemple, aux fichiers dans les dossiers réseaux partagés du serveur).

- Pour la tâche de génération automatique des règles, si à l'issue de l'exécution de la tâche, les règles générées sont importées dans un fichier de configuration situé dans un emplacement inaccessible au compte système (par exemple, dans un des dossiers réseau partagés du serveur).

Vous pouvez lancer les tâches de mise à jour, d'analyse à la demande et de génération automatique des règles d'autorisation avec les autorisations du compte système. Lors de l'exécution de ces tâches, Kaspersky Security contacte les dossier partagés sur l'autre ordinateur du réseau si cet ordinateur est enregistré dans le même domaine que le serveur protégé. Dans ce cas, le compte système doit posséder les autorisations d'accès à ces dossiers. Kaspersky Security contactera cet ordinateur avec les privilèges du compte **<Nom_de_domaine\nom_d'ordinateur>**.

Définition du compte utilisateur pour l'exécution de la tâche

► *Pour sélectionner le compte utilisateur sous lequel la tâche sera exécutée, procédez comme suit :*

1. Ouvrez le menu contextuel du nom de la tâche pour laquelle vous souhaitez configurez le lancement avec les autorisations du compte.

2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

3. Dans la fenêtre qui s'ouvre, réalisez les opérations suivantes sous l'onglet **Exécuter en tant que** :

   a. Choisissez l'option **Nom d'utilisateur**.

   b. Saisissez le nom et le mot de passe de l'utilisateur dont vous souhaitez utiliser le compte.

L'utilisateur que vous sélectionnez doit être enregistré sur le serveur protégé ou dans le même domaine.

c. Confirmez le mot de passe saisi.

4. Cliquez sur le bouton **Appliquer**.

Les paramètres modifiés d'exécution des tâches sous les autorisations du compte sont enregistrés.

Importation et exportation des paramètres

Cette section aborde l'exportation des valeurs des paramètres de fonctionnement de Kaspersky Security ou des paramètres de fonctionnement de composants distincts de l'application dans un fichier de configuration au format XML et l'importation de ces valeurs depuis le fichier de configuration dans l'application.

Dans cette section

A propos de l'importation et de l'exportation des paramètres

Vous pouvez exporter les paramètres de Kaspersky Security dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.

Quand vous exportez tous les paramètres de Kaspersky Security, le fichier reprend les paramètres généraux de l'application et les paramètres des fonctions et modules suivants de Kaspersky Security :

- Protection des fichiers en temps réel ;
- Utilisation du KSN ;
- Analyse des scripts ;
- Protection des stockages réseau connectés via le protocole RPC/ICAP ;
- Blocage de l'accès aux fichiers réseau ;
- Protection contre le chiffrement ;
- Contrôle du lancement des applications ;
- Génération automatique des règles d'autorisation ;
- Analyse à la demande ;
- Mise à jour des bases et des modules logiciels de Kaspersky Security ;
- Quarantaine ;
- Sauvegarde.
- Journaux ;
- Notifications de l'administrateur et des utilisateurs ;
- Zone de confiance ;

Vous pouvez également exporter dans un fichier les paramètres généraux de Kaspersky Security et les privilèges des comptes utilisateur.

Vous ne pouvez pas exporter les paramètres des tâches de groupe.

Kaspersky Security exporte tous les mots de passe qui sont utilisés par l'application, par exemple, les données des comptes d'exécution des tâches ou de connexion au serveur proxy. Les mots de passe exportés dans le fichier de configuration sont chiffrés. Vous pouvez importer les mots de passe uniquement à l'aide d'une version de Kaspersky Security installée sur le même ordinateur où l'application a été réinstallée ou mise à jour.

Vous ne pouvez pas importer des mots de passe préalablement enregistrés à l'aide d'une version de Kaspersky Security installée sur un autre ordinateur. Après l'importation des paramètres sur un autre ordinateur, vous devrez saisir tous les mots de passe manuellement.

Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, Kaspersky Security exporte les valeurs appliquées par la stratégie.

Vous pouvez importer les paramètres depuis le fichier de configuration qui contient les paramètres uniquement de certains composants de Kaspersky Security (par exemple, créé dans une version de Kaspersky Security sans la totalité des composants). Après l'importation des paramètres dans Kaspersky Security, seuls les paramètres repris dans le fichier de configuration sont modifiés. Les autres paramètres demeurent inchangés.

Les paramètres importés des tâches ne sont pas appliqués lors de l'exécution de la tâche. Pour appliquer les paramètres importés, il faut redémarrer la tâche.

Les paramètres verrouillés de la stratégie active de Kaspersky Security Center ne sont pas modifiés lors de l'importation des paramètres.

Exportation des paramètres

► *Pour exporter les paramètres dans un fichier de configuration, procédez comme suit :*

1. Dans la console de Kaspersky Security, réalisez une des opérations suivantes :

   - Dans le menu contextuel de l'entrée **Kaspersky Security**, choisissez l'option **Exporter les paramètres** afin d'exporter tous les paramètres de Kaspersky Security.

   - Dans le menu contextuel du nom de la tâche dont vous souhaitez exporter les paramètres, choisissez l'option **Exporter les paramètres** afin d'exporter les paramètres d'un module individuel de l'application.

- Pour exporter les paramètres du composant Zone de confiance :

    a. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.

    b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

    La fenêtre **Zone de confiance** s'ouvre.

    c. Cliquez sur le bouton **Exporter**.

    La fenêtre de bienvenue de l'Assistant d'exportation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : indiquez le nom du fichier de configuration dans lequel vous souhaitez enregistrer les paramètres ainsi que le chemin d'accès à celui-ci.

    Pour désigner le chemin d'accès, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

    > Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, Kaspersky Security exporte les valeurs des paramètres de la stratégie.

3. Dans la fenêtre **L'exportation des paramètres de l'application est terminée**, cliquez sur **OK**.

L'Assistant d'exportation des paramètres se fermera et l'exportation des paramètres sera terminée.

Importation des paramètres

► *Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :*

1. Dans la console de Kaspersky Security, réalisez une des opérations suivantes :

    - Dans le menu contextuel de l'entrée **Kaspersky Security**, choisissez l'option **Importer les paramètres** afin d'importer tous les paramètres de Kaspersky Security.

- Dans le menu contextuel du nom de la tâche dont vous souhaitez importer les paramètres, choisissez l'option **Importer les paramètres**, afin d'importer les paramètres d'un module individuel.

- Pour importer les paramètres du composant Zone de confiance :

    a. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.

    b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

    La fenêtre **Zone de confiance** s'ouvre.

    c. Cliquez sur **Importer**.

    La fenêtre de bienvenue de l'Assistant d'importation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : identifiez le fichier de configuration que vous souhaitez importer.

    Une fois que les paramètres de Kaspersky Security et de ses composants auront été importés, vous ne pourrez plus revenir à leurs valeurs antérieures.

3. Dans la fenêtre **L'importation des paramètres de l'application est terminée**, cliquez sur **OK**.

    L'Assistant d'importation des paramètres se ferme ; les paramètres importés sont enregistrés.

4. Cliquez sur le bouton **Mettre à jour** dans la barre d'outils de la console de Kaspersky Security,

Les paramètres importés apparaissent dans la fenêtre de la console.

Kaspersky Security n’importe pas les mots de passe (les données des comptes utilisateur pour l’exécution de tâches ou la connexion au serveur proxy) d’un fichier créé sur un autre ordinateur ou sur ce même ordinateur après une réinstallation ou de mise à jour de Kaspersky Security. Après la fin de l’importation, vous devrez saisir les mots de passe manuellement.

Utilisation des modèles de paramètres de sécurité

Cette section explique l'utilisation des modèles des paramètres de sécurité dans les tâches de protection et d'analyse de Kaspersky Security.

Dans cette section

Présentation des modèles des paramètres de sécurité

Vous pouvez configurer manuellement les paramètres de sécurité de l'entrée dans l'arborescence des ressources fichier du serveur et enregistrer les valeurs définies dans un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Security.

L'utilisation de modèles est accessible lors de la configuration des paramètres de sécurité des tâches suivantes de Kaspersky Security :

- Protection des fichiers en temps réel ;
- Protection des stockages réseau connectés via le protocole RPC ;
- tâches d'analyse à la demande : analyse au démarrage du système d'exploitation, analyse des zones critiques, tâches d'analyse à la demande définies par l'utilisateur.

Les valeurs des paramètres de sécurité du modèle appliqué à l'entrée mère dans l'arborescence des ressources fichier du serveur sont appliquées à toutes les sous-entrées. Le modèle de l'entrée mère n'est pas appliqué aux sous-entrées dans les cas suivants :

- Si les paramètres de sécurité des sous-entrées ont été configurés séparément (cf. section "Application du modèle de paramètres de sécurité" à la page 123).
- Si les sous-entrées sont virtuelles. Il faudra alors appliquer le modèle pour chaque entrée virtuelle séparément.

Création d'un modèle de paramètres de sécurité

► *Pour enregistrer manuellement les paramètres de sécurité de l'entrée et les enregistrer dans le modèle, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le panneau des résultats de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
4. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Enregistrer comme modèle**.

   La fenêtre **Propriétés du modèle** s'ouvre.
5. Dans le champ **Nom du modèle**, saisissez le nom du modèle.
6. Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.
7. Cliquez sur **OK**.

Le modèle avec la sélection de paramètres de sécurité sera conservé.

Consultation des paramètres de sécurité du modèle

► *Pour consulter les valeurs des paramètres de sécurité dans le modèle créé, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche dont vous souhaitez consulter le modèle de sécurité.

2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

   > Vous pouvez passer à la création d'un modèle de paramètres pour les tâches d'analyse à la demande depuis le panneau des résultats de l'entrée principale **Analyse à la demande**.

   La fenêtre **Modèles** s'ouvre.

3. Dans la liste des modèles de la fenêtre qui s'ouvre, sélectionnez le modèle que vous souhaitez consulter.

4. Cliquez sur le bouton **Voir**.

La fenêtre **<Nom du modèle>** s'ouvre. L'onglet **Général** reprend les noms des modèles et les informations complémentaires sur le modèle ; l'onglet **Paramètres** reprend la liste des valeurs des paramètres de sécurité enregistrés dans le modèle.

Application du modèle de paramètres de sécurité

► *Pour appliquer les modèles de sécurité du modèle à l'entrée sélectionnée, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.

2. Dans le panneau des résultats de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.

3. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée pour laquelle vous souhaitez appliquer un modèle.
4. Sélectionnez **Appliquer un modèle → <Nom du modèle>**.
5. Dans l'arborescence de la console, ouvrez le menu contextuel du nom de la tâche à configurer.
6. Sélectionnez l'option **Enregistrer la tâche**.

Le modèle des paramètres de sécurité sera appliqué à l'entrée sélectionnée dans l'arborescence des ressources fichier du serveur. Sous l'onglet **Niveau de sécurité** de l'entrée sélectionnée, la valeur **Personnalisé** apparaîtra.

Les valeurs des paramètres de sécurité du modèle appliqué à l'entrée mère dans l'arborescence des ressources fichier du serveur sont appliquées à toutes les sous-entrées.

Si la zone de protection ou d'analyse des sous-entrées dans l'arborescence des ressources fichier du serveur a été configurée séparément, les paramètres de sécurité du modèle appliqué à l'entrée mère ne sont pas appliqués automatiquement aux sous-entrées.

► *Pour définir les paramètres de sécurité du modèle pour toutes les sous-entrées, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le panneau des résultats de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée pour laquelle vous souhaitez appliquer un modèle.
4. Sélectionnez **Appliquer un modèle → <Nom du modèle>**.
5. Dans l'arborescence de la console, ouvrez le menu contextuel de la tâche à configurer.
6. Sélectionnez l'option **Enregistrer la tâche**.

Le modèle des paramètres de sécurité sera appliqué à l'entrée mère et à toutes les sous-entrées dans l'arborescence des ressources fichier du serveur. Sous l'onglet **Niveau de sécurité** de l'entrée sélectionnée, la valeur **Personnalisé** apparaîtra.

Suppression du modèle de paramètres de sécurité

► *Pour supprimer un modèle de paramètres de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche pour la configuration de laquelle vous ne souhaitez plus utiliser un modèle de paramètres de sécurité.
2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

   Vous pouvez passer à la création d'un modèle de paramètres pour les tâches d'analyse à la demande depuis le panneau des résultats de l'entrée principale **Analyse à la demande**.

   La fenêtre **Modèles** s'ouvre.
3. Dans la liste des modèles de la fenêtre qui s'ouvre, sélectionnez le modèle que vous souhaitez supprimer.
4. Cliquez sur le bouton **Supprimer**.

   La fenêtre de confirmation de la suppression s'ouvre.
5. Dans la fenêtre de confirmation, cliquez sur **Oui**.

Le modèle sélectionné sera supprimé.

Si le modèle de paramètres de sécurité a été appliqué à la protection ou à l'analyse d'entrées des ressources fichiers du serveur, les paramètres de sécurité configurés pour ces entrées seront conservés après la suppression du modèle.

Protection en temps réel

Cette section présente les tâches de protection en temps réel : la tâche Protection des fichiers en temps réel, la tâche Analyse des scripts et la tâche Utilisation du KSN. La section contient également les instructions relatives à la configuration des paramètres des tâches de protection en temps réel et des paramètres de la sécurité du serveur protégé.

Dans cette section

Protection des fichiers en temps réel

Cette section contient des informations sur la tâche Protection des fichiers en temps réel et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Protection des fichiers en temps réel

Au cours de l'exécution de la tâche Protection des fichiers en temps réel, Kaspersky Security analyse les objets du serveur protégé suivants lorsqu'ils sont sollicités :

- les fichiers ;
- les flux alternatifs des systèmes de fichiers (flux NTFS) ;
- l'enregistrement principal de démarrage et les secteurs d'amorçage des disques durs locaux ou des périphériques externes.

Lorsqu'un programme quelconque enregistre un fichier sur le serveur ou tente de le lire, Kaspersky Security intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace, il exécute les actions définies : il tente de réparer le fichier, le place en quarantaine ou il le supprime. Kaspersky Security rend le fichier au programme uniquement s'il est sain ou si sa réparation a réussi.

> Le module Protection des fichiers en temps réel est disponible dans les suites logicielles suivantes : Kaspersky Security Standard, Kaspersky Security Basic, Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41).

Vous pouvez configurer les paramètres de la tâche Protection des fichiers en temps réel (cf. section « Configuration des paramètres de la tâche Protection des fichiers en temps réel » à la page 130).

Statistiques de la tâche Protection des fichiers en temps réel

Pendant que la tâche Protection des fichiers en temps réel est exécutée, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis le lancement de cette tâche jusqu'à maintenant.

► *Pour consulter les statistiques de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

L'onglet **Consultation et administration** dans le panneau des résultats du groupe **Statistiques**, affichera les statistiques actuelles de la tâche.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Si la valeur dans le champ **Total des événements** dans la fenêtre du journal d'exécution de la tâche de la Protection des fichiers en temps réel est plus que zéro, on recommande de procéder des événements dans l'onglet **Evénements** à la main.

Tableau 20. Statistiques de la tâche Protection des fichiers en temps réel

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security. Par exemple, si Kaspersky Security a découvert un programme malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres objets détectés	Nombre d'objets que Kaspersky Security détecte et classifie comme infectés ou nombre de fichiers de logiciels légitimes détectés, qui n'ont pas été exclus de l'analyse en temps réel et de la zone d'analyse des tâches à la demande, et qui ont été classés en tant que riskware.
Objets potentiellement infectés détectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Security.
Objets non réparés	Nombre d'objets que Kaspersky Security n'a pas pu réparer pour les raisons suivantes : • le type d'objet détecté ne peut être réparé ; • une erreur s'est produite lors de la réparation.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Security a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.

Champ	Description
Objets non supprimés	Nombre d'objets que Kaspersky Security a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone de protection que Kaspersky Security n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
Erreurs de traitement	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets réparés	Nombre d'objets réparés par Kaspersky Security.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Security.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Security.
Objets protégés par mot de passe	Nombre d'objets (archives, par exemple) que Kaspersky Security a ignorés en raison d'une protection par mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Security a ignorés à cause de leur format endommagé.
Objets traités	Nombre total d'objets traités par Kaspersky Security.

Configuration des paramètres de la tâche Protection des fichiers en temps réel

Par défaut, la tâche prédéfinie Protection des fichiers en temps réel contient les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 21. Paramètres par défaut de la tâche Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
Zone de protection	L'ensemble du serveur, à l'exception des disques virtuels	Vous pouvez limiter la zone de protection.
Niveau de sécurité	Identique pour toutes les zones de protection ; correspond au niveau de sécurité **Recommandé**.	Pour les entrées sélectionnées dans l'arborescence des ressources fichiers du serveur, vous pouvez : • appliquer un autre niveau de sécurité prédéfini ; • modifier manuellement le niveau de sécurité ; • enregistrer la configuration des paramètres de sécurité de l'entrée sélectionnée dans un modèle en vue de l'appliquer par la suite à n'importe quelle autre entrée.
Mode de protection	À l'accès et à la modification	Vous pouvez sélectionner le mode de protection des objets et indiquer dans quel type d'accès aux objets Kaspersky Security les analyse.
Analyseur heuristique	Le niveau de sécurité **Moyenne** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.

Paramètre	Valeur par défaut	Description
Zone de confiance	Appliquée Les programmes d'administration à distance **RemoteAdmin** ainsi que les fichiers recommandés par Microsoft Corporation sont exclus si, au moment de l'installation de Kaspersky Security, vous avez sélectionné **Ajouter les objets sous le masque not-a-virusRemoteAdmin* aux exclusions** et **Ajouter les exclusions recommandées par Microsoft**.	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.
Utilisation des services du KSN	Appliquée	Vous pouvez améliorer l'efficacité de la protection de l'ordinateur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Enrichissement de la liste des ordinateurs douteux	Pas appliqué	Vous pouvez activer l'ajout des ordinateurs qui manifestent une activité malveillante à la liste des ordinateurs douteux dans la tâche Blocage de l'accès aux fichiers réseau.
Planification du lancement de la tâche	Au lancement de l'application	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

► *Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, suivez le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Configurez les paramètres de la tâche suivants :

   - Sous l'onglet **Général** :

     - Mode de protection des objets (cf. section « Sélection du mode de protection des objets » à la page 133) ;
     - Application de l'analyseur heuristique (à la page 134) ;
     - Paramètres d'intégration aux autres modules de Kaspersky Security (cf. section "Intégration de la tâche aux autres modules de Kaspersky Security" à la page 136).

   - Sous les onglets **Planification** et **Avancé** :

     - Paramètres de lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

6. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, sélectionnez l'onglet **Configuration de la zone de la protection**.

7. Exécutez les actions suivantes :

   - Dans l'arborescence des ressources fichiers du serveur, sélectionnez les entrées que vous souhaitez inclure dans la zone de protection de la tâche (cf. section "A propos de la zone de protection de la tâche Protection des fichiers en temps réel" à la page142).

   - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section « Sélection des niveaux de sécurité prédéfinis » à la page 149) ou configurez manuellement les paramètres de protection des objets (cf. section « Configuration manuelle des paramètres de sécurité » à la page 152).

8. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Sélection du mode de protection des objets

La tâche Protection des fichiers en temps réel vous permet de sélectionner le mode de protection des objets. Le groupe **Mode de protection d'objets** permet de définir le type d'accès aux objets déclenchant une analyse par Kaspersky Security.

Le paramètre **Mode de protection d'objets** possède une valeur unique pour toutes les zones de protection reprises dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les nœuds particuliers.

► *Pour sélectionner le mode de protection des objets, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection des objets que vous souhaitez définir :

   - **Mode intelligent**.

     Kaspersky Security sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si un processus contacte et modifie plusieurs fois un objet pendant son exécution, Kaspersky Security analysera à nouveau cet objet uniquement après la dernière sauvegarde effectuée par ce processus.

   - **A l'accès e à la modification**.

     Kaspersky Security analyse l'objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié.

     Cette option est sélectionnée par défaut.

   - **A l'accès**.

     Kaspersky Security analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

   - **A l'exécution**.

     Kaspersky Security analyse le fichier uniquement en cas d'ouverture pour exécution.

5. Cliquez sur **OK**.

Le mode de protection des objets sélectionné sera adopté.

Application de l'analyseur heuristique

Vous pouvez, dans la tâche Protection des fichiers en temps réel, appliquer l'analyse heuristique et configurer le niveau de l'analyse.

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

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Cochez ou décochez la case **Utiliser l'analyseur heuristique**.

5. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

   Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

   Il existe trois niveaux de détail pour l'analyse

   - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
   - **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

     Il s'agit du niveau par défaut.
   - **Minutieuse**. L'analyseur heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

   Le curseur est actif quand la case **Utiliser l'analyseur heuristique** est cochée.

6. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Intégration de la tâche aux autres modules de Kaspersky Security

La tâche Protection des fichiers en temps réel vous permet de configurer les paramètres d'intégration de la tâche aux autres modules opérationnels de Kaspersky Security.

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN.

Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer une tâche manuellement (cf. section "Lancement et arrêt d'une tâche Utilisation du KSN" à la page 166) ou planifier son exécution (cf. section "Configuration des paramètres d'une tâche Utilisation du KSN" à la page 167).

► *Pour configurer les interactions entre la tâche Protection des fichiers en temps réel et les autres modules de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Configurez les paramètres suivants dans le groupe **Intégration aux autres composants de Kaspersky Security** :

   - Cochez ou décochez la case **Appliquer la zone de confiance**.

     La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

     Si la case est cochée, Kaspersky Security ajoute les opérations de fichiers des processus de confiance aux exclusions de l'analyse définies dans la configuration des paramètres de la tâche.

     Si la case est décochée, Kaspersky Security ne prend pas en compte les opérations de fichiers des processus de confiance lors de la création de la zone de protection dans la tâche Protection des fichiers en temps réel.

     Cette case est cochée par défaut.

- Cochez ou décochez la case **Utiliser le KSN pour la protection**.

  La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

  Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

  Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

  Cette case est cochée par défaut.

- Cochez ou décochez la case **Ajouter les ordinateurs à l'origine de l'activité malveillante à la liste des ordinateurs douteux**.

  La case active ou désactive le blocage de l'accès aux fichiers réseau pour les ordinateurs ayant été identifiés comme présentant une activité de chiffrement lors des tâches de protection contre le chiffrement et de protection des fichiers en temps réel.

  Si la case est cochée, l'application bloque l'accès au stockage réseau à protéger pour les ordinateurs de la part desquels une activité malveillante a été détectée. La liste des ordinateurs bloqués est affichée dans le panneau des résultats de l'entrée **Blocage de l'accès aux fichiers réseau**. Vous pouvez indiquer la durée de blocage des ordinateurs dans les propriétés de la tâche Blocage de l'accès aux fichiers réseau.

  Si la case est décochée, l'application ne bloque pas l'accès au stockage réseau à protéger pour les ordinateurs de la part desquels une activité malveillante a été détectée.

  Cette case est décochée par défaut.

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Liste des extensions de fichiers analysés par défaut dans la tâche Protection des fichiers en temps réel

Kaspersky Security analyse par défaut les fichiers possédant les extensions suivantes :

- *386*
- *acm*
- *ade*, *adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*
- *chm*
- *cla*, *clas**
- *cmd*
- *com*
- *cpl*
- *crt*
- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*

- *efi*
- *emf*
- *eml*
- *exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm*, *html**
- *htt*
- *ico*
- *inf*
- *ini*
- *ins*
- *isp*
- *jpg*, *jpe*
- *js*, *jse*
- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*
- *msp*
- *mst*

- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*
- *pht*
- *phtm**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*
- *shb*
- *shs*
- *sht*

- *shtm**
- *swf*
- *sys*
- *the*
- *them**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*
- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

Zone de protection dans la tâche Protection des fichiers en temps réel

Cette section contient des informations sur la constitution et l'utilisation de la zone de protection dans la tâche Protection des fichiers en temps réel et sur son utilisation.

Dans cette section

Présentation de la zone de protection dans la tâche Protection des fichiers en temps réel

Par défaut, la tâche Protection des fichiers en temps réel protège tous les objets du système de fichiers du serveur. Si les exigences en matière de sécurité ne requièrent pas la protection de tous les objets du système de fichiers, vous pouvez limiter la zone de protection.

Dans la Console de Kaspersky Security, la zone de protection se présente sous la forme d'une arborescence de ressources fichiers du serveur que l'application peut contrôler.

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrés de la manière suivante :

☑ Nœud repris dans la zone de protection.

☐ Nœud exclu de la zone de protection.

☑ Au moins un des nœuds intégrés à ce nœud est exclu de la zone de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

L'icône ☑ s'affiche si toutes les sous-entrées ont été sélectionnées mais pas l'entrée mère. Dans ce cas, les modifications du contenu des fichiers et dossiers de l'entrée mère ne sont pas automatiquement prises en compte lors de la constitution de la zone de protection de la sous-entrée.

Le nom des nœuds virtuels de la zone de protection apparaît en lettres bleues.

Zones de protection prédéfinies

L'arborescence des ressources fichiers du serveur est affichée dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel** via le lien **Configuration de la zone de la protection**.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

L'arborescence des ressources fichiers du serveur contient les zones de protection prédéfinies suivantes :

- **Disques durs locaux**. Kaspersky Security protège les fichiers sur les disques durs du serveur.
- **Disques amovibles**. Kaspersky Security protège les fichiers sur les périphériques externes tels que les disques compacts ou amovibles. Vous pouvez inclure ou exclure de la zone de protection tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.

- **Emplacements réseau**. Kaspersky Security protège les fichiers qui sont enregistrés dans les répertoires réseau ou qui y sont lus par les applications exécutées sur le serveur. Kaspersky Security ne protège pas les fichiers dans les répertoires réseau lorsqu'ils sont sollicités par des applications d'autres ordinateurs.

- **Unités virtuelles**. Vous pouvez inclure dans la zone de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe.

La zone de protection inclut par défaut tous les secteurs prédéfinis, à l'exception des disques virtuels.

Les pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la Console de Kaspersky Security. Pour inclure les objets d'un pseudo-disque dans la zone de protection, il faut inclure le répertoire du serveur auquel ce pseudo-disque est lié.

Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. Pour inclure les objets d'un disque de réseau dans la zone de protection, indiquez le chemin d'accès au répertoire correspondant à ce disque de réseau au format UNC (Universal Naming Convention).

Constitution de la zone de protection

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

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de la protection** s'ouvre.

4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.

5. Déployez l'arborescence des ressources fichiers du serveur pour afficher toutes les entrées et procédez comme suit :

    - Pour exclure certaines entrées de la zone de protection, décochez les cases à côté des noms de ces entrées.

    - Pour inclure certaines entrées à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :

        - si vous souhaitez inclure tous les disques d'un même type, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**) ;
        - Si vous souhaitez inclure un disque particulier du type requis, déployez le nœud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque. Par exemple, pour sélectionner le disque amovible **F:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:** ;
        - si vous souhaitez inclure à la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case à côté de ce dossier ou de ce fichier.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Vous pouvez également composer une zone de protection à l'aide du bouton **Ajouter**, disponible en mode de consultation **Afficher sous forme de liste**.

Vous ne pourrez exécuter la tâche **Protection des fichiers en temps réel** que si au moins un nœud de l'arborescence des ressources fichiers du serveur est inclus dans la zone de protection.

Si vous définissez une zone de protection complexe, par exemple en attribuant différentes valeurs aux paramètres de sécurité pour divers nœuds distincts de l'arborescence des ressources fichiers du serveur, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.

A propos de la zone de protection virtuelle

Kaspersky Security peut analyser non seulement les fichiers et les répertoires existants sur les disques durs et les disques amovibles mais également ceux présents sur les disques qui sont montés temporairement sur le serveur, par exemple les disques partagés de la grappe ou les fichiers et les répertoires qui sont créés dynamiquement sur le serveur par diverses applications et services.

Si vous avez inclus tous les objets du serveur dans la zone de protection, ces nœuds dynamiques seront automatiquement repris dans la zone de protection. Toutefois, si vous souhaitez attribuer des valeurs particulières aux paramètres de protection de ces nœuds dynamiques ou si vous avez sélectionné pour la protection en temps réel non pas tout le serveur, mais uniquement quelques secteurs, alors pour pouvoir inclure les disques, les fichiers ou les répertoires dans la zone de protection, vous devrez d'abord les créer dans la Console de Kaspersky Security ; c'est ce que l'on appelle la création d'une zone de protection virtuelle. Les disques, les fichiers ou les répertoires que vous créez existent uniquement dans la Console de Kaspersky Security et non pas dans la structure du système de fichiers du serveur protégé.

Si au moment de composer la zone de protection, vous sélectionnez tous les fichiers ou les répertoires inclus sans choisir le répertoire parent, les répertoires ou les fichiers dynamiques qui s'y trouvent ne seront pas repris automatiquement dans la zone de protection. Vous devez créer des "copies virtuelles" dans la Console de Kaspersky Security et les ajouter à la zone de protection.

Création d'une zone de protection virtuelle

Vous pouvez ajouter à la zone de protection/d'analyse des disques virtuels des dossiers ou des fichiers distincts uniquement si la zone de protection/d'analyse se présente sous la forme d'une arborescence des ressources fichiers.

► *Pour ajouter à la zone de protection un disque virtuel, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de la protection** s'ouvre.

4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.

5. Ouvrez le menu contextuel de l'entrée **Unités virtuelles** et choisissez le nom du disque virtuel à créer dans la liste des noms disponibles

6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone de protection.

7. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

► *Pour ajouter un dossier ou un fichier virtuel dans la zone de protection, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de la protection** s'ouvre.

4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.

5. Ouvrez le menu contextuel du disque virtuel auquel vous souhaitez ajouter un dossier ou un fichier, puis choisissez une des options suivantes :

   - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone de protection.

   - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone de protection.

6. Dans le champ, saisissez le nom du dossier ou du fichier.

   Vous pouvez définir un masque de nom de fichier en utilisant les caractères * et ?.

7. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone de protection.

8. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Paramètres de sécurité de l'entrée sélectionnée dans la tâche Protection des fichiers en temps réel

Dans la tâche Protection des fichiers en temps réel, vous pouvez modifier les valeurs des paramètres de sécurité par défaut de la même manière pour toute la zone de protection ou d'analyse ou avec des variations pour divers nœuds dans l'arborescence des ressources fichier du serveur.

Les paramètres de sécurité configurés pour l'entrée mère sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Vous pouvez configurer les paramètres de la zone d'analyse sélectionnée de l'une des manières suivantes :

- Sélectionner un des trois niveaux de sécurité prédéfinis (**Performance maximale**, **Recommandé** ou **Protection maximale**) ;
- Modifier manuellement les paramètres de sécurité pour les entrées sélectionnées de l'arborescence des ressources fichiers du serveur (le niveau de sécurité prend alors la valeur **Personnalisé**).

Vous pouvez enregistrer la sélection de paramètres du nœud dans un modèle afin de l'appliquer à d'autres nœuds.

Sélection des niveaux prédéfinis de sécurité

Pour les nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivant : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Performance maximale

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 22. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Protection des objets	Selon l'extension	En fonction du format	En fonction du format
Optimisation	Activée	Activée	Désactivée

Paramètres	Niveau de sécurité		
Actions à exécuter sur les objets infectés	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible
Action à exécuter sur les objets probablement infectés	Quarantaine	Quarantaine	Quarantaine
Exclure les objets	Non	Non	Non
Ne pas détecter	Non	Non	Non
Arrêter si l'analyse dure plus de (s.)	60 s	60 s	60 s
Ne pas analyser les objets composés de plus de (Mo)	8 Mo	8 Mo	Non défini
Analyser les flux NTFS alternatifs	Oui	Oui	Oui
Analyser les secteurs d'amorçage et la partition MBR	Oui	Oui	Oui
Protection des objets composés	• Objets compactés* • Uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* • Uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* *Tous les objets

Les paramètres **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Application de l'analyse heuristique** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si, après avoir choisi un des niveaux de protection prédéfini, vous modifiez les paramètres de protection **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyseur heuristique**, le niveau prédéfini que vous aviez choisi ne change pas**.**

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de la protection** s'ouvre.
4. Sélectionnez l'entrée pour laquelle vous souhaitez sélectionner un niveau de sécurité prédéfini.
5. Confirmez que ce nœud est repris dans la zone de protection.
6. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez dans la liste le niveau de sécurité que vous souhaitez appliquer.

   La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau que vous avez sélectionné.
7. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Configuration manuelle des paramètres de sécurité

Par défaut, la tâche Protection des fichiers en temps réel applique les mêmes paramètres de sécurité à toutes les zones de protection. Leurs valeurs correspondent aux valeurs du niveau de sécurité prédéfini **Recommandé** (cf. section « **Sélection des niveaux de sécurité prédéfinis** » à la page 149).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour divers nœuds dans l'arborescence des ressources fichier du serveur.

Les paramètres de sécurité configurés pour l'entrée mère sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Kaspersky Security n'analyse pas les archives crées avec certains algorithmes de la compression. Vous trouverez les informations détaillées sur la page de l'application dans la Base de la connaissance.

► *Pour configurer manuellement les paramètres de sécurité du nœud sélectionné, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le panneau des résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de la protection** s'ouvre.
4. Dans la partie gauche de la fenêtre, sélectionnez l'entrée dont vous souhaitez configurer les paramètres de sécurité.

   Pour la zone de protection sélectionnée, vous pouvez appliquer un modèle prédéfini contenant un ensemble de paramètres de sécurité (cf. section "A propos des modèles de paramètres de sécurité" à la page 121).

5. Configurez les paramètres de sécurité requis pour le nœud sélectionné en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, configurez les paramètres suivants, si nécessaire :

     Dans le groupe **Protection des objets**, indiquez les objets que vous souhaitez inclure à la zone de protection :

     - **Tous les objets** ;

       Kaspersky Security analyse tous les objets.

     - **Objets analysés en fonction du format** ;

       Kaspersky Security analyse uniquement les fichiers infectables sur la base du format du fichier.

       La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus** ;

       Kaspersky Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

       La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée** ;

       Kaspersky Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

     - **Secteurs d'amorçage des disques MBR** ;

       Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

       Quand la case est cochée, Kaspersky Security analyse les secteurs et les enregistrements d'amorçage sur les disques durs et les disques amovibles du serveur.

Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**.

  Analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

  Quand la case est cochée, Kaspersky Security analyse les flux complémentaires des fichiers et des dossiers.

  Cette case est cochée par défaut.

Dans le groupe **Optimisation**, cochez ou décochez la case :

- **Analyse uniquement des nouveaux fichiers et des fichiers modifiés**.

  La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security a identifié comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

  Quand la case est cochée, Kaspersky Security analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Security analyse et protège tous les fichiers.

  La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Recommandé** ou **Protection maximale**, la case est décochée.

Dans le groupe **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :

- **Toutes les / Les nouvelles archives** ;

  Analyse des archives au format ZIP (sauf BZip2, LZMA, PPMd algorithmes de la compression), CAB, RAR, ARJ et autres.

  Si la case est cochée, Kaspersky Security analyse les archives.

  Si la case est décochée, Kaspersky Security ignore les archives lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Toutes les / Les nouvelles archives SFX** ;

  Analyse des archives qui contiennent un module logiciel de décompactage.

  Si la case est cochée, Kaspersky Security analyse les archives SFX.

  Si la case est décochée, Kaspersky Security ignore les archives SFX lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données de messagerie** ;

  Analyse des fichiers des bases de données de messagerie de Microsoft Office Outlook® et Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Security analyse les fichiers des bases de données de messagerie.

  Quand la case est décochée, Kaspersky Security ignore les fichiers des bases de données de messagerie lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / les nouveaux objets compactés** ;

  Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

  Quand la case est cochée, Kaspersky Security analyse les fichiers exécutables compactés par des logiciels de compression.

  Quand la case est décochée, Kaspersky Security ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux messages de texte plat** ;

  Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Security analyse les fichiers aux formats de messagerie.

Quand la case est décochée, Kaspersky Security ignore les fichiers aux formats de messagerie lors de l'analyse.

- **Tous les / Les nouveaux objets OLE incorporés**.

  Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

  Si la case est cochée, Kaspersky Security analyse les objets intégrés au fichier.

  Quand la case est décochée, Kaspersky Security ignore les objets intégrés au fichier lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

> Vous pouvez choisir de protéger tous les objets composés ou uniquement les nouveaux si la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés** est cochée. Si la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés** est décochée, Kaspersky Security protège tous les objets composés désignés.

- Sous l'onglet **Actions**, configurez les paramètres suivants, si nécessaire :
  - Sélectionnez l'action à exécuter sur les objets infectés.
  - Sélectionnez l'action à exécuter sur les objets probablement infectés.
  - Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter.
- Sous l'onglet **Optimisation**, configurez les paramètres suivants, si nécessaire :

  Dans le groupe **Exclusions** :

  - **Exclure les fichiers** ;

    Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

    Si la case est cochée, Kaspersky Security ignore les objets indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Security analyse tous les objets.

Cette case est décochée par défaut.

- **Ne pas détecter**.

  Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque de nom d'objet à détecter. Par exemple, vous pouvez exclure les utilitaires d'administration à distance à l'aide du masque `not-a-virus:RemoteAdmin*`. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

  Si la case est cochée, Kaspersky Security ignore les objets à détecter indiqués pendant l'analyse.

  Si la case est décochée, Kaspersky Security détecte tous les objets indiqués par défaut dans l'application.

  Cette case est décochée par défaut.

Dans le groupe **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)** ;

  Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

  Si la case est cochée, la durée maximale de l'analyse d'un objet est égale à la valeur indiquée.

  Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

  Cette case est cochée par défaut.

- **Ne pas analyser les objets composés de plus de (Mo)** ;

  Exclut de l'analyse les objets complexes dont la taille est supérieure à la valeur indiquée. La valeur par défaut est de 8 Mo.

  Si la case est cochée, Kaspersky Security n'analyse pas les objets complexes dont la taille est supérieure à la valeur indiquée.

  Si la case est décochée, Kaspersky Security analyse les objets complexes sans tenir compte de la taille.

  La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- **Utiliser la technologie iChecker** ;

Analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse.

Si la case est cochée, Kaspersky Security analyse uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

Si la case est décochée, Kaspersky Security analyse les fichiers sans tenir compte de la date de création ou de modification.

Cette case est cochée par défaut.

- **Utiliser la technologie iSwift**.

  Analyse uniquement des nouveaux objets ou des fichiers objets depuis la dernière analyse dans le système de fichiers NTFS.

  Si la case est cochée, Kaspersky Security analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse du système de fichiers NTFS.

  Si la case est décochée, Kaspersky Security analyse les objets du système de fichiers NTFS sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Analyse des scripts

Cette section contient des informations sur la tâche Analyse des scripts et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Analyse des scripts

Au cours de l'exécution de la tâche Analyse des scripts, Kaspersky Security contrôle l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies (ou Active Scripting), par exemple les scripts VBScript ou JScript®. Kaspersky Security autorise l'exécution d'un script uniquement s'il le considère comme inoffensif. Kaspersky Security interdit l'exécution d'un script qu'il juge dangereux. Si Kaspersky Security a considéré un script comme potentiellement dangereux, il exécute l'action que vous avez choisie : interdiction ou autorisation de l'exécution de ce script.

Par défaut, la tâche Analyse des scripts est exécutée automatiquement au démarrage de Kaspersky Security.

Le module Analyse des scripts n'est pas installé par défaut sur le serveur car l'exécution de cette tâche peut provoquer des erreurs de serveur.

L'utilisation de ce module peut réduire la capacité de protection du serveur et elle est déconseillée par les experts de Kaspersky Lab, sauf en cas de nécessité.

Si vous souhaitez utiliser le module Analyse des scripts, il faut le sélectionner dans la liste des modules à installer manuellement lors de l'installation de Kaspersky Security.

Le *Manuel d'installation de Kaspersky Security 10 for Windows Server* présente en détails la sélection des modèles de l'application lors de l'installation.

Vous pouvez configurer les paramètres de la tâche Analyse des scripts (cf. section "Configuration des paramètres de la tâche Analyse des scripts" à la page 160).

Le module Analyse des scripts est disponible dans les suites logicielles suivantes : Kaspersky Security Standard, Kaspersky Security Basic, Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41).

Configuration des paramètres de la tâche Analyse des scripts

La tâche prédéfinie Analyse des scripts possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 23. Paramètres par défaut de la tâche Analyse des scripts

Paramètre	Valeur par défaut	Description
Exécution de scripts dangereux	Interdit	Kaspersky Security interdit toujours l'exécution des scripts qu'il considère dangereux.
Exécution de scripts potentiellement dangereux	Interdit	Vous pouvez indiquer les actions à effectuer en cas de détection de scripts potentiellement dangereux : interdire ou autoriser leur exécution.
Analyseur heuristique	Le niveau de sécurité **Moyenne** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Zone de confiance	Appliquée	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.

► *Pour configurer la tâche Analyse des scripts, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez la sous-entrée **Analyse des scripts**.

3. Dans le panneau des résultats de l'entrée, suivez le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Dans le groupe **Actions à exécuter sur les scripts présumés dangereux**, réalisez l'une des opérations suivantes :

   - Si vous souhaitez autoriser l'exécution des scripts potentiellement dangereux, sélectionnez l'option **Autoriser l'exécution**.

     Kaspersky Security autorise l'exécution du script présumé dangereux.

   - Si vous souhaitez interdire l'exécution des scripts potentiellement dangereux, sélectionnez l'option **Interdire l'exécution**.

     Kaspersky Security empêche l'exécution du script présumé dangereux.

     Cette option est sélectionnée par défaut.

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

   - Cochez ou décochez la case **Utiliser l'analyseur heuristique**.

     La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

     Quand la case est cochée, l'analyse heuristique est activée.

     Quand la case est décochée, l'analyse heuristique est désactivée.

     Cette case est cochée par défaut.

   - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

     Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

     Il existe trois niveaux de détail pour l'analyse

     - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.

- **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

  Il s'agit du niveau par défaut.

- **Minutieuse**. L'analyseur heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyseur heuristique** est cochée.

6. Dans le groupe **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.

   La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

   Si la case est cochée, Kaspersky Security ajoute les opérations de fichiers des processus de confiance aux exclusions de l'analyse définies dans la configuration des paramètres de la tâche.

   Si la case est décochée, Kaspersky Security ne prend pas en compte les opérations de fichiers des processus de confiance lors de la création de la zone de protection dans la tâche Protection des fichiers en temps réel.

   Cette case est cochée par défaut.

7. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Statistiques de la tâche Analyse des scripts

Au cours de l'exécution de la tâche Analyse des scripts, vous pouvez consulter les informations sur la quantité de scripts traités par Kaspersky Security entre le moment de lancement de la tâche et le moment présent.

► *Pour consulter les statistiques de la tâche Analyse des scripts, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez la sous-entrée **Analyse des scripts**.

   Le groupe **Statistiques**, sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée, affichera les statistiques actuelles de la tâche.

Vous pouvez consulter les informations sur les objets que Kaspersky Security a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 24. Statistiques de la tâche Analyse des scripts

Champ	Description
Nombre de scripts bloqués	Nombre de script dont l'exécution a été interdite par Kaspersky Security.
Scripts dangereux	Nombre de scripts dangereux découverts.
Scripts présumés dangereux détectés	Nombre de scripts potentiellement dangereux découverts.
Scripts traités	Nombre total de scripts traités.

Utilisation du KSN

Cette section contient des informations sur la tâche Utilisation du KSN et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Utilisation du KSN

Le *Kaspersky Security Network* (ci-après, KSN) est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des applications. L'utilisation des données du Kaspersky Security Network assure une vitesse de réaction plus élevée de Kaspersky Security face aux nouvelles menaces, augmente l'efficacité de certains modules de la protection et réduit la possibilité de faux positifs.

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN.

Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer une tâche manuellement (cf. section "Lancement et arrêt d'une tâche Utilisation du KSN" à la page 166) ou planifier son exécution (cf. section "Configuration des paramètres d'une tâche Utilisation du KSN" à la page 167).

Kaspersky Security obtient uniquement du Kaspersky Security Network les informations sur la réputation des applications.

La participation des utilisateurs au KSN 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 des modules de l'application.

Pendant l'utilisation du KSN, des statistiques définies obtenues suite au fonctionnement de Kaspersky Security sont automatiquement envoyées à Kaspersky Lab.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour de plus amples informations sur la collecte, le traitement, la conservation et la destruction des informations sur l'utilisation de l'application, vous pouvez consulter le Règlement du KSN sous l'onglet **Règlement du KSN** dans la fenêtre des propriétés de la tâche Utilisation du KSN, et sur le site Internet de Kaspersky Lab http://www.kaspersky.com/fr/privacy.

La participation au Kaspersky Security Network est volontaire. La décision de participer au Kaspersky Security Network peut être prise après installation de Kaspersky Security, et peut être modifiée à tout moment (cf. section "Lancement et arrêt d'une tâche Utilisation de KSN" à la page 166).

Kaspersky Security Network peut être utilisé dans les tâches suivantes de Kaspersky Security :

- Protection des fichiers en temps réel (cf. section « Configuration des paramètres de la tâche Protection des fichiers en temps réel » à la page 130).
- Analyse à la demande (cf. section "Configuration des paramètres de la tâche d'analyse à la demande" à la page 222).
- Contrôle du lancement des applications (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page 181).
- Protection des stockages réseau connectés via le protocole ICAP ;

  > Kaspersky Security ne peut supprimer ou bloquer des fichiers utilisés par des stockages de réseau connectés via le protocole ICAP car au moment de la réception d'une réponse négative des services KSN, l'application ne dispose pas d'un accès direct aux catalogues réseau du stockage. Les informations relatives à la réception d'une réponse négative sont consignées dans le journal d'exécution de la tâche Utilisation du KSN.

- Protection des stockages réseau connectés via le protocole RPC ;

Le module Utilisation du KSN est disponible dans les suites logicielles suivantes : Kaspersky Security Standard, Kaspersky Security Basic, Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41).

Lancement et arrêt de la tâche Utilisation du KSN

Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer l'exécution de la tâche manuellement.

► *Pour lancer la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Sélectionnez l'onglet **Règlement du KSN**.
5. Cochez la case **J'accepte les conditions de prestation des services du KSN** si vous acceptez les conditions de la Déclaration de Kaspersky Security Network et souhaitez activer l'utilisation du KSN.

   Si la case **J'accepte les conditions de prestation des services du KSN** est décochée pendant le fonctionnement de la tâche Utilisation du KSN, cette tâche sera interrompue.
6. Cliquez sur le bouton **OK**.

   Les modifications apportées aux paramètres de la tâche seront enregistrées.
7. Dans le groupe **Administration** du panneau des résultats de l'entrée **Utilisation du KSN**, suivez le lien **Démarrer**.

La tâche Utilisation du KSN sera lancée.

Le lancement de la tâche Utilisation du KSN est impossible si le Règlement du KSN n'a pas été accepté. Avant de lancer la tâche, assurez-vous que la case **J'accepte les conditions de prestation des services du KSN** est cochée.

► *Pour arrêter la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la console, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le groupe **Administration** du panneau des résultats de l'entrée **Utilisation du KSN**, cliquez sur le lien **Arrêter**.

La tâche Utilisation du KSN sera arrêtée.

Configuration de la tâche Utilisation du KSN

La tâche Utilisation du KSN possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 25. Paramètres par défaut de la tâche Utilisation du KSN

Paramètre	Valeur par défaut	Description
Actions à exécuter sur les objets infectés	Supprimer	Vous pouvez préciser les actions que Kaspersky Security exécutera sur les objets réputés comme étant infectés dans le KSN.
Productivité	La somme de contrôle (hash MD5) est calculée pour les fichiers dont la taille ne dépasse pas 2 Mo.	Vous pouvez définir la taille maximale des fichiers dont la somme de contrôle sera calculée à l'aide de l'algorithme MD5 pour envoi à KSN. Si la case est décochée, Kaspersky Security calcule les hash MD5 pour les fichiers de n'importe quelle taille.
Règlement du KSN	La case **J'accepte les conditions de prestation des services du KSN** est décochée.	Vous pouvez modifier votre choix concernant l'utilisation du KSN à tout moment.

Paramètre	Valeur par défaut	Description
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer les paramètres de la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Configurez les paramètres de la tâche :

   - Dans le groupe **Actions à exécuter sur les objets infectés**, indiquez l'action que Kaspersky Security doit exécuter en cas de détection d'un objet réputé infecté dans le KSN :

     - **Supprimer**.

       Kaspersky Security supprime l'objet considéré comme infecté selon les données du KSN et place une copie de celui-ci dans la sauvegarde.

       Cette option est sélectionnée par défaut.

     - **Consigner les informations dans le rapport**.

       Kaspersky Security consigne dans le journal d'exécution des tâches les informations sur l'objet considéré comme infecté selon les données du KSN détecté. Kaspersky Security ne supprime pas l'objet infecté.

- Dans le groupe **Optimisation**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :

    a. Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi au KSN si la taille du fichier dépasse (Mo)**.

    La case active ou désactive le calcul de la somme de contrôle des fichiers d'une taille définie pour l'envoi de ces informations au service KSN.

    La durée du calcul de la somme de contrôle dépend de la taille du fichier.

    Si la case est cochée, Kaspersky Security ne calcule pas la somme de contrôle pour les fichiers dont la taille dépasse la valeur définie (Mo).

    Si la case est décochée, Kaspersky Security calcule la somme de contrôle pour les fichiers de n'importe quelle taille.

    Cette case est cochée par défaut.

    b. Le cas échéant, saisissez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Security calculera la somme de contrôle.

5. Si nécessaire, configurez la planification du lancement de la tâche sous les onglets **Planification** et **Avancé**. Par exemple, vous pouvez activer le lancement d'une tâche planifiée et choisir la fréquence de lancement **Au lancement de l'application**, si vous souhaitez que la tâche soit lancée automatiquement après le redémarrage de l'ordinateur.

   L'application lancera la tâche Utilisation du KSN selon la planification.

   Le lancement de la tâche Utilisation du KSN est impossible si le Règlement du KSN n'a pas été accepté. Avant de lancer la tâche, assurez-vous que la case **J'accepte les conditions de prestation des services du KSN**, sous l'onglet **Règlement du KSN** est cochée.

6. Cliquez sur **OK**.

Les modifications des paramètres de la tâche seront appliquées. La date et l'heure de modification des paramètres, ainsi que les informations sur les paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Statistiques de la tâche Utilisation du KSN

Pendant que la tâche Utilisation du KSN est exécutée, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis son lancement jusqu'à maintenant. Les informations relatives à tous les événements survenus pendant l'exécution d'une tâche sont consignées dans le journal d'exécution de la tâche (cf. section "A propos des journaux d'exécution des tâches" à la page 307).

► *Pour consulter les statistiques de la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez la sous-entrée **Utilisation du KSN**.

L'onglet **Consultation et administration** dans le panneau des résultats du groupe **Statistiques**, affichera les statistiques actuelles de la tâche.

Vous pouvez consulter les informations sur les objets que Kaspersky Security a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 26. Statistiques de la tâche Utilisation du KSN

Champ	Description
Requêtes fichier envoyées	Nombre de requêtes sur la réputation de fichiers que Kaspersky Security a envoyées aux services du KSN pour examen.
Conclusions suspectes reçues	Nombre d'objets identifiés comme douteux par les services du KSN.
Erreurs d'envoi des requêtes	Nombre de requêtes à KSN dont le traitement a entraîné une erreur de tâche.
Objets supprimés	Nombre d'objets que Kaspersky Security a supprimé suite au fonctionnement de la tâche Utilisation du KSN.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security.

Champ	Description
Objets non supprimés	Nombre d'objets que Kaspersky Security a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque. L'application ne répare pas et ne supprime pas les fichiers qui n'ont pas pu être placés dans la sauvegarde. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.

Contrôle du serveur

Cette section contient des informations sur la fonctionnalité de Kaspersky Security relative au contrôle de l'accès aux fichiers réseau et au contrôle des applications exécutées sur le serveur.

Dans cette section

Blocage de l'accès aux fichiers réseau

Cette section contient des informations sur la tâche Blocage de l'accès aux fichiers réseau et les instructions sur la configuration de cette tâche.

Dans cette section

Présentation de la tâche Blocage de l'accès aux fichiers réseau

La tâche de blocage de l'accès aux fichiers réseau permet de protéger le serveur sur lequel est installé Kaspersky Security contre les programmes malveillants. La tâche empêche les ordinateurs distants d'accéder aux fichiers publics du serveur, si lors de l'exécution de la tâche Protection des fichiers en temps réel ou Protection contre le chiffrement, une activité malveillante ou de chiffrement a été détectée de la part des ordinateurs distants accédant aux fichiers réseau.

Les informations relatives aux ordinateurs bloqués sont accessibles dans la liste des ordinateurs douteux (cf. section "Modification de la liste des ordinateurs douteux" à la page 175) qui s'ouvre via le lien **Liste des ordinateurs douteux** de l'entrée **Blocage de l'accès aux fichiers réseau**.

La liste des ordinateurs douteux se remplit au cours de l'exécution des tâches Protection des fichiers en temps réel et Protection contre le chiffrement. Kaspersky Security ne bloque pas l'accès aux ordinateurs ajoutés à la liste si la tâche Blocage de l'accès aux fichiers réseau n'est pas lancée.

Le module Blocage de l'accès aux fichiers réseau est disponible dans les suites logicielles suivantes : Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41). Le module n'est pas disponible sur abonnement.

Lancement de la tâche Blocage de l'accès aux fichiers réseau

► *Pour activer le blocage de l'accès aux fichiers réseau pour les ordinateurs ayant une activité malveillante ou de chiffrement, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre des paramètres de la tâche, sous l'onglet **Général**, s'ouvre.

4. Dans le groupe **Paramètres avancés**, cochez la case **Bloquer les ordinateurs ayant une activité malveillante**, si vous souhaitez que Kaspersky Security empêche les ordinateurs pour lesquels une activité malveillante a été détectée lors de l'exécution des tâches Protection des fichiers en temps réel ou Protection contre le chiffrement, d'accéder aux fichiers réseau.

5. Cliquez sur le bouton **OK** dans la fenêtre des paramètres de la tâche Protection des fichiers en temps réel.

   Les paramètres de la tâche définis seront enregistrés.

6. Sous l'onglet **Consultation et administration**, dans le groupe **Administration**, cliquez sur le lien **Démarrer** afin de lancer la tâche de Protection des fichiers en temps réel, si celle-ci n'est pas déjà en cours d'exécution.

7. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

8. Sélectionnez la sous-entrée **Protection contre le chiffrement**.

9. Dans le panneau des résultats du groupe **Administration**, cliquez sur le bouton **Démarrer** afin de lancer la tâche de Protection contre le chiffrement, si celle-ci n'est pas déjà en cours d'exécution.

10. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

11. Sélectionnez la sous-entrée **Blocage de l'accès aux fichiers réseau**.

12. Dans le panneau des résultats du groupe **Administration**, cliquez sur le bouton **Démarrer** afin de lancer la tâche de Blocage de l'accès aux fichiers réseau, si celle-ci n'est pas déjà en cours d'exécution.

13. Sous les onglets **Planification** et **Avancé**, de la fenêtre **Paramètres de la tâche**, configurez, si nécessaire, la planification de lancement de la tâche. Par exemple, vous pouvez activer le lancement d'une tâche planifiée et choisir la fréquence de lancement **Au lancement de l'application**, si vous souhaitez que la tâche soit lancée automatiquement après le redémarrage de l'ordinateur.

La tâche Blocage de l'accès aux fichiers réseau sera lancée. En cas de détection d'une activité malveillante ou de chiffrement de la part d'un ordinateur distant accédant au serveur, Kaspersky Security bloque l'accès de cet ordinateur aux fichiers réseau.

Modification de la liste des ordinateurs douteux

La liste des ordinateurs douteux contient des informations relatives aux ordinateurs à l'origine d'une activité malveillante ou de chiffrement et découverts pendant l'exécution des tâches Protection des fichiers en temps réel et Protection contre le chiffrement ou bloqués pendant l'exécution de la tâche Blocage de l'accès aux fichiers réseau.

Si la tâche Blocage de l'accès aux fichiers réseau n'est pas lancée, la liste des ordinateurs douteux reprend les périphériques à l'origine de l'activité malveillante ou de chiffrement, mais l'accès de ces périphériques aux fichiers réseau n'est pas bloqué.

Vous pouvez restaurer l'accès aux fichiers réseau sur des ordinateurs bloqués antérieurement ou purger la liste des ordinateurs douteux.

► *Pour restaurer l'accès pour des ordinateurs bloqués antérieurement ou pour supprimer les ordinateurs de la liste des ordinateurs douteux, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Blocage de l'accès aux fichiers réseau**.
3. Dans le panneau des résultats du groupe **Propriétés**, cliquez sur le lien **Liste des ordinateurs douteux**.
4. Exécutez une des actions suivantes :
   - Dans la fenêtre **Liste des ordinateurs douteux** qui s'ouvre, sélectionnez les modules auxquels vous souhaitez restaurer l'accès, puis cliquez sur le bouton **Supprimer de la liste**.
   - Cliquez sur le bouton **Purger toute la liste** pour supprimer les ordinateurs de la liste des ordinateurs douteux ou pour rétablir l'accès pour tous les ordinateurs bloqués.
5. Cliquez sur le bouton **OK**.

Les ordinateurs sélectionnés seront débloqués ou supprimés de la liste des ordinateurs douteux.

Configuration des paramètres de déblocage automatique de l'accès des ordinateurs au serveur

Vous pouvez indiquer la durée au terme de laquelle les ordinateurs bloqués seront automatiquement débloqués. Ces ordinateurs auront alors la possibilité d'accéder aux fichiers réseau.

Par défaut, la durée de blocage de l'accès des ordinateurs aux fichiers réseau est égale à 30 minutes. Cette durée est décomptée à partir de la date de blocage de l'ordinateur.

► *Pour modifier la durée de blocage de l'accès des ordinateurs aux fichiers réseau, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Blocage de l'accès aux fichiers réseau**.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Dans le groupe **Paramètres du blocage des ordinateurs**, indiquez le nombre de jours, d'heures ou de minutes à décompter à partir du moment du blocage de l'ordinateur et au terme desquels les ordinateurs bloqués sont autorisés à accéder fichiers réseau.
5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Contrôle du lancement des applications

Cette section contient des informations sur la tâche de contrôle du lancement des applications et les instructions sur la configuration de cette tâche.

Dans cette section

Présentation de la tâche Contrôle du lancement des applications

La tâche Contrôle du lancement des applications permet de protéger les serveurs du réseau contre les programmes malveillants. La tâche surveille les tentatives de lancement d'applications par les utilisateurs et autorise ou interdit le lancement des applications conformément aux *règles de contrôle du lancement des applications (cf. section "A propos des règles de contrôle du lancement des applications" à la page 179) (ci-après, les règles)*.

> Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution des tâches (cf. section "A propos des journaux d'exécution des tâches" à la page 307).

La tâche Contrôle du lancement des applications bloque le lancement de toute application interdite par les règles de contrôle du lancement des applications créées. Afin de faciliter la création des règles d'autorisation, vous pouvez utiliser la tâche Génération automatique des règles d'autorisation. Vous pouvez également créer des règles d'autorisation et d'interdiction manuellement.

Le Contrôle du lancement des applications peut fonctionner selon deux modes :

- **Appliquer les règles de contrôle du lancement des applications**. Kaspersky Security contrôle, à l'aide de règles définies, le lancement des applications qui entrent dans la zone d'action des règles de la tâche. La zone d'action des règles de la tâche Contrôle du lancement des applications peut être définie dans les paramètres de cette tâche. Si une application entre dans la zone d'action des règles définie dans la tâche et que ses paramètres ne respectent aucune des règles de contrôle du lancement des applications, le lancement de cette application sera interdit.

  Le lancement des applications n'entrant pas dans la zone d'action des règles définie dans la tâche est autorisé, indépendamment des paramètres des règles de contrôle du lancement des applications.

  Le lancement de la tâche Contrôle du lancement des applications en mode Appliquer les règles de contrôle du lancement des applications est impossible si aucune règle n'a été définie ou si le nombre de règles définies pour un seul serveur est supérieur à 65 535.

- **Statistiques seulement**. Kaspersky Security ne contrôle pas le lancement des applications à l'aide des règles de contrôle du lancement des applications et consigne simplement dans le journal d'exécution des tâches les informations sur les lancements des applications et les règles de contrôle du lancement des applications que respectent les applications exécutées. Le lancement de toutes les applications est autorisé. Il s'agit du mode par défaut.

  Vous pouvez utiliser ce mode pour la composition d'une liste de règles de contrôle du lancement des applications sur la base des informations consignées dans le journal d'exécution des tâches.

Si les fichiers système du système d'exploitation tombent sous le coup de l'application de la tâche Contrôle du lancement des applications, assurez-vous lors de la création des règles de contrôle du lancement des applications que le lancement de ces applications est autorisé par les règles créées. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Le module Contrôle du lancement des applications est disponible dans les suites logicielles suivantes : Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41). Le module n'est pas disponible sur abonnement.

A propos des règles de contrôle du lancement des applications

Le fonctionnement des règles de contrôle du lancement des applications est basé sur les composantes suivantes :

- Type de règle.

  Les règles de contrôle du lancement des applications peuvent autoriser ou interdire le lancement d'applications et sont respectivement nommées règles *d'autorisation* et règles *d'interdiction*. Pour créer des règles d'autorisation du contrôle du lancement des applications, vous pouvez utiliser la tâche de génération automatique des règles d'autorisation (cf. section "Composition de la zone d'application des règles dans la tâche Génération automatique des règles d'autorisation" à la page 193) ou ajouter des règles d'autorisation manuellement (cf. section "Ajout d'une règle" à la page 205).

- Utilisateur et/ou groupe d'utilisateurs.

  Les règles de contrôle du lancement des applications contrôlent les lancements des applications initiés par l'utilisateur et/ou le groupe d'utilisateurs défini dans la règle.

- Zone d'action de la règle.

  Les règles de contrôle du lancement des applications peuvent s'appliquer aux lancements des *fichiers exécutables des applications* ou aux lancements des *scripts* et *paquets MSI*.

- Critères de déclenchement de la règle.

  Les règles de contrôle du lancement des applications contrôlent le lancement des fichiers répondant à un critère défini dans les paramètres de la règle : présenter le *certificat numérique* indiqué, disposer du *code de hachage SHA256* indiqué ou être situé à l'*emplacement* indiqué.

  Si le critère de déclenchement de la règle est le paramètre **Certificat numérique**, la règle créée contrôle le lancement de n'importe quelle application de confiance dans le système d'exploitation. Vous pouvez créer des conditions plus strictes pour ce critère en cochant les cases :

  - **Utiliser l'en-tête**.

    La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que critère de déclenchement de la règle.

    Si la case est cochée, l'en-tête du certificat numérique indiqué sera utilisé en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications uniquement pour l'éditeur repris dans l'en-tête.

Si la case est décochée, l'application n'utilise pas les en-têtes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, la règle contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quel en-tête.

L'en-tête du certificat numérique dont dispose le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Indiquer le critère de déclenchement de la règle à partir des propriétés du fichier**, situé sous le groupe **Critère de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**.

  La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de déclenchement de la règle.

  Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications signées par le certificat numérique doté de l'empreinte indiquée.

  Si la case est décochée, l'application n'utilise pas les empreintes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, l'application contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quelle empreinte.

  L'empreinte du certificat numérique dont dispose le fichier ne peut être indiquée que depuis les propriétés du fichier à l'aide du bouton **Indiquer le critère de déclenchement de la règle à partir des propriétés du fichier**, situé sous le groupe **Critère de déclenchement de la règle**.

  Cette case est décochée par défaut.

Le recours à l'empreinte limite de manière plus stricte le déclenchement des règles de lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée, à la différence de l'en-tête du certificat numérique.

Vous pouvez définir des exclusions pour une règle de contrôle du lancement des applications. Les exclusions d'une règle de contrôle du lancement des applications sont basées sur les mêmes critères que ceux déclenchant la règle : certificat numérique, code hachage SHA256 ou chemin

d'accès au fichier. Des exclusions des règles de contrôle du lancement des applications peuvent se justifier pour préciser des règles d'autorisation : par exemple, si vous souhaitez permettre aux utilisateurs de lancer les applications au chemin C:\Windows, mais que vous souhaitez interdire l'exécution du fichier Regedit.exe.

Si les fichiers système du système d'exploitation tombent sous le coup de l'application de la tâche Contrôle du lancement des applications, assurez-vous lors de la création des règles de contrôle du lancement des applications que le lancement de ces applications est autorisé par les règles créées. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Configuration des paramètres de la tâche Contrôle du lancement des applications

La tâche Contrôle du lancement des applications possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 27. Paramètres par défaut de la tâche Contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Mode de fonctionnement de la tâche	**Statistiques seulement**. La tâche consigne dans le journal d'exécution tous les événements de blocage et de lancement des applications conformément aux paramètres définis. Le lancement des applications n'est pas vraiment bloqué.	Vous pouvez sélectionner **Appliquer les règles de contrôle du lancement des applications définies** pour protéger le serveur après la composition de la liste définitive des règles.
Zone d'application des règles dans la tâche	La règle contrôle l'exécution des fichiers exécutables, des scripts et des paquets MSI.	Vous pouvez indiquer les types de fichier dont l'exécution sera contrôlée par les règles.

Paramètre	Valeur par défaut	Description
Utilisation du KSN	Les conclusions sur la fiabilité des applications dans KSN ne sont pas utilisées.	Vous pouvez utiliser les conclusions de KSN sur la fiabilité des applications dans le fonctionnement de la tâche de contrôle du lancement des applications.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Sous l'onglet **Consultation et administration** du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez les paramètres de la tâche suivants :
   - Sous l'onglet **Général** :
     - Mode de fonctionnement de la tâche Contrôle du lancement des applications (cf. section "Sélection du mode de fonctionnement de la tâche Contrôle du lancement des applications" à la page 183).
     - Zone d'application des règles dans la tâche (cf. section "Composition de la zone d'application de la tâche Contrôle du lancement des applications" à la page 185).
     - Utilisation du KSN (cf. section "Utilisation du KSN dans la tâche Contrôle du lancement des applications" à la page 186).
   - Sous les onglets **Planification** et **Avancé** :
     - Paramètres de lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

6. Dans la partie inférieure du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

7. Le cas échéant, modifiez la liste des règles de contrôle du lancement des applications.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Sélection du mode de fonctionnement de la tâche Contrôle du lancement des applications

► *Pour configurer le mode de fonctionnement de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Sous l'onglet **Consultation et administration** du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Sélectionnez le mode d'exécution de la tâche dans la liste **Mode de fonctionnement de la tâche Contrôle du lancement des applications**.

   La liste déroulante vous permet de sélectionner l'un des modes d'exécution de la tâche Contrôle du lancement des applications :

   - **Appliquer les règles de contrôle du lancement des applications**. Kaspersky Security contrôle le lancement des applications à l'aide des règles indiquées.

- **Statistiques seulement**. Kaspersky Security ne contrôle pas le lancement des applications à l'aide des règles indiquées et consigne simplement dans le journal d'exécution des tâches les informations sur les lancements des applications. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles de contrôle du lancement des applications sur la base des informations consignées dans le journal d'exécution des tâches.

Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques seulement**.

5. Décochez ou cochez la case **Contrôler les nouveaux lancements des applications à l'aide du cache**.

   La case active ou désactive le contrôle d'un nouveau lancement de l'application sur la base des enregistrements à l'aide du cache.

   Quand la case est cochée, Kaspersky Security interdit ou autoriser l'exécution d'un nouveau lancement de l'application sur la base de la décision prise au premier lancement de l'application par la tâche de contrôle du lancement des applications. Par exemple, si le premier lancement de l'application avait été autorisé par les règles de contrôle du lancement des applications, l'enregistrement relatif à cet événement est enregistré dans le cache et le nouveau lancement de cette application sera autorisé.

   Si la case est désactivée, Kaspersky Security analyse l'application à chacun de ses lancements ultérieurs.

   Cette case est cochée par défaut.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution des tâches.

Composition de la zone d'application de la tâche Contrôle du lancement des applications

► *Pour créer une zone d'application de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Sous l'onglet **Consultation et administration** du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Définissez les valeurs des paramètres suivants dans le groupe **Zone d'application des règles** :

   - **Utiliser les règles pour les fichiers exécutables**.

     La case active/désactive le contrôle du lancement des fichiers exécutables des applications.

     Si la case est cochée, Kaspersky Security autorise ou interdit le lancement des fichiers exécutables des applications à l'aide des règles indiquées et dont les paramètres prévoient la couverture des Fichiers exécutables par la zone d'application.

     Si la case est décochée, Kaspersky Security ne contrôle pas le lancement des fichiers exécutables des applications à l'aide des règles indiquées. Le lancement des fichiers exécutables des applications est autorisé.

     Cette case est cochée par défaut.

   - **Surveiller le lancement des modules DLL**.

     La case active/désactive le contrôle du chargement des modules DLL.

     Si la case est cochée, Kaspersky Security autorise ou interdit le chargement des modules DLL à l'aide des règles indiquées et dont les paramètres prévoient la couverture des Fichiers exécutables par la zone d'application.

Si la case est décochée, Kaspersky Security ne contrôle pas le chargement des modules DLL à l'aide des règles indiquées. Le chargement des modules DLL est autorisé.

La case est accessible si la case **Utiliser les règles pour les fichiers exécutables** est cochée.

Cette case est décochée par défaut.

> Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation.

- **Utiliser les règles pour les scripts et les paquets MSI**.

  La case active ou désactive le contrôle du lancement des scripts et des paquets MSI.

  Si la case est cochée, Kaspersky Security autorise ou interdit le lancement des scripts et paquets MSI à l'aide des règles indiquées et dont les paramètres prévoient la couverture des Scripts et paquets MSI par la zone d'application.

  Si la case est décochée, Kaspersky Security ne contrôle pas le lancement des scripts et des paquets MSI à l'aide des règles indiquées. Le lancement des scripts et des paquets MSI est autorisé.

  Cette case est cochée par défaut.

5. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Utilisation du KSN dans la tâche Contrôle du lancement des applications

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN.

> Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer une tâche manuellement (cf. section "Lancement et arrêt d'une tâche Utilisation du KSN" à la page 166) ou planifier son exécution (cf. section "Configuration des paramètres d'une tâche Utilisation du KSN" à la page 167).

► *Pour configurer les paramètres d'utilisation des services KSN dans la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Sous l'onglet **Consultation et administration** du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Définissez dans le groupe **Utilisation du KSN** les paramètres d'utilisation des services de Kaspersky Security Network :

   - **Interdire le lancement des programmes n'étant pas des programmes de confiance dans le KSN**.

     La case active ou désactive le contrôle du lancement des applications selon leur réputation dans le KSN.

     Si la case est cochée, Kaspersky Security interdit le lancement des applications étant considérées comme douteuses dans le KSN. Dans ce cas, les règles d'autorisation du contrôle du lancement des applications couvrant des applications considérées comme douteuses dans le KSN ne se déclenchent pas. Cocher cette case permet d'assurer une protection complémentaire du stockage réseau contre les programmes malveillants.

     Si la case est décochée, Kaspersky Security ne prend pas en compte la réputation des applications considérées comme douteuses dans le KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

     Cette case est décochée par défaut.

   - **Autoriser le lancement des programmes étant des programmes de confiance dans le KSN**.

     La case active ou désactive le contrôle du lancement des applications selon leur réputation dans le KSN.

     Si la case est cochée, Kaspersky Security interdit le lancement des applications

considérées comme douteuses dans le KSN. Dans ce cas, les règles d'interdiction du contrôle du lancement des applications couvrant des applications considérées comme fiables dans le KSN ne se déclenchent pas. Cocher cette case permet d'améliorer la précision de la mise en œuvre des règles de contrôle du lancement des applications, par exemple, lorsque les règles interdisent le lancement d'applications n'étant pas considérées comme malveillantes selon les données des services du KSN.

Si la case est décochée, Kaspersky Security ne prend pas en compte la réputation des applications considérées comme douteuses dans KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

> La réputation de l'application dans le KSN prévaut sur la règle de contrôle du lancement des applications dans la zone d'action de laquelle se trouve l'application à exécuter. Par exemple, si une application a le statut d'application de confiance dans le KSN tout en se trouvant dans la zone d'action d'une règle d'interdiction, et que la case **Autoriser le lancement des programmes étant des programmes de confiance dans le KSN** est cochée, le lancement de cette application sera autorisé.

- Indiquez les utilisateurs et/ou groupes d'utilisateurs pour lesquels le lancement d'applications considérées comme des applications de confiance dans le KSN sera autorisé. Pour ce faire, procédez comme suit :

  a. Cliquez sur le bouton **Modifier**.

  La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

  b. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

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

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Génération automatique des règles d'autorisation pour le contrôle du lancement des applications

Cette section contient des informations sur la tâche Génération automatique des règles d'autorisation pour le contrôle du lancement des applications et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Génération automatique des règles d'autorisation pour le contrôle du lancement des applications

La tâche de génération automatique des règles d'autorisation permet de générer automatiquement une liste de règles d'autorisation pour le contrôle du lancement des applications sur la base des types de fichiers indiqués, issus des dossiers indiqués. Par exemple, si vous indiquez les fichiers exécutables du dossier C:\Program Files (x86) en tant que paramètres de la tâche, l'application créera automatiquement des règles autorisant le lancement de ces fichiers. L'application autorisera par la suite le lancement des applications pour lesquelles des règles d'autorisation ont été générées automatiquement.

Les règles créées s'affichent dans la fenêtre après que vous avez cliqué sur le lien **Règles du contrôle du lancement des applications** dans l'entrée **Contrôle du lancement des applications**.

Configuration des paramètres de la tâche Génération automatique des règles d'autorisation pour le contrôle du lancement des applications

La tâche Génération automatique des règles d'autorisation pour le contrôle du lancement des applications possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 28. Paramètres par défaut de la tâche Génération automatique des règles d'autorisation pour le contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Préfixe des noms des règles	Correspond au nom de l'ordinateur sur lequel Kaspersky Security est installé.	Vous pouvez modifier le préfixe des noms des règles d'autorisation.
Zone d'action des règles d'autorisation	La zone d'application des règles d'autorisation reprend par défaut les catégories de fichiers suivantes : • fichiers portant l'extension EXE et placés dans les dossiers C:\Windows, C:\Program Files (x86) et C:\Program Files ; • paquets MSI, placés dans le dossier C:\Windows; • scripts placés dans le dossier C:\Windows. La tâche crée également des règles pour toutes les applications déjà en cours d'exécution, quels que soient leur emplacement ou leur format.	Vous pouvez modifier la zone de protection en ajoutant ou en supprimant des chemins d'accès aux dossiers et en indiquant l'emplacement des dossiers et les types de fichiers dont le lancement est autorisé par les règles générées automatiquement. Vous pouvez également ne pas tenir compte des applications déjà en cours d'exécution lors de la création des règles d'autorisation.

Paramètre	Valeur par défaut	Description
Critères de génération de règles d'autorisation.	Utilisation de l'en-tête et de l'empreinte du certificat numérique ; les règles sont générées pour tous les utilisateurs et groupes d'utilisateurs.	Vous pouvez utiliser le hash SHA256 lors de la génération de règles d'autorisation. Vous pouvez sélectionner l'utilisateur ou le groupe d'utilisateurs pour lesquels les règles d'autorisation doivent être générées automatiquement.
Actions une fois la tâche terminée	Les règles d'autorisation sont ajoutées à la liste des règles de contrôle du lancement des applications ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont effectués.	Vous pouvez ajouter des règles à des règles existantes sans fusion et sans suppression des doublons, ou remplacer les règles existantes par de nouvelles règles d'autorisation, ainsi que configurer les paramètres d'exportation des règles d'autorisation dans un fichier.
Paramètres du lancement de la tâche en tant que	La tâche est lancée sous les autorisations du compte système.	Vous pouvez autoriser le lancement de la tâche de génération automatique des règles d'autorisation sous l'autorisation du compte du système ou du compte d'un utilisateur que vous aurez choisi.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Génération automatique des règles d'autorisation n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer les paramètres de la tâche Génération automatique des règles d'autorisation, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Génération automatique des règles d'autorisation**.

3. Dans le panneau d'administration de l'entrée **Génération automatique des règles d'autorisation**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre. Configurez les paramètres suivants :

   - Sous l'onglet **Général** :

     - Indiquez le préfixe des noms des règles.

       Première partie du nom de la règle. La deuxième partie du nom de la règle est constituée à partir du nom de l'objet dont le lancement est interdit.

       Par défaut, le nom de l'ordinateur sur lequel est installé Kaspersky Security est utilisé comme préfixe.

     - Configurez la zone d'application des règles d'autorisation (cf. section "Composition de la zone d'application des règles dans la tâche Génération automatique des règles d'autorisation" à la page 193).

   - Sous l'onglet **Actions**, définissez les actions que Kaspersky Security doit réaliser :

     - Lors de la génération de règles (cf. section "Actions lors de la génération de règles automatiques" à la page 194).

     - A la fin d'une tâche (cf. section "Actions à réaliser à la fin de la génération automatique des règles" à la page 197).

   - Sous les onglets **Planification** et **Avancé** :

     - Paramètres de lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

- Sous l'onglet **Exécuter en tant que** :
  - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115).

4. Cliquez sur **OK**.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Composition de la zone d'application des règles dans la tâche Génération automatique des règles d'autorisation

► *Pour configurer les paramètres généraux de la tâche Génération automatique des règles d'autorisation, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Génération automatique des règles d'autorisation**.
3. Dans le panneau d'administration de l'entrée **Génération automatique des règles d'autorisation**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Configurez les paramètres de la tâche suivants :
   - **Créer des règles d'autorisation sur la base des applications en cours d'exécution**.

     La case active ou désactive la génération automatique des règles d'autorisation pour le contrôle du lancement des applications pour les applications déjà exécutées. Cette option est recommandée si une sélection représentative d'applications est en cours d'exécution sur l'ordinateur et que vous souhaitez utiliser celle-ci pour générer les règles d'autorisation.

Si la case est cochée, les règles d'autorisation pour le contrôle du lancement des applications sont créées conformément aux applications exécutées.

Si la case est décochée, les applications en cours d'exécution ne sont pas prises en compte pour la génération des règles d'autorisation.

Cette case est cochée par défaut.

La case ne peut être décochée si aucun dossier n'est sélectionné dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**.

- **Créer des règles d'autorisation pour les applications des dossiers**.

  Le tableau permet de sélectionner ou d'indiquer la zone d'analyse de la tâche et les types de fichiers exécutables qui seront pris en compte lors de la génération des règles de contrôle du lancement des applications. La tâche génèrera des règles d'autorisation pour les fichiers des types sélectionnés et situés dans les dossiers indiqués.

5. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Actions lors de la génération de règles automatiques

► *Pour configurer les actions que Kaspersky Security doit réaliser pendant l'exécution de la tâche de génération automatique des règles, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Génération automatique des règles d'autorisation**.

3. Dans le panneau d'administration de l'entrée **Génération automatique des règles d'autorisation**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Ouvrez l'onglet **Actions**.

5. Configurez les paramètres suivants dans le groupe **Lors de la génération des règles d'autorisation** :

   - **Utiliser un certificat numérique**.

     Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Cette option est conseillée si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

     Cette option est sélectionnée par défaut.

   - **Utiliser l'en-tête et l'empreinte du certificat numérique**.

     La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique.

     Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique indiqués dans la règle.

     L'utilisation de cette case limite de manière plus stricte le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée.

     Si la case est désélectionnée, le critère de déclenchement des règles d'autorisation du contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation.

     La case est accessible si vous avez choisi l'option **Utiliser un certificat numérique**.

     Cette case est cochée par défaut.

- **En cas d’absence de certificat, utiliser**.

  Liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le contrôle du lancement des applications dans le cas où le fichier sur la base duquel est créée la règle ne dispose pas d'un certificat numérique.

  - **Code de hachage SHA256**. La valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
  - **Chemin du fichier**. Le chemin d'accès au fichier sur la base duquel est créée la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications par les fichiers qui se trouvent dans les dossiers indiqués sous l'onglet **Dossiers de sélection** dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**.

- **Utiliser le code de hachage SHA256**.

  Si cette option est sélectionnée, la valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la valeur de la somme de contrôle indiquée.

- **Créer des règles pour un utilisateur et/ou un groupe d'utilisateurs**.

  Champ affichant l'utilisateur et/ou le groupe d'utilisateurs. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini.

  Par défaut, le groupe **Tous** est sélectionné.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Actions à réaliser à la fin de la génération automatique des règles

► *Pour configurer les actions que Kaspersky Security doit réaliser à la fin de la génération automatique des règles, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Génération automatique des règles d'autorisation**.

3. Dans le panneau d'administration de l'entrée **Génération automatique des règles d'autorisation**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Ouvrez l'onglet **Actions**.

5. Configurez les paramètres suivants dans le groupe **Une fois la tâche terminée** :

   - **Ajouter les règles d'autorisation à la liste des règles de contrôle du lancement des applications**.

     La case active ou désactive l'ajout des règles d'autorisation créés à la liste des règles de contrôle du lancement des applications. La liste des règles de contrôle du lancement des applications est affichée via le lien **Règles du contrôle du lancement des applications** du panneau des résultats de l'entrée **Contrôle du lancement des applications**.

     Si la case est cochée, Kaspersky Security ajoute les règles créées au cours de l'exécution de la tâche Génération automatique des règles d'autorisation à la liste de règles de contrôle du lancement des applications conformément au principe d'ajout défini.

     Si la case est décochée, Kaspersky Security n'ajoute pas les règles d'autorisation créées à la liste de règles de contrôle du lancement des applications. Les règles créées sont exportées uniquement dans un fichier.

     Cette case est cochée par défaut.

     La case ne peut être décochée si la case **Exporter les règles d'autorisation vers un fichier** n'est pas cochée.

- **Principe d'ajout**.

  Liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles de contrôle du lancement des applications.

  - **Ajouter aux règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques se superposent.
  - **Modifier les règles existantes**. Les règles sont ajoutées à la place des règles existantes.
  - **Fusionner avec les règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

  Le mode **Fusionner avec les règles existantes** est défini par défaut.

- **Exporter les règles d'autorisation vers un fichier**.

  La case active ou désactive l'exportation des règles d'autorisation créées pour le contrôle du lancement des applications vers un fichier.

  Si la case est cochée, Kaspersky Security exporte les règles créées dans le fichier indiqué dans le champ ci-dessous, une fois la tâche de génération automatique de règles d'autorisation terminée.

  Si la case est décochée, Kaspersky Security n'exporte pas dans un fichier les règles créées à la fin de la tâche de génération automatique des règles d'autorisation. Il se contente de les ajouter à la liste des règles de contrôle du lancement des applications.

  Cette case est décochée par défaut.

  La case ne peut être décochée si la case **Ajouter les règles d'autorisation à la liste des règles de contrôle du lancement des applications** n'est pas cochée.

- **Ajouter des informations sur le serveur dans le nom du fichier**.

  La case active ou désactive l'ajout des informations relatives au serveur à protéger dans le nom du fichier dans lequel sont exportées les règles de contrôle du lancement des applications créées.

Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur à protéger, la date et l'heure de création du fichier.

Quand la case est décochée, l'application n'ajoute pas les informations relatives au serveur à protéger dans le nom du fichier d'exportation.

La case est accessible si la case **Exporter les règles d'autorisation vers un fichier** est cochée.

Cette case est cochée par défaut.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Administration des règles de contrôle du lancement des applications

Vous pouvez réaliser les opérations suivantes au niveau des règles de contrôle du lancement des applications :

- Ajouter des règles de contrôle du lancement des applications manuellement.
- Importer des règles de contrôle du lancement des applications d'autorisation depuis le fichier de configuration :
  - enrichir la liste des règles à l'aide d'une tâche de génération automatique des règles d'autorisation ;
  - enrichir la liste des règles à l'aide d'une tâche Contrôle du lancement des applications lancée en mode **Statistiques seulement**.
- Supprimer des règles de contrôle du lancement des applications.
- Exporter les règles de contrôle du lancement des applications dans un fichier de configuration.
- Vérifier si les fichiers sélectionnés possèdent des règles de contrôle du lancement des applications déclenchées lorsqu'ils sont exécutés.
- Filtrer les règles de contrôle du lancement des applications selon un critère défini.

Dans cette section

Suppression des règles de contrôle du lancement des applications

► *Pour supprimer des règles de contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
4. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
5. Cliquez sur le bouton **Supprimer la sélection**.

Les règles de contrôle du lancement des applications sélectionnées seront supprimées.

Exportation des règles de contrôle du lancement des applications

► *Pour exporter des règles de contrôle du lancement des applications dans un fichier de configuration, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
4. Cliquez sur le lien **Exporter vers un fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.
5. Dans la fenêtre qui s'ouvre, indiquez le fichier vers lequel vous souhaitez exporter les règles. Si ce fichier n'existe pas, il sera créé. Si un fichier portant ce nom existe déjà, son contenu sera écrasé après l'exportation des règles.
6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la règle seront enregistrés dans le fichier indiqué.

Vérification des règles de contrôle du lancement des applications

Avant d'appliquer les règles de contrôle du lancement des applications définies, vous pouvez les tester sur n'importe quelle application afin d'identifier les règles qui contrôlent le lancement des applications sélectionnées.

Par défaut, Kaspersky Security bloque les applications dont le lancement n'est contrôlé par aucune application. Pour éviter le blocage du lancement d'applications importantes, il faut créer des règles d'autorisation.

Si le lancement de l'application est contrôlé par plusieurs règles de différents types, les règles d'interdiction ont la priorité : le lancement de l'application est bloqué si elle est couverte par au moins une règle d'interdiction.

► *Pour tester des règles de contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Afficher les règles pour le fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.
5. Sélectionnez le fichier pour lequel vous souhaitez tester la règle de contrôle.

Le chemin d'accès au fichier indiqué apparaît dans la ligne de recherche. La liste des règles reprend toutes les règles trouvées qui seront déclenchées au lancement du fichier indiqué.

Enrichissement de la liste des règles de contrôle du lancement des applications

Vous pouvez enrichir la liste des règles de contrôle du lancement des applications dans la Console de Kaspersky Security de deux manières :

- Ajouter les règles une à une et configurer leurs paramètres manuellement.
- Importer une liste de règles depuis des fichiers XML créés lors de l'exécution de la tâche Contrôle du lancement des applications ou de la tâche Génération automatique des règles d'autorisation.

Dans cette section

Présentation de l'importation depuis un fichier au format XML

Vous pouvez importer une liste de règles de contrôle du lancement des applications depuis des fichiers XML créés automatiquement lors de l'exécution de la tâche Contrôle du lancement des applications ou de la tâche Génération automatique des règles d'autorisation. Les listes contenues dans ces fichiers XML peuvent servir uniquement à la création de règles d'autorisation de contrôle du lancement des applications.

Les règles d'interdiction de contrôle du lancement des applications sont créées manuellement.

Utilisation du rapport de la tâche Génération automatique des règles d'autorisation

Le fichier XML créé à la fin de la tâche Génération automatique des règles d'autorisation contient les règles d'autorisation pour le lancement des applications désignées lors de la configuration des paramètres de la tâche lors de son lancement. Pour les applications dont le lancement n'est pas

autorisé dans les paramètres de la tâche, aucune règle ne sera créée et leur exécution sera bloquée par défaut.

Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles de la tâche Contrôle du lancement des applications.

Utilisation du rapport de la tâche Contrôle du lancement des applications

Le fichier XML, obtenu à la fin de la tâche Contrôle du lancement des applications, repose sur les statistiques de fonctionnement de la tâche en mode **Statistiques seulement**.

Au cours de l'exécution de la tâche, Kaspersky Security consigne tous les lancements d'application bloqués et autorisés sur le serveur à protéger. Vous pouvez créer des règles d'autorisation en fonction des événements de la tâche et les exporter dans un fichier XML. Avant de lancer la tâche en mode de consignation des statistiques, vous devez configurer la période d'exécution de la tâche de telle sorte que tous les scénarios possibles du fonctionnement du serveur à protéger aient pu se dérouler pendant l'intervalle de temps et que le serveur ait redémarré au moins une fois.

► *Pour composer des règles sur la base des événements de la tâche Contrôle du lancement des applications en mode Statistiques seulement,*

cliquez sur le bouton **Créer des règles selon les événements** dans le journal d'exécution de la tâche Contrôle du lancement des applications.

Les fichiers XML qui contiennent la liste des règles d'autorisation, sont créés sur la base de l'analyse des tâches lancées sur le serveur à protéger. Le lancement de la tâche de génération automatique des règles d'autorisation et du contrôle du lancement des applications en mode de consignation des statistiques pour composer les listes doit être réaliser sur la machine modèle de l'organisation afin de tenir compte de toutes les applications utilisées sur le réseau.

Vous pouvez utiliser la liste des règles obtenues à l'issue de l'analyse du lancement des applications sur la machine modèle, lors de la configuration de la stratégie de contrôle du serveur depuis Kaspersky Security Center et de l'application des règles d'autorisation créées pour tous les serveurs du réseau (cf. section "A propos de la création de règles de contrôle du lancement des applications pour tous les serveurs dans Kaspersky Security Center" à la page 406).

Ajout d'une règle

► *Pour ajouter une règle de contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
4. Cliquez sur **Ajouter**.
5. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.

   La fenêtre contextuelle **Paramètres des règles** s'ouvre.
6. Spécifiez les paramètres suivants :

   a. Dans le champ **Nom**, saisissez le nom de la règle.

   b. Dans la liste déroulante **Type**, sélectionnez le type de la règle :

   - **Autorisé**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
   - **Interdit**, si vous souhaitez que la règle interdise le lancement des applications conformément aux critères définis dans les paramètres de la règle.

   c. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :

   - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables des applications.
   - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.

d. Dans le champ **Utilisateur et/ou groupe d'utilisateurs**, indiquez les utilisateurs qui pourront ou non lancer des applications en fonction du type de règle. Pour ce faire, procédez comme suit :

   i. Cliquez sur le bouton **Sélectionner**.

   ii. La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateur ou Groupes** s'ouvre.

   iii. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

   iv. Cliquez sur le bouton **OK**.

e. Réalisez les opérations suivantes si vous souhaitez extraire les valeurs pour les critères de déclenchement de la règle listés dans le groupe **Critère de déclenchement de la règle**, depuis un fichier :

   i. Cliquez sur le bouton **Définir le critère de déclenchement du fichier depuis les propriétés du fichier**.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

   ii. Sélectionnez le fichier et cliquez sur le bouton **OK**.

Les valeurs des critères du fichier s'afficheront dans les champs du groupe **Critère de déclenchement de la règle**. Par défaut, c'est le premier critère de la liste dont les données figurent dans les propriétés du fichier qui est sélectionné.

f. Dans le groupe **Critère de déclenchement de la règle**, sélectionnez une des options suivantes :

- **Certificat numérique**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique :
  - Cochez la case **Utiliser l'en-tête**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'en-tête indiquée.
  - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'empreinte indiquée.

- **Code de hachage SHA256**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers dont la somme de contrôle correspond à celle indiquée.
- **Chemin du fichier**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.

g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :

   i. Dans le groupe **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion de la règle** s'ouvre.

   ii. Dans le champ **Nom**, saisissez le nom de l'exclusion de la règle.

   iii. Indiquez les paramètres d'exclusions des fichiers du lancement des applications de la règle de contrôle du lancement des applications. Vous pouvez remplir les champs des paramètres depuis les propriétés du fichier en cliquant sur le bouton **Définir l'exclusion selon les propriétés du fichier**.

- **Certificat numérique**.

Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique.

Ce critère est sélectionné par défaut.

- **Utiliser l'en-tête**.

La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que critère de rattachement des fichiers aux exclusions de la règle.

Si la case est cochée, l'en-tête du certificat numérique indiqué sera utilisé en tant que critère de rattachement des fichiers aux exclusions de la règle. L'application ne rattache aux exclusions de la règle que les fichiers disposant d'un certificat numérique portant cet en-tête.

Si la case est décochée, l'en-tête du certificat numérique indiqué ne sera pas utilisé en tant que critère de rattachement des fichiers aux exclusions de la règle. Si le critère **Certificat numérique** est sélectionné, l'application rattache aux exclusions de la règle les fichiers disposant de la signature d'un certificat numérique portant n'importe quel en-tête.

L'en-tête du certificat numérique dont dispose le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des**

propriétés d’un fichier.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**.

La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de rattachement des fichiers aux exclusions de la règle.

Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de rattachement des fichiers aux exclusions de la règle. L'application ne rattache aux exclusions de la règle que les fichiers disposant d'un certificat numérique portant cette empreinte.

Si la case est décochée, l'empreinte du certificat numérique indiquée ne sera pas utilisée en tant que critère de rattachement des fichiers aux exclusions de la règle. Si le critère **Certificat numérique** est sélectionné, l'application rattache aux exclusions de la règle les fichiers disposant de la signature d'un certificat numérique portant n'importe quelle empreinte.

L'empreinte du certificat numérique dont dispose le fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des propriétés d’un fichier**.

Cette case est décochée par défaut.

- **Code de hachage SHA256**.

Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide d'un fichier présentant la somme de contrôle indiquée.

La somme de contrôle du fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des propriétés d’un fichier**.

- **Chemin du fichier**.

Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.

i. Cliquez sur le bouton **OK**.

ii. Répétez les points (i) à (iv) pour ajouter des exclusions supplémentaires.

7. Dans la fenêtre **Paramètres des règles**, cliquez sur **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

Importation des règles depuis un fichier XML

► *Pour importer des règles de contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans le panneau des résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
4. Cliquez sur **Ajouter**.
5. Dans le menu contextuel du bouton, choisissez l'option **Importer des règles depuis un fichier**.
6. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez l'une des options du menu contextuel du bouton **Importer des règles depuis le fichier** :

   - **Ajouter les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles dont les paramètres sont identiques se superposent.
   - **Modifier les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
   - **Fusionner les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

7. Dans la fenêtre Microsoft Windows **Ouvrir**, sélectionnez le fichier XML qui contient les paramètres des règles de contrôle du lancement des applications.

8. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du contrôle du lancement des applications**.

Protection contre le chiffrement

Cette section contient des informations sur la tâche Protection contre le chiffrement et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Protection contre le chiffrement

La tâche Protection contre le chiffrement permet d'empêcher les ordinateurs distants d'accéder au serveur, si une activité de chiffrement a été détectée de la part d'un ordinateur envoyant une requête.

L'interdiction de l'accès des ordinateurs distants pendant l'exécution de la protection contre le chiffrement est possible si la tâche Blocage de l'accès aux fichiers réseau est exécutée.

Si au cours de l'exécution de la tâche Protection contre le chiffrement, une activité malveillante de la part d'un ordinateur distant est détectée, Kaspersky Security bloque l'accès de cet ordinateur aux fichiers réseau pendant 30 minutes.

La tâche Protection contre le chiffrement ne permet de bloquer l'accès d'un ordinateur distant aux fichiers réseau qu'à partir du moment où l'activité de celui-ci a été considérée comme malveillante. Cela peut durer un certain temps pendant lequel le malware de chiffrement peut réaliser son activité malveillante.

Si la tâche Blocage de l'accès aux fichiers réseau n'est pas exécutée, Kaspersky Security ajoute l'ordinateur distant d'où provient l'activité de chiffrement à la liste des ordinateurs douteux.

Le module Protection contre le chiffrement est disponible dans les suites logicielles suivantes : Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41). Le module n'est pas disponible sur abonnement.

Statistiques de la tâche Protection contre le chiffrement

Quand la tâche Protection contre le chiffrement est en cours d'exécution, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis son lancement jusqu'à maintenant, autrement dit, les statistiques de la tâche.

► *Pour consulter les statistiques de la tâche Protection contre le chiffrement, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Protection contre le chiffrement**.

   L'onglet **Consultation et administration** dans le panneau des résultats du groupe **Statistiques**, affichera les statistiques actuelles de la tâche.

Vous pouvez consulter les informations sur les objets que Kaspersky Security a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 29. Statistiques de la tâche Protection contre le chiffrement

Champ	Description
Logiciels de cryptage détectés	Nombre de programmes accédant au stockage réseau et de la part desquels Kaspersky Security a identifié une activité de chiffrement.
Erreurs de traitement	Nombre de requêtes d'applications envoyées au stockage réseau dont le traitement a entraîné une erreur de tâche.
Objets traités	Nombre total de requêtes traitées par Kaspersky Security.

Configuration des paramètres de la Protection contre le chiffrement

La tâche Protection contre le chiffrement possède les paramètres par défaut suivants :

- **Zone de protection**. Par défaut, Kaspersky Security applique la tâche Protection contre le chiffrement à tous les dossiers réseau partagés du serveur. Vous pouvez modifier la zone de protection en indiquant les dossiers publics auxquels doit s'appliquer la tâche.
- **Analyseur heuristique**. Par défaut, le niveau de détail de l'analyse appliqué par Kaspersky Security est le niveau **Moyenne**. Vous pouvez activer ou désactiver l'utilisation de l'analyseur heuristique et régler le niveau de détail de l'analyse.
- **Lancement d'une tâche planifiée**. Par défaut, le premier lancement de la tâche n'est pas défini. La tâche Protection contre le chiffrement n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer les paramètres de la tâche Protection contre le chiffrement, procédez comme suit* :

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Protection contre le chiffrement**.

3. Dans le panneau des résultats de l'entrée **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Configurez les paramètres suivants dans la fenêtre qui s'ouvre :

   - Sous l'onglet **Général** :

     - Zone de protection (cf. section "Constitution de la zone de protection" à la page 213).
     - Utilisation de l'analyse heuristique (cf. section "Application de l'analyse heuristique" à la page 216).

   - Sous les onglets **Planification** et **Avancé** :

     - Lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

5. Cliquez sur **OK**.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Constitution de la zone de protection

La tâche de protection contre le chiffrement accepte les types de zone de protection suivants :

- **Prédéfinie**. Vous pouvez utiliser la zone de protection définie par défaut et qui reprend tous les dossiers réseau partagés du serveur. Cette valeur est appliquée quand le paramètre **Tous les dossiers réseau partagés du serveur** a été sélectionné.

- **Utilisateur**. Vous pouvez configurer vous-même la zone de protection en sélectionnant les dossiers à inclure dans la zone de protection contre le chiffrement. Cette valeur est appliquée quand le paramètre **Uniquement les dossiers partagés indiqués**.

► *Pour configurer la zone de protection pour la tâche Protection contre le chiffrement, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Protection contre le chiffrement**.

3. Dans le panneau des résultats de l'entrée **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Sélectionnez dans le groupe **Zone de protection** les dossiers que Kaspersky Security analysera lors de l'exécution de la tâche Protection contre le chiffrement :

   - **Tous les dossiers réseau partagés du serveur**.

     Si vous avez choisi cette option, Kaspersky Security analyse tous les dossiers réseau partagés du serveur lors de l'exécution de la tâche Protection contre le chiffrement.

     Cette option est sélectionnée par défaut.

   - **Uniquement les dossiers partagés indiqués**.

     Si vous avez choisi cette option, Kaspersky Security analyse uniquement les dossiers réseau partagés que vous avez désignés manuellement lors de l'exécution de la tâche Protection contre le chiffrement.

     a. Cliquez sur le bouton **Ajouter** et choisissez l'option **Ajouter une zone de protection** afin d'indiquer les dossiers partagés du serveur que vous souhaitez inclure dans la zone de protection du chiffrement.

     b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Sélectionner**.

     La fenêtre standard de Microsoft Windows s'ouvre.

     c. Sélectionnez le dossier que vous souhaitez ajouter à la zone de protection de la tâche.

d. Cliquez sur le bouton **OK**.

e. Le cas échéant, répétez les étapes a à d pour ajouter d'autres dossiers.

> Le bouton **Ajouter une zone de protection** est accessible si le paramètre **Uniquement les dossiers partagés indiqués** a été coché.

5. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Que ce soit lors de l'utilisation d'une zone de protection prédéfinie ou définie par l'utilisateur, il est possible d'exclure des dossiers sélectionnés de la zone de protection, par exemple si les données de ces dossiers sont chiffrées à l'aide d'applications installées sur des périphériques distants.

► *Pour ajouter des exclusions de la zone de protection contre le chiffrement, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.
2. Sélectionnez la sous-entrée **Protection contre le chiffrement**.
3. Dans le panneau des résultats de l'entrée **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Dans le groupe **Zone de protection**, cliquez sur le bouton **Ajouter**.
5. Choisissez l'option **Ajouter une exclusion à la protection** pour désigner les dossiers partagés du serveur que vous souhaitez exclure de la zone de protection contre le chiffrement.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton Sélectionner.

   La fenêtre standard de Microsoft Windows s'ouvre.
7. Sélectionnez le dossier que vous souhaitez exclure de la zone de protection de la tâche.
8. Cliquez sur le bouton **OK**.

9. Le cas échéant, répétez les étapes 4 à 8 pour ajouter d'autres exclusions.

   Vous pouvez également inclure ou exclure de la zone de protection des dossiers ajoutés manuellement en cochant ou en décochant les cases en regard de ces dossiers.

10. Cochez la case **Prendre en compte les zones de protection exclues**.

    La case active ou désactive la prise en compte de la liste des exclusions définies dans les paramètres de la zone de protection pour la tâche Protection contre le chiffrement.

    Si la case est cochée, les dossiers exclus de la zone de protection sont pris en compte lors de l'exécution de la tâche.

    Si la case est décochée, les dossiers exclus de la zone de protection ne sont pas pris en compte lors de l'exécution de la tâche.

    Cette case est décochée par défaut.

11. Cliquez sur **OK**.

Les modifications apportées à la configuration des paramètres seront enregistrées.

Application de l'analyseur heuristique

Vous pouvez, dans la tâche Protection contre le chiffrement, utiliser l'analyseur heuristique et configurer le niveau de l'analyse.

► *Pour activer ou désactiver l'analyse heuristique, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Contrôle du serveur**.

2. Sélectionnez la sous-entrée **Protection contre le chiffrement**.

3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Cochez ou décochez la case **Utiliser l'analyseur heuristique**.

5. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

   Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

   Il existe trois niveaux de détail pour l'analyse

   - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
   - **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

     Il s'agit du niveau par défaut.
   - **Minutieuse**. L'analyseur heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

   Le curseur est actif quand la case **Utiliser l'analyseur heuristique** est cochée.

6. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande. La section contient également les instructions relatives à la configuration des paramètres des tâches d'analyse à la demande et des paramètres de la sécurité du serveur protégé.

Dans cette section

A propos des tâches d'analyse à la demande

Kaspersky Security recherche une fois des virus et autres menaces informatique dans la zone indiquée. Kaspersky Security analyse les fichiers, la mémoire vive du serveur et les objets de démarrage.

Kaspersky Security prévoit quatre tâches prédéfinies d'analyse à la demande :

- La tâche Analyse au démarrage du système d'exploitation est exécutée à chaque démarrage de Kaspersky Security. Kaspersky Security analyse les secteurs d'amorçage et les principaux enregistrements d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. A chaque exécution de la tâche, Kaspersky Security crée une copie des secteurs d'amorçage sains et si lors de l'exécution suivante de la tâche il découvre une menace, il remplace les secteurs d'amorçage infectés par les copies de sauvegarde saines.

- La tâche Analyse des zones critiques est exécutée par défaut chaque semaine selon une planification. Kaspersky Security analyse les objets situés dans les zones critiques du système d'exploitation : objets de démarrage, secteurs d'amorçage et entrées principales d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. Il analyse les fichiers qui se trouvent dans les répertoires système, par exemple dans le dossier %windir%\system32. Kaspersky Security applique les paramètres de sécurité dont les valeurs correspondent au niveau **Recommandé** (cf. section "**Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande**" à la page 240). Vous pouvez modifier les paramètres la tâche Analyse des zones critiques.

- La tâche Analyse des objets en quarantaine est exécutée par défaut selon la programmation après chaque mise à jour des bases de données. Vous ne pouvez pas modifier les paramètres de la tâche Analyse des objets en quarantaine.

- La tâche Vérification de l'intégrité de l'application est exécutée à chaque démarrage de Kaspersky Security. Elle permet de vérifier si les composants de Kaspersky Security ont été endommagés ou modifiés. Le dossier d'installation de l'application est analysé. Les statistiques sur l'exécution des tâches contiennent des informations sur le nombre de composants analysés ou endommagés. Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. La planification du lancement de la tâche peut être modifiée.

Vous pouvez créer des tâches définies par l'utilisateur dans le nœud Analyse à la demande. Par exemple, vous pouvez créer une tâche d'analyse du dossier partagé sur le serveur.

Kaspersky Security peut exécuter simultanément plusieurs tâches d'analyse à la demande.

Les modules qui interviennent dans les tâches d'analyse à la demande sont disponibles dans les suites logicielles suivantes : Kaspersky Security Standard, Kaspersky Security Basic, Kaspersky Security Extended, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage (cf. section "A propos des solutions accessibles de Kaspersky Security" à la page 41).

Statistiques des tâches d'analyse à la demande

Pendant que la tâche d'analyse à la demande est exécutée, vous pouvez consulter des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis son lancement jusqu'à maintenant.

Ces informations seront accessibles même si vous arrêtez la tâche. Vous pourrez consulter les statistiques de la tâche dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).

A la conclusion de l'analyse à la demande on recommande d'analyser des événements dans le journal d' exécution des tâches sur l'onglet **Evénements** à la main.

► *Pour consulter les statistiques de la tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la Console, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.

Le groupe Statistiques, sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée sélectionnée, affichera les statistiques actuelles de la tâche.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 30. Statistiques des tâches d'analyse à la demande

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security. Par exemple, si Kaspersky Security a découvert un programme malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres objets détectés	Nombre d'objets que Kaspersky Security détecte et classifie comme infectés ou nombre de fichiers de logiciels légitimes détectés, qui n'ont pas été exclus de l'analyse en temps réel et de la zone d'analyse des tâches à la demande, et qui ont été classés en tant que riskware.
Objets potentiellement infectés détectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Security.

Champ	Description
Objets non réparés	Nombre d'objets que Kaspersky Security n'a pas pu réparer pour les raisons suivantes : • le type d'objet détecté ne peut être réparé ; • une erreur s'est produite lors de la réparation.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Security a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Security a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone de protection que Kaspersky Security n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
Erreurs de traitement	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets réparés	Nombre d'objets réparés par Kaspersky Security.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Security.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Security.
Objets protégés par mot de passe	Nombre d'objets (archives, par exemple) que Kaspersky Security a ignorés en raison d'une protection par mot de passe.

Champ	Description
Objets endommagés	Nombre d'objets que Kaspersky Security a ignorés à cause de leur format endommagé.
Objets traités	Nombre total d'objets traités par Kaspersky Security.

Configuration des tâches d'analyse à la demande

Par défaut, les tâches d'analyse à la demande possèdent les paramètres décrits dans le tableau ci-dessous. Vous pouvez configurer les tâches d’analyse à la demande prédéfinies et définies par l'utilisateur.

Tableau 31. Paramètres des tâches d'analyse à la demande

Paramètre	Valeur	Configuration
Zone d'analyse	S'applique aux tâches prédéfinies et définies par l'utilisateur : • Analyse au démarrage du système d'exploitation : tout le serveur, à l'exception des dossiers partagés et des objets de démarrage ; • Analyse rapide : tout le serveur, à l'exception des dossiers partagés et de certains fichiers du système d'exploitation ; • Tâches d'analyse à la demande définie par l'utilisateur : tout le serveur.	Vous pouvez modifier la zone d'analyse. Il est impossible de configurer la zone de protection pour les tâches prédéfinies Analyse des objets en quarantaine et Vérification de l'intégrité de l'application.

Paramètre	Valeur	Configuration
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; correspondent au niveau de sécurité **Recommandé**.	Pour les entrées sélectionnées dans l'arborescence des ressources fichiers du serveur, vous pouvez exécuter les actions suivantes : • sélectionner un autre niveau de sécurité prédéfini ; • modifier manuellement les paramètres de sécurité. Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud.
Analyseur heuristique	Les tâches Analyse rapide et Analyse au démarrage du système d'exploitation, aussi que les tâches d'analyse définies par l'utilisateur, sont exécutées selon la valeur **Moyenne**. La tâche Analyse des objets en quarantaine est réalisée selon la valeur **Minutieuse**.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse. Vous ne pouvez pas configurer le niveau d'analyse pour la tâche Analyse des objets en quarantaine. L'application de l'analyse heuristique n'est pas prévue dans la tâche Vérification de l'intégrité de l'application.
Zone de confiance	Appliquée Les programmes d'administration à distance **RemoteAdmin** sont exclus si vous aviez choisi pendant l'installation de Kaspersky Security l'option **Ajouter les objets sous le masque not-a-virusRemoteAdmin* aux exclusions**.	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.

Paramètre	Valeur	Configuration
Utilisation du KSN	Appliquée	Vous pouvez améliorer l'efficacité de la protection de l'ordinateur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Paramètres du lancement de la tâche en tant que	La tâche est lancée sous les autorisations du compte système.	Vous pouvez modifier les paramètres de lancement sous les autorisations d'un compte pour tous les tâches d'analyse à la demande prédéfinies ou définies par l'utilisateur, sauf pour les tâches Analyse des objets en quarantaine et Vérification de l'intégrité de l'application.
Exécution en arrière-plan (priorité basse)	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.
Planification du lancement de la tâche	S'applique aux tâches prédéfinies : • Analyse au démarrage du système d'exploitation : **Au lancement de l'application** ; • analyse des zones critiques : **Chaque semaine** ; • Analyse des objets en quarantaine : **A la mise à jour des bases de l'application** ; • vérification de l'intégrité de l'application : **Au lancement de l'application**. Pas appliqué dans les tâches définies par l'utilisateur recréées.	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

Paramètre	Valeur	Configuration
Enregistrement de l'exécution de l'analyse et de la mise à jour de l'état de la protection du serveur	L'état de la protection du serveur est actualisé chaque semaine après l'exécution de la tâche Analyse des zones critiques.	Vous pouvez configurer les paramètres d'enregistrement de l'exécution de l'analyse des zones critiques d'une des manières suivantes : • en modifiant les paramètres de la planification du lancement de la tâche Analyse des zones critiques ; • en modifiant la zone de protection de la tâche Analyse des zones critiques ; • en créant des tâches d'analyse à la demande définies par l'utilisateur.

► *Pour configurer une tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.
3. Sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre. Configurez les paramètres de la tâche suivants :

   - Sous l'onglet **Général** :
     - Application de l'analyseur heuristique (à la page 227).
     - Exécution de la tâche en arrière-plan (cf. section "Exécution en arrière-plan de la tâche d'analyse à la demande" à la page 228).
     - Utilisation de KSN (à la page 229).
     - Application de la zone de confiance (cf. section "Activation et désactivation de l'application de la zone de confiance dans les tâches de Kaspersky Security" à la page 100).
     - Enregistrement de l'exécution de l'analyse des zones critiques (à la page 230)

- Sous les onglets **Planification** et **Avancé** :
  - Paramètres de lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).
- Sous l'onglet **Exécuter en tant que** :
  - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115).

4. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

5. Le cas échéant, ouvrez l'onglet **Configuration de la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   Exécutez les actions suivantes :

   - Dans l'arborescence des ressources fichier du serveur, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.
   - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section "Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande" à la page 240) ou configurez manuellement les paramètres de protection des objets (cf. section "Configuration manuelle des paramètres de sécurité" à la page 243).

6. Dans le menu contextuel du nom de la tâche sélectionnée, sélectionnez **Enregistrer la tâche**.

Kaspersky Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'exécution de la tâche.

Application de l'analyseur heuristique

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

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.
3. Dans le panneau de résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Utiliser l'analyseur heuristique**.
5. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

   Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

   Il existe trois niveaux de détail pour l'analyse

   - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
   - **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

     Il s'agit du niveau par défaut.
   - **Minutieuse**. L'analyseur heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

   Le curseur est actif quand la case **Utiliser l'analyseur heuristique** est cochée.

6. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Exécution en arrière-plan de la tâche d'analyse à la demande

Par défaut, les processus dans lesquels les tâches de Kaspersky Security sont exécutées ont la priorité de base **Moyenne** (**Normal**).

Vous pouvez attribuer la priorité de base **Bas** (**Low**) au processus dans lequel la tâche d'analyse à la demande sera exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter quelques tâches en arrière-plan. Vous pouvez définir le nombre maximum de processus pour les tâches d'analyse à la demande en arrière-plan.

► *Pour modifier la priorité de la tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche dont vous souhaitez modifier la priorité.
3. Dans le panneau des résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Exécuter la tâche en arrière-plan**.

   La case modifie la priorité de la tâche.

   Quand la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et du système de fichiers du serveur par les autres tâches de Kaspersky Security ou les autres applications. Par conséquente la vitesse d'exécution de la tâche diminuera quand la charge augmentera et augmentera dans le cas contraire.

Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

Cette case est décochée par défaut.

5. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Utilisation du KSN

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN.

Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security. Vous pouvez lancer une tâche manuellement (cf. section "Lancement et arrêt d'une tâche Utilisation de KSN" à la page 166) ou planifier son exécution (cf. section "Configuration des paramètres d'une tâche Utilisation de KSN" à la page 167).

► *Pour configurer l'utilisation du KSN dans les tâches d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.

3. Sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. cochez ou décochez la case **Utiliser le KSN pour la protection** ;

   La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

Cette case est cochée par défaut.

5. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Enregistrement de l'exécution de l'analyse des zones critiques

Par défaut, l'état de la protection du serveur apparaît dans le panneau des résultats de l'entrée **Kaspersky Security** et il est actualisé chaque semaine après la fin de la tâche Analyse des zones critiques.

L'heure de l'actualisation de l'état de la protection du serveur est liée à la planification de la tâche d'analyse à la demande où la case **Considérer l'exécution de la tâche comme une analyse rapide** a été cochée. La case est cochée uniquement pour la tâche Analyse des zones critiques et ne peut être modifiée.

Vous pouvez réaffecter la tâche d'analyse à la demande à l'état de la protection du serveur uniquement au départ de Kaspersky Security Center.

► *Pour configurer les paramètres d'enregistrement de l'état de la protection du serveur à l'aide d'une tâche Analyse des zones critiques prédéfinies, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.

2. Sélectionnez la sous-entrée **Analyse rapide**.

3. Sous l'onglet **Consultation et administration** dans le panneau des résultats de l'entrée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Sous les onglets **Planification** et **Avancé**, configurez les paramètres du lancement de la tâche selon la planification.

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

6. Dans le panneau des résultats de l'entrée **Analyse rapide**, ouvrez l'onglet **Configuration de la zone d'analyse**.

7. Dans l'arborescence des ressources fichier du serveur, sélectionnez les dossiers auxquels vous souhaitez attribuer l'état de "zone critique".

8. Sélectionnez le niveau de sécurité prédéfini ou configurez manuellement les paramètres de sélection des fichiers à analyser.

9. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Les paramètres configurés seront enregistrés ; l'état de la protection du serveur dans le panneau des résultats de l'entrée **Kaspersky Security** sera actualisé conformément à la planification du lancement de la tâche Analyse rapide.

Zone d'analyse dans les tâches d'analyse à la demande

Cette section fournit des informations sur la création et l'utilisation d'une zone d'analyse dans les tâches d'analyse à la demande.

Dans cette section

Présentation de la zone d'analyse

Vous pouvez configurer la zone d'analyse pour les tâches Analyse au démarrage du système d'exploitation et Analyse rapide ainsi que pour les tâches d'analyse à la demande définies par l'utilisateur.

Par défaut, les tâches d'analyse à la demande analyse tous les objets du système de fichiers du serveur. Si les exigences en matière de sécurité ne nécessitent pas une analyse de tous les objets du système de fichiers, vous pouvez limiter la zone d'analyse.

Dans la Console de Kaspersky Security, la zone d'analyse se présente sous la forme d'une arborescence de ressources fichiers du serveur que l'application peut analyser.

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrés de la manière suivante :

☑ Nœud repris dans la zone d'analyse.

☐ Nœud exclu de la zone d'analyse.

☑ Au moins un des nœuds intégrés à ce nœud est exclu de la zone d'analyse ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

> L'icône ☑ s'affiche si toutes les sous-entrées ont été sélectionnées mais pas l'entrée mère. Le cas échéant, les modifications du contenu des fichiers et dossiers de l'entrée principale ne sont pas automatiquement prises en compte lors de la constitution de la zone d'analyse de la sous-entrée sélectionnée.

Le nom des nœuds virtuels de la zone d'analyse apparaît en lettres bleues.

Zones d'analyse prédéfinies

L'arborescence des ressources fichiers du serveur est affichée dans le panneau des résultats de l'entrée de la tâche d'analyse à la demande sélectionnée sous l'onglet **Configuration de la zone d'analyse**.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

L'arborescence des ressources fichiers du serveur contient les zones d'analyse prédéfinies suivantes :

- **Poste de travail**. Kaspersky Security analyse tout le serveur.
- **Disques durs locaux**. Kaspersky Security analyse les objets sur les disques durs du serveur. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Disques amovibles**. Kaspersky Security analyse les objets sur les périphériques externes tels que les disques compacts ou amovibles. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Emplacements réseau**. Vous pouvez ajouter à la zone d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux répertoires de réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte système.
- **Mémoire système**. Kaspersky Security analyse les fichiers exécutables et les modules des processus exécutés dans le système d'exploitation au moment de l'analyse.
- **Objets exécutés au démarrage du système**. Kaspersky Security analyse les objets sur lesquels les clés de la base de registres et les fichiers de configuration, par exemple WIN.INI ou SYSTEM.INI, s'appuient ainsi que les modules logiciels des applications qui sont exécutées automatiquement au démarrage de l'ordinateur.
- **Dossiers partagés**. Vous pouvez ajouter les dossiers partagés du serveur à protéger à la zone d'analyse.

- **Unités virtuelles**. Vous pouvez inclure dans la zone d'analyse les disques, les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés sur le serveur, par exemple les disques partagés d'une grappe.

Par défaut, les tâches d'analyse à la demande sont exécutées dans les secteurs suivants :

- Tâche Analyse au démarrage du système d'exploitation :
  - **Disques durs locaux** ;
  - **Disques amovibles** ;
  - **Mémoire système**.
- Tâche Analyse rapide :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles** ;
  - **Mémoire système** ;
  - **Objets exécutés au démarrage du système**.
- Tâche d'analyse à la demande définie par l'utilisateur :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles** ;
  - **Mémoire système** ;
  - **Objets exécutés au démarrage du système** ;
  - **Dossiers partagés**.

Les pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la Console de Kaspersky Security. Pour analyser les objets d'un pseudo-disque, il faut inclure dans la zone d'analyse le répertoire du serveur auquel ce pseudo-disque est lié.

Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. Pour inclure les objets d'un disque de réseau dans la zone d'analyse, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

Constitution de la zone d'analyse

Si vous administrez Kaspersky Security sur le serveur protégé à distance via la console de Kaspersky Security installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.

Si vous modifiez la zone d'analyse dans les tâches Analyse au démarrage du système et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la restauration de Kaspersky Security (**Démarrer** → **Programmes** → **Kaspersky Security 10 for Windows Server** → **Modification ou suppression**). Dans l'Assistant d'installation cochez la case **Rétablir les paramètres recommandés de fonctionnement de l'application**.

► *Pour établir la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez constituer une zone d'analyse.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Déployez l'arborescence des ressources fichiers du serveur pour afficher toutes les entrées et procédez comme suit :

   - Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.
   - Pour inclure certaines entrées à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :

     - Si vous souhaitez inclure tous les disques d'un même type, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**).

- Si vous souhaitez inclure un disque particulier du type requis, déployez le nœud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque. Par exemple, pour sélectionner le disque amovible **F:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:.**
- Si vous souhaitez inclure à la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case à côté de ce dossier ou de ce fichier.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Vous pouvez également créer une zone d'analyse à l'aide du bouton **Ajouter**, accessible en mode de consultation **Afficher sous forme de liste**.

Vous ne pourrez exécuter la tâche d'analyse à la demande que si au moins un nœud de l'arborescence des ressources fichiers du serveur est inclus dans la zone d'analyse.

Si vous définissez une zone de protection complexe, par exemple en attribuant différentes valeurs aux paramètres de sécurité pour divers nœuds distincts de l'arborescence des ressources fichiers du serveur, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.

Inclusion des objets réseau dans la zone d'analyse

Vous pouvez inclure dans la zone d'analyse des disques réseau, des répertoires ou des fichiers en indiquant leur chemin d'accès de réseau au format UNC (Universal Naming Convention).

Vous ne pouvez pas analyser les dossiers réseau en cas d'utilisation du compte système.

► *Pour inclure un objet de réseau dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dans la zone d'analyse de laquelle vous souhaitez ajouter un chemin de réseau.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Dans le menu contextuel du nom de l'entrée **Emplacements réseau**, réalisez les opérations suivantes :
   - Choisissez l'option **Ajouter un dossier de réseau** si vous souhaitez ajouter un dossier réseau à la zone d'analyse.
   - Choisissez l'option **Ajouter un fichier de réseau** si vous souhaitez ajouter un fichier réseau à la zone d'analyse.
6. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et appuyez sur la touche **ENTER**.
7. Cochez la case en regard du nom de l'objet réseau ajouté afin de l'inclure dans la zone d'analyse.
8. Le cas échéant, modifiez les paramètres de sécurité de l'objet réseau ajouté.
9. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Création d'une zone d'analyse virtuelle

Vous pouvez inclure dans la zone d'analyse les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe – créer couverture de protection virtuelle.

Vous pouvez ajouter à la zone de protection/d'analyse des disques virtuels des dossiers ou des fichiers distincts uniquement si la zone de protection/d'analyse se présente sous la forme d'une arborescence des ressources fichiers.

► *Pour inclure un disque virtuel dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez constituer une zone d'analyse.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Dans l'arborescence des ressources fichier du serveur, ouvrez le menu contextuel de l'entrée **Unités virtuelles** et sélectionnez le nom du disque virtuel créé dans la liste des noms disponibles.
6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone d'analyse.
7. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

► *Pour ajouter un dossier ou un fichier virtuel dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la Console, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez composer une zone d'analyse virtuelle.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel de l'unité à laquelle vous souhaitez ajouter le répertoire ou le fichier et sélectionnez l'une des options suivantes :
   - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone de protection.
   - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone de protection.
6. Dans le champ, saisissez le nom du dossier ou du fichier.

   Vous pouvez définir un masque de nom de fichier en utilisant les caractères * et ?.
7. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone d'analyse.
8. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Paramètres de sécurité de l'entrée sélectionnée dans la tâche d'analyse à la demande

Dans la tâche d'analyse à la demande sélectionnée, vous pouvez modifier les valeurs des paramètres de sécurité par défaut de la même manière pour toute la zone de protection ou d'analyse avec des variations pour divers nœuds dans l'arborescence des ressources fichier du serveur.

Les paramètres de sécurité configurés pour l'entrée mère sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Vous pouvez configurer les paramètres de la zone d'analyse sélectionnée de l'une des manières suivantes :

- Sélectionner un des trois niveaux de sécurité prédéfinis (**Performance maximale**, **Recommandé** ou **Protection maximale**) ;
- Modifier manuellement les paramètres de sécurité pour les entrées sélectionnées de l'arborescence des ressources fichiers du serveur (le niveau de sécurité prend alors la valeur **Personnalisé**).

Vous pouvez enregistrer la sélection de paramètres du nœud dans un modèle afin de l'appliquer à d'autres nœuds.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour le nœud sélectionné dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivant : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité prédéfinis possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Performance maximale

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab

en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 32. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondants

Paramètres	**Niveau de sécurité**		
	Performance maximale	**Recommandé**	**Protection maximale**
Analyse des objets	En fonction du format	Analyser tous les objets	Analyser tous les objets
Optimisation	Activée	Désactivée	Désactivée
Actions à exécuter sur les objets infectés	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible (**Exécuter l'action recommandée**)	Réparer, supprimer si la réparation est impossible
Action à exécuter sur les objets probablement infectés	Quarantaine	Mettre en quarantaine (**Exécuter l'action recommandée**)	Quarantaine
Exclure les fichiers	Non	Non	Non
Ne pas détecter	Non	Non	Non
Arrêter si l'analyse dure plus de (s.)	60 s	Non	Non
Ne pas analyser les objets composés de plus de (Mo)	8 Mo	Non	Non

Paramètres	Niveau de sécurité		
	Performance maximale	**Recommandé**	**Protection maximale**
Analyser les flux NTFS alternatifs	Oui	Oui	Oui
Analyser les secteurs d'amorçage et la partition MBR	Oui	Oui	Oui
Analyse des objets composés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* * uniquement les objets nouveaux et modifiés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * Tous les objets	• Archives* • Archives SFX* • Bases de données de messagerie électronique* • Message de texte plat* • Objets compactés* • Objets OLE intégrés* * Tous les objets
Traitement des fichiers autonomes (n'est pas utilisé par défaut)	Ne pas analyser	Analyser seulement la partie résidente du fichier	Analyser le fichier en entier

Les paramètres de sécurité **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyseur heuristique** et **Vérifier la signature Microsoft des fichiers** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si vous modifiez la valeur des paramètres **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyseur heuristique** ou **Vérifier la signature Microsoft des fichiers**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche pour laquelle vous souhaitez configurer les paramètres de sécurité.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée pour laquelle vous souhaitez sélectionner un niveau de sécurité prédéfini.
5. Assurez-vous que le nœud sélectionné se trouve dans la zone d'analyse.
6. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez le niveau que vous souhaitez appliquer.

   La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau que vous avez sélectionné.
7. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Configuration manuelle des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse. Leurs valeurs correspondent aux valeurs du niveau de sécurité prédéfini **Recommandé** (cf. section "**Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande**" à la page 240).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone d'analyse ou avec des variations pour divers nœuds dans l'arborescence des ressources fichier du serveur.

Les paramètres de sécurité configurés pour l'entrée mère sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Kaspersky Security n'analyse pas les archives crées avec certains algorithmes de la compression. Vous trouverez les informations détaillées sur la page de l'application dans la Base de la connaissance.

► *Pour configurer les paramètres de sécurité manuellement, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche pour laquelle vous souhaitez configurer les paramètres de sécurité.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la partie gauche de la fenêtre, sélectionnez l'entrée dont vous souhaitez configurer les paramètres de sécurité.

   Pour la zone de protection sélectionnée, vous pouvez appliquer un modèle prédéfini contenant un ensemble de paramètres de sécurité (cf. section "A propos des modèles de paramètres de sécurité" à la page 121).
5. Configurez les paramètres de sécurité requis pour le nœud sélectionné en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, configurez les paramètres suivants, si nécessaire :

     Dans le groupe **Couverture de l'analyse**, indiquez les objets que vous souhaitez inclure à la zone d'analyse :

- **Tous les objets** ;

  Kaspersky Security analyse tous les objets.

- **Objets analysés en fonction du format** ;

  Kaspersky Security analyse uniquement les fichiers infectables sur la base du format du fichier.

  La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

- **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus** ;

  Kaspersky Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

  La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

- **Objets analysés en fonction de la liste d'extensions indiquée** ;

  Kaspersky Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- **Secteurs d'amorçage des disques MBR** ;

  Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

  Quand la case est cochée, Kaspersky Security analyse les secteurs et les enregistrements d'amorçage sur les disques durs et les disques amovibles du serveur.

  Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**

  Analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

  Quand la case est cochée, Kaspersky Security analyse les flux complémentaires des fichiers et des dossiers.

  Cette case est cochée par défaut.

Dans le groupe **Optimisation**, cochez ou décochez la case :

- **Analyse uniquement des nouveaux fichiers et des fichiers modifiés**

  La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security a identifié comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

  Quand la case est cochée, Kaspersky Security analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Security analyse et protège tous les fichiers.

  La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Recommandé** ou **Protection maximale**, la case est décochée.

Dans le groupe **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone d'analyse :

- **Toutes les / Les nouvelles archives** ;

  Analyse des archives au format ZIP (sauf BZip2, LZMA, PPMd algorithmes de la compression), CAB, RAR, ARJ et autres.

  Si la case est cochée, Kaspersky Security analyse les archives.

  Si la case est décochée, Kaspersky Security ignore les archives lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Toutes les / Les nouvelles archives SFX** ;

  Analyse des archives qui contiennent un module logiciel de décompactage.

  Si la case est cochée, Kaspersky Security analyse les archives SFX.

  Si la case est décochée, Kaspersky Security ignore les archives SFX lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données de messagerie** ;

  Analyse des fichiers des bases de données de messagerie de Microsoft Office Outlook® et Microsoft Outlook Express.

Quand la case est cochée, Kaspersky Security analyse les fichiers des bases de données de messagerie.

Quand la case est décochée, Kaspersky Security ignore les fichiers des bases de données de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / les nouveaux objets compactés** ;

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Quand la case est cochée, Kaspersky Security analyse les fichiers exécutables compactés par des logiciels de compression.

Quand la case est décochée, Kaspersky Security ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux messages de texte plat** ;

Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

Quand la case est cochée, Kaspersky Security analyse les fichiers aux formats de messagerie.

Quand la case est décochée, Kaspersky Security ignore les fichiers aux formats de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security analyse les objets intégrés au fichier.

Quand la case est décochée, Kaspersky Security ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

Vous pouvez choisir d'analyser tous les objets composés ou uniquement les nouveaux si la case **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** est cochée. Si la case **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** est décochée, Kaspersky Security analyse tous les objets composés indiqués.

- Sur l'onglet **Actions**, réalisez les actions suivantes, le cas échéant :
  - Sélectionnez l'action à exécuter sur les objets infectés.
  - Sélectionnez l'action à exécuter sur les objets probablement infectés.
  - Le cas échéant, configurez les actions en fonction du type d'objet à détecter.
- Sous l'onglet **Optimisation**, configurez les paramètres suivants, si nécessaire :

  Dans le groupe **Exclusions** :

  - **Exclure les fichiers** ;

    Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

    Si la case est cochée, Kaspersky Security ignore les objets indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Security analyse tous les objets.

    Cette case est décochée par défaut.

  - **Ne pas détecter**.

    Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque de nom d'objet à détecter. Par exemple, vous pouvez exclure les utilitaires d'administration à distance à l'aide du masque `not-a-virus:RemoteAdmin*`. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

    Si la case est cochée, Kaspersky Security ignore les objets à détecter indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Security détecte tous les objets indiqués par défaut dans l'application.

    Cette case est décochée par défaut.

Dans le groupe **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)** ;

  Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

  Si la case est cochée, la durée maximale de l'analyse d'un objet est égale à la valeur indiquée.

  Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

  Cette case est cochée par défaut.

- **Ne pas analyser les objets composés de plus de (Mo)** ;

  Exclut de l'analyse les objets complexes dont la taille est supérieure à la valeur indiquée. La valeur par défaut est de 8 Mo.

  Si la case est cochée, Kaspersky Security n'analyse pas les objets complexes dont la taille est supérieure à la valeur indiquée.

  Si la case est décochée, Kaspersky Security analyse les objets complexes sans tenir compte de la taille.

  La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- **Utiliser la technologie iChecker** ;

  Analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse.

  Si la case est cochée, Kaspersky Security analyse uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Security analyse les fichiers sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

- **Utiliser la technologie iSwift**.

  Analyse uniquement des nouveaux objets ou des fichiers objets depuis la dernière analyse dans le système de fichiers NTFS.

  Si la case est cochée, Kaspersky Security analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse du système de fichiers NTFS.

Si la case est décochée, Kaspersky Security analyse les objets du système de fichiers NTFS sans tenir compte de la date de création ou de modification.

Cette case est cochée par défaut.

- **Vérifier la signature Microsoft des fichiers**.

La case active ou désactive la vérification de la présence d'une signature numérique Microsoft dans les fichiers.

Quand la case est cochée, Kaspersky Security ignore les fichiers dotés de la signature numérique Microsoft pendant l'exécution de la tâche d'analyse à la demande.

Si la case est décochée, l'application ne recherche pas la présence d'une signature numérique Microsoft dans les fichiers.

La case est cochée par défaut pour tous les niveaux de sécurité.

- Sous l'onglet **Stockage hiérarchique**, sélectionnez le mode de traitement des fichiers autonomes :

  - **Ne pas analyser**.

  Kaspersky Security n'analyse pas les fichiers autonomes dans le stockage distant.

  - **Analyser seulement la partie résidente du fichier**.

  Kaspersky Security analyse uniquement les parties des fichiers autonomes enregistrées sur le disque dur. Kaspersky Security n'analyse pas les parties des fichiers autonomes situées dans le stockage distant.

  Cette option est sélectionnée par défaut.

  - **Analyser le fichier en entier**.

  Kaspersky Security analyse complètement les fichiers autonomes dans le stockage distant.

    - **Uniquement si le fichier a été sollicité durant la période indiquée (jours)**.

  La case active ou désactive l'analyse uniquement des fichiers autonomes dans le stockage distant qui ont été modifiés au cours de la période indiquée.

  Quand la case est cochée, Kaspersky Security analyse uniquement les fichiers autonomes du stockage distant qui ont été modifiés lors de la période indiquée.

Si la case est décochée, il n'y a aucune limite sur l'analyse des fichiers autonomes.

La case est accessible lorsque l'option **Analyser le fichier en entier** a été sélectionnée.

Cette case est cochée par défaut.

- **Ne pas copier le fichier sur le disque dur local si possible**.

La case active ou désactive l'analyse des fichiers autonomes dans le stockage temporaire sans les restaurer sur le disque dur.

Quand la case est cochée, Kaspersky Security analyse les fichiers autonomes dans le stockage temporaire sans les restaurer sur le disque dur. L'analyse dans le stockage temporaire est possible si le système HSM en place prend en charge l'analyse des fichiers sans restauration sur le disque dur.

Si la case est décochée, Kaspersky Security restaure les fichiers autonomes sur le disque dur avant de les analyser.

La case est accessible lorsque l'option **Analyser le fichier en entier** a été sélectionnée.

Cette case est décochée par défaut.

> Vous pouvez indiquer le mode de traitement des fichiers autonomes uniquement si vous avez préalablement défini la méthode utilisée par le système HSM pour déterminer l'emplacement des fichiers à analyser.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Création d'une tâche d'analyse à la demande

Vous pouvez créer des tâches définies par l'utilisateur dans le nœud **Analyse à la demande**. Les autres composants de Kaspersky Security ne prévoient pas la création de tâches définies par l'utilisateur.

► *Pour créer une nouvelle tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Analyse à la demande**.
2. Choisissez l'option **Ajouter tâche**.

   La fenêtre **Ajouter tâche** s'ouvre.
3. Saisissez les informations suivantes relatives à la tâche :

   - **Nom** : nom de la tâche, 100 caractères maximum, peut contenir n'importe quel caractère sauf**% ? l \ | / : * < >**.

     Vous ne pouvez pas enregistrer une nouvelle tâche ou passer à la configuration des paramètres de la nouvelle tâche sous les onglets **Planification**, **Avancé** et **Exécuter en tant que** si le nom de la tâche n'est pas défini.
   - **Description** : toute information complémentaire relative à la tâche, 2 000 caractères maximum. Ces informations figurent dans la fenêtre des propriétés de la tâche.
4. Le cas échéant, configurez les paramètres suivants de la tâche :
5. Sous l'onglet **Général** :

   - **Utiliser l'analyseur heuristique**.

     La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

     Quand la case est cochée, l'analyse heuristique est activée.

     Quand la case est décochée, l'analyse heuristique est désactivée.

     Cette case est cochée par défaut.
   - **Exécuter la tâche en arrière-plan**.

     La case modifie la priorité de la tâche.

     Quand la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et du système de fichiers du serveur par les autres tâches de Kaspersky Security ou les autres applications. Par

conséquente la vitesse d'exécution de la tâche diminuera quand la charge augmentera et augmentera dans le cas contraire.

Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

Cette case est décochée par défaut.

- **Appliquer la zone de confiance**.

  La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

  Si la case est cochée, Kaspersky Security ajoute les opérations de fichiers des processus de confiance aux exclusions de l'analyse définies dans la configuration des paramètres de la tâche.

  Si la case est décochée, Kaspersky Security ne prend pas en compte les opérations de fichiers des processus de confiance lors de la création de la zone de protection dans la tâche Protection des fichiers en temps réel.

  Cette case est cochée par défaut.

- **Considérer l'exécution de la tâche comme une analyse rapide**.

  La case modifie la priorité de la tâche : active ou désactive l'enregistrement de l'événement *Analyse rapide réalisée* et l'actualisation de l'état de la protection du serveur. La case n'est pas accessible dans les propriétés des tâches locales de Kaspersky Security prédéfinies ou définies par l'utilisateur. Vous pouvez modifier la valeur de ce paramètre du côté de Kaspersky Security Center.

  Quand la case est cochée, le Serveur d'administration consigne l'événement *Analyse rapide réalisée* et actualise l'état de la protection du serveur suite à l'exécution de la tâche. La priorité de la tâche d'analyse est élevée.

  Si la case est décochée, la tâche d'analyse est exécutée selon une priorité faible.

  La case est cochée par défaut pour la tâche Analyse rapide.

- **Utiliser le KSN pour la protection**.

  La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

Cette case est cochée par défaut.

- Sous les onglets **Planification** et **Avancé** :
  - Paramètres de lancement de la tâche selon la planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).
- Sous l'onglet **Exécuter en tant que** :
  - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115).

6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   La tâche d'analyse à la demande définie par l'utilisateur a été créée. L'entrée portant le nom de la nouvelle tâche apparaîtra dans l'arborescence de la console. L'opération sera consignée dans le journal d'audit système (cf. section "Journal d'audit système" à la page 303).

7. Le cas échéant, ouvrez l'onglet **Configuration de la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   Exécutez les actions suivantes :

   - Dans l'arborescence des ressources fichier du serveur, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.
   - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section "Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande" à la page 240) ou configurez manuellement les paramètres de protection des objets (cf. section "Configuration manuelle des paramètres de sécurité" à la page 243).

8. Dans le menu contextuel du nom de la tâche sélectionnée, sélectionnez **Enregistrer la tâche**.

La tâche d'analyse à la demande définie par l'utilisateur a été créée. Les paramètres configurés seront appliqués lors de la prochaine exécution de la tâche.

Suppression d'une tâche

Vous pouvez supprimer uniquement des tâches d'analyse à la demande définies par l'utilisateur. Vous ne pouvez pas supprimer les tâches prédéfinies, ni les tâches de groupe.

► *Pour supprimer une tâche, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Ouvrez le menu contextuel du nom de la tâche définie par l'utilisateur que vous souhaitez supprimer.
3. Choisissez l'option **Supprimer la tâche**.

   La fenêtre de confirmation de la suppression s'ouvre.
4. Cliquez sur le bouton **Oui** pour confirmer la suppression.

La tâche sera supprimée et cette opération sera consignée dans le journal d'audit système.

Changement de nom d'une tâche

Vous pouvez changer le nom uniquement des tâches définies par l'utilisateur dans la Console de Kaspersky Security. Vous ne pouvez pas renommer les tâches prédéfinies, ni les tâches de groupe.

► *Pour renommer une tâche, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Ouvrez le menu contextuel du nom de la tâche définie par l'utilisateur que vous souhaitez renommer.
3. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, saisissez le nouveau nom de la tâche dans le champ **Nom**.
5. Cliquez sur **OK**.

La tâche sera ainsi renommée. L'opération sera consignée dans le journal d'audit système.

Mise à jour des bases de données et des modules de Kaspersky Security

Cette section présente les tâches de mises à jour des bases et des modules logiciels de Kaspersky Security, la copie des mises à jour et le retour à l'état antérieur aux mises à jour. Elle explique également comment configurer les paramètres des tâches de mise à jour des bases et des modules de l'application.

Dans cette section

Présentation des tâches de mise à jour

Kaspersky Security prévoit quatre tâches prédéfinies pour la mise à jour : Mise à jour des bases de données de l'application, Mise à jour des modules de l'application, Copie des mises à jour et Annulation de la mise à jour des bases de l'application.

Par défaut Kaspersky Security établit la connexion à la source des mises à jour, un des serveurs de mise à jour de Kaspersky Lab, en définissant automatiquement les paramètres du serveur proxy dans le réseau et sans recourir à l’authentification lors de l'accès au serveur proxy.

Vous pouvez configurez toutes les tâches de mises à jour (cf. section "Configuration des tâches de mise à jour" à la page 265), à l'exception de la tâche Annulation de la mise à jour des bases de l'application. Une fois que les paramètres de la tâche ont été modifiés, Kaspersky Security appliquera les nouvelles valeurs au prochain lancement de l'application.

Vous ne pouvez pas suspendre et reprendre une tâche de mise à jour.

Mise à jour des bases de l'application

Par défaut, Kaspersky Security copie les bases depuis la source des mises à jour sur le serveur protégé et les utilise directement dans la tâche Protection en temps réel en cours. Les tâches Analyse à la demande et Protection des stockages réseau utiliseront les bases mises à jour à leur prochaine exécution.

Kaspersky Security lance la tâche Mise à jour des bases de données de l'application toutes les heures par défaut.

Mise à jour des modules de l'application

Par défaut, Kaspersky Security copie les mises à jour de ses modules logiciels depuis la source des mises à jour sur le serveur protégé et les installe. L'application des modules logiciels installés peut impliquer le redémarrage de l'ordinateur et/ou de Kaspersky Security.

Par défaut, Kaspersky Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé). Pendant l'exécution de la tâche, l'application recherche la présence éventuelle de mises à jour prévues ou extraordinaires pour les modules de Kaspersky Security, mais ne les copie pas.

Copie des mises à jour

Par défaut, lors de l'exécution de la tâche, Kaspersky Security télécharge les fichiers des mises à jour des bases de données et des modules et les enregistre dans le répertoire de réseau ou local indiqué, sans les installer.

La Copie des mises à jour n'est pas exécutée par défaut.

Annulation de la mise à jour des bases de l'application

Au cours de cette tâche, Kaspersky Security utilise à nouveau les bases de la mise à jour antérieure.

La tâche Annulation de la mise à jour des bases de l'application n'est pas exécutée par défaut.

Présentation de la mise à jour des modules de Kaspersky Security

Kaspersky Lab peut diffuser des paquets de mise à jour des modules de Kaspersky Security. Les mises à jour sont réparties entre les *mises à jour urgentes* (ou *critiques*) et les *mises à jour prévues*. Les mises à jour urgentes suppriment des vulnérabilités et corrigent les erreurs tandis que les mises à jour prévues peuvent ajouter de nouvelles fonctions ou améliorer des fonctions existantes.

Les mises à jour urgentes sont publiées sur les serveurs de mise à jour de Kaspersky Lab. Vous pouvez configurer l'installation automatique grâce à la tâche Mise à jour des modules de l'application. Par défaut, Kaspersky Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez obtenir des informations sur la diffusion des mises à jour prévues de Kaspersky Security à l'aide des tâches Mises à jour des modules de l'application.

Vous pouvez télécharger les mises à jour urgentes depuis Internet sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez les mises à jour sans les installer avant de les diffuser sur les serveurs. Pour copier et enregistrer les mises à jour sans les installer, utilisez la tâche Copie des mises à jour.

Avant d'installer les mises à jour des modules, Kaspersky Security crée une copie de sauvegarde des modules installés antérieurement. Si la mise à jour des modules de l'application est interrompue ou si elle se solde par un échec, Kaspersky Security utilisera à nouveau automatiquement les modules installés précédemment. Vous pouvez aussi décider de revenir manuellement à l'état antérieur à la mise à jour des modules.

Lors de l’installation des mises à jour récupérées, le service Kaspersky Security s’arrête puis redémarre automatiquement.

Présentation de la mise à jour des bases de données de Kaspersky Security

Les bases de Kaspersky Security sur le serveur protégé sont très vite dépassées. Les experts en virus de Kaspersky Lab découvrent chaque jour des centaines de nouvelles menaces, créent les définitions qui permettent de les identifier et les intègrent aux mises à jour des bases de l'application. Une Mise à jour des bases est un fichier ou un ensemble de fichiers contenant les définitions capables d'identifier les menaces qui ont fait leur apparition depuis la diffusion de la mise à jour précédente. Pour réduire le risque d'infection du serveur au minium, il est conseillé de réaliser une mise à jour régulière des bases.

Par défaut, si les bases de Kaspersky Security n'ont pas été mises à jour dans la semaine qui suit la création de la dernière mise à jour des bases de données installée, l'événement *Les bases de l'application sont dépassées* est déclenché. Si les bases restent deux semaines sans mises à jour, l'événement *Les bases de l'application sont fortement dépassées* est déclenché. Les informations relatives à l'actualité des bases sont affichées à l'entrée **Kaspersky Security** de l'arborescence de la console (cf. "Consultation de l'état de la protection et des informations sur Kaspersky Security" à la page 77) de l'arborescence de la console. Vous pouvez désigner un autre intervalle avant le déclenchement de ces événements à l'aide des paramètres généraux de Kaspersky Security (cf. section "Configuration des paramètres de fonctionnement de Kaspersky Security dans la Console" à la page 62) et configurer les paramètres de notification de l'administrateur sur ces événements (cf. section "Configuration des notifications de l'administrateur et des utilisateurs" à la page 320).

Kaspersky Security télécharge la mise à jour des bases et des modules de l'application depuis des serveurs FTP ou HTTP de mises à jour de Kaspersky Lab, depuis le serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.

Vous pouvez télécharger les mises à jour sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les serveurs. Si vous utilisez Kaspersky Security Center pour l'administration centralisée de la protection des ordinateurs de l'entreprise, vous pouvez utiliser le serveur d'administration de Kaspersky Security Center en guise d'intermédiaire pour le chargement des mises à jour.

Vous pouvez lancer la tâche de mise à jour manuellement ou selon une planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

Kaspersky Security lance la tâche Mise à jour des bases de données de l'application toutes les heures par défaut.

Si le chargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Security reviendra automatiquement à l'utilisation des dernières mises à jour installées. Si les bases de Kaspersky Security sont endommagées, vous pouvez revenir à l'état antérieur à la mise à jour des bases installées (cf. section « Remise à l'état antérieur à la mise à jour des bases de Kaspersky Security » à la page 274).

Schémas de mise à jour des bases et des modules des applications antivirus dans l'entreprise

Votre sélection de la source des mises à jour dans les tâches de mise à jour dépend du schéma de mise à jour des bases et des modules logiciels des applications antivirus que vous utilisez dans votre entreprise.

Vous pouvez actualiser les bases et les modules de Kaspersky Security sur les serveurs protégés selon les schémas suivants :

- Télécharger les mises à jour directement depuis Internet sur chaque serveur protégé (schéma 1) ;
- Télécharger les mises à jour depuis Internet sur l'ordinateur intermédiaire et les diffuser sur les serveurs au départ de cet ordinateur.

  L'intermédiaire peut être n'importe quel ordinateur sur lequel une des applications suivantes est installée :

  - Kaspersky Security (un des serveurs protégés) (schéma 2) ;
  - Serveur d'administration Kaspersky Security Center (schéma 3).

La mise à jour via un ordinateur intermédiaire permet non seulement de réduire le trafic Internet mais également d'offrir une sécurité supplémentaire aux serveurs de fichiers.

Les différents schémas de mise à jour sont décrits ci-après.

Schéma 1. Mise à jour directement depuis Internet

► *Pour configurer la récupération des mises à jour de Kaspersky Security directement depuis Internet,*

dans les paramètres des tâches Mise à jour des bases de données de l'application et Mise à jour des modules de l'application de chaque serveur à protéger, désignez les serveurs de mise à jour de Kaspersky Lab en tant que sources des mises à jour.

En guise de source, vous pouvez indiquer d'autres serveurs HTTP ou FTP qui contiennent un répertoire avec les fichiers des mises à jour.

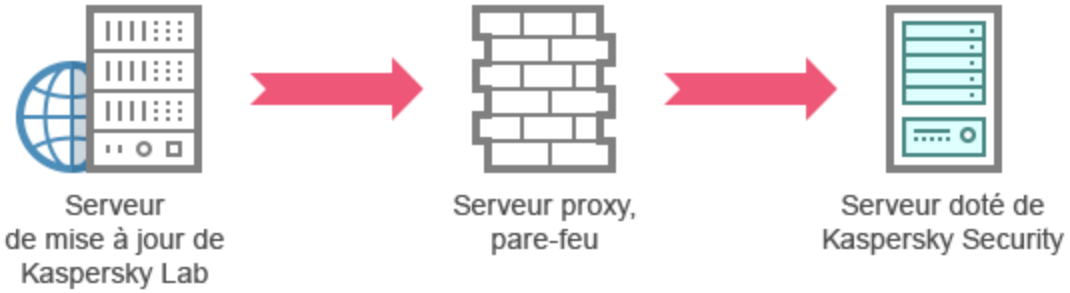


Illustration 1. Sous-système de mise à jour des bases et des modules d'application

Schéma 2. Mise à jour via un des serveurs protégés

► *Pour configurer la récupération des mises à jour de Kaspersky Security via un des serveurs à protéger, procédez comme suit :*

1. Copiez les mises à jour sur le serveur protégé sélectionné. Pour ce faire, procédez comme suit :

   - Sur le serveur sélectionné, configurez les paramètres de la tâche Copie des mises à jour :

     a. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.

     b. Désignez le dossier partagé en guise de dossier d'enregistrement des mises à jour.

2. Diffusez les mises à jour sur les autres serveurs protégés. Pour ce faire, procédez comme suit :

   - Sur chaque serveur protégé, configurez les paramètres de la tâche Mise à jour des bases de l'application (Mise à jour des modules de l'application) (cf. ill. ci-après).

     a. En guise de source des mises à jour, saisissez le répertoire de l'ordinateur intermédiaire dans lequel vous avez copié les mises à jour.

Kaspersky Security récupèrera les mises à jour via un des serveurs à protéger.

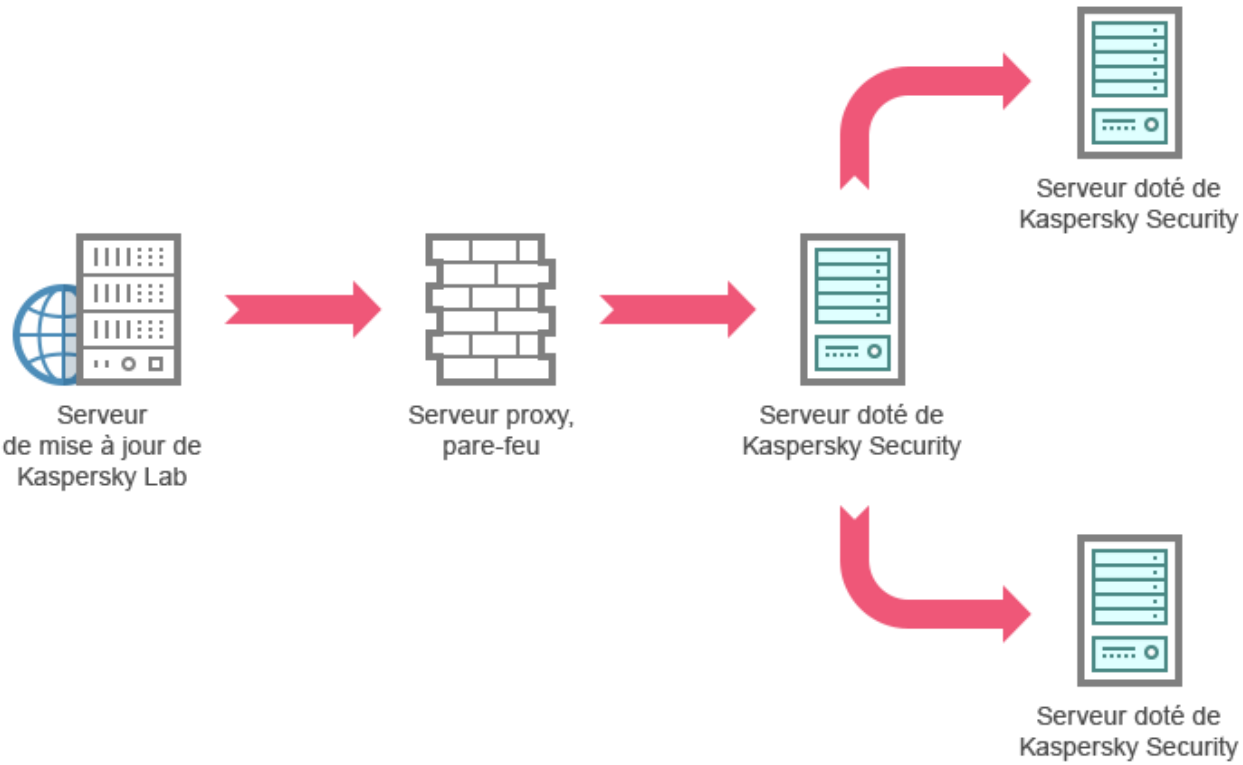


Illustration 2. Mise à jour via un des serveurs protégés

Schéma 3. Mise à jour via le serveur d'administration Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center pour assurer l'administration centralisée de la protection de l'ordinateur, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Security Center (cf. ill. ci-après).

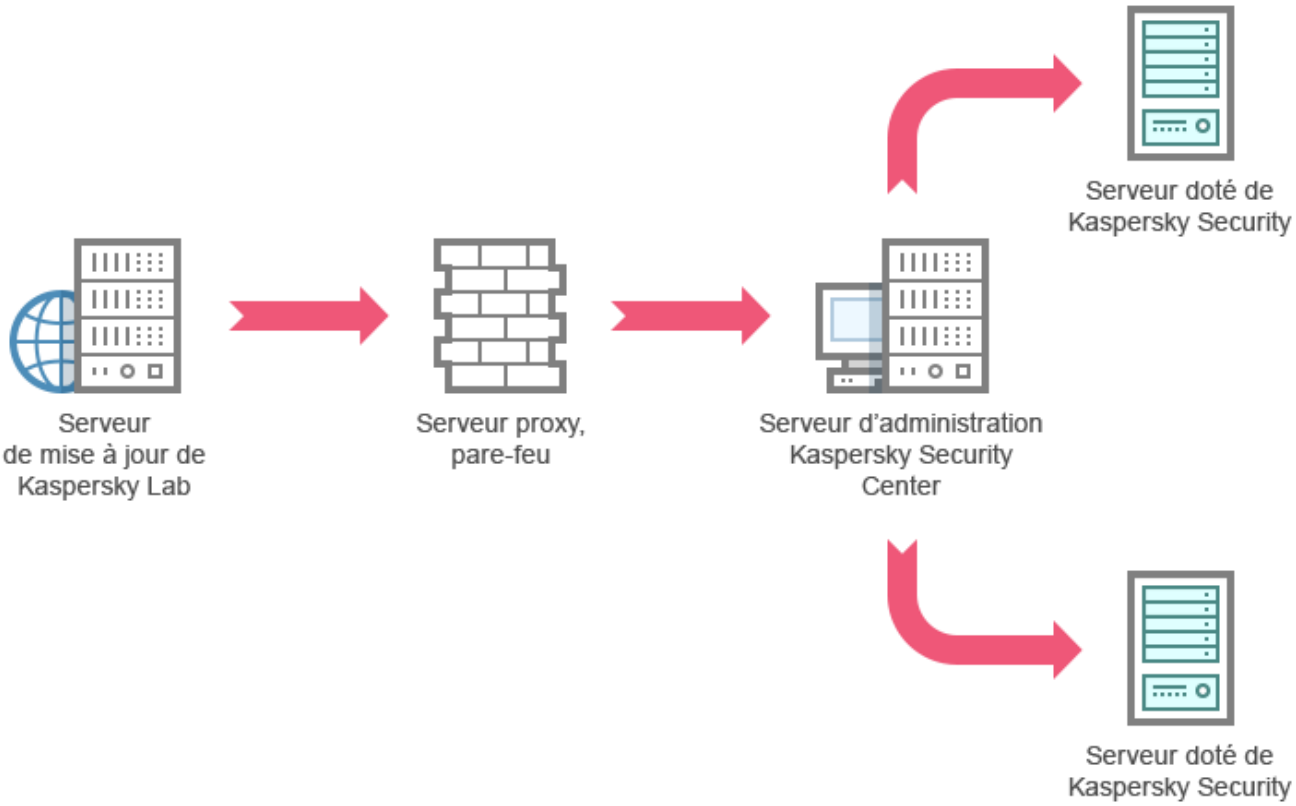


Illustration 3. Mise à jour via le serveur d'administration Kaspersky Security Center

► *Pour configurer la récupération des mises à jour de Kaspersky Security via le serveur d'administration Kaspersky Security Center, procédez comme suit.*

1. Téléchargement des mises à jour depuis le serveur de mise à jour de Kaspersky Lab vers le serveur d'administration Kaspersky Security Center Pour ce faire, procédez comme suit :

   - Configurez la tâche Réception des mises à jour par le serveur d'administration pour une sélection d'ordinateurs indiquée :

     a. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.

2. Diffusez les mises à jour sur les serveurs protégés. Pour ce faire, réalisez une des opérations suivantes :

   - Sur le serveur d'administration Kaspersky Security Center, configurez une tâche de groupe de mise à jour pour la copie des mises à jour sur les serveurs protégés :

     a. Dans la programmation de la tâche, choisissez la fréquence **Après réception des mises à jour par le serveur d'administration**.

     Le serveur d'administration exécutera la tâche chaque fois qu'il reçoit les mises à jour (cette méthode est la méthode recommandée).

     Vous ne pouvez pas sélectionner la fréquence d'exécution **Après réception des mises à jour par le serveur d'administration** dans la console de Kaspersky Security.

   - Configurez sur chaque serveur protégé les tâches Mise à jour de la base de l'application et Mise à jour des modules de l'application :

     a. En guise de source des mises à jour, désignez le Serveur d'administration Kaspersky Security Center.

     b. Le cas échéant, planifiez l'exécution de la tâche.

   Kaspersky Security récupèrera les mises à jour via le Serveur d'administration Kaspersky Security Center.

Si vous avez l'intention d'utiliser le serveur d'administration Kaspersky Security Center pour la diffusion des mises à jour, installez au préalable sur chaque serveur protégé le module logiciel Agent d'administration qui fait partie de l'application Kaspersky Security Center. Il assure l'interaction entre le serveur d'administration et Kaspersky Security sur le serveur protégé. Pour obtenir de plus amples informations sur l'agent d'administration et sur sa configuration à l'aide de l'application Kaspersky Security Center, consultez le document *Kaspersky Security Center. Manuel de l'administrateur*.

Configuration des tâches de mise à jour

Cette section contient des instructions sur la configuration des tâches de mise à jour de Kaspersky Security.

Dans cette section

Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Security

Pour chaque tâche de mise à jour, à l'exception de la tâche Annulation de la mise à jour des bases de l'application, il est possible de définir une ou plusieurs sources de mise à jour, d'ajouter des sources de mise à jour définies par l'utilisateur et de configurer les paramètres de connexions aux sources indiquées.

En cas de modification des paramètres des tâches de mises à jour, sachez que les nouvelles valeurs ne sont pas appliquées immédiatement dans les tâches de mises à jour en cours d'exécution. Les nouveaux paramètres seront appliqués uniquement à la prochaine exécution de la tâche.

► *Pour définir le type de source des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le panneau des résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Dans le groupe **Source des mises à jour**, sélectionnez le type de source de mises à jour pour Kaspersky Security:

   - **Serveur d'administration Kaspersky Security Center**.

     Kaspersky Security utilise le Serveur d'administration Kaspersky Security Center en tant que source de mise à jour.

     Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'accès distant de Kaspersky Security Center et si L'Agent d'administration (composant de Kaspersky Security Center qui gère les connexions entre les ordinateurs et le serveur d'administration) est installé sur le serveur sécurisé.

   - **Serveurs de mises à jour de Kaspersky Lab**.

     Kaspersky Security utilise les sites Web de Kaspersky Lab comme source de mises à jour. Ces serveurs hébergent les mises à jour des bases et des modules de programme de tous les logiciels de Kaspersky Lab.

     Cette option est sélectionnée par défaut.

   - **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

     Kaspersky Security utilise en guise de source de mises à jour les serveurs HTTP, FTP ou les dossiers des serveurs du réseau local désignés par l'administrateur.

     Vous pouvez composer la liste des sources qui contient la sélection la plus récente des mises à jour en cliquant sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

5. Le cas échéant, configurez les paramètres complémentaires des sources de mise à jour définie par l'utilisateur :

    a. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

        i. Dans la fenêtre **Serveurs de mise à jour** qui s'ouvre, cochez ou décochez les cases en regard des sources de mise à jour définies par l'utilisateur afin de commencer à les utiliser ou de suspendre leur utilisation.

        ii. Cliquez sur **OK**.

    b. Dans le groupe **Source des mises à jour**, sous l'onglet **Général**, cochez ou décochez la case **Utiliser les serveurs de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles**.

    La case active ou désactive la fonction d'utilisation des serveurs de mise à jour de Kaspersky Lab en guise de source des mises à jour si les sources que vous avez sélectionnées ne sont pas disponibles.

    Quand la case est cochée, la fonction est active.

    Cette case est cochée par défaut.

    Vous pouvez cocher la case **Utiliser les serveurs de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles** quand l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** est sélectionnée.

6. Dans la fenêtre **Paramètres de la tâche**, choisissez l'onglet **Paramètres de connexion**, afin de configurer les paramètres de connexion à la source des mises à jour :

    Exécutez les actions suivantes :

    - Décochez ou cochez la case **Utiliser le FTP en mode passif si possible**.

        La case active ou désactive la fonction qui permet de télécharger les mises à jour depuis des serveurs FTP en mode passif.

        Quand la case est cochée, la connexion est ouverte en mode passif.

        Quand la case est décochée, la connexion est ouverte en mode normal.

        Cette case est cochée par défaut.

    - Le cas échéant, définissez le délai d'attente (en secondes).

Dans le groupe **Paramètres de connexion aux sources des mises à jour** :

- Cochez ou décochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab**.

  La case active ou désactive l'utilisation des paramètres du serveur proxy si la mise à jour s'opère depuis des serveurs de Kaspersky Lab ou si la case **Utiliser les serveurs de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles** est cochée.

  Quand la case est cochée, les paramètres du serveur proxy sont utilisés.

  Quand la case est décochée, les paramètres du serveur proxy ne sont pas utilisés.

  Cette case est décochée par défaut.

- Cochez ou décochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux autres serveurs**.

  La case active ou désactive l'utilisation des paramètres du serveur proxy si l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

  Quand la case est cochée, les paramètres du serveur proxy sont utilisés.

  Cette case est décochée par défaut.

7. Cliquez sur **OK**.

Les paramètres configurés de la source de mises à jour de Kaspersky Security seront enregistrés et appliqués au prochain lancement de la tâche.

Vous pouvez gérer la liste des sources de mises à jour de Kaspersky Security définies par l'utilisateur.

► *Pour modifier la liste des sources de mises à jour définies par l'utilisateur, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le panneau des résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

   La fenêtre **Serveurs de mise à jour** s'ouvre.

5. Exécutez les actions suivantes :

   - Pour ajouter une nouvelle source de mise à jour définie par l'utilisateur, saisissez dans la zone de saisie l'adresse du répertoire contenant les fichiers de mise à jour sur le serveur FTP ou HTTP ; saisissez le répertoire local ou de réseau au format UNC (Universal Naming Convention). Appuyez sur la touche **ENTER**.

     Par défaut, le dossier ajouté est utilisé en guise de source de mises à jour.

   - Pour suspendre l'utilisation de la source définie par l'utilisateur, décochez la case en regard de la source dans la liste.

   - Pour activer l'utilisation de la source définie par l'utilisateur, cochez la case en regard de la source dans la liste.

   - Pour modifier l'ordre de sollicitation des sources par Kaspersky Security, déplacez la source sélectionnée vers le haut ou vers le bas de la liste (si vous voulez l'utiliser plus tôt ou plus tard) à l'aide des boutons **Monter** et **Descendre**.

   - Pour modifier le chemin d'accès à une source définie par l'utilisateur, sélectionnez la source dans la liste et cliquez sur le bouton **Modifier**. Introduisez les modifications nécessaires dans le champ, puis appuyez sur la touche **RETOUR**.

   - Pour supprimer une source définie par l'utilisateur, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

     > La liste doit toujours compter au moins une source.

6. Cliquez sur **OK**.

Les modifications introduites dans la liste des sources de mises à jour de l'application définies par l'utilisateur sont enregistrées.

Optimisation de l'utilisation du sous-système disque lors de l'exécution de la tâche Mise à jour des bases de l'application

Dans le cadre de l'exécution de la tâche Mise à jour des bases de l'application, Kaspersky Security place les fichiers de la mise à jour sur le disque local de l'ordinateur. Vous pouvez réduire la charge sur le sous-système disque de l'ordinateur en plaçant les fichiers des mises à jour sur un disque virtuel dans la mémoire vive lors de l'exécution de la mise à jour.

Cette fonction est disponible sous Microsoft Windows Server 2008 ainsi que les versions plus récentes du système d'exploitation.

Si vous utilisez cette fonction lors de l'exécution de la tâche Mise à jour des bases de l'application, un disque logique supplémentaire peut apparaître dans le système d'exploitation. Ce disque logique disparaît du système d'exploitation quand la tâche est terminée.

► *Pour réduire la charge sur le sous-système disque de l'ordinateur lors de l'exécution de la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée **Mise à jour des bases de l'application**.
3. Dans le panneau des résultats de l'entrée **Mise à jour des bases de l'application**, cliquez sur le lien **Propriétés**.
4. La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
5. Configurez les paramètres suivants dans le groupe **Optimisation de l'utilisation du sous-système disque** :
   - Cochez ou décochez la case **Réduire la charge sur le sous-système disque**.

     La case active ou désactive la fonction d'optimisation du sous-système disque grâce à un placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive.

Quand la case est cochée, la fonction est active.

Cette case est décochée par défaut.

- Définissez le volume de mémoire vive en méga-octets dans le champ **Volume de mémoire vive utilisé pour l'optimisation**. Le système d'exploitation affecte temporairement ce volume de mémoire vive à l'hébergement des fichiers des mises à jour pendant l'exécution de la tâche. Le volume de mémoire vive défini par défaut est de 512 Mo.

6. Cliquez sur **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Configuration des paramètres de la tâche Copie des mises à jour

► *Pour configurer les paramètres de la tâche Copie des mises à jour, procédez comme suit* :

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée **Copie des mises à jour**.
3. Dans le panneau des résultats de l'entrée **Copie des mises à jour**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Les onglets **Général** et **Configuration de connexion permettent** de configurer les paramètres d'utilisation des sources de mises à jour (cf. section "Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Security" à la page 265).
5. Dans le groupe **Paramètres de copie des mises à jour** de l'onglet **Général**, procédez comme suit :
   - Définissez les conditions de copie des mises à jour de l'application :
     - **Copier les mises à jour de l'application**.

       Kaspersky Security télécharge uniquement les mise à jour des bases de données de Kaspersky Security.

       Cette option est sélectionnée par défaut.

- **Copier les mises à jour critiques des modules de l'application**.

  Kaspersky Security télécharge uniquement les mises à jour urgentes des modules de Kaspersky Security.

- **Copier les mises à jour des bases de l'application et les mises à jour critiques des modules de l'application**.

  Kaspersky Security télécharge les mises à jour des bases et les mises à jour critiques des modules de Kaspersky Security.

- Indiquez le répertoire local ou de réseau dans lequel Kaspersky Security copiera les mises à jour reçues.

6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110).

7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115).

8. Cliquez sur **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Configuration des paramètres de la tâche Mise à jour des modules de l'application

► *Pour configurer les paramètres de la tâche Mise à jour des modules de l'application, procédez comme suit* :

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.

2. Sélectionnez la sous-entrée **Mise à jour des modules de l'application**.

3. Dans le panneau des résultats de l'entrée **Mise à jour des modules de l'application**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Les onglets **Général** et **Configuration de connexion** permettent de configurer les paramètres d'utilisation des sources de mises à jour (cf. section "Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Security" à la page 265).

5. Dans le groupe **Paramètres de la mise à jour** du groupe **Général**, configurez les paramètres de la mise à jour des modules de l'application :

   - **Rechercher uniquement la présence des mises à jour critiques des modules de l'application**.

     Kaspersky Security signale la présence de mises à jour urgentes des modules de l'application sur la source sans les télécharger. La notification a lieu si la notification pour ce type d'événement a été configurée.

     Cette option est sélectionnée par défaut.

   - **Copier et installer les mises à jour critiques des modules de l'application**.

     Kaspersky Security copie et installe les mises à jour critiques des modules de l'application.

   - **Autoriser le redémarrage de l'ordinateur**.

     Redémarrage du système d'exploitation après l'installation de mises à jour qui requièrent le redémarrage.

     Quand la case est cochée, Kaspersky Security redémarre le système d'exploitation après l'installation des mises à jour qui requièrent le redémarrage.

     La case est active si l'option **Copier et installer les mises à jour critiques des modules de l'application** a été sélectionnée.

     Cette case est décochée par défaut.

   - **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

     Réception des notifications sur toutes les mises à jour des modules de Kaspersky Security prévues disponibles sur la source. Kaspersky Security envoie les notifications si les notifications de ce type d'événement ont été configurées.

Quand la case est cochée, Kaspersky Security envoie les notifications relatives à toutes les mises à jour prévues des modules de l'application disponibles sur la source.

Cette case est cochée par défaut.

6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110). Par défaut, Kaspersky Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).

7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115).

8. Cliquez sur **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement *Une mise à jour prévue des modules d'application est disponible*. Celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées.

Annulation de la mise à jour des bases de données de Kaspersky Security

Avant d'appliquer la mise à jour des bases de données, Kaspersky Security crée une copie de sauvegarde des bases utilisées antérieurement. Si la mise à jour est interrompue ou se solde par un échec, Kaspersky Security reviendra automatiquement à l'utilisation des mises à jour installées antérieurement.

Si vous rencontrez des problèmes après la mise à jour des bases, vous pouvez revenir à l'état antérieur des bases grâce à la tâche Retour à l'état antérieur à la mise à jour des bases.

► *Pour lancer la tâche Annulation de la mise à jour des bases de l'application,*

cliquez sur le lien **Démarrer** dans le panneau des résultats du volet **Annulation de la mise à jour des bases de l'application**.

Remise à l'état antérieur à la mise à jour des modules logiciels

> Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Avant d'appliquer la mise à jour des modules logiciels, Kaspersky Security crée une copie de sauvegarde des modules utilisés actuellement. Si la mise à jour des modules est interrompue ou se solde par un échec, Kaspersky Security reviendra automatiquement à l'utilisation des derniers modules actualisés installés.

Pour revenir à l'état antérieur des modules logiciels, utilisez le composant **Ajout/suppression de programme** du panneau de configuration de Microsoft Windows.

Statistiques sur les tâches de mise à jour

Tandis que la tâche de mise à jour est exécutée, vous pouvez consulter les informations en temps réel relatives aux données reçues depuis le lancement de la tâche jusqu'à maintenant.

Après l'arrêt ou la suspension de la tâche, vous pouvez consulter les informations dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).

► *Pour consulter les statistiques de la tâche de mise à jour, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée qui correspond à la tâche dont vous souhaitez consulter les statistiques.

   Le panneau des résultats de l'entrée sélectionnée reprend les statistiques de la tâche dans le groupe **Statistiques**.

Si vous consultez la tâche Mise à jour des bases de l'application ou la tâche Copie des mises à jour, le groupe **Statistiques** affiche le volume de données téléchargées par Kaspersky Security en ce moment (**Données récupérées**).

Si vous consultez la tâche Mise à jour des modules de l'application, vous verrez les informations décrites dans le tableau ci-dessous.

Tableau 33. Informations sur la tâche Mise à jour des modules de l'application

Champ	Description
Données récupérées	Volume totale de données téléchargées
Mises à jour critiques disponibles	Nombre de mises à jour critiques prêtes pour l'installation.
Mises à jour prévues disponibles	Nombre de mises à jour prévues disponibles pour l'installation.
Erreur d'application des mises à jour	Si la valeur de ce champ est différente de zéro, la mise à jour n'a pas été appliquée. Vous pouvez consulter le nom de la mise à jour pendant laquelle l'erreur s'est produite dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).

Sauvegardes de Kaspersky Security

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur réparation ou leur suppression. Elle fournit également des instructions sur l'isolement des fichiers probablement infectés.

Dans cette section

Isolement des objets probablement infectés. Utilisation de la quarantaine

Cette section aborde l'isolement des objets probablement infectés, c.-à-d. le placement de ces objets en quarantaine, et la configuration de la quarantaine.

Dans cette section

À propos de l'isolement des objets probablement infectés

Kaspersky Security place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers la *quarantaine*. Pour des raisons de sécurité, une fois en quarantaine, les objets sont chiffrés.

Consultation des objets en quarantaine

Vous pouvez consulter les objets en quarantaine dans le nœud **Quarantaine** de la console de Kaspersky Security.

► *Pour consulter les objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.

   Les informations relatives aux objets placés en quarantaine apparaissent dans le panneau des résultats de l'entrée sélectionnée.

► *Pour trouver l'objet requis dans la liste des objets en quarantaine,*

triez les objets ou filtrez-les.

Dans cette section

Tri des objets en quarantaine

Par défaut, les objets dans la liste des objets en quarantaine sont triés par date de placement dans l'ordre chronologique inverse. Pour trouver l'objet souhaité, vous pouvez trier la liste selon le contenu des colonnes reprenant les informations sur les objets. Les résultats du tri sont préservés si vous fermez et ouvrez à nouveau l'entrée **Quarantaine**, ou si vous fermez la console de Kaspersky Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour trier les objets, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Dans le panneau de résultats de l'entrée **Quarantaine**, sélectionnez l'en-tête de la colonne selon lequel vous souhaitez trier les objets de la liste.

Les objets de la liste seront triés selon le paramètre sélectionné.

Filtrage des objets en quarantaine

Pour trouver l'objet souhaité en quarantaine, vous pouvez filtrer les objets de la liste et afficher uniquement ceux qui répondent aux critères de filtrage que vous avez définis. Les résultats du filtrage sont préservés si vous quittez et ouvrez à nouveau le nœud Quarantaine, ou si vous fermez la console de Kaspersky Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour définir un ou plusieurs filtres, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Dans le menu contextuel du nom de l'entrée, sélectionnez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.
4. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

   d. Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez les étapes a à d pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, observez les règles suivantes :

- Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
- Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la fenêtre **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer.**

5. Une fois que tous les filtres auront été ajoutés, cliquez sur le bouton **Appliquer**.

Les filtres créés sont enregistrés.

► *Pour afficher à nouveau tous les objets dans la liste des objets en quarantaine,* sélectionnez l'option **Supprimer le filtre** dans le menu contextuel de l'entrée **Quarantaine**.

Analyse des objets en quarantaine

Par défaut, Kaspersky Security exécute la tâche prédéfinie Analyse des objets en quarantaine après chaque mise à jour des bases de données. Les paramètres de la tâche sont présentés dans le tableau ci-après. Vous ne pouvez pas modifier les paramètres de la tâche Analyse des objets en quarantaine.

Vous pouvez planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 110), la lancer manuellement et modifier les autorisations du compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page 115) sous lequel la tâche est lancée.

Suite à l'analyse des objets en quarantaine après la mise à jour des bases, Kaspersky Security peut décider que certains d'entre eux sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés par Kaspersky Security, auquel cas il exécutera les actions définies dans les paramètres de la tâche d'analyse à la demande Analyse des objets en quarantaine : réparer, supprimer si la réparation est impossible.

Tableau 34. Paramètres de la tâche Analyse des objets en quarantaine

Paramètres de la tâche Analyse des objets en quarantaine	Valeur
Zone d'analyse	Répertoire de quarantaine
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; les valeurs possibles sont reprises au tableau suivant.

Tableau 35. Paramètres de sécurité de la tâche Analyse des objets en quarantaine

Paramètre de sécurité	Valeur
Analyse des objets	Analyser tous les objets
Optimisation	Désactivée
Actions à exécuter sur les objets infectés	Réparer, supprimer si la réparation est impossible
Action à exécuter sur les objets probablement infectés	Rapport uniquement
Exclure les objets	Non
Ne pas détecter	Non
Arrêter si l'analyse dure plus de (s.)	Non définie
Ne pas analyser les objets composés de plus de (Mo)	Non définie
Analyser les flux NTFS alternatifs	Activée
Analyser les secteurs d'amorçage et la partition MBR	Désactivée
Utiliser la technologie iChecker	Désactivée
Utiliser la technologie iSwift	Désactivée

Paramètre de sécurité	Valeur
Analyse des objets composés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * L'analyse uniquement des nouveaux fichiers et des fichiers modifiés est désactivée.
Vérification de la signature Microsoft des fichiers	Non exécutée
Utiliser l'analyseur heuristique	Appliqué au niveau d'analyse **Minutieuse**
Zone de confiance (cf. page 97)	Pas appliqué

Restauration d'un objet depuis la quarantaine

Kaspersky Security place les objets probablement infectés sous une forme cryptée dans le répertoire de quarantaine afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer n'importe quel objet de la quarantaine. La restauration d'un objet peut s'imposer dans les situations suivantes :

- Après l'analyse de la quarantaine à l'aide des bases actualisées, l'état d'un objet est devenu **Fausse alerte** ou **Réparé** ;
- Vous estimez que l'objet ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Security n'isole plus cet objet lors des analyses ultérieures, il faut l'exclure du traitement dans la tâche Protection des fichiers en temps réel et des tâches d'analyse à la demande. Pour ce faire, désignez l'objet comme valeur du paramètre de sécurité **Exclure les objets** (selon le nom du fichier) ou **Ne pas détecter** dans ces tâches ou ajoutez-le à la zone de confiance (cf. section "Zone de confiance" à page 97).

Lors de la restauration des objets, vous pouvez sélectionner l'endroit où sera placé l'objet : dans l'emplacement d'origine (défini par défaut), dans un dossier de restauration spécial sur le serveur protégé, dans un répertoire désigné de l'ordinateur où est installée la console de Kaspersky Security, ou sur un autre ordinateur du réseau.

Pour que Kaspersky Security n'analyse pas les objets volumineux lors de la restauration des fichiers depuis la quarantaine, définissez une exclusion pour le dossier %Temp%\wseeqbfiles\.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce répertoire est défini par les paramètres de la quarantaine.

La restauration d'objets de la quarantaine peut entraîner l'infection de l'ordinateur.

Vous pouvez restaurer l'objet en conservant une copie dans le répertoire de quarantaine afin de pouvoir l'utiliser ultérieurement, par exemple afin de pouvoir analyser une nouvelle fois l'objet après la mise à jour des bases.

Si l'objet placé en quarantaine fait partie d'un objet composé (une archive par exemple), Kaspersky Security ne l'inclut pas à nouveau dans cet objet lors de la restauration mais l'enregistre séparément dans le répertoire indiqué.

Vous pouvez restaurer un ou plusieurs objets.

► *Pour restaurer des objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Dans le panneau des résultats de l'entrée **Quarantaine**, exécutez une des actions suivantes :
   - pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer ;
   - pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez la commande **Restaurer**.

   La fenêtre **Restauration de l'objet** s'ouvre.

4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chaque objet sélectionné le répertoire dans lequel vous souhaitez conserver la copie restaurée (le nom de l'objet figure dans le champ **Objet** de la partie supérieure de la fenêtre ; si vous avez sélectionné plusieurs objets, ce champ reprend le nom du premier objet de la liste de sélection).

   Exécutez une des actions suivantes :

   - pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine** ;
   - Pour restaurer l'objet dans le répertoire que vous avez défini en tant que répertoire de restauration dans les paramètres de la quarantaine, sélectionnez **Restaurer dans le dossier du serveur par défaut** ;
   - pour restaurer l'objet dans un autre répertoire de l'ordinateur où vous avez installé la console de Kaspersky Security ou dans un répertoire de réseau, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis sélectionnez le répertoire souhaité ou saisissez le chemin d'accès à celui-ci.

5. Si vous souhaitez conserver une copie de l'objet dans le dossier de quarantaine après la restauration, désélectionnez la case **Supprimer les objets sauvegardés après leur restauration**.

6. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les objets sélectionnés seront restaurés et enregistrés à l'emplacement que vous aurez désigné : si vous avez choisi **Restaurer dans le dossier d'origine sur le serveur**, chacun de ces objets sera enregistré dans son emplacement d'origine ; si vous aviez choisi **Restaurer dans le dossier du serveur par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, tous les objets seront enregistrés dans le dossier indiqué.

7. Cliquez sur **OK**.

   Kaspersky Security commence par restaurer le premier des objets que vous avez sélectionnés.

8. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

    a. Choisissez l'une des actions suivantes pour Kaspersky Security :

    - **Remplacer** afin d'enregistrer l'objet restauré au lieu du fichier existant ;
    - **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet et son chemin d'accès dans le champ ;
    - **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

    b. Si vous avez sélectionné plusieurs objets pour la restauration, alors pour appliquer l'action **Remplacer** ou **Renommer en ajoutant un suffixe** à tous les objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).

    c. Cliquez sur **OK**.

    L'objet sera restauré ; les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, alors la fenêtre **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 3 des présentes instructions).

Mise en quarantaine d'objets

Vous pouvez mettre manuellement des fichiers en quarantaine.

► *Pour mettre un fichier en quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel du nom de l'entrée **Quarantaine**.
2. Choisissez l'option **Ajouter**.
3. Dans la fenêtre **Ouvrir**, sélectionnez le fichier que vous souhaitez placer en quarantaine.

4. Cliquez sur **OK**.

   Kaspersky Security place le fichier indiqué en quarantaine.

Suppression des objets de la quarantaine

Conformément aux paramètres de la tâche **Analyse des objets en quarantaine** (cf. page 280), Kaspersky Security supprime automatiquement du répertoire de quarantaine les objets dont l'état est devenu **Infecté** suite à l'analyse à l'aide des bases actualisées et qui n'ont pas pu être réparés. Kaspersky Security ne supprime pas les autres objets.

Vous pouvez supprimer manuellement un ou plusieurs objets de la quarantaine.

► *Pour supprimer un ou plusieurs objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Exécutez une des actions suivantes :
   - pour supprimer un objet, choisissez l'option **Supprimer** dans le menu contextuel du nom de l'objet ;
   - Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez l'option **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

Les objets sélectionnés seront supprimés de la quarantaine.

Envoi des objets potentiellement infectés à Kaspersky Lab pour examen

Si le comportement d'un objet quelconque indique selon vous la présence éventuelle d'une menace et que Kaspersky Security le considère comme un fichier sain, il se peut que vous soyez en présence d'un nouveau virus inconnu dont la description n'a pas encore été ajoutée à la base. Vous pouvez envoyer ce fichier à Kaspersky Lab pour examen. Les experts antivirus de Kaspersky Lab analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de réparation aux bases. Il se peut que lors d'une analyse ultérieure après la mise à jour des bases que Kaspersky Security le considère comme un fichier infecté et parvienne à le réparer. Vous pourrez alors non seulement conserver l'objet mais également éviter une épidémie virale.

Seuls les fichiers de la quarantaine peuvent être envoyés pour examen. Les fichiers en quarantaine sont conservés sous forme cryptée et lors de transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

Vous ne pouvez pas envoyer un objet de la quarantaine à Kaspersky Lab une fois que la licence n'est plus valide.

► *Pour envoyer un fichier à Kaspersky Lab pour examen, procédez comme suit :*

1. Si le fichier ne se trouve pas encore en quarantaine, placez-le à titre préventif (cf. page 285).
2. Dans le nœud **Quarantaine**, dans la liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous souhaitez envoyer à Kaspersky Lab pour examen et sélectionnez l'option **Envoyer l'objet pour analyse**.
3. Dans la fenêtre de confirmation de l'opération, cliquez sur **Oui** si vous voulez vraiment envoyer l'objet sélectionné pour le soumettre à un examen.
4. Si un client de messagerie est configuré sur le poste où la console de Kaspersky Security est installée, un nouveau message électronique sera créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

   Le champ **Destinataire** du message contient l'adresse email de Kaspersky Lab newvirus@kaspersky.com. Le champ **Sujet** contient le texte "Objet de la quarantaine".

Le corps du message contient le texte "Le fichier sera envoyé à Kaspersky Lab pour examen". Vous pouvez reprendre dans le corps du message n'importe quelle information complémentaire sur le fichier : raisons pour lesquelles il vous semble probablement infecté ou dangereux, son comportement et ses effets sur le système.

Le message est accompagné de l'archive <nom de l'objet>.cab. Il contient le fichier <uuid>.klq avec l'objet crypté (où uuid est l'identificateur unique de l'objet dans Kaspersky Security), le fichier <uuid>.txt avec les informations obtenues par Kaspersky Security sur l'objet et le fichier Sysinfo.txt qui contient les informations relatives à Kaspersky Security et au système d'exploitation du serveur :

- Nom et version du système d'exploitation ;
- Nom et version de Kaspersky Security ;
- Date d'édition des dernières mises à jour des bases installées ;
- Numéro de la clé active.

Ces informations sont indispensables aux experts de Kaspersky Lab afin de pouvoir analyser le fichier le plus vite et le plus efficacement possible. Toutefois, si vous ne souhaitez pas les transmettre, vous pouvez supprimer le fichier Sysinfo.txt de l'archive.

Si aucun client de messagerie n'est installé sur l'ordinateur où se trouve la console de Kaspersky Security, l'application propose d'enregistrer l'objet chiffré sélectionné dans un fichier. Ce fichier peut être envoyé seul à Kaspersky Lab.

► *Pour enregistrer l'objet crypté dans un fichier, procédez comme suit :*

1. Dans la fenêtre qui vous invite à enregistrer l'objet, cliquez sur le bouton **Oui**.
2. Sélectionnez le répertoire sur le disque du serveur protégé ou le répertoire de réseau dans lequel vous souhaitez enregistrer le fichier avec l'objet.

L'objet sera enregistré dans un fichier au format CAB.

Configuration des paramètres de la quarantaine

Vous pouvez configurer les paramètres de la quarantaine. Les nouvelles valeurs des paramètres de la quarantaine sont appliquées directement après l'enregistrement.

► *Pour configurer les paramètres de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Ouvrez le menu contextuel du nom de la sous-entrée **Quarantaine**.
3. Choisissez l'option **Propriétés**.
4. Dans fenêtre **Paramètres du stockage**, configurez les paramètres requis de la quarantaine en fonction de vos besoins :

   Dans le groupe **Paramètres de quarantaine** :

   - **Dossier de quarantaine**.

     Chemin d'accès au dossier de la quarantaine au format UNC (Universal Naming Convention).

     Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Quarantine\.

   - **Taille maximale de la quarantaine**.

     La case active ou désactive la fonction qui surveille le volume total des objets placés en quarantaine. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Security consigne l'événement *Dépassement de la taille maximum de quarantaine* et une notification est générée conformément aux paramètres pour ce type d'événement.

     Si la case est cochée, Kaspersky Security surveille le volume total des objets placés en quarantaine.

     Si la case est décochée, Kaspersky Security ne surveille pas le volume total des objets placés en quarantaine.

     Cette case est décochée par défaut.

- **Seuil d'espace disponible**.

  La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est en dessous de ce seuil, Kaspersky Security consigne l'événement *Seuil d'espace libre disponible dans la sauvegarde dépassé* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

  Si la case est cochée, Kaspersky Security surveille le volume d'espace disponible dans la sauvegarde.

  La case **Seuil d'espace disponible (Mo)** est active si la case **Taille maximale de sauvegarde (Mo)** a été cochée.

  Cette case est cochée par défaut.

  > Si le volume des objets en quarantaine dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Security vous le signale sans arrêter de placer les objets en quarantaine.

Dans le groupe **Paramètres de restauration** :

- **Dossier dans lequel sont rétablis les objets**.

  Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

  Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

5. Cliquez sur **OK**.

Les paramètres de la quarantaine définis seront enregistrés.

Statistiques de quarantaine

Vous pouvez consulter les informations relatives au nombre d'objets en quarantaine ; il s'agit des statistiques de la quarantaine.

► *Pour consulter les statistiques de la quarantaine,*

choisissez l'option **Statistiques** dans le menu contextuel du nom de l'entrée **Quarantaine** de l'arborescence de la console de Kaspersky Security.

La fenêtre **Statistiques** reprend les informations sur le nombre d'objets en quarantaine à l'heure actuelle (cf. tableau ci-dessous).

Tableau 36. Informations sur les objets en quarantaine dans la fenêtre Statistiques de quarantaine

Champ	Description
Objets potentiellement infectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Security.
Espace de quarantaine utilisé	Volume général de données dans le dossier de quarantaine.
Faux positifs	Nombre d'objets qui ont reçu l'état *Fausse alerte* car l'analyse de la quarantaine à l'aide des bases actualisées a indiqué ces objets comme étant sains.
Objets réparés	Nombre d'objets qui ont reçu l'état *Réparé* après l'analyse de la quarantaine.
Nombre total d'objets	Nombre total d'objets en quarantaine.

Sauvegarde des objets avant la réparation ou la suppression. Utilisation de la sauvegarde

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur réparation ou leur suppression. Elle fournit également des instructions sur la configuration des paramètres de la Sauvegarde.

Dans cette section

A propos de la copie de sauvegarde des objets avant la réparation ou la suppression

Kaspersky Security enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Potentiellement infecté* dans la *sauvegarde* avant de procéder à la réparation ou à la suppression de ces objets.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Security enregistre cet objet composé dans la sauvegarde. Par exemple, si Kaspersky Security considère un des objets de la base de messagerie comme étant suspect, il place en sauvegarde l'ensemble de la base de messagerie.

Si la taille de l'objet que Kaspersky Security copie dans la sauvegarde est importante, le système peut ralentir et l'espace disponible sur le disque dur de l'ordinateur peut être réduit.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur le serveur protégé ou sur un autre ordinateur du réseau local de l'organisation. Vous pouvez restaurer le fichier du dossier de sauvegarde si, par exemple, le fichier original infecté contenait des informations cruciales et que lors de la réparation, Kaspersky Security n'a pas réussi à le préserver, ce qui a rendu inaccessibles les informations qu'il contenait.

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Consultation des objets dans la sauvegarde

Vous pouvez consulter les objets du dossier de sauvegarde uniquement via la console de Kaspersky Security dans le nœud **Sauvegarde**. Vous ne pouvez pas les consulter à l'aide des gestionnaires de fichiers de Microsoft Windows.

► *Pour consulter les objets de la sauvegarde,*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.

Les informations relatives aux objets placés dans la sauvegarde apparaissent dans le panneau des résultats de l'entrée sélectionnée.

► *Pour trouver l'objet requis dans la liste des objets de la sauvegarde,*

triez les objets ou filtrez-les.

Dans cette section

Tri des fichiers de la sauvegarde

Par défaut, les fichiers de la sauvegarde sont classés par date d'enregistrement dans l'ordre chronologique inversé. Pour trouver le fichier requis, vous pouvez trier les fichiers selon le contenu de n'importe quelle colonne dans le panneau de résultats.

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Dans la liste des fichiers de la sauvegarde, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les objets.

Les fichiers de la sauvegarde seront triés en fonction du critère sélectionné.

Filtrage des fichiers de la sauvegarde

Pour trouver le fichier qu'il vous faut dans la sauvegarde, vous pouvez filtrer les fichiers, c.-à-d. afficher dans le nœud **Sauvegarde** uniquement les fichiers qui répondent aux conditions de filtrage que vous avez définies (les filtres).

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier

► *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Sauvegarde** et choisissez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.

2. Pour ajouter un filtre, procédez comme suit :

    a. Dans la liste **Nom du champ**, sélectionnez le champ dont la valeur sera comparée à la valeur du filtre.

    b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans le champ **Nom du champ**.

    c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

    d. Cliquez sur **Ajouter**.

    Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, vous pouvez observer les règles suivantes :

    - Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
    - Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
    - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
    - Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la fenêtre **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer**.

    Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les fichiers qui répondent aux conditions des filtres.

► *Pour afficher tous les fichiers dans la liste des fichiers dans la sauvegarde,*

sélectionnez l'option **Supprimer le filtre** dans le menu contextuel de l'entrée **Sauvegarde**.

Restauration des fichiers depuis la sauvegarde

Kaspersky Security place les fichiers sous une forme cryptée dans la sauvegarde afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer les fichiers de la sauvegarde.

La restauration d'un fichier peut s'imposer dans les situations suivantes :

- Si le fichier original, qui était infecté, contenait des informations importantes et que Kaspersky Security n'a pas pu préserver son intégrité lors de la réparation, ce qui a rendu les informations du fichier inaccessibles ;

- Vous estimez que le fichier ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Security ne considère plus ce fichier comme un fichier infecté ou probablement infecté lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche Protection des fichiers en temps réel et dans les tâches d'analyse à la demande. Pour ce faire désignez le fichier en tant que valeur du paramètre **Exclure les objets** ou du paramètre **Ne pas détecter** de ces tâches.

  La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Lors de la restauration d'un objet, vous pouvez sélectionner l'emplacement où l'objet restauré sera conservé : dans le répertoire d'origine (par défaut), dans un dossier spécial de restauration sur le serveur protégé ou dans un autre dossier indiqué sur l'ordinateur où la console de Kaspersky Security est installée ou sur un autre ordinateur du réseau.

Pour que Kaspersky Security n'analyse pas les objets volumineux lors de la restauration des fichiers depuis la sauvegarde, définissez une exclusion pour le dossier %Temp%\wseeqbfiles\.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès au dossier est défini dans les paramètres de la Sauvegarde (cf. section "Configuration des paramètres de la sauvegarde" à la page 299).

Par défaut, quand Kaspersky Security restaure un fichier, il enregistre une copie dans la sauvegarde. Vous pouvez supprimer la copie du fichier de la sauvegarde après la restauration.

► *Pour restaurer des fichiers depuis la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Exécutez une des actions suivantes :
   - pour restaurer un fichier, ouvrez le menu contextuel du fichier, dans la liste des fichiers de la sauvegarde, que vous souhaitez restaurer et sélectionnez l'option **Restaurer**.
   - pour restaurer plusieurs fichiers, sélectionnez les fichiers souhaités dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez l'option **Restaurer**.
4. Dans la fenêtre **Restauration de l'objet**, spécifiez le répertoire dans lequel le fichier restauré sera enregistré.

   Le nom du fichier apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous avez sélectionné plusieurs objets, dans ce champ est le nom du premier de la liste qui est affiché.

   Exécutez une des actions suivantes :

   - Pour enregistrer le fichier restauré sur le serveur protégé, sélectionnez une des options suivantes :
     - **Restaurer dans le dossier d'origine**, si vous souhaitez restaurer le fichier dans le dossier d'origine.
     - **Restaurer dans le dossier du serveur par défaut**, si vous souhaitez restaurer le fichier dans le dossier que vous avez désigné en guise de dossier pour la restauration dans les paramètres de la sauvegarde.
   - Pour enregistrer le fichier restauré dans un autre répertoire, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis sélectionnez le répertoire souhaité (sur l'ordinateur où est installée la console de Kaspersky Security ou dans un répertoire de réseau) ou saisissez le chemin d'accès à celui-ci.

5. Si vous ne souhaitez pas conserver une copie du fichier dans la sauvegarde après la restauration, cochez la case **Supprimer les objets sauvegardés après leur restauration** (case décochée par défaut)

6. Si vous avez sélectionné plusieurs fichiers pour la restauration, alors pour appliquer les conditions de conservation définies aux autres fichiers sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les fichiers sélectionnés seront restaurés et enregistrés dans le dossier que vous aurez désigné : si vous avez sélectionné l'option **Restaurer dans le dossier d'origine du serveur ou dans le dossier de réseau indiqué**, chacun des fichiers sera enregistré dans son dossier d'origine ; si vous avez sélectionné **Restaurer dans le dossier du serveur par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, tous les fichiers seront conservés dans le répertoire spécifié.

7. Cliquez sur **OK**.

   Kaspersky Security commence par restaurer le premier des fichiers que vous avez sélectionnés.

   Si un fichier portant le même nom existe déjà dans le répertoire indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

8. Exécutez les actions suivantes :

   a. Sélectionnez une des conditions suivantes de conservation du fichier restauré :

   - **Remplacer** afin d'enregistrer le fichier restauré au lieu du fichier existant.
   - **Renommer** afin d'enregistrer le fichier restauré sous un autre nom. Saisissez le nouveau nom du fichier et son chemin d'accès complet dans le champ
   - **Renommer en ajoutant un suffixe** afin de renommer le fichier en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

   b. Si vous souhaitez appliquer l'action **Remplacer** ou **Renommer** en ajoutant un suffixe aux fichiers restants, cochez la case **Appliquer à tous les objets**.

   Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets** ne sera pas accessible.

   c. Cliquez sur **OK**.

Le fichier sera restauré. Les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, alors la fenêtre **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer le répertoire dans lequel le prochain fichier de la sélection sera enregistré après la restauration (cf. étape 3 des présentes instructions).

Suppression des fichiers de la Sauvegarde

► *Pour supprimer un ou plusieurs fichiers de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Exécutez une des actions suivantes :
   - pour supprimer un fichier, ouvrez le menu contextuel du fichier que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;
   - Pour supprimer plusieurs objets, sélectionnez les objets souhaités dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez la commande **Supprimer**.
4. Dans la fenêtre **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

Les fichiers sélectionnés seront supprimés de la sauvegarde.

Configuration des paramètres de la sauvegarde

► *Pour configurer les paramètres de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Stockages**.
2. Ouvrez le menu contextuel du nom de la sous-entrée **Sauvegarde**.
3. Choisissez l'option **Propriétés**.

4. Dans fenêtre **Paramètres du stockage**, configurez les paramètres requis de la sauvegarde en fonction de vos besoins :

   Dans le groupe **Paramètres de Sauvegarde** :

   - **Dossier de sauvegarde**.

     Chemin d'accès à la sauvegarde au format UNC (Universal Naming Convention).

     Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Backup\.

   - **Taille maximale de sauvegarde (Mo)**.

     La case active ou désactive la fonction qui surveille le volume total des objets placés dans la sauvegarde. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Security consigne l'événement *Dépassement de la taille maximale de sauvegarde* et une notification est générée conformément aux paramètres pour ce type d'événement.

     Quand la case est cochée, Kaspersky Security surveille le volume total des objets placés dans la sauvegarde.

     Cette case est décochée par défaut.

   - **Seuil d'espace disponible (Mo)**.

     La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est en dessous de ce seuil, Kaspersky Security consigne l'événement *Seuil d'espace libre disponible dans la sauvegarde dépassé* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

     Si la case est cochée, Kaspersky Security surveille le volume d'espace disponible dans la sauvegarde.

     La case **Seuil d'espace disponible (Mo)** est active si la case **Taille maximale de sauvegarde (Mo)** a été cochée.

     Cette case est cochée par défaut.

   > Si le volume des objets de la sauvegarde dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Security vous le signale sans arrêter de placer les objets dans la sauvegarde.

Dans le groupe **Paramètres de restauration** :

- **Dossier dans lequel sont rétablis les objets**.

  Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

  Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

5. Cliquez sur **OK**.

Les paramètres configurés de la sauvegarde seront enregistrés.

Statistiques de sauvegarde

Vous pouvez consulter les informations relatives à l'état de la sauvegarde en ce moment ; il s'agit des statistiques de la sauvegarde.

► *Pour consulter les statistiques de la sauvegarde,*

dans l'arborescence de la Console, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez **Statistiques**. La fenêtre **Statistiques de sauvegarde** s'ouvre.

La fenêtre **Statistiques de sauvegarde** reprend les informations relatives à l'état de la sauvegarde à l'heure actuelle (cf. tableau ci-dessous).

Tableau 37. Informations sur l'état de la sauvegarde

Champ	Description
Taille actuelle de la sauvegarde	Volume de données dans la sauvegarde ; tient compte de la taille des fichiers chiffrés
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde

Consignation des événements. Journaux de Kaspersky Security

Cette section contient des informations sur l'utilisation des journaux de Kaspersky Security : journal d'audit système, journaux d'exécution des tâches de Kaspersky Security et journal des événements de Kaspersky Security.

Dans cette section

Modes d'enregistrement des événements de Kaspersky Security

Les événements de Kaspersky Security sont scindés en deux groupes :

- événements liés au traitement des objets dans les tâches de Kaspersky Security ;
- événements liés à l'administration de Kaspersky Security, par exemple lancement d'une application, création ou suppression de tâches, exécution de tâches, modification des paramètres d'une tâche.

Kaspersky Security utilise les méthodes suivantes pour consigner les événements :

- **Journaux d'exécution des tâches**. Le journal d'exécution des tâches contient des informations sur l'état actuel de paramètres de la tâche ou sur les événements survenus pendant l'exécution de la tâche.
- **Journal d'audit système**. Le journal d'audit système contient les informations relatives aux événements en rapport avec l'administration de Kaspersky Security.
- **Journal des événements**. Le journal des événements contient les informations relatives aux événements nécessaires au diagnostic des échecs de fonctionnement de Kaspersky Security. Ce journal est accessible dans la console Observateur d'événements de Microsoft Windows.

Si un problème survient durant l'utilisation de Kaspersky Security (par exemple, Kaspersky Security ou une tâche particulière s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un fichier de traçage et des fichiers dump de la mémoire des processus de Kaspersky Security et envoyer ces fichiers avec ces informations au service d'assistance technique de Kaspersky Lab pour analyse. Pour en savoir plus sur la création d'un fichier de traçage et de fichiers dump de mémoire, lisez la rubrique « Procédure de configuration des paramètres de fonctionnement généraux de Kaspersky Security dans la console de Kaspersky Security » (cf. page 62).

Kaspersky Security consigne les informations dans les fichiers de trace et le fichier dump de mémoire en clair.

Journal d'audit système

Kaspersky Security réalise un audit système des événements liés à l'administration de Kaspersky Security. L'application enregistre les informations relatives au lancement de l'application, au lancement et à l'arrêt de tâches de Kaspersky Security, aux modifications des paramètres des tâches, à la création et à la suppression de tâches d'analyse à la demande. Les enregistrements de ces événements apparaissent dans le panneau des résultats après la sélection du nœud **Journal d'audit système** dans la console de Kaspersky Security.

Par défaut, Kaspersky Security conservera les entrées du journal d'audit système pendant une durée indéterminée. Vous pouvez instaurer une limite pour la durée de conservation des enregistrements dans le journal d'audit système.

Vous pouvez désigner le dossier dans lequel Kaspersky Security enregistrera les fichiers du journal d'audit système, différent du dossier choisi par défaut.

Dans cette section

Tri des événements dans le journal d'audit système

Par défaut, les événements sont classés dans le journal d'audit système par ordre chronologique inverse.

Vous pouvez les trier selon le contenu de n'importe quelle colonne, à l'exception de la colonne Evénement.

► *Pour trier les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journal d'audit système**.
3. Dans le panneau de résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les événements de la liste.

   Le résultat du tri est conservé jusque la prochaine consultation du journal d'audit système.

Filtrage des événements dans le journal d'audit système

Si vous le souhaitez, vous pouvez afficher dans le journal d'audit système uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage que vous définissez (filtres).

► *Pour filtrer les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.
3. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez filtrer les événements.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.

   c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.
4. Le cas échéant, réalisez une des opérations suivantes :

   - Afin de réunir quelques filtres à l'aide de l'opérateur logique "ET", sélectionnez l'option **Quand toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres à l'aide de l'opérateur logique "OU", sélectionnez l'option **Quand n'importe quelle condition est remplie**.

5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements du journal d'audit système.

   La liste des événements du journal d'audit système affiche alors uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusque la prochaine consultation du journal d'audit système.

► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **Supprimer le filtre**.

   La liste des événements du journal d'audit système reprend alors tous les événements.

Suppression des événements du journal d'audit système

Par défaut, Kaspersky Security conservera les entrées du journal d'audit système pendant une durée indéterminée. Vous pouvez instaurer une limite pour la durée de conservation des enregistrements dans le journal d'audit système.

Vous pouvez supprimer manuellement tous les événements du journal d'audit système.

► *Pour supprimer des événements du journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **Effacer**.
3. Exécutez une des actions suivantes :

   - Si vous souhaitez exporter le contenu du journal d'audit système dans un fichier au format CSV ou TXT avant de supprimer les événements, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de la suppression. Indiquez le nom et l'emplacement du fichier dans la fenêtre qui s'ouvre.

- Si vous ne souhaitez pas exporter le contenu du journal dans un fichier, cliquez sur le bouton **Non** dans la fenêtre de confirmation de la suppression.

Le contenu du journal d'audit système est effacé.

Journaux d'exécution des tâches

Cette section contient des informations relatives aux journaux d'exécution des tâches de Kaspersky Security et à leur manipulation.

Dans cette section

A propos des journaux d'exécution des tâches

Les informations relatives à l'exécution des tâches de Kaspersky Security apparaissent dans le panneau des résultats lorsque le nœud **Journaux d'exécution des tâches** a été sélectionné dans la console de Kaspersky Security.

Le journal d'exécution de chaque tâche permet de voir les statistiques de l'exécution de la tâche, les informations relatives à chaque objet traité par l'application depuis le lancement de la tâche jusqu'à maintenant ainsi que les paramètres de la tâche.

Par défaut, Kaspersky Security conservera les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez désigner un dossier dans lequel Kaspersky Security enregistrera les fichiers des journaux d'exécution des tâches différent du dossier par défaut. Vous pouvez également sélectionner les événements qui seront consignés dans les journaux d'exécution des tâches de Kaspersky Security.

Consultation de la liste des événements dans les journaux d'exécution des tâches

► *Pour consulter la liste des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

   La liste des événements consignés dans les journaux d'exécution des tâches de Kaspersky Security apparaît dans le panneau des résultats.

Vous pouvez les trier selon le contenu de n'importe quelle colonne ou appliquer un filtre.

Tri des événements dans les journaux d'exécution des tâches

Par défaut, les événements sont classés dans les journaux d'exécution des tâches par ordre chronologique inverse. Vous pouvez les trier selon le contenu de n'importe quelle colonne.

► *Pour trier les événements repris dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

3. Dans le panneau de résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les événements des journaux d'exécution des tâches de Kaspersky Security.

   Le résultat du tri est conservé jusque la prochaine consultation des journaux d'exécution des tâches.

Filtrage des événements dans les journaux d'exécution des tâches

Si vous le souhaitez, vous pouvez afficher dans la liste des événements des journaux d'exécution des tâches uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage que vous définissez (filtres).

► *Pour filtrer les événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.
3. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez filtrer les événements.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.

   c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.

4. Le cas échéant, réalisez une des opérations suivantes :

   - Afin de réunir quelques filtres à l'aide de l'opérateur logique "ET", sélectionnez l'option **Quand toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres à l'aide de l'opérateur logique "OU", sélectionnez l'option **Quand n'importe quelle condition est remplie**.

5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements dans la liste des événements des journaux d'exécution des tâches.

La liste des événements des journaux d'exécution des tâches affiche alors uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusque la prochaine consultation des journaux d'exécution des tâches.

► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Supprimer le filtre**.

La liste des événements des journaux d'exécution des tâches reprend alors tous les événements.

Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security dans les journaux d'exécution des tâches

Les journaux d'exécution des tâches reprennent des informations détaillées sur tous les événements survenus dans ces tâches depuis leur lancement jusqu'au moment de la consultation ainsi que les statistiques d'exécution des tâches et leurs paramètres.

► *Pour consulter les statistiques et les informations relatives à une tâche de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

3. Dans le panneau des résultats, ouvrez la fenêtre **Journal d'exécution** d'une des méthodes suivantes :

   - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.

   - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal et choisissez l'option **Voir le journal**.

4. La fenêtre qui s'ouvre affiche les informations suivantes :

   - l'onglet **Statistiques** indique l'heure de lancement et de fin de la tâche et ses statistiques ;

   - l'onglet **Evénements** présente la liste des événements consignés pendant l'exécution de la tâche ;

   - l'onglet **Paramètres** reprend les paramètres de la tâche.

5. Le cas échéant, cliquez sur le bouton **Filtre** pour filtrer les événements dans le journal d'exécution de la tâche.

6. Le cas échéant, cliquez sur le bouton **Exporter** pour exporter les données du journal dans un fichier au format CSV ou TXT

7. Cliquez sur le bouton **Fermer** pour fermer la fenêtre **Journal d'exécution**.

Exportation des informations depuis le journal d'exécution des tâches

Vous pouvez exporter les données contenues dans le journal d'exécution d'une tâche dans un fichier au format CSV ou TXT.

► *Pour exporter les données du journal d'exécution d'une tâche, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.

2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

3. Dans le panneau des résultats, ouvrez la fenêtre **Journal d'exécution** d'une des méthodes suivantes :

   - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.
   - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal et choisissez l'option **Voir le journal**.

4. Dans la partie inférieure de la fenêtre **Journal d'exécution**, cliquez sur le bouton **Exporter**.

   La fenêtre **Enregistrer sous** s'ouvre.

5. Indiquez le nom, l'emplacement et le type d'encodage dans lequel vous souhaitez exporter les informations du journal d'exécution de la tâche, puis cliquez sur le bouton **Enregistrer**.

Suppression des événements des journaux d'exécution des tâches

Par défaut, Kaspersky Security conservera les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez supprimer manuellement tous les événements des journaux d'exécution des tâches terminées à ce moment.

> Les événements des journaux des tâches en cours d'exécution et les journaux utilisés par d'autres utilisateurs ne seront pas supprimés.

► *Pour supprimer des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

3. Exécutez une des actions suivantes :

   - Si vous souhaitez supprimer des événements de tous les journaux d'exécution des tâches terminées en ce moment, ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Effacer**.

   - Si vous souhaitez effacer le contenu du journal d'exécution d'une tâche distincte, ouvrez, dans le panneau des résultats, le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez efface le journal d'exécution et choisissez l'option **Supprimer**.

   - Si vous souhaitez effacer le contenu des journaux d'exécution de plusieurs tâches, procédez comme suit :

     a. Dans le panneau des résultats, enfoncez la touche **Ctrl** ou **Maj** et sélectionnez les événements survenus dans les tâches dont vous souhaitez supprimer les journaux d'exécution.

     b. Ouvrez le menu contextuel du menu de n'importe lequel des événements enregistrés et choisissez l'option **Supprimer**.

4. Dans la fenêtre de confirmation de la suppression, cliquez sur **Oui** afin de confirmer la suppression de la clé.

Les journaux d'exécution des tâches sélectionnés seront effacés. La suppression des événements des journaux d'exécution des tâches seront consignées dans le journal d'audit système.

Consultation du journal des événements de Kaspersky Security dans la console Observateur d'événements

A l'aide du composant logiciel enfichable **Observateur d'événements** pour Microsoft Management Console, vous pouvez consulter le journal des événements de Kaspersky Security. Kaspersky Security y consigne les événements nécessaires au diagnostic des échecs de fonctionnement de Kaspersky Security.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements selon les critères suivants :

- **selon le type d'événement** ;
- **selon le niveau de détail**. Le niveau de détail correspond au niveau d'importance des événements consignés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est **Evénements d'information** : les événements de tous les niveaux d'importance sont consignés ; le moins détaillé est le niveau **Evénements critiques** où seuls les événements critiques sont consignés Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) ; pour le composant **Mise à jour**, c'est le niveau **Evénements d'information** qui est sélectionné.

► *Pour consulter le journal des événements de Kaspersky Security, procédez comme suit :*

1. Si vous configurez les paramètres localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `mmc`, puis appuyez sur la touche **ENTER**.

   La fenêtre de Microsoft Management Console s'ouvre.

2. Choisissez **Fichier → Ajouter ou supprimer des composants logiciels enfichables**.

   La fenêtre **Ajout et suppression de composants logiciels enfichables** s'ouvre.

3. Dans la liste des composants logiciels enfichables disponibles, sélectionnez **Observateur d'événements** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection d'ordinateur** s'ouvre.

4. Indiquez dans la fenêtre **Sélection d'ordinateur** l'ordinateur sur lequel Kaspersky Security est installé, puis cliquez sur le bouton **OK**.

5. Dans la fenêtre **Ajout et suppression de composants logiciels enfichables**, cliquez sur **OK**.

   Le noeud **Observateur d'événements** apparaît dans l'arborescence de la Console.

6. Dans l'arborescence de la Console, développez le nœud **Observateur d'événements**, puis sélectionnez le nœud secondaire **Journaux des applications et des services → Kaspersky Security**.

   Le journal des événements de Kaspersky Security s'ouvre.

Configuration des paramètres des journaux dans la console de Kaspersky Security

Vous pouvez configurer les paramètres suivants pour les journaux de Kaspersky Security :

- durée de la conservation des événements dans les journaux d'exécution des tâches et du journal d'audit système ;
- emplacement du dossier dans lequel Kaspersky Security enregistre les fichiers des journaux d'exécution des tâches et du journal d'audit système ;
- événements consignés par Kaspersky Security dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements de Kaspersky Security dans la console Observateur d'événements.

► *Pour configurer les paramètres des journaux de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, ouvrez le menu contextuel du nœud **Journaux** et choisissez la commande **Propriétés**.

   La fenêtre **Propriétés : journaux** s'ouvre.

2. Dans la fenêtre **Propriétés : Journaux**, configurez les paramètres des journaux en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, sélectionnés, le cas échéant, les événements consignés par Kaspersky Security dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements de Kaspersky Security dans la console Observateur d'événements. Pour ce faire, procédez comme suit :

     - Dans la liste **Composant**, sélectionnez le composant de Kaspersky Security dont vous souhaitez configurer le niveau de détails.

Pour les composants Protection des fichiers en temps réel, Protection des stockages réseau connectés via le protocole RPC, Protection des stockages réseau connectés via le protocole ICAP, Analyse des scripts, Analyse à la demande et Mise à jour, il est prévu de consigner les événements dans les journaux d'exécution des tâches et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Journaux** et **Journal des événements**. Pour les composants Quarantaine et Sauvegarde, les événements sont consignés dans le journal d'audit système et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Audit** et **Journal des événements**.

- La liste **Niveau d'importance** permet de sélectionner le niveau de détail des événements dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements pour le composant fonctionnel sélectionné.

  Le tableau de la liste des événements en dessous reprend des cases cochées en regard des événements consignés dans les journaux d'exécution des tâches, le journal d'audit système et le journal des événements en fonction du niveau de détail sélectionné.

- Si vous souhaitez activer manuellement la consignation d'événements distincts pour le module fonctionnel sélectionné, procédez comme suit :

  a. Dans la liste **Niveau d'importance**, choisissez **Personnalisé**.

  b. Dans le tableau de la liste des événements, cochez la case en regard des événements dont vous souhaitez activer la consignation dans les journaux d'exécution des tâches, le journal d'audit système et le journal des événements

- Le cas échéant, sous l'onglet **Avancé**, sélectionnez le dossier dans lequel Kaspersky Security va enregistrer les fichiers des journaux et définissez la durée de conservation des événements dans les journaux d'exécution des tâches et dans le journal d'audit système :

  - **Dossier des journaux**.

    Chemin d'accès au dossier contenant les journaux; au format UNC (Universal Naming Convention).

    Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Reports\.

  - **Supprimer les journaux d'exécution des tâches et événements de plus de (jours)**.

    La case active ou désactive la fonction qui supprime les journaux contenant les résultats de l'exécution des tâches terminées et les événements publiés dans le journal d'exécution des tâches à l'issue de la période définie (par défaut, 30 jours).

    Quand la case est cochée, Kaspersky Security supprime les journaux des résultats d'exécution des tâches terminées et les événements publiés dans les journaux d'exécution des tâches à l'issue de la période définie.

    Cette case est cochée par défaut.

  - **Supprimer les événements du journal d'audit de plus de (jours)**.

    La case active ou désactive la fonction qui supprime les événements enregistrés dans le journal d'audit à l'issue de la période définie (par défaut, 60 jours).

    Quand la case est cochée, Kaspersky Security supprime les événements enregistrés dans le journal d'audit à l'issue de la période définie.

    Cette case est cochée par défaut.

3. Cliquez sur **OK**.

Les modifications seront enregistrées.

Configuration des notifications

Cette section contient des informations sur les différentes méthodes de notification des utilisateurs et des administrateurs de Kaspersky Security sur les événements de l'application et l'état de la protection du serveur, ainsi que les instructions relatives à la configuration des notifications.

Dans cette section

Moyens de notification de l'administrateur et des utilisateurs

Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Security et à l'état de la protection antivirus du serveur.

L'application assure l'exécution des tâches suivantes :

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peuvent obtenir des informations sur les événements de type *Objet détecté* qui surviennent pendant la tâche Protection des fichiers en temps réel.

Dans la console de Kaspersky Security, vous pouvez activer les notifications de l'administrateur et des utilisateurs de plusieurs manières :

- Moyens de notification des utilisateurs :

    a. Outils des services des terminaux.

    Vous pouvez utiliser cette méthode pour la notification des utilisateurs de terminaux si le serveur protégé est un serveur de terminaux.

    b. Outils du service Windows Messenger.

    Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger. Ce mode n'est pas utilisé si le serveur protégé fonctionne sous Microsoft Windows Server 2008.

- Moyens de notification des administrateurs :

    a. Outils du service Windows Messenger.

    Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger. Ce mode n'est pas utilisé si le serveur protégé fonctionne sous Microsoft Windows Server 2008.

    b. Lancement du fichier exécutable.

    Cette méthode lance un fichier exécutable stocké sur le disque local du serveur protégé en fonction de l'événement.

    c. Envoi par email.

    Ce mode transmet les messages via le courrier électronique.

Vous pouvez créer un texte différent pour chaque type d'événement. Ce texte peut contenir des champs avec les informations sur l'événement. Un texte prédéfini du message est utilisé par défaut pour les notifications des utilisateurs.

Configuration des notifications de l'administrateur et des utilisateurs

La configuration des notifications sur les événements porte sur le mode de notification et sur la composition du texte du message.

► *Pour configurer les notifications sur les événements, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security** et sélectionnez l'option **Configurer les paramètres des notifications**.

   La boîte de dialogue **Notifications** s'ouvre.

2. Exécutez les actions suivantes dans la fenêtre **Notifications** :

   - Si vous souhaitez définir les moyens de notification de l'administrateur, réalisez les actions suivantes :

     a. Dans la liste **Type d'événement**, sélectionnez les types d'événements.

     b. Dans le groupe de paramètres **Informer les administrateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

   - Si vous souhaitez définir les moyens de notification des utilisateurs, cochez la case en regard des options souhaitées dans le groupe **Informer les utilisateurs**. Vous pouvez configurer les notifications des utilisateurs uniquement pour l'événement **Objet détecté**.

3. Si vous souhaitez modifier le texte de la notification, procédez comme suit :

   a. Cliquez sur le bouton **Texte du message** dans le groupe **Informer les administrateurs** ou dans le groupe **Informer les utilisateurs**. Dans la fenêtre **Texte du message**, saisissez le texte qui sera affiché dans le message relatif à l'événement.

   Vous pouvez composer un texte du message de notification pour plusieurs types d'événements : après avoir choisi le mode de notification pour un type d'événement, sélectionnez, à l'aide de la touche **CTRL** ou **MAJ**, les autres types d'événements pour lesquels vous souhaitez créer ce même texte du message avant de clique sur le bouton **Texte du message**.

b. Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Macro** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette rubrique.

c. Pour restaurer le texte du message prévu par défaut pour l'événement, cliquez sur **Par défaut**.

4. Si vous souhaitez configurer les modes de notification sélectionnés de l'administrateur sur un événement sélectionné, cliquez sur le bouton **Configuration** dans la fenêtre **Notifications** et dans la fenêtre **Paramètres avancés**, procédez à la configuration des modes sélectionnés. Pour ce faire, procédez comme suit :

   a. Pour les notifications via email, ouvrez l'onglet **Courriel** et saisissez les adresses email des destinataires (séparez les adresses par un point-virgule), le nom ou l'adresse de réseau du serveur SMTP, ainsi que son port, dans les champs prévus à cet effet. Si nécessaire, indiquez le texte qui figurera dans les champs **Sujet** et **De**. Le texte du champ **Sujet** peut contenir des valeurs de champs d'informations (cf. tableau ci-dessous).

   Si vous souhaitez utiliser la vérification de l'authenticité selon le compte utilisateur lors de la connexion au serveur SMTP, il faudra dans ce cas cochez la case **Authentification SMTP requise** dans le groupe **Paramètres d'authentification** et saisir le nom et le mot de passe de l'utilisateur dont l'authenticité sera vérifiée.

   b. Pour les notifications via le service de messagerie, sous l'onglet **Service de messagerie**, composez la liste des ordinateurs des destinataires des messages : pour chaque ordinateur que vous souhaitez ajouter, cliquez sur le bouton **Ajouter** et dans le champ, saisissez son nom de réseau.

   > N'oubliez pas que les notifications via le **Service Windows Messenger** ne sont pas utilisées si le serveur protégé tourne sous Microsoft Windows Server 2008 et les versions suivantes de Microsoft Windows Server.

   c. Pour le lancement d'un fichier exécutable, sélectionnez le fichier sur le disque local du serveur protégé qui sera exécuté sur le serveur lorsque l'événement se produira dans l'onglet **Fichier exécutable** ou saisissez le chemin d'accès à ce dernier. Saisissez le nom et le mot de passe de l'utilisateur sous le compte duquel le fichier sera exécuté.

En indiquant le chemin d'accès au fichier exécutable, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Si vous souhaitez limiter le nombre de messages de notification en fonction d'événements d'un même type par unité de temps, cochez la case **Ne pas répéter la notification plus de** sous l'onglet **Avancé** et indiquez la valeur souhaitée par unité de temps.

5. Cliquez sur **OK**.

Les paramètres de la notification définis seront enregistrés.

Tableau 38. Champs d'information sur les événements

Champ	Description
%EVENT_TYPE%	Type d'événement.
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%EVENT_SEVERITY%	Niveau d'importance de l'événement.
%OBJECT%	Nom de l'objet (dans les tâches de protection en temps réel et d'analyse à la demande) Dans la tâche de mise à jour des modules de l'application, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.
%VIRUS_NAME%	Nom de l'objet détecté selon la classification de l'Encyclopédie des virus (http://www.securelist.fr). Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Security renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).

Champ	Description
%VIRUS_TYPE%	Type de l'objet détecté selon la classification de Kaspersky Lab, par exemple "virus" ou "cheval de Troie". Figure dans le nom complet de l'objet détecté renvoyé par Kaspersky Security lorsque celui-ci considère l'objet comme infecté ou probablement infecté. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).
%USER_COMPUTER%	Dans les tâches Protection des fichiers en temps réel et Protection des stockages réseau connectés via le protocole RPC, désigne le nom de l'ordinateur de l'utilisateur qui a sollicité l'objet sur le serveur.
%USER_NAME%	Dans les tâches Protection des fichiers en temps réel et Protection RPC des stockages réseau connectés, désigne le nom de l'utilisateur qui a sollicité l'objet sur le serveur.
%FROM_COMPUTER%	Nom du serveur protégé d'où provient la notification
%EVENT_REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements)
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement "erreur interne de la tâche")
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)

Administration du stockage hiérarchique

Cette section contient des informations sur l'analyse antivirus des fichiers qui se trouvent dans des stockages hiérarchiques et dans des systèmes de sauvegarde.

Dans cette section

A propos du stockage hiérarchique

Le système d'administration de stockage hiérarchique (Hierarchical Storage Management, HSM) (ci-après système HSM) permet de déplacer des données entre des disques locaux rapides et des périphériques lents de conservation de données à long terme. Malgré les avantages évidents des périphériques de rappel rapides, leur utilisation reste chère pour la majorité des entreprises. Les systèmes HSM garantissent le transfert des informations non utilisées vers des périphériques bon marché de stockage à distance, ce qui réduit les dépenses de la société.

Les systèmes HSM enregistrent une partie des informations dans des référentiels distants et les restaure en cas de besoin. Les systèmes HSM assurent un contrôle permanent de l'utilisation des fichiers et définissent ceux qui peuvent être déplacés dans le stockage distant et ceux qu'il est préférable de laisser sur les périphériques de stockage local. Les fichiers sont déplacés vers le stockage distant s'ils ne sont pas sollicités pendant une période définie. Si l'utilisateur sollicite le fichier situé dans le stockage distant, celui est transféré à nouveau vers le disque local. Ce principe garantit à l'utilisateur un accès rapide à un volume important d'informations qui est bien supérieur à la capacité du disque.

Lors du déplacement d'un fichier depuis le disque local vers le stockage distant, le système HSM conserve le lien vers l'emplacement effectif de ce fichier. En cas de sollicitation d'un fichier contenant un lien, le système définit l'emplacement des données sur le périphérique d'archives. Le remplacement des fichiers par des liens dans l'emplacement de stockage permet d'obtenir un stockage à la capacité quasiment illimitée.

Certains systèmes HSM permettent de conserver une partie des fichiers dans le stockage local. Dans ce cas, une grande partie du fichier est déplacée vers stockage distant tandis qu'une petite partie du fichier source reste sur le stockage local.

Les systèmes HSM proposent deux méthodes d'accès aux informations situées dans le stockage hiérarchique :

- points de traitement réitéré ;
- attributs élargis du fichier.

Configuration de paramètres du système HSM

Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut du paramètre **Type d'accès au stockage hiérarchique** (**Aucun système HSM**).

Pour configurer l'accès au stockage hiérarchique, vous devez indiquer la manière dont le système HSM détermine l'emplacement du fichier analysé. Ces informations figurent dans la documentation du système HSM utilisé.

► *Pour désigner le mode d'accès au stockage hiérarchique, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security, ouvrez le menu contextuel de l'entrée **Kaspersky Security**.
2. Sélectionnez l'option **Stockage hiérarchique**.

   La fenêtre **Paramètres du système HSM** s'ouvre

3. Sous l'onglet **Stockage hiérarchique**, définissez les paramètres du système HSM :

   - **Aucun système HSM**.

     Kaspersky Security n'utilise pas les paramètres du système HSM lors de l'exécution des tâches d'analyse à la demande.

     Cette option est sélectionnée par défaut.

   - **Le système HSM utilise des points de traitement réitéré**.

     Kaspersky Security utilise des points de traitement réitéré pour l'analyse des fichiers dans le stockage distant lors de l'exécution des tâches d'analyse à la demande.

   - **Le système HSM utilise les attributs élargis du fichier**.

     Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

     Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

   - **Système HSM non identifié**.

     Kaspersky Security analyse tous les fichiers, comme les fichiers situés dans un stockage distant, lors de l'exécution des tâches d'analyse à la demande.

     Il est déconseillé d'utiliser cette option.

     > Si vous désignez une option incorrecte ou si vous choisissez l'option **Système HSM non identifié**, Kaspersky Security pourrait se tromper dans la définition de l'emplacement des objets, ce qui augmenterait la durée de traitement des objets.

4. Cliquez sur le bouton **OK**.

Les paramètres du système HSM définis seront enregistrés.

Administration de Kaspersky Security via la ligne de commande

Cette section contient des informations et des instructions sur la gestion du fonctionnement de Kaspersky Security via la ligne de commande.

Dans cette section

Commandes pour l'administration de Kaspersky Security via la ligne de commande

Vous pouvez exécuter les principales instructions d'administration de Kaspersky Security via la ligne de commande du serveur protégé, si vous avez inclus le composant **Utilitaire de ligne de commande** dans la liste des composants à installer lors de l'installation de Kaspersky Security.

La ligne de commande permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Security.

Certaines commandes de Kaspersky Security sont exécutées dans les modes suivants :

- Mode synchrone : l'administration revient à la console uniquement après la fin de l'exécution de la commande.
- Mode asynchrone : l'administration revient à la console directement après le lancement de la commande.

► *Pour interrompre l'exécution d'une commande en mode synchrone,*

appuyez sur la combinaison de touches **Ctrl**+**C**.

Lors de la saisie d'une instruction de Kaspersky Security, respectez les règles suivantes :

- Saisissez les paramètres et les instructions en majuscules ou en minuscules ;
- Séparez les paramètres par des espaces ;
- si le nom du fichier attribué en tant que valeur d'un paramètre contient un espace, alors saisissez ce nom (et son chemin d'accès) entre guillemets, par exemple : "C:\TEST\test cpp.exe" ;
- le cas échéant, vous pouvez utiliser des caractères génériques dans les noms des fichiers ou des chemins, par exemple : « C:\Temp\Temp*\ », « C:\Temp\Temp???.doc », « C:\Temp\Temp*.doc »

La ligne de commande vous permet d'effectuer toutes les opérations de gestion et d'administration de Kaspersky Security (cf. tableau ci-dessous).

Tableau 39. Commandes de Kaspersky Security

Instruction	Description
KAVSHELL HELP (cf. page 330)	Affiche l'aide sur les instructions de Kaspersky Security.
KAVSHELL START (cf. page 331)	Lance le service Kaspersky Security.
KAVSHELL STOP (cf. page 331)	Arrête le service Kaspersky Security.
KAVSHELL SCAN (cf. page 332)	Crée et lance une tâche d'analyse à la demande temporaire dont la zone d'analyse et les paramètres de sécurité sont définis par les arguments de l'instruction.
KAVSHELL SCANCRITICAL (cf. page 338)	Lance la tâche prédéfinie Analyse des zones critiques.
KAVSHELL TASK (cf. page 339)	Lance/suspend/relance/arrête la tâche indiquée en mode asynchrone/rend l'état actuelle de la tâche/les statistiques de la tâche.

Instruction	Description
KAVSHELL RTP (cf. page 341)	Lance ou arrête toutes les tâches de protection en temps réel.
KAVSHELL UPDATE (cf. page 342)	Lance la tâche de mise à jour des bases de Kaspersky Security selon les paramètres définis à l'aide des arguments de l'instruction.
KAVSHELL ROLLBACK (cf. page 347)	Remet les bases à l'état antérieur à la mise à jour.
KAVSHELL LICENSE (cf. page 348)	Gère les clés et les codes d'activation.
KAVSHELL TRACE (cf. page 349)	Active ou désactive la création du journal de trace, gère les paramètres du journal de trace.
KAVSHELL DUMP (cf. page 353)	Active ou désactive la création de fichiers dump de mémoire des processus de Kaspersky Security en cas d'arrêt suite à une erreur.
KAVSHELL IMPORT (cf. page 354)	Importe les paramètres généraux de Kaspersky Security, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration créé au préalable.
KAVSHELL EXPORT (cf. page 355)	Exporte tous les paramètres de Kaspersky Security et des tâches existantes dans un fichier de configuration.

Dans cette section

Affichage de l'aide sur les instructions de Kaspersky Security. KAVSHELL HELP

Pour obtenir la liste de toutes les instructions de Kaspersky Security, utilisez une des commandes suivantes :

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une commande, saisissez une des commandes suivantes :

```
KAVSHELL HELP <instruction>

KAVSHELL <instruction> /?
```

Exemples d'instruction KAVSHELL HELP

Pour consulter des informations plus détaillées sur l'instruction KAVSHELL SCAN, exécutez la commande suivante :

```
KAVSHELL HELP SCAN
```

Lancement et arrêt du service Kaspersky Security. KAVSHELL START, KAVSHELL STOP

Pour lancer le service de Kaspersky Security, utilisez l'instruction `KAVSHELL START`.

Le lancement du service de Kaspersky Security s'accompagne par défaut de l'activation de la Protection des fichiers en temps réel, de l'Analyse des scripts, de l'Analyse au démarrage du système ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Pour arrêter le service de Kaspersky Security, utilisez l'instruction `KAVSHELL STOP`.

Analyse du secteur indiqué. KAVSHELL SCAN

Pour lancer la tâche d'analyse de secteurs définis du serveur protégé, utilisez l'instruction `KAVSHELL SCAN`. Les arguments de cette commande définissent les paramètres de la zone d'analyse et paramètres de sécurité de l'entrée sélectionnée.

La tâche d'analyse à la demande lancée à l'aide de l'instruction `KAVSHELL SCAN` est temporaire. Elle apparaît dans la console de Kaspersky Security uniquement pendant son exécution (la console de Kaspersky Security ne vous permet pas de consulter les paramètres de la tâche). Le journal d'exécution de la tâche est enregistré en même temps ; il apparaît dans l'entrée **Journaux d'exécution des tâches** de la Console de Kaspersky Security. Les tâches créées et lancées via la commande SCAN peuvent être soumises à une stratégie de l'application Kaspersky Security Center.

Vous pouvez employer une variable système pour désigner le chemin dans la tâche d'analyse de zones distinctes. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL SCAN` avec les privilèges de cet utilisateur.

L'instruction `KAVSHELL SCAN` est exécutée en mode synchrone.

Pour lancer une tâche existante d'analyse à la demande depuis la ligne de commande, utilisez l'instruction KAVSHELL TASK (cf. page 339).

Syntaxe de l'instruction KAVSHELL SCAN

```
KAVSHELL SCAN <zones d'analyse>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< nom du
fichier contenant la liste des zones d'analyse >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"masque">] [/ES:<taille>] [/ET:<nombre de secondes>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<nom du
fichier du journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la
tâche>]
```

L'instruction KAVSHELL SCAN contient les arguments obligatoires et additionnels dont l'utilisation n'est pas obligatoire (cf. tableau ci-dessous).

Exemples d'instruction KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\
C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED
/AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.ff?;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL
/NOISWIFT:1 /W:report.log

KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Tableau 40. Syntaxe de l'instruction `KAVSHELL SCAN` et destination de ces arguments

Clé	Description
Zone d'analyse. Argument obligatoire.	
<fichiers>	Zone d'analyse : liste de fichiers, de répertoires, de chemins de réseau et de zones prédéfinies. Indiquez les chemins de réseau au format UNC (Universal Naming Convention). Dans l'exemple suivant, le répertoire Folder4 est indiqué sans son chemin d'accès. Il se trouve dans le répertoire d'où l'instruction KAVSHELL est exécutée : KAVSHELL SCAN Folder4 Si le nom de l'objet à analyser contient des espaces, il faudra l'indiquer entre guillemets. Si vous avez choisi un dossier, Kaspersky Security analysera également tous les sous-dossiers du dossier en question. Pour analyser un groupe de fichiers, vous pouvez utiliser les caractères * ou ?
<répertoires>	
<chemin de réseau>	
/MEMORY	Analyse les objets dans la mémoire vive.
/SHARED	Analyse les dossiers partagés sur le serveur.
/STARTUP	Analyse les objets de démarrage.
/REMDRIVES	Analyse les disques amovibles.
/FIXDRIVES	Analyse les disques durs.

Clé	Description
/MYCOMP	Analyse tous les secteurs du serveur protégé.
/L: <nom du fichier contenant la liste des zones d'analyse>	Nom du fichier contenant la liste des zones d'analyse, y compris le chemin d'accès complet au fichier. Les zones d'analyse dans le fichier sont séparées par un retour à la ligne. Vous pouvez indiquer les couvertures d'analyse prédéfinies comme indiqué dans l'exemple ci-après de fichier contenant la liste des zones d'analyse : C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Objets à analyser (File types). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security analysera les objets en fonction du format.	
/FA	Analyse tous les objets
/FC	Analyse les objets en fonction du format (par défaut). Kaspersky Security analyse uniquement les objets dont le format figure dans la liste des formats propres aux objets pouvant être infectés.
/FE	Analyse les objets en fonction de l'extension. Kaspersky Security analyse uniquement les objets dont l'extension figure dans la liste des extensions propres aux objets pouvant être infectés.
/NEWONLY	Analyse uniquement des nouveaux fichiers et des fichiers modifiés. Si vous n'utilisez pas cet argument, Kaspersky Security analysera tous les objets.
/Al: **Actions à exécuter sur les objets infectés**. Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security appliquera l'action **Ignorer**.	
DISINFECT	Réparer, ignorer si la réparation est impossible
DISINFDEL	Réparer, supprimer si la réparation est impossible

Clé	Description
DELETE	Supprimer Les paramètres DISINFECT et DELETE ont été préservés dans la version actuelle de Kaspersky Security pour garantir la compatibilité avec les versions antérieures. Vous pouvez utiliser ces paramètres au lieu des arguments de commande /AI: et /AS:. Dans ce cas, Kaspersky Security ne traitera pas les objets probablement infectés.
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée
/AS: **Actions à exécuter sur les objets potentiellement infectés** (**actions**). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security appliquera l'action **Ignorer**.	
QUARANTINE	Quarantaine
DELETE	Supprimer
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée
Exclusions (Exclusions)	
/E:ABMSPO	L'argument exclut les objets composés des types suivants : A : archives SFX ; B : bases de données de messagerie électronique ; M : message de texte plat ; S : archives (y compris les archives SFX) ; P : objets compactés ; O : objets OLE intégrés.
/EM:<"masques">	Exclut les fichiers en fonction du masque. Vous pouvez définir plusieurs masques, par exemple EM:"*.txt;*.png; C\Videos*.avi".

Clé	Description
/ET:<nombre de secondes>	Arrête le traitement de l'objet s'il dure plus longtemps que la durée indiquée en secondes. Par défaut, l'analyse n'est pas limitée dans le temps.
/ES:<taille>	Exclut de l'analyse les objets composés dont la taille, en mégaoctets, dépasse la valeur de l'argument <taille>. Par défaut, Kaspersky Security analyse les objets de n'importe quelle taille.
/TZOFF	Annule les exclusions de la zone de confiance.
/AI: **Actions sur les fichiers autonomes** (options HSM)	
/SKIP	Ignore les fichiers autonomes.
/RESIDENT	Analyser seulement la partie résidente du fichier
/SCAN	Analyse tous les fichiers autonomes.
/SCAN=<jours>	Analyse uniquement les fichiers autonomes sollicités par Kaspersky Security durant la période indiquée (jours).
/SCAN NORECALL	Analyse les fichiers autonomes sans les copier, si possible, sur le disque dur.
/SCAN=<jours>	Analyse uniquement les fichiers autonomes sollicités par Kaspersky Security durant la période indiquée (jour) sans les copier, dans la mesure du possible, sur le disque dur.
Paramètres avancés (Options)	
/NOICHECKER	Désactive l'utilisation de la technologie iChecker (activée par défaut).
/NOISWIFT	Désactive l'utilisation de la technologie iSwift (activée par défaut).
/ANALYZERLEVEL:<niveau d'analyse>	Activation de l'utilisation de l'analyse heuristique et configuration du niveau d'analyse. L'analyse heuristique peut être effectuée à plusieurs niveaux : 1 – superficielle ;

Clé	Description
	2 – moyenne ; 3 – minutieuse. Si vous n'utilisez pas cet argument, Kaspersky Security n'utilisera pas l'analyse heuristique.
/NOCHECKMSSIGN	Exclusion de l'analyse des fichiers possédant une signature numérique électronique de Microsoft (activé par défaut).
/ALIAS:<nom alternatif de la tâche>	L'argument permet d'attribuer un nom temporaire à la tâche d'analyse à la demande. Ce nom permet de consulter la tâche durant son exécution, par exemple pour consulter les statistiques à l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Security. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple update_1234. Dans la console de Kaspersky Security, la tâche reçoit le nom Scan objects (<date heure>), par exemple, Scan objects 8/16/2007 5:13:14 PM.
Paramètres des journaux d'exécution des tâches (Report settings)	
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Security dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.

Clé	Description
	Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Security. Si Kaspersky Security ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche pas de message sur l'erreur.
/ANSI	La clé permet d'enregistrer les événements dans le journal d'exécution des tâches dans l'encodage ANSI. La clé ANSI ne sera pas appliquée, si la clé W n'est pas définie. Si la clé ANSI n'est pas spécifiée, alors le journal d'exécution des tâches s'effectue dans l'encodage UNICODE.

Lancement de la tâche Analyse rapide. KAVSHELL SCANCRITICAL

Utilisez la commande `KAVSHELL SCANCRITICAL` pour lancer la tâche prédéfinie d'analyse à la demande Analyse rapide selon les paramètres définis dans la console de Kaspersky Security.

Syntaxe de l'instruction KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<nom du fichier du journal d'exécution de la tâche>]
```

Exemple de l'instruction KAVSHELL SCANCRITICAL

Pour exécuter la tâche d'analyse à la demande Analyse rapide ; enregistrer le journal d'exécution de la tâche dans le fichier scancritical.log dans le répertoire en cours, exécutez l'instruction suivante :

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Vous pouvez configurer l'emplacement du fichier journal d'exécution de la tâche en fonction de la syntaxe de l'argument (cf. tableau ci-dessous).

Tableau 41. Syntaxe de l'argument `/W` de l'instruction `KAVSHELL SCANCRITICAL`

Clé	Description
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de l'application dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Security. Si Kaspersky Security ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche pas de message sur l'erreur.

Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK

A l'aide de l'instruction `KAVSHELL TASK`, vous pouvez administrer la tâche indiquée : lancer, suspendre, reprendre ou arrêter la tâche ainsi que consulter son état actuel et ses statistiques. L'instruction est exécutée en monde asynchrone.

Cette instruction ne permet pas d'administrer les tâches de groupe de Kaspersky Security Center.

Instruction de la commande KAVSHELL TASK

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemples de l'instruction KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

L'instruction `KAVSHELL TASK` peut être exécutée sans clé de licence ou avec une ou plusieurs clés de licence (cf. tableau ci-dessous).

Tableau 42. Instruction de la commande KAVSHELL TASK

Clé	Description
Sans argument	L'instruction renvoie la liste de toutes les tâches existantes de Kaspersky Security. La liste contient les champs : nom alternatif de la tâche, catégorie de tâche (tâche prédéfinie et tâche définie par utilisateur) et état actuel de la tâche.
<nom alternatif de la tâche>	Au lieu du nom de la tâche dans la commande SCAN TASK, utilisez son nom alternatif : bref nom complémentaire attribué aux tâches par Kaspersky Security. Pour consulter les noms alternatifs des tâches dans Kaspersky Security, saisissez l'instruction KAVSHELL TASK sans argument.
/START	Lance la tâche indiquée en mode asynchrone
/STOP	Arrête la tâche indiquée
/PAUSE	Suspend la tâche indiquée
/RESUME	Relance la tâche indiquée en mode asynchrone

Clé	Description
/STATE	Récupère l'état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée**, **En pause**, **Stoppé**, **Echec**, **Lancement en cours**, **Restauration en cours**)
/STATISTICS	Affiche les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche jusqu'à ce moment.

Codes de retour de l'instruction KAVSHELL TASK (cf. page 358)

Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP

L'instruction `KAVSHELL RTP` vous permet de lancer ou d'arrêter toutes les tâches de protection en temps réel.

Syntaxe de l'instruction KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Exemples de l'instruction KAVSHELL RTP

Pour lancer toutes les tâches de protection en temps réel, exécutez l'instruction suivante :

```
KAVSHELL RTP /START
```

L'instruction `KAVSHELL RTP` peut inclure n'importe quel des deux arguments obligatoires (cf. tableau ci-dessous).

Arguments de l'instruction KAVSHELL RTP

Tableau 43. Arguments de l'instruction KAVSHELL RTP

Clé	Description
/START	Lance toute les tâches de protection en temps réel : Protection des fichiers en temps réel, Analyse des scripts et Utilisation du KSN.
/STOP	Arrête toutes les tâches de protection en temps réel.

Lancement de la tâche de mise à jour des bases de données de Kaspersky Security. KAVSHELL UPDATE

La commande `KAVSHELL UPDATE` vous permet de lancer la tâche de mise à jour des bases de Kaspersky Security en mode synchrone.

La tâche de mise à jour des bases de Kaspersky Security, lancée à l'aide de la commande `KAVSHELL UPDATE`, est une tâche temporaire. Elle est affichée dans la console de Kaspersky Security uniquement pendant son exécution. Le journal d'exécution de la tâche est enregistré en même temps ; il est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Security. Les stratégies de l'application Kaspersky Security Center peuvent s'appliquer aux tâches de mise à jour créées et lancées via l'instruction `KAVSHELL UPDATE`, ainsi qu'aux tâches de mises à jour créées dans la console de Kaspersky Security. Pour en savoir plus sur l'administration de Kaspersky Security sur les serveurs à l'aide de Kaspersky Security Center, lisez la section "Administration de Kaspersky Security via Kaspersky Security Center"

Vous pouvez utiliser des variables système pour indiquer la source des mises à jour dans cette tâche. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL UPDATE` avec les privilèges de cet utilisateur.

Syntaxe de l'instruction KAVSHELL UPDATE

```
KAVSHELL UPDATE < Source de la mise à jour | /AK | /KL> [/NOUSEKL]
[/PROXY:<adresse>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nom
d'utilisateur>] [/PROXYPWD:<mot de passe>] [/NOPROXYFORKL]
[/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE] [/TIMEOUT:<nombre
de secondes>] [/REG:<code iso3166>] [/W:<nom du fichier du journal
d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction KAVSHELL UPDATE contient les arguments obligatoires et les arguments complémentaires dont l'utilisation facultative (cf. tableau ci-dessous).

Exemples de l'instruction KAVSHELL UPDATE

Pour lancer une tâche de mise à jour des bases définie par l'utilisateur, exécutez l'instruction suivante :

```
KAVSHELL UPDATE
```

Pour lancer une tâche de mise à jour des bases dont les fichiers de mise à jour se trouvent dans le dossier \\Server\bases, exécutez l'instruction suivante :

```
KAVSHELL UPDATE \\Server\bases
```

Pour lancer une tâche de mise à jour depuis le serveur FTP ftp://dnl-ru1.kaspersky-labs.com/ et enregistrer tous les événements de la tâche dans le fichier journal c:\update_report.log, exécutez l'instruction suivante :

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log
```

Pour recevoir les mises à jour des bases de Kaspersky Security depuis le serveur de mise à jour de Kaspersky Lab ; connectez-vous à la source des mises à jour via le serveur proxy (adresse du serveur proxy : proxy.company.com, port : 8080) ; pour accéder au serveur, utilisez l'authentification intégrée de Microsoft Windows (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser, mot de passe : 123456), puis exécutez l'instruction suivante :

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456 :
```

Tableau 44. Arguments de l'instruction KAVSHELL UPDATE

Clé	Description
Sources de la mise à jour (argument obligatoire). Indiquez une ou plusieurs sources. Kaspersky Security contactera chacune des sources dans l'ordre de la liste. Séparez les sources par un espace.	
<chemin au format UNC>	Source de mise à jour définie par l'utilisateur : chemin d'accès au répertoire de réseau contenant les mises à jour au format UNC (Universal Naming Convention).
<URL>	Source des mises à jour définie par l'utilisateur : adresse du serveur FTP ou HTTP sur lequel se trouve le répertoire contenant les mises à jour.

Clé	Description
<Dossier local>	Source des mises à jour définie par l'utilisateur : dossier sur le serveur protégé
/AK	Serveur d'administration de Kaspersky Security Center en guise de source des mises à jour
/KL	Serveurs de mises à jour de Kaspersky Lab en guise de source des mises à jour
/NOUSEKL	N'utilise pas les serveurs de mise à jour de Kaspersky Lab si les autres sources des mises à jour indiquées sont inaccessibles (utilisés par défaut).
Paramètres du serveur proxy	
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas cet argument, Kaspersky Security identifiera automatiquement les paramètres du serveur proxy utilisé dans le réseau local.
/AUTHTYPE:<0-2>	Cet argument définit la méthode d'authentification pour l'accès au serveur proxy. Le paramètre peut prendre les valeurs suivantes : **0** : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Security contactera le serveur proxy sous le compte **Système local** (**SYSTEM**) ; **1** : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Security contactera le serveur proxy sous le compte utilisateur dont les données sont définies par les arguments /PROXYUSER et /PROXYPWD ; **2** : authentification selon le nom et le mot de passe de l'utilisateur définis par les arguments /PROXYUSER et /PROXYPWD (Basic authentication). Si l'accès au serveur proxy ne requiert pas l'authentification, alors il n'est pas nécessaire d'indiquer cet argument.

Clé	Description
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur employé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> è /PROXYPWD:<mot de passe> sont ignorés.
/PROXYPWD:<mot de passe>	Mot de passe qui utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> è /PROXYPWD:<mot de passe> sont ignorés. Si vous définissez l'argument /PROXYUSER mais pas l'argument /PROXYPWD, le système considère que le mot de passe est vide.
/NOPROXYFORKL	N'utilise pas les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab (utilisés par défaut)
/USEPROXYFORCUSTOM	Utilise les paramètres du serveur proxy pour la connexion aux sources de mises à jour définies par l'utilisateur (non utilisées par défaut)
/USEPROXYFORLOCAL	Utilise les paramètres du serveur proxy pour la connexion aux sources locales des mises à jour. Si cet argument n'est pas indiqué, la valeur **Ne pas utiliser les paramètres de proxy spécifiés pour se connecter aux sources des mises à jour locales est appliquée**.
Paramètres généraux du serveur FTP ou HTTP	
/NOFTPPASSIVE	Si vous utilisez cet argument, Kaspersky Security utilisera le mode actif du serveur FTP pour se connecter au serveur protégé. Si vous n'utilisez pas cet argument, Kaspersky Security utilisera le mode passif du serveur FTP si cela est possible.
/TIMEOUT:<nombre de secondes>	Délai d'attente lors de la connexion au serveur FTP ou HTTP. Si vous n'utilisez pas cet argument, Kaspersky Security utilisera la valeur par défaut : 10 sec. Vous ne pouvez entrer que des nombres entiers.

Clé	Description
/REG:<code iso3166>	L'argument des paramètres régionaux intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab. Kaspersky Security optimalise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mises à jour le plus proche. En guise de valeur pour cet argument, saisissez le code alphabétique du pays où se trouve le serveur protégé conformément à la norme ISO 3166-1, par exemple /REG:gr ou /REG:RU. Si vous n'utilisez pas cet argument ou si vous indiquez un code inexistant, alors Kaspersky Security identifiera l'emplacement du serveur protégé selon les paramètres régionaux du serveur protégé (pour Microsoft Windows 2008 Server ou suivant, il s'agit de la variable **Emplacement** (Location)).
/ALIAS:<nom alternatif de la tâche>	Cet argument permet d'attribuer un nom temporaire à la tâche afin de pouvoir la consulter durant l'exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à la l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Security. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple, update_1234. Dans la console de Kaspersky Security, la tâche reçoit le nom Update-bases (<date time>), par exemple, Update-bases 8/16/2007 05:41:02 PM.
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche.

Clé	Description
	Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Security dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Security. Si Kaspersky Security ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais n'affiche pas de message sur l'erreur.

Codes de retour de la commande KAVSHELL UPDATE (cf. section "Codes de retour de l'instruction KAVSHELL RTP" à la page 359)

Annulation de la mise à jour des bases de données de Kaspersky Security KAVSHELL ROLLBACK

L'instruction `KAVSHELL ROLLBACK` vous permet d'exécuter la tâche prédéfinie **Annulation de la mise à jour** pour remettre les bases de Kaspersky Security à l'état antérieur à la mise à jour. La commande est exécutée en mode synchrone.

Syntaxe de l'instruction

```
KAVSHELL ROLLBACK
```

Codes de retour de l'instruction KAVSHELL ROLLBACK (cf. page 361)

Activation de l'application. KAVSHELL LICENSE

La commande `KAVSHELL LICENSE` permet de gérer les clés et les codes d'activation dans Kaspersky Security.

Syntaxe de l'instruction KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<fichier clé | code d'activation> [/R] | /DEL:<numéro de la clé | numéro du code d'activation>]
```

Exemples de l'instruction KAVSHELL LICENSE

Pour activer l'application, exécutez la commande :

```
KAVSHELL.EXE LICENSE / ADD: <code d'activation ou numéro de la clé> / PASSWORD = <mot de passe>
```

Pour obtenir les informations sur les clés ajoutées, exécutez l'instruction suivante :

```
KAVSHELL LICENSE
```

Pour supprimer la clé ajoutée avec le numéro de série 0000-000000-00000001, exécutez l'instruction suivante :

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

L'instruction `KAVSHELL LICENSE` peut être exécutée avec ou sans les clés de licence (cf. tableau ci-dessous).

Tableau 45. Arguments de l'instruction KAVSHELL LICENSE

Clé	Description
Sans argument	L'instruction affiche les informations suivantes sur les clés ajoutées : • Numéro de la clé. • Type de licence (commerciale ou d'évaluation). • Durée de validité de la licence associée à la clé. • Etat de la clé (active ou complémentaire). Si la valeur * est définie, la clé ajoutée est une licence complémentaire.

Clé	Description
/ADD:<nom du fichier clé ou code d'activation>	Ajoute la clé à l'aide du fichier ou du code d'activation indiqué. Pour désigner le chemin d'accès au fichier clé, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
/R	Le code d'activation ou la clé /R vient compléter le code d'activation ou la clé /ADD et signale que ce code d'activation ou cette clé est ajout en tant que clé ou code complémentaire.
/DEL:<numéro de la clé ou du code d'activation>	Supprime la clé portant le numéro indiqué ou le code d'activation indiqué.

Codes de retour de l'instruction KAVSHELL LICENSE (cf. page 361)

Activation, configuration et désactivation de la constitution d'un journal de traçage. KAVSHELL TRACE

L'instruction `KAVSHELL TRACE` vous permet d'activer ou de désactiver la création d'un journal de traçage de tous les sous-systèmes de Kaspersky Security ainsi que de définir le niveau de détail des informations reprises dans le journal.

Kaspersky Security consigne les informations dans les fichiers de trace et le fichier dump de mémoire en clair.

Syntaxe de l'instruction KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<dossier contenant les fichiers du journal de traçage>
[/S:<taille maximale du fichier de traçage en mégaoctets>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Si le journal de traçage est constitué et vous souhaitez modifier ses paramètres, saisissez l'instruction `KAVSHELL TRACE` avec l'argument /ON et définissez les paramètres du journal à l'aide des arguments /S et /LVL (cf. tableau ci-dessous).

Tableau 46. Arguments de l'instruction KAVSHELL TRACE

Clé	Description
/ON	Active la constitution du journal de traçage.
/F:<dossier contenant les fichiers du journal de traçage>	Cet argument indique le chemin d'accès complet au dossier dans lequel les fichiers du journal de traçage seront conservés (argument obligatoire). Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Vous pouvez indiquer les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques réseau du serveur protégé. Si le nom du dossier dont vous saisissez le chemin d'accès pour cet argument contient un espace, il faudra saisir le nom entre guillemets, par exemple, /F:"C\Trace Folder". Pour désigner le chemin d'accès au dossier contenant les fichiers du journal de traçage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
/S:<Taille maximale du fichier journal en mégaoctets>	Cet argument définit la taille maximale d'un fichier du journal de traçage. Dès que la taille du journal atteint la valeur maximale, Kaspersky Security consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé. Si vous ne définissez pas cet argument, la taille maximale d'un journal sera limitée à 50 Mo.

Clé	Description
/LVL:debug|info|warning|error|critical	Cette clé définit le niveau de détail du journal depuis le niveau le plus détaillé (**informations de débogage**) où tous les événements sont enregistrés jusqu'au niveau minimum (**Evénements critiques**) où seuls les événements critiques sont consignés dans le journal. Si vous ne définissez pas cet argument, le journal de traçage contiendra les événements correspondant au niveau de détail **Informations de débogage**.
/OFF	Cet argument désactive la constitution du journal de traçage.

Exemples de l'instruction KAVSHELL TRACE :

Pour activer le contenu du journal de traçage avec le niveau de détail Informations de débogage et la taille maximale du fichier du journal de 200 Mo et enregistrer le fichier du journal dans le répertoire C:\Trace Folder, exécutez l'instruction suivante :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

Pour activer le contenu du journal de traçage avec le niveau de détail Evénements importants et enregistrer le fichier journal dans le répertoire C:\Trace Folder, exécutez l'instruction suivante :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

Pour désactiver le contenu du journal de traçage, exécutez l'instruction suivante :

```
KAVSHELL TRACE OFF
```

Codes de retour de l'instruction KAVSHELL TRACE (cf. page 362)

Purge de la base iSwift. KAVSHELL FBRESET

Kaspersky Security utilise la technologie iSwift qui permet de ne pas devoir analyser à nouveau un fichier si celui-ci n'a pas été modifié depuis l'analyse antérieure (**Utiliser la technologie iSwift**).

Dans le répertoire système %SYSTEMDRIVE%\System Volume Information, Kaspersky Security crée les fichiers fidbox.dat et fidbox2.dat qui contiennent les informations relatives aux objets sains déjà analysés. Plus le nombre de fichiers différents analysés par Kaspersky Security est élevé, plus la taille du fichier fidbox.dat (fidbox2.dat) sera importante. Ce fichier contient uniquement les informations actuelles sur les fichiers existant vraiment dans le système : si un fichier quelconque est supprimé, Kaspersky Security supprime les informations qui le concerne du fichier fidbox.dat (fidbox2.dat).

Pour purger ce fichier, utilisez l'instruction `KAVSHELL FBRESET`**.**

Tenez compte des particularités suivantes de l'instruction `KAVSHELL FBRESET` :

- Lors de la purge du fichier fidbox.dat à l'aide de l'instruction KAVSHELL FBRESET, Kaspersky Security ne suspend pas la protection (à la différence de la suppression manuelle du fichier).
- Après la purge du fichier fidbox.dat, Kaspersky Security peut augmenter la charge sur le serveur. Dans ce cas, le logiciel antivirus analyse tous les fichiers sollicités pour la première fois après la purge du fichier fidbox.dat. Après l'analyse, Kaspersky Security introduit à nouveau dans le fichier fidbox.dat les informations relatives à l'objet analysé. Lorsque cet objet sera à nouveau sollicité, la technologie iSwift permet de ne pas devoir l'analyser à nouveau, pour autant qu'il n'ait pas été modifié.

Si votre système d'exploitation utilise le contrôle des comptes utilisateur (UAC, User Account Control), pour pouvoir exécuter l'instruction `KAVSHELL FBRESET`, **il faudra posséder les autorisations d'administrateur**.

Activation et désactivation de la création d'un fichier dump. KAVSHELL DUMP

L'instruction `KAVSHELL DUMP` vous permet d'activer ou de désactiver la création de modèles de mémoire (fichier dump) des processus de Kaspersky Security en cas d'arrêt provoqué par une erreur (cf. tableau ci-dessous). De plus, vous pouvez prendre à n'importe quel moment un exemple de la mémoire des processus de Kaspersky Security en cours d'exécution.

Syntaxe de l'instruction KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<dossier contenant le fichier dump>|/SNAPSHOT
/F:<dossier contenant le fichier dump> / P:<pid> | /OFF>
```

Exemples d'instruction KAVSHELL DUMP

Pour activer la création d'un fichier dump ; enregistrer le fichier dump dans le répertoire C:\Dump, exécutez la commande suivante :

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Pour enregistrer une image de la mémoire du processus avec l'identifiant 1234 dans le répertoire C:/Dumps, exécutez l'instruction suivante :

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

Pour désactiver la création d'un fichier dump, exécutez la commande suivante :

```
KAVSHELL DUMP OFF
```

Tableau 47. Arguments de l'instruction KAVSHELL DUMP

Clé	Description
/ON	Active la création d'un fichier dump du processus en cas d'arrêt suite à une erreur.
/F:<dossier contenant les fichiers dump>	Argument obligatoire ; indique le chemin d'accès au répertoire où le fichier dump sera enregistré. Si vous saisissez un chemin d'accès à un répertoire inexistant, le fichier dump ne sera pas créé. Vous pouvez utiliser les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques réseau du serveur protégé. Pour désigner le chemin d'accès au dossier contenant le fichier dump, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
/SNAPSHOT	Crée un instantané du modèle de mémoire du processus de Kaspersky Security en exécution indiqué et enregistre le fichier dump dans le dossier dont le chemin d'accès est défini par l'argument /F.
/P	Identificateur du processus PID ; repris dans le **gestionnaire des tâches** de Microsoft Windows
/OFF	Désactive la création d'un fichier dump en cas d'arrêt suite à une erreur.

Codes de retour de l'instruction KAVSHELL DUMP (cf. page 363)

Importations des paramètres. KAVSHELL IMPORT

L'instruction `KAVSHELL IMPORT` vous permet d'importer les paramètres de Kaspersky Security, de ses fonctions et de ses tâches depuis un fichier de configuration dans Kaspersky Security sur le serveur protégé. Vous pouvez créer le fichier de configuration à l'aide de l'instruction `KAVSHELL EXPORT`.

Syntaxe de l'instruction KAVSHELL IMPORT

```
KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de l'instruction KAVSHELL IMPORT

```
KAVSHELL IMPORT Server1.xml
```

Tableau 48. Arguments de l'instruction KAVSHELL IMPORT

Clé	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration d'où les paramètres vont être importés. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL IMPORT (cf. page 364)

Exportation des paramètres. KAVSHELL EXPORT

L'instruction `KAVSHELL EXPORT` vous permet d'exporter tous les paramètres de Kaspersky Security et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Security sur d'autres serveurs.

Syntaxe de l'instruction KAVSHELL EXPORT

```
KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de l'instruction KAVSHELL EXPORT

```
KAVSHELL EXPORT Server1.xml
```

Tableau 49. Arguments de l'instruction KAVSHELL EXPORT

Clé	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration dans lequel les paramètres vont être enregistrés. Vous pouvez attribuer n'importe quelle extension au fichier de configuration. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL EXPORT (cf. page 365)

Codes de retour

Dans cette section

Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Tableau 50. Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Description	
0	L'opération a réussi
-3	Erreur de privilèges d'accès
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (par exemple, le service de Kaspersky Security est déjà exécuté ou est déjà arrêté)
-7	Le service n'est pas enregistré
-8	Le lancement du service est interdit
-9	La tentative d'exécution du service sous un autre compte utilisateur a échoué (par défaut, le service de Kaspersky Security fonctionne sous compte utilisateur **Système local**).
-99	Erreur inconnue

Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL

Tableau 51. Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL

Code de retour	Description
0	L'opération a réussi (Aucune menace n'a été découverte)
1	L'opération a été annulée
-2	Le service n'est pas lancé

Code de retour	Description
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le fichier avec la liste des zones d'analyse est introuvable).
-5	Syntaxe de l'instruction incorrecte ou zone d'analyse non définie.
-80	Des objets infectés et autres objets détectés ont été découverts
-81	Des objets potentiellement infectés ont été découverts
-82	Des erreurs de traitement ont été découvertes
-83	Des objets non analysés ont été découverts
-84	Objets endommagés détectés
-85	Impossible de créer le fichier du journal d'exécution de la tâche
-99	Erreur inconnue
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL TASK

Tableau 52. Codes de retour de l'instruction KAVSHELL TASK

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (la tâche est introuvable)

Code de retour	Description
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (par exemple, la tâche n'est pas lancée, est déjà lancée ou ne peut être arrêtée)
-99	Erreur inconnue
-301	Clé non valide
401	La tâche n'est pas lancée (pour l'argument /STATE)
402	La tâche est déjà lancée (pour l'argument /STATE)
403	La tâche est déjà arrêtée (pour l'argument /STATE)
-404	Erreur d'exécution de l'opération (la modification de l'état de la tâche a entraîné son échec)

Codes de retour de l'instruction KAVSHELL RTP

Tableau 53. Codes de retour de l'instruction KAVSHELL RTP

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (une des tâches de protection en temps réel ou toutes les tâches de protection en temps réel sont introuvables)
-5	Syntaxe de l'instruction incorrecte

Code de retour	Description
-6	Opération invalide (par exemple, la tâche est déjà exécutée ou est déjà arrêtée)
-99	Erreur inconnue
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL UPDATE

Tableau 54. Codes de retour de l'instruction KAVSHELL UPDATE

Code de retour	Description
0	L'opération a réussi
200	Tous les objets sont d'actualité (les bases ou les modules logiciels sont d'actualité)
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe de l'instruction incorrecte
-99	Erreur inconnue
-206	Les fichiers des mises à jour ne sont pas présents dans la source indiquée ou leur format est inconnu
-209	Erreur de connexion à la source des mises à jour
-232	Erreur d'authentification lors de la connexion au serveur proxy
-234	Erreur de connexion à l'application Kaspersky Security Center
-235	Kaspersky Security n'a pas subi d'authentification lors de la connexion à la source des mises à jour

Code de retour	Description
-236	Les bases de Kaspersky Security sont endommagées
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL ROLLBACK

Tableau 55. Codes de retour de l'instruction KAVSHELL ROLLBACK

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-99	Erreur inconnue
-221	La copie de sauvegarde des bases est introuvable
-222	La copie de sauvegarde des bases est corrompue

Codes de retour de l'instruction KAVSHELL LICENSE

Tableau 56. Codes de retour de l'instruction KAVSHELL LICENSE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé

Code de retour	Description
-3	Privilèges insuffisants pour l'administration des clés
-4	Clé portant le numéro indiqué introuvable
-5	Syntaxe de l'instruction incorrecte
-6	Opération incorrecte (la clé a déjà été ajoutée)
-99	Erreur inconnue
-301	Clé non valide
-303	Licence destinée à une autre application

Codes de retour de l'instruction KAVSHELL TRACE

Tableau 57. Codes de retour de l'instruction KAVSHELL TRACE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin d'accès indiqué en tant que chemin d'accès au dossier contenant les fichiers du journal de traçage est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (tentative d'exécution de KAVSHELL TRACE /OFF si la création du journal de traçage a déjà été désactivée)
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL FBRESET

Tableau 58. Codes de retour de l'instruction KAVSHELL FBRESET

Code de retour	Description
0	L'opération a réussi
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL DUMP

Tableau 59. Codes de retour de l'instruction KAVSHELL DUMP

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin indiqué en guise de chemin d'accès au dossier contenant les fichiers dump est introuvable ; le processus avec le PID indiqué est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (tentative d'exécution de KAVSHELL DUMP /OFF si la création des fichiers dump a déjà été désactivée)
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL IMPORT

Tableau 60. Codes de retour de l'instruction KAVSHELL IMPORT

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le fichier de configuration à importer est introuvable)
-5	Syntaxe incorrecte
-99	Erreur inconnue
501	L'opération a réussi, toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple Kaspersky Security n'a pas importé des paramètres d'un composant fonctionnel quelconque
-502	Le format du fichier à importer est inconnu ou le fichier manque
-503	Paramètres incompatibles (le fichier de configuration provient d'une autre application ou d'une version de Kaspersky Security postérieure ou incompatible)

Codes de retour de l'instruction KAVSHELL EXPORT

Tableau 61. Codes de retour de l'instruction KAVSHELL EXPORT

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe incorrecte
-10	Impossible de créer le fichier de configuration (par exemple, accès interdit au répertoire indiqué dans le chemin d'accès au fichier)
-99	Erreur inconnue
501	L'opération a réussi, toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple Kaspersky Security n'a pas exporté les paramètres d'un composant fonctionnel quelconque

Administration de Kaspersky Security via Kaspersky Security Center

Cette section contient les informations et les instructions relatives à l'administration de Kaspersky Security et à la configuration de ses paramètres via la console d'administration Kaspersky Security Center.

Dans cette section

Présentation des modes d'administration de Kaspersky Security depuis Kaspersky Security Center

La console d'administration Kaspersky Security Center permet d'administrer centralement plusieurs serveurs dotés de Kaspersky Security et repris dans un *Groupe d'administration*. Kaspersky Security Center permet également de configurer séparément les paramètres de fonctionnement de chaque serveur qui fait partie du groupe d'administration.

Le *groupe d'administration* est créé manuellement du côté de Kaspersky Security Center et contient plusieurs serveurs dotés de Kaspersky Security et pour lesquels vous souhaitez configurer des paramètres d'administration et de protection identiques. Pour en savoir plus sur l'utilisation de groupes d'administration, consultez le *Manuel de l'administrateur de Kaspersky Security Center*.

Les paramètres de l'application pour un serveur ne peuvent être configurés si le fonctionnement de Kaspersky Security sur ce serveur est contrôlée par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Security depuis Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center**. Les stratégies de Kaspersky Security Center permettent de configurer à distance des paramètres de protection unique pour un groupe de serveurs. Les paramètres de la tâche, définis dans une stratégie active, ont priorité sur les paramètres des tâches définis localement dans la Console de Kaspersky Security ou à distance dans la fenêtre **Propriétés : <nom du serveur>** de Kaspersky Security Center.

  Les stratégies permettent de configurer les paramètres généraux de fonctionnement de l'application, les paramètres des tâches de contrôle du serveur, les paramètres des tâches de protection des stockages réseau, les paramètres de planification des tâches prédéfinies et les paramètres d'utilisation des profils.

- **A l'aide de tâches de groupe de Kaspersky Security Center**. Les tâches de groupe de Kaspersky Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai d'exécution limité pour un groupe de serveurs.

  Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche de génération automatique des règles d'autorisation.

- **A l'aide de tâches pour une sélection d'ordinateurs**. Les tâches pour une sélection d'ordinateurs permettent de configurer à distance des paramètres uniques de tâches ayant un délai d'exécution limité pour les serveurs qui ne figurent dans aucun des groupes d'administration créés.

- **A l'aide de la fenêtre de configuration des paramètres d'un serveur**. La fenêtre **Propriétés : <nom du serveur>** permet de configurer à distance les paramètres d'une tâche pour un serveur appartenant au groupe d'administration. Vous pouvez configurer ainsi les paramètres généraux de fonctionnement de l'application et les paramètres de toutes les tâches de Kaspersky Security, si le serveur sélectionné n'est pas administré par une stratégie active de Kaspersky Security Center.

Les paramètres de l'application que vous pouvez configurer aussi bien pour un groupe de serveurs que pour un serveur unique sont décrits dans le tableau ci-après.

Tableau 62. Paramètres généraux de Kaspersky Security

Section		Paramètres
Paramètres	**Zone de confiance**	Le bouton **Configuration** du groupe **Zone de confiance** permet de configurer les paramètres suivants d'application d'une zone de confiance : • composer la liste des exclusions de la zone de confiance ; • activer ou désactiver l'analyse des opérations de sauvegarde des fichiers ; • composer la liste des processus de confiance.
	Stockages	Le bouton **Configuration** du groupe **Stockages** permet de configurer les paramètres suivants de la quarantaine et de la sauvegarde : • chemin d'accès du dossier dans lequel vous souhaitez placer les objets en quarantaine ou dans la sauvegarde ; • taille maximale de la sauvegarde ou de la quarantaine et seuil d'espace disponible ; • dossier où seront placés les objets restaurés depuis la sauvegarde ou la quarantaine ; • transmission au Serveur d'administration des informations relatives aux objets dans la sauvegarde ou la quarantaine.
	Montée en puissance et fiabilité	Le bouton **Configuration** du groupe **Montée en puissance et fiabilité** permet de configurer les paramètres généraux de montée en puissance et de fiabilité des tâches.

	Avancé	Le bouton **Configuration** du groupe **Avancé** sous l'onglet **Général** permet de configurer les paramètres suivants : • affichage de l'icône de l'application ; • actions de l'application en cas de passage à l'alimentation via la batterie ; • seuils de déclenchement des événements Les bases de l'application sont dépassées, Les bases de l'application sont fortement dépassées et L'analyse des zones critiques de l'ordinateur n'a pas été réalisée depuis longtemps. Si vous utilisez un système d'archivage HSM, l'onglet **Stockage hiérarchique** permet de configurer les paramètres du système HSM.
	Paramètres de connexion	Le bouton **Configuration** du groupe **Paramètres de connexion** permet de configurer les paramètres suivants de connexion aux serveurs de mise à jour et d'activation, ainsi qu'aux services KSN : • définition des paramètres d'utilisation du serveur proxy ; • définition des paramètres d'authentification au serveur proxy.
Journaux et notifications	**Journaux d'exécution des tâches**	Le bouton **Configuration** du groupe **Journaux d'exécution des tâches** permet de configurer les paramètres suivants : • définition du niveau d'importance des événements enregistrés pour les composants de l'application sélectionnés ; • définition des paramètres de conservation des journaux d'exécution des tâches.

	Notifications sur les événements	Le bouton **Configuration** du groupe **Notifications sur les événements** permet de configurer les paramètres suivants : • paramètres de notification des utilisateurs pour l'événement Script dangereux détecté ; • paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements du groupe **Configuration des notifications**.
Autorisations d'accès		Le bouton **Configuration** du groupe **Autorisations d'accès** permet de configurer les paramètres d'accès aux fonctions de l'application : • accès des utilisateurs ou d'un groupe d'utilisateurs à l'administration de Kaspersky Security. • accès des utilisateurs ou d'un groupe d'utilisateurs à l'administration du service Kaspersky Security.

Configuration des paramètres généraux de l'application dans Kaspersky Security Center

Vous pouvez configurer les paramètres généraux de Kaspersky Security depuis Kaspersky Security Center pour un groupe de serveurs ou pour un serveur individuel.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres généraux de l'application depuis Kaspersky Security Center, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Dans la section **Paramètres** du groupe dont vous souhaitez configurer les paramètres, cliquez sur le bouton **Configuration**. Dans la fenêtre qui s'ouvre, configurez les paramètres en fonction de vos besoins.

4. Une fois que les paramètres requis de Kaspersky Security ont été modifiés selon vos besoins, cliquez sur le bouton **OK** dans la fenêtre **Paramètres de l'application** ou dans la fenêtre **Propriétés : <nom de la stratégie>**.

Les paramètres généraux de Kaspersky Security seront configurés conformément aux exigences définies.

Application de la zone de confiance dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

La zone de confiance est appliquée par défaut dans les nouvelles tâches ou stratégies.

► *Pour configurer les paramètres de la zone de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Dans la section **Paramètres** du groupe **Zone de confiance**, cliquez sur le bouton **Configuration**.

4. Sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**, indiquez les objets qui seront ignorés par Kaspersky Security lors de l'analyse :

   - Pour ajouter les exclusions recommandées, cliquez sur le bouton **Ajouter les exclusions recommandées**.

     Cliquer sur ce bouton permet d'ajouter les exclusions recommandées par la société Microsoft, les exclusions Kaspersky Lab et les exclusions des outils d'administration à distance sous le masque not-a-virus:RemoteAdmin* à la liste des exclusions.

   - Pour importer des exclusions, cliquez sur le bouton **Importer** et dans la fenêtre qui s'ouvre, sélectionnez les fichiers que Kaspersky Security considèrera comme des fichiers de confiance.

   - Si vous souhaitez indiquer manuellement la condition qui, une fois satisfaite, permettra de considérer un fichier comme un fichier de confiance, cliquez sur le bouton **Ajouter**. Définissez les paramètres suivants dans la fenêtre qui s'ouvre :

     - **Objet à analyser**.

     Nom ou masque de nom du fichier, du disque local ou amovible du serveur, du dossier local ou réseau, de la zone prédéfinie.

     - **Objets à détecter**.

     Nom ou masque de nom d'objet à détecter tel qu'il apparaît dans l'Encyclopédie des virus accessible via www.securelist.com/fr/.

     - **Zone d'application des règles**.

     Nom de la tâche de Kaspersky Security dans laquelle la règle est appliquée.

     - Le cas échéant, ajoutez des informations dans le champ **Commentaires** pour expliquer l'exclusion.

5. Sous l'onglet **Processus de confiance** de la fenêtre **Zone de confiance**, indiquez les processus qui seront ignorés par Kaspersky Security lors de l'analyse :

   - **Ne pas vérifier les opérations de sauvegarde de fichiers**.

     La case active ou désactive l'analyse des opérations de lecture des fichiers si ces opérations sont réalisées par des outils de copie de sauvegarde installés sur le serveur.

     Quand la case est cochée, Kaspersky Security ignore pendant l'analyse les opérations de lecture de fichiers réalisées par les outils de copie de sauvegarde installés sur le serveur.

     Quand la case est décochée, Kaspersky analyse les opérations de lecture des fichiers exécutées par les outils de copie de sauvegarde installés sur le serveur.

     Cette case est cochée par défaut.

   - **Ne pas surveiller les actions sur les fichiers des processus spécifiés**.

     La case active ou désactive l'analyse des actions des processus de confiance sur les fichiers.

     Si la case est cochée, Kaspersky Security ignore les opérations des processus de confiance sur les fichiers lors de l'analyse.

     Quand la case est décochée, Kaspersky Security analyse les opérations des processus de confiance sur les fichiers.

     Cette case est décochée par défaut.

     - Le cas échéant, cliquez sur **Ajouter** pour ajouter les processus pour lesquels vous ne souhaitez pas contrôler l'activité de fichier.

6. Cliquez sur **OK**.

Les paramètres de la zone de confiance définis seront enregistrés.

Configuration des paramètres de la quarantaine et de la sauvegarde dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres de la sauvegarde dans Kaspersky Security Center, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Dans la section **Paramètres** du groupe **Stockages**, cliquez sur le bouton **Configuration**.
4. Sous l'onglet **Sauvegarde** de la fenêtre **Paramètres de quarantaine et de sauvegarde**, configurez les paramètres suivants de la sauvegarde :
   - Si vous souhaitez définir le dossier qui abritera la sauvegarde, sélectionnez, dans le champ **Dossier de sauvegarde**, le dossier requis sur le disque local du serveur protégé ou saisissez le chemin d'accès complet à celui-ci.
   - Si vous souhaitez définir la taille maximale de la sauvegarde, cochez la case **Taille maximale de sauvegarde (Mo)** et saisissez la valeur souhaitée en mégaoctets dans le champ.
   - Si vous souhaitez définir le seuil d'espace disponible dans la sauvegarde, définissez la valeur de **Taille maximale de sauvegarde (Mo)**, cochez la case **Seuil d'espace disponible (Mo)** et saisissez la valeur minimale souhaitée d'espace disponible dans la sauvegarde en mégaoctets.
   - Si vous souhaitez indiquer le répertoire de restauration, dans le groupe de paramètres **Paramètres de restauration**, sélectionnez le répertoire requis sur le disque local du serveur protégé ou dans le champ **Dossier dans lequel sont rétablis les objets**, saisissez le nom du dossier et son chemin d'accès complet.
5. Dans la fenêtre **Paramètres de quarantaine et de sauvegarde**, choisissez l'onglet **Quarantaine** et configurez les paramètres de la quarantaine :
   - Si vous souhaitez modifier le dossier de la quarantaine, indiquez le chemin d'accès au dossier sur le disque local du serveur protégé dans le champ **Dossier de quarantaine**.
   - Si vous souhaitez définir la taille maximale de la quarantaine, cochez la case **Taille maximale de la quarantaine (Mo)** et saisissez la valeur en Mo dans le champ.
   - Si vous souhaitez définir la valeur minimale d'espace disponible dans la quarantaine, cochez les cases **Taille maximale de la quarantaine (Mo)** et **Seuil d'espace disponible (Mo)**, puis saisissez la valeur seuil du paramètre en Mo dans le champ de saisie.
   - Si vous souhaitez modifier le dossier dans lequel les fichiers de la quarantaine sont restaurés, saisissez le chemin d'accès complet au dossier sur le disque local du serveur à protéger dans le champ **Dossier dans lequel sont rétablis les objets**.
6. Cliquez sur **OK**.

Les paramètres configurés de la quarantaine et de la sauvegarde seront enregistrés.

Configuration de paramètres de montée en puissance et de fiabilité dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres de la montée en puissance et de fiabilité, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Dans la section **Paramètres** du groupe **Montée en puissance et fiabilité**, cliquez sur le bouton **Configuration**.

4. Configurez les paramètres suivants dans la fenêtre **Paramètres de la montée en puissance et de la fiabilité** :

   - La section **Paramètres d'optimisation** permet de configurer les paramètres qui définissent le nombre de processus de travail utilisés par Kaspersky Security :

     - **Détecter automatiquement les paramètres d'adaptabilité**.

     Kaspersky Security détermine automatiquement le nombre de processus utilisés.

     Cette valeur est définie par défaut.

     - **Indiquer manuellement le nombre de processus actifs**.

     Kaspersky Security régit le nombre de processus de travail actifs en fonction des valeurs indiquées.

       - **Quantité maximale de processus actifs**.

     Nombre maximum de processus utilisés par Kaspersky Security.

     Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.

       - **Nombre de processus de protection en temps réel**.

     Nombre maximum de processus utilisés par les modules de protection des fichiers en temps réel, d'analyse des scripts et de protection des stockages réseau.

     Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.

       - **Nombre de processus pour les tâches d'analyse à la demande en arrière-plan**.

     Nombre maximum de processus utilisés par le module d'analyse à la demande quand cette analyse est réalisée en arrière-plan.

     Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.

- Le groupe **Paramètres de restauration du logiciel** permet de configurer les paramètres de restauration des tâches de Kaspersky Security en cas d'échec de l'application ou d'arrêt forcé de celle-ci.

  - **Réaliser la restauration des tâches**.

    La case active ou désactive la restauration des tâches de Kaspersky Security après un échec de l'application ou un arrêt forcé de celle-ci.

    Quand la case est cochée, Kaspersky Security restaure automatiquement ses tâches après un échec de l'application ou un arrêt forcé de celle-ci.

    Quand la case est décochée, Kaspersky Security ne restaure pas ses tâches après un échec de l'application ou un arrêt forcé de celle-ci.

    Cette case est cochée par défaut.

  - **Ne pas réaliser la restauration des tâches d'analyse à la demande plus de (fois)**.

    Nombre de tentatives de restauration des tâches d'analyse à la demande après un échec de Kaspersky Security.

    Le champ de saisie est accessible si la case **Réaliser la restauration des tâches** a été cochée.

5. Cliquez sur **OK**.

Les paramètres définis de la montée en puissance et de la fiabilité seront enregistrés.

Configuration des paramètres avancés de l'application dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres avancés de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Dans la section **Paramètres** du groupe **Avancé**, cliquez sur le bouton **Configuration**.

4. Sous l'onglet **Général** de la fenêtre **Paramètres avancés de l'application**, configurez les paramètres suivants :

   - Dans le groupe **Interaction avec l'utilisateur**, configurez l'affichage de l'icône de Kaspersky Security dans la zone de notification de la barre des tâche : décochez ou cochez la case **Afficher l'icône de l'application dans la barre des tâches**.

   - Le groupe **Actions lors du passage à une source d'alimentation sans interruption** permet de limiter la charge de Kaspersky Security sur le serveur dans le cadre de l'alimentation de secours :

     - **Ne pas démarrer de tâches d'analyse planifiées**.

       La case active ou désactive le lancement des tâches d'analyse programmées entre l'entrée en action de l'alimentation sans interruption et le rétablissement de l'alimentation normale.

       Quand la case est cochée, Kaspersky Security ne lance pas les tâches d'analyse programmées d'analyse à la demande entre l'entrée en action de l'alimentation de secours et le rétablissement de l'alimentation normale.

       Si la case est décochée, Kaspersky Security lance les tâches d'analyse programmées quelle que soit la source d'alimentation du serveur.

       Cette case est cochée par défaut.

     - **Stopper les tâches d'analyse en cours**.

       La case active ou désactive la suspension des tâches d'analyse en cours d'exécution lors du passage à une source d'alimentation sans interruption.

       Quand la case est cochée, Kaspersky Security arrête l'exécution des tâches d'analyse en cours lors du passage du serveur à une source d'alimentation de secours.

       Quand la case est décochée, Kaspersky Security poursuit l'exécution des tâches d'analyse en cours lors du passage du serveur à une source d'alimentation de secours.

       Cette case est cochée par défaut.

- Définissez dans le groupe **Seuil de déclenchement des événements** les intervalles à l'issue desquels Kaspersky Security enregistre les événements Les *bases de l'application sont dépassées, Les bases de l'application sont fortement dépassées, L'analyse des zones critiques n'a pas été réalisée depuis longtemps*.

  - **Les bases de l'application sont dépassées**.

    Nombre de jours écoulés depuis la dernière mise à jour des bases de l'application.

    La valeur par défaut est de 7 jours.

  - **Les bases de l'application sont fortement dépassées**.

    Nombre de jours écoulés depuis la dernière mise à jour des bases de l'application.

    La valeur par défaut est de 14 jours.

  - **L'analyse rapide de l'ordinateur n'a pas été réalisée depuis longtemps (jours)**.

    Nombre de jours depuis la dernière exécution réussie de la tâche d'analyse rapide de l'ordinateur.

    La valeur par défaut est de 30 jours.

- Dans le groupe **Licence**, cochez ou décochez la case **Utiliser Kaspersky Security Center en tant que serveur proxy pour l'activation de l'application**.

5. Sous l'onglet **Stockage hiérarchique** de la fenêtre **Paramètres avancés de l'application**, sélectionnez une des options suivantes d'accès à la sauvegarde hiérarchique :

   - **Aucun système HSM**.

     Kaspersky Security n'utilise pas les paramètres du système HSM lors de l'exécution des tâches d'analyse à la demande.

     Cette option est sélectionnée par défaut.

   - **Le système HSM utilise des points de traitement réitéré**.

     Kaspersky Security utilise des points de traitement réitéré pour l'analyse des fichiers dans le stockage distant lors de l'exécution des tâches d'analyse à la demande.

- **Le système HSM utilise les attributs élargis du fichier**.

  Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

  Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

- **Système HSM non identifié**

  Kaspersky Security analyse tous les fichiers, comme les fichiers situés dans un stockage distant, lors de l'exécution des tâches d'analyse à la demande.

  Il est déconseillé d'utiliser cette option.

  > Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut pour le paramètre **Paramètres du système HSM** (**Aucun système HSM**).

6. Cliquez sur **OK**.

Les paramètres d'application définis seront enregistrés.

Configuration de paramètres de connexion dans Kaspersky Security Center

> La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Security et les serveurs de mises à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services KSN.

► *Pour configurer les paramètres de la connexion, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

     Si l'application est soumise à une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

   - Si vous souhaitez configurer les paramètres de l'application pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Sous l'onglet **Paramètres** du groupe **Paramètres de connexion**, cliquez sur le bouton **Configuration**.

4. Configurez les paramètres suivants dans la fenêtre **Configuration des paramètres de connexion** :

   - Définissez les paramètres d'utilisation du serveur proxy dans le groupe **Paramètres du serveur proxy** :

     - **Ne pas utiliser de serveur proxy**.

       Si cette option est sélectionnée, Kaspersky Security n'utilise pas le serveur proxy pour la connexion aux services du KSN et effectue la connexion directement.

- **Détecter automatiquement les paramètres du serveur proxy**.

  Si cette option est sélectionnée, Kaspersky Security définit automatiquement les paramètres de connexion aux services du KSN à l'aide du protocole Web Proxy Auto-Discovery Protocol (WPAD).

  Cette option est sélectionnée par défaut.

- **Utiliser les paramètres du serveur proxy indiqué**.

  Si cette option est sélectionnée, Kaspersky Security utilise les paramètres du serveur proxy indiqués manuellement pour la connexion au KSN.

- Adresse IP ou nom symbolique du serveur proxy et numéro de port.
- **Ne pas utiliser le serveur proxy pour les adresses locales**.

  La case active ou désactive l'utilisation du serveur proxy lors des échanges avec les autres ordinateurs du réseau auquel appartient l'ordinateur disposant de Kaspersky Security.

  Si la case est cochée, les échanges avec les autres ordinateurs du réseau auquel appartient l'ordinateur disposant de Kaspersky Security se font directement. Le serveur proxy n'est pas utilisé.

  Cette case est cochée par défaut.

- Définissez les paramètres d'authentification dans le groupe **Paramètres d'authentification sur le serveur proxy** :
  - Sélectionnez les paramètres d'authentification dans la liste déroulante.

    Vous pouvez sélectionner dans la liste déroulante le mode d'authentification utilisé pour accéder au serveur proxy.

    - **Ne pas utiliser l'authentification** : l'authentification n'est pas utilisée. Ce mode est sélectionné par défaut.
    - **Utiliser l'authentification NTLM** : authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft.
    - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** : authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft, et du nom d'utilisateur et du mot de passe.
    - **Utiliser le nom d'utilisateur et le mot de passe** : authentification à l'aide du nom d'utilisateur et du mot de passe.
  - Si nécessaire, indiquez le nom d'utilisateur et le mot de passe.

5. Cliquez sur **OK**.

Les paramètres de la connexion définis seront enregistrés.

Configuration des autorisations d'accès à Kaspersky Security Center

Vous pouvez configurer les autorisations d'accès à l'administration de l'application et à l'administration du service Kaspersky Security dans Kaspersky Security Center pour un groupe de serveurs ou un serveur individuel.

> La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les autorisations d'accès à l'application et au service Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les autorisations d'accès.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les autorisations d'accès pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les autorisations d'accès et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

   - Si vous souhaitez configurer les paramètres d'accès pour un serveur, ouvrez l'onglet **Ordinateurs**. Ouvrez ensuite la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center**" à la page 436).

3. Ouvrez la section **Autorisations d'accès** et réalisez les opérations suivantes :

   - Si vous souhaitez configurer les autorisations d'accès pour l'administration de Kaspersky Security pour un utilisateur ou un groupe d'utilisateurs, cliquez sur le bouton **Configuration** dans le groupe **Autorisation des utilisateurs pour l'administration de l'application**.

   - Si vous souhaitez configurer les autorisations d'accès pour l'administration du service Kaspersky Security pour un utilisateur ou un groupe d'utilisateurs, cliquez sur le bouton **Configuration** dans le groupe **Autorisations des utilisateurs pour l'administration de Kaspersky Security Service**.

4. Dans la fenêtre qui s'ouvre, configurez les autorisations d'accès en fonction de vos exigences (cf. section "Configuration des autorisations d'accès à l'administration de Kaspersky Security et du service Kaspersky Security" à la page 92).

Les paramètres définis seront enregistrés.

Présentation de la configuration des notifications dans Kaspersky Security Center

La Console d'administration de Kaspersky Security Center permet de configurer les notifications adressées à l'administrateur et aux utilisateurs concernant les événements liés à l'utilisation de Kaspersky Security et à l'état de la protection antivirus du serveur protégé (cf. section « Configuration des notifications adressées à l'administrateur et aux utilisateurs » à la page 320) :

- L'administrateur peut obtenir des informations sur les événements de certains types.

- les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peuvent obtenir des informations sur les événements de type *Objet détecté*.

Vous pouvez configurer les notifications relatives aux événements de Kaspersky Security pour un serveur dans la fenêtre **Propriétés :<nom du serveur>** ou pour un groupe de serveurs dans la fenêtre **Propriétés: <nom de la stratégie>** du groupe d'administration sélectionné.

Vous pouvez configurer les notifications sous l'onglet **Evénements** ou dans la fenêtre **Paramètres des notifications**. Vous pouvez configurer les types suivants de notification :

- L'onglet **Evénements** (onglet standard de Kaspersky Security Center) permet de configurer les notifications adressées à l'administrateur sur les événements de certains types. Pour en savoir plus sur les modes de notification, consultez le *Manuel de l'administrateur de Kaspersky Security Center*.

- La fenêtre **Paramètres des notifications** permet de configurer les notifications pour l'administrateur et pour les utilisateurs.

  La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Les notifications relatives aux événements de certains types peuvent être configurées uniquement sous l'onglet ou dans la fenêtre tandis que les notifications relatives à d'autres événements peuvent être configurées dans les deux.

Si vous configurez les notifications sur les événements d'un même type via une méthode identique sous l'onglet **Evénements** et dans la fenêtre **Paramètres des notifications**, l'administrateur système recevra les notifications relatives à ces événements via la méthode indiquée deux fois.

Dans cette section

Configuration des paramètres des journaux et des notifications dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres des journaux de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres généraux de l'application.

2. Dans le panneau des résultats du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres généraux de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**. Dans la liste des stratégies existantes, sélectionnez celle que vous souhaitez utiliser pour configurer les paramètres généraux de l'application et dans le menu contextuel de la stratégie sélectionnée, choisissez l'option **Propriétés**. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

   - Si vous souhaitez configurer les paramètres généraux de l'application pour un serveur, ouvrez l'onglet Ordinateurs. Ouvrez ensuite la fenêtre Paramètres de l'application (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page 436).

3. Dans la section **Journaux et notifications**, dans le groupe **Journaux d'exécution des tâches**, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Paramètres des journaux**, configurez les paramètres suivants de Kaspersky Security :
   - Configurez le niveau de détail des événements dans les journaux. Pour ce faire, procédez comme suit :
     a. Dans la liste **Composant**, sélectionnez le composant de Kaspersky Security pour lequel vous souhaitez indiquer le niveau de détails.
     b. Pour définir le niveau de détails dans les journaux d'exécution des tâches et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Niveau d'importance**.
   - Pour modifier l'emplacement des journaux par défaut, indiquez le chemin d'accès complet au dossier ou cliquez sur le bouton **Parcourir**.
   - Indiquez la durée de conservation en jour des journaux d'exécution des tâches.
   - Indiquez le nombre de jours pendant lesquels les informations reprises dans le nœud **Journal d'audit système** seront conservées.
5. Cliquez sur **OK**.
6. Dans la section **Journaux et notifications**, dans le groupe **Notifications sur les événements**, cliquez sur le bouton **Configuration**.
7. Dans la fenêtre **Paramètres des notifications**, configurez les paramètres suivants de Kaspersky Security en fonction de vos besoins (cf. section "Configuration des notifications de l'administrateur et des utilisateurs" à la page 320):
   a. Sélectionnez le type de notification dont vous souhaitez configurer les paramètres dans la liste **Configuration des notifications**.
   b. Configurez le mode de notification de l'utilisateur dans le groupe **Informer les utilisateurs**. Le cas échéant, rédigez le texte de la notification.
   c. Configurez le mode de notification de l'utilisateur dans le groupe **Informer les administrateurs**. Le cas échéant, rédigez le texte de la notification. Le cas échéant, cliquez sur **Configuration** pour configurer les paramètres avancés des notifications.
8. Cliquez sur **OK**.
9. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de l'application**.

Les paramètres des journaux et des notifications définis seront enregistrés.

Création et configuration des stratégies

Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Security sur plusieurs serveurs.

Dans cette section

A propos des stratégies

Vous pouvez créer des stratégies de Kaspersky Security Center unique pour l'administration de la protection de plusieurs serveurs sur lesquels Kaspersky Security est installé.

Une stratégie applique les paramètres de Kaspersky Security, de ses fonctions et de ses tâches à l'ensemble des serveurs protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la console d'administration, la stratégie active dans le groupe en ce moment possède l'état *active*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Security. Vous pouvez la consulter dans la console de Kaspersky Security dans le nœud **Journal d'audit système**.

Il existe dans Kaspersky Security Center une méthode unique pour appliquer des stratégies aux ordinateurs locaux : *Interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Security applique aux ordinateurs locaux les valeurs des paramètres en regard desquels vous avez placé l'icône 🔒 dans les propriétés de la stratégie au lieu de la valeur des paramètres définis localement avant l'application de la stratégie. Les paramètres de la stratégie active accompagnés de l'icône 🔓 dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Security.

Si la stratégie est active, les paramètres dans la Console de Kaspersky Security qui sont accompagnés de l'icône 🔒 dans la stratégie ne peuvent pas être modifiés. Les valeurs des autres paramètres (accompagnés de l'icône 🔓 dans la stratégie) peuvent être modifiées dans la Console de Kaspersky Security.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône 🔒 empêchent également la modification des paramètres dans Kaspersky Security Center pour un serveur depuis la fenêtre **Propriétés : <Nom de l'ordinateur>**.

Si la stratégie définit les paramètres d'une tâche quelconque de protection en temps réel ou d'une tâche de protection des stockages réseau et si cette tâche est en exécution, les paramètres définis par la stratégie sont modifiés directement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

Création d'une stratégie

La création d'une stratégie comporte les étapes suivantes :

1. Création d'une stratégie à l'aide de l'Assistant de création de stratégies. Vous pouvez définir les paramètres de la protection en temps réel dans les fenêtres de l'Assistant.

2. Configuration des paramètres de la stratégie. La fenêtre **Propriétés : <nom de la stratégie>** de la stratégie créée permet de configurer les paramètres de la protection en temps réel, les paramètres de la protection des stockages réseau, les paramètres généraux de Kaspersky Security, les paramètres de la quarantaine et de la sauvegarde, le niveau de détail des journaux d'exécution des tâches ainsi que les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Security.

   > Vous pouvez également importer une stratégie créée antérieurement à l'aide de Kaspersky Anti-Virus for Windows Servers Enterprise Edition. Une stratégie de Kaspersky Anti-Virus 6.0 ou 8.0 peut être importée uniquement via la création d'une nouvelle stratégie à l'aide de l'Assistant de création de stratégies.

► *Pour créer une stratégie pour un groupe de serveurs sur lesquels Kaspersky Security est installé, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration, déployez l'entrée **Ordinateurs administrés**, puis sélectionnez le groupe d'administration pour les serveurs duquel vous souhaitez créer une stratégie.

2. Dans le panneau des résultats du groupe d'administration sélectionné, choisissez l'onglet **Stratégies** et ouvrez la fenêtre de l'Assistant de création de stratégies via le lien **Créer une stratégie**.

3. Dans la fenêtre **Définition du nom de la stratégie de groupe pour l'application**, saisissez le nom de la stratégie créée dans le champ **Nom**. Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ / |`).

4. Dans la fenêtre **Sélection d'une application pour la création d'une stratégie de groupe**, dans la liste **Nom de l'application**, choisissez l'option **Kaspersky Security 10 for Windows Server**.

5. Sélectionnez une des options suivantes dans la fenêtre **Sélection du type d'opération** :

   - **Créer**, pour créer une stratégie reprenant les paramètres définis par défaut pour les stratégies nouvellement créées ;
   - **Importer une stratégie créée à l'aide de Kaspersky Anti-Virus 6.0 ou 8.0**, pour utiliser une stratégie de Kaspersky Anti-Virus 6.0 ou 8.0 en tant que modèle.

     Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de configuration dans lequel vous aviez enregistré la stratégie existante.

6. Dans la fenêtre **Protection en temps réel**, configurez, le cas échéant, les paramètres des tâches Protection des fichiers en temps réel, Analyse des scripts et Utilisation du KSN en fonction de vos besoins. Autorisez ou interdisez l'application des tâches configurées de la stratégie sur les ordinateurs locaux du réseau :

   - Cliquez sur le bouton 🔒 pour débloquer la configuration des paramètres d'une tâche sur les serveurs du réseau et interdire l'application des paramètres de la tâche configurés dans la stratégie.
   - Cliquez sur le bouton 🔓 pour bloquer la configuration des paramètres d'une tâche sur les serveurs du réseau et autoriser l'application des paramètres de la tâche configurés dans la stratégie.

Dans une stratégie recréée, les paramètres des tâches de protection en temps réel sont définis par défaut.

- Si vous souhaitez modifier les paramètres d'une tâche Protection des fichiers en temps réel définis par défaut, cliquez sur le bouton **Configuration** dans le groupe **Protection des fichiers en temps réel**. Dans la boîte de dialogue **Paramètres**, configurez les paramètres de la tâche en fonction de vos exigences. Cliquez sur **OK**.
- Si vous souhaitez modifier les paramètres d'une tâche Analyse des scripts définis par défaut, cliquez sur le bouton **Configuration** dans le groupe **Analyse des scripts**. Dans la boîte de dialogue **Paramètres**, configurez les paramètres de la tâche en fonction de vos exigences. Cliquez sur **OK**.
- Si vous souhaitez modifier les paramètres d'une tâche Utilisation du KSN définis par défaut, cliquez sur le bouton **Configuration** dans le groupe **Utilisation du KSN**. Dans la boîte de dialogue **Paramètres**, configurez les paramètres de la tâche en fonction de vos exigences. Cliquez sur **OK**.

  La tâche Utilisation du KSN est disponible sur le Règlement du KSN a été accepté.

7. Sélectionnez l'un des états de la stratégie suivants dans la fenêtre **Création d'une stratégie de groupe pour les applications** :

   - **Stratégie active**, si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, celle-ci deviendra inactive et la stratégie que vous venez de créer sera activée.
   - **Stratégie inactive**, si vous ne voulez pas appliquer immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.
   - **Stratégie pour les utilisateurs autonomes**, si vous souhaitez créer une stratégie pour un ordinateur administré situé en dehors du réseau de l'organisation. La stratégie pour les utilisateurs autonomes est uniquement accessible sur Kaspersky Security pour postes de travail (tournant sous Windows).

8. Dans la fenêtre **Fermeture** de l'Assistant, cliquez sur le bouton **Terminer**.

La stratégie créée sera affichée dans la liste des stratégies sous l'onglet **Stratégies** du groupe d'administration sélectionné. La fenêtre **Propriétés: <nom de la stratégie>** permet de configurer d'autres paramètres, tâches et fonctions de Kaspersky Security.

Configuration de stratégies

La fenêtre **Propriétés :<Nom de la stratégie>** de la stratégie existante permet de configurer les paramètres généraux de Kaspersky Security, les paramètres de la quarantaine et de la sauvegarde, les paramètres de la zone de confiance, les paramètres de la protection en temps réel, la paramètres du contrôle du serveur, les paramètres de la protection des stockages réseau, le niveau de détail des journaux d'exécution des tâches, les notifications des utilisateurs et des administrateurs relatives aux événements de Kaspersky Security, les privilèges d'accès à l'administration de l'application et du service Kaspersky Security Service et les paramètres d'application des profils de stratégie.

► *Pour configurer les paramètres d'une stratégie, procédez comme suit :*

1. Dans l'arborescence de la console d'administration Kaspersky Security Center, déployez le nœud **Ordinateurs administrés**, puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie et sélectionnez enfin l'onglet **Stratégies** dans le panneau des résultats.

2. Dans le menu contextuel de la stratégie dont vous souhaitez modifier les paramètres, choisissez l'option **Propriétés**.

3. Configurez les paramètres requis de la stratégie dans la fenêtre **Propriétés : <nom de la stratégie>**, configurez les paramètres requis de la stratégie.

4. Activez ou désactivez l'application de la stratégie dans la section **Général** du groupe **Etat de la stratégie**. Pour ce faire, sélectionnez l'une des options suivantes :

   - **Stratégie active** si vous souhaitez que la stratégie s'applique à tous les services appartenant au groupe d'administration sélectionné.
   - **Stratégie inactive** si vous souhaitez que la stratégie s'applique à tous les services appartenant au groupe sélectionné.

   > L'option **Stratégie pour les utilisateurs autonomes** n'est pas disponible avec Kaspersky Security for Windows Server.

5. Les sections **Evénements**, **Paramètres**, **Journaux et notifications**, **Autorisations d'accès** et **Profils de la stratégie** permettent de configurer les paramètres de fonctionnement de l'application (cf. tableau ci-après).

6. Les sections **Protection en temps réel**, **Contrôle du serveur**, **Protection des stockages réseau** et **Tâches prédéfinies** permettent de configurer l'exécution des tâches de l'application ainsi que les paramètres de leur lancement (cf. tableau ci-dessous).

   Vous pouvez activer ou désactiver l'exécution de n'importe quelle tâche sur tous les serveurs appartenant au groupe d'administration à l'aide d'une stratégie de Kaspersky Security Center.

   Vous pouvez configurer l'application des paramètres définis dans la stratégie sur tous les serveurs du réseau pour chaque composant distinct de l'application.

7. Cliquez sur **OK**.

Les paramètres définis seront appliqués dans la stratégie.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Les paramètres de Kaspersky Security que vous pouvez configurer à l'aide de stratégies sont décrits dans le tableau ci-après.

Tableau 63. Paramètres d'une stratégie dans Kaspersky Security Center

Section	Paramètres
Général	La section **Général** permet de configurer les paramètres de stratégie suivants : • état de la stratégie ; • héritage des paramètres des stratégies parent pour les stratégies fille. Les détails sur l'utilisation de cette section sont repris dans le *Manuel de l'administrateur de Kaspersky Security Center*.
Evénements	La section **Evénements** permet de configurer les paramètres pour les catégories d'événements suivants : • *Evénements critiques* ; • *Panne* ; • *Avertissement* ; • *Informations*. Le bouton **Propriétés** permet de configurer les paramètres suivants pour les événements sélectionnés : • emplacement et durée de conservation des informations sur l'événement enregistré ; • sélection du mode de notification sur les événements enregistrés. Les détails sur l'utilisation de cette section sont repris dans le *Manuel de l'administrateur de Kaspersky Security Center*.

Section		Paramètres
Paramètres	**Zone de confiance**	Le bouton **Configuration** du groupe **Zone de confiance** permet de configurer les paramètres suivants d'application d'une zone de confiance : • composer la liste des exclusions de la zone de confiance ; • activer ou désactiver l'analyse des opérations de sauvegarde des fichiers ; • composer la liste des processus de confiance.
	Stockages	Le bouton **Configuration** du groupe **Stockages** permet de configurer les paramètres suivants de la quarantaine et de la sauvegarde : • chemin d'accès du dossier dans lequel vous souhaitez placer les objets en quarantaine ou dans la sauvegarde ; • taille maximale de la sauvegarde ou de la quarantaine et seuil d'espace disponible ; • dossier où seront placés les objets restaurés depuis la sauvegarde ou la quarantaine ; • transmission au Serveur d'administration des informations relatives aux objets dans la sauvegarde ou la quarantaine.
	Montée en puissance et fiabilité	Le bouton **Configuration** du groupe **Montée en puissance et fiabilité** permet de configurer les paramètres généraux de montée en puissance et de fiabilité des tâches.
	Avancé	Le bouton **Configuration** du groupe **Avancé** sous l'onglet **Général** permet de configurer les paramètres suivants : • affichage de l'icône de l'application ;

Section		Paramètres
		• actions de l'application en cas de passage à l'alimentation via la batterie ; • seuils de déclenchement des événements *Les bases de l'application sont dépassées, Les bases de l'application sont fortement dépassées et L'analyse des zones critiques de l'ordinateur n'a pas été réalisée depuis longtemps* ; • désignation de Kaspersky Security Center en tant que serveur proxy pour l'activation de l'application. Si vous utilisez un système d'archivage HSM, l'onglet **Stockage hiérarchique** permet de configurer les paramètres du système HSM.
	Paramètres de connexion	Le bouton **Configuration** du groupe **Paramètres de connexion** permet de configurer les paramètres suivants du serveur proxy pour la connexion aux serveurs de mise à jour, aux serveurs d'activation et à KSN. • définition des paramètres d'utilisation du serveur proxy ; • définition des paramètres d'authentification au serveur proxy.
Journaux et notifications	**Journaux d'exécution des tâches**	Le bouton **Configuration** du groupe **Journaux d'exécution des tâches** permet de configurer les paramètres suivants : • définition du niveau d'importance des événements enregistrés pour les composants de l'application sélectionnés ; • définition des paramètres de conservation des journaux d'exécution des tâches.

Section		Paramètres
	Notifications sur les événements	Le bouton **Configuration** du groupe **Notifications sur les événements** permet de configurer les paramètres suivants : • paramètres de notification des utilisateurs pour l'événement Script dangereux détecté ; • paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements du groupe **Configuration des notifications**.
Protection en temps réel	**Protection des fichiers en temps réel**	Le bouton **Configuration** de la tâche Protection des fichiers en temps réel permet de configurer les paramètres suivants d'exécution de la tâche : • mode de protection des objets ; • utilisation de l'analyse heuristique ; • application de la zone de confiance ; • composition de la zone de protection ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de la sécurité ; • paramètres de lancement de la tâche.
	Analyse des scripts	Le bouton **Configuration** de la tâche Analyse des scripts permet de configurer les paramètres suivants d'exécution de la tâche : • autorisation ou interdiction de l'exécution de scripts potentiellement dangereux ; • utilisation de l'analyse heuristique ; • application de la zone de confiance ; • paramètres de lancement de la tâche.

Section		Paramètres
	Utilisation du KSN	Le bouton **Configuration** de la tâche Utilisation du KSN permet de configurer les paramètres suivants d'exécution de la tâche : • action à exécuter sur les objets infectés et autres objets détectés ; • performances de la tâche ; • paramètres d'utilisation de Kaspersky Security Center en tant que serveur proxy de KSN ; • acceptation du Règlement de KSN ; • paramètres de lancement de la tâche.
Contrôle du serveur	**Blocage de l'accès aux fichiers réseau**	Le bouton **Configuration** de la tâche Blocage de l'accès aux fichiers réseau permet de configurer les paramètres de déblocage des ordinateurs bloqués et les paramètres de lancement de la tâche.
	Contrôle du lancement des applications	Le bouton **Configuration** de la tâche Contrôle du lancement des applications permet de configurer les paramètres suivants d'exécution de la tâche : • mode de fonctionnement de la tâche ; • configuration des paramètres du contrôle du nouveau lancement des applications ; • zone d'application des règles de contrôle du lancement des applications ; • utilisation du KSN ; • paramètres de lancement de la tâche.
	Protection contre le chiffrement	Le bouton **Configuration** de la tâche Protection contre le chiffrement permet de configurer les paramètres suivants d'exécution de la tâche : • composition de la zone de protection ; • utilisation de l'analyse heuristique ; • paramètres de lancement de la tâche.

Section		Paramètres
Protection des stockages réseau	**Protection des stockages réseau connectés via le protocole RPC**	Le bouton **Configuration** de la tâche Protection des stockages réseau connectés via le protocole RPC permet de configurer les paramètres suivants d'exécution de la tâche : • composition de la zone de protection ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de la sécurité ; • utilisation de l'analyse heuristique ; • application de la zone de confiance et utilisation du KSN ; • paramètres de connexion au stockage réseau ; • paramètres de lancement de la tâche. Pour en savoir plus sur la configuration des paramètres de la tâche, consultez le *Manuel d'implantation de la protection des stockages réseau de Kaspersky Security for Windows Server*.
	Protection des stockages réseau connectés via le protocole ICAP	Le bouton **Configuration** de la tâche Protection des stockages réseau connectés via le protocole ICAP permet de configurer les paramètres suivants d'exécution de la tâche : • utilisation de l'analyse heuristique ; • paramètres de connexion au stockage réseau ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de la sécurité ; • utilisation du KSN ; • paramètres de lancement de la tâche.

Section		Paramètres
		Pour en savoir plus sur la configuration des paramètres de la tâche, consultez le *Manuel d'implantation de la protection des stockages réseau de Kaspersky Security for Windows Server*.
Tâches prédéfinies		Le bouton **Configuration** de la section **Tâches système** permet d'interdire ou d'autoriser le lancement des tâches système planifiées suivantes, configurée sur les ordinateurs locaux : • tâches d'analyse à la demande ; • tâches de mise à jour et de copie des mises à jour.
Autorisations d'accès		Le bouton **Configuration** du groupe **Autorisations d'accès** permet de configurer les paramètres d'accès aux fonctions de l'application : • accès des utilisateurs ou groupes d'utilisateurs à l'administration de Kaspersky Security. • accès des utilisateurs ou groupes d'utilisateurs à l'administration du service Kaspersky Security.
Profils de stratégie		La section **Profils de stratégie** permet d'administrer la liste des profils : ajout de nouveaux profils, modification des paramètres des profils de la liste, application d'un profil pour le contrôle du lancement des applications.

Configuration du lancement planifié des tâches locales prédéfinies

Les stratégies permettent d'autoriser ou d'interdire le lancement des tâches prédéfinies d'analyse à la demande et de mise à jour programmée, défini localement sur chaque serveur du groupe d'administration :

- Si le lancement d'une tâche planifiée, configuré localement, est interdit par la stratégie, c'est la planification définie dans les paramètres de la tâche de groupe qui sera appliquée.
- Si le lancement d'une tâche planifiée, configuré localement, est autorisé dans la stratégie, la planification configurée dans les paramètres de la tâche de groupe sera ignorée.

Il est conseillé d'interdire le lancement planifié des tâches prédéfinies locales d'analyse à la demande et de mise à jour pour tous les serveurs de la stratégie si la planification du lancement de ces tâches est contrôlé par des tâches de groupe de Kaspersky Security Center.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales prédéfinies suivantes :

- tâches d'analyse à la demande : Analyse rapide, Analyse des objets en quarantaine, Analyse au démarrage du système d'exploitation et Vérification de l'intégrité des modules de l'application ;
- tâches de mise à jour : Mise à jour des bases de l'application, Mise à jour des modules de l'application et Copie des mises à jour.

Si vous excluez le serveur protégé du groupe d'administration, la planification des tâches prédéfinies sera automatiquement activée.

► *Pour autoriser ou interdire le lancement planifié des tâches prédéfinies de Kaspersky Security dans une stratégie, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, déployez ensuite le groupe requis puis, sélectionnez le nœud **Stratégies** dans le panneau des résultats.
2. Sous l'onglet **Stratégies**, ouvrez le menu contextuel de la stratégie à l'aide de laquelle vous souhaitez configurer le lancement planifié des tâches prédéfinies de Kaspersky Security sur les serveurs du groupe et choisissez l'option **Propriétés**.

3. Dans la fenêtre **Propriétés** : **<Nom de la stratégie>**, ouvrez la section **Tâches prédéfinies**. Exécutez une des actions suivantes :
   - Cochez les cases **Autoriser le lancement de la tâche d'analyse à la demande** et **Autoriser l'exécution des tâches de mise à jour et de copie des mises à jour** pour autoriser le lancement planifié des tâches citées.
   - Décochez les cases **Autoriser le lancement de la tâche d'analyse à la demande** et **Autoriser l'exécution des tâches de mise à jour et de copie des mises à jour** pour interdire le lancement planifié des tâches citées.
4. Assurez-vous que la stratégie que vous configurez est active et agit dans le groupe de serveurs d'administration (cf. section "A propos des stratégies" à la page 391).
5. Cliquez sur **OK**.

Les paramètres définis du lancement planifié des tâches sélectionnées seront enregistrés.

Administration du lancement de l'application via Kaspersky Security Center

Vous pouvez autoriser ou interdire le lancement d'applications sur tous les serveurs du réseau de l'organisation en créant des listes communes de règles de contrôle du lancement des applications du côté de Kaspersky Security Center pour des groupes de serveurs.

Dans cette section

A propos de la création de règles de contrôle du lancement des applications pour tous les serveurs dans Kaspersky Security Center

Vous pouvez créer des listes de règles de contrôle du lancement des applications à l'aide de tâches de Kaspersky Security Center directement pour tous les serveurs et groupes de serveurs du réseau de l'organisation. Cette option est conseillée si le réseau de l'organisation ne comporte pas une machine modèle et si vous n'êtes pas en mesure de créer une liste générale de règles à l'aide d'une tâche de génération automatique des règles d'autorisation sur la base des applications installées sur cette machine modèle (cf. section “A propos de l'importation de règles depuis un fichier au format XML” à la page 203).

Vous pouvez créer des listes de règles de contrôle du lancement des applications dans Kaspersky Security Center de deux manières :

- Via une tâche de groupe de génération automatique des règles de contrôle du lancement des applications.

  Dans ce scénario, la tâche de groupe crée pour chaque serveur du réseau sa propre liste de règles de contrôle du lancement des applications et les enregistre dans un fichier XML dans le dossier réseau partagé indiqué. Par la suite, vous pouvez importer manuellement les listes de règles créées dans la tâche Contrôle du lancement des applications dans la stratégie Kaspersky Security Center. A la différence d'une tâche sur l'ordinateur local, la tâche sur Kaspersky Security Center n'accepte pas la configuration de l'ajout automatique des règles créées dans la liste des règles de contrôle du lancement des applications à la fin de la tâche de groupe de génération automatique des règles d'autorisation.

  Il est conseillé d'utiliser ce scénario quand il faut créer rapidement des listes de règles de contrôle du lancement des applications. Le lancement de la tâche Génération automatique des règles selon une planification ne doit être configuré que si la zone d'application des règles d'autorisations contient des dossiers contenant des fichiers réputés sûrs.

- Sur la base du rapport relatif aux événements de la tâche, généra dans Kaspersky Security Center suite au fonctionnement du Contrôle du lancement des applications en mode **Statistiques seulement**.

Dans ce cas de figure, Kaspersky Security Center ne bloque pas les lancements des applications mais consigne dans la section **Evénements** tous les lancements et blocages de lancements des applications sur tous les serveurs du réseau au cours de la période d'exécution de la tâche de contrôle du lancement des applications en mode **Statistiques seulement**. Kaspersky Security Center établit ensuite, sur la base du journal d'exécution de la tâche, une liste unique des événements de blocage des applications.

Il faut configurer la période d'exécution de la tâche de telle sorte que tous les scénarios envisageables de fonctionnement des serveurs à protéger et des groupes de serveur ainsi qu'au moins un redémarrage de ceux-ci aient pu se dérouler au cours de l'intervalle indiqué. Par la suite, lors de l'ajout de règles à la tâche de contrôle du lancement des applications, vous pouvez importer les données relatives aux lancements d'application depuis le fichier de rapport sur les événements de Kaspersky Security Center enregistré au format TXT et créer, sur la base de ces données, des règles d'autorisation pour le contrôle du lancement de ces applications.

Il est conseillé d'utiliser ce scénario quand le réseau de l'organisation compte un nombre élevé de serveurs de différents types (avec différentes applications installées) (cf. section "Utilisation d'un profil lors de la configuration de la tâche Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center" à la page 408).

Il est conseillé d'actualiser les listes de règles après toute modification de la composition des applications installées sur les serveurs du réseau (par exemple, en cas d'installation d'une mise à jour ou de réinstallation du système d'exploitation). Il est conseillé de créer la liste actualisée des règles à l'aide de la tâche de groupe Génération automatique des règles d'autorisation ou la stratégie Contrôle du lancement des applications en mode **Statistiques seulement**, exécutées sur les serveurs du *groupe d'administration d'essai*.

Le groupe d'administration d'essai réunit les serveurs indispensables à la vérification du lancement de nouvelles applications avant leur installation sur les serveurs du réseau.

Utilisation d'un profil lors de la configuration de la tâche Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center

Les règles de contrôle du lancement des applications, configurées dans une stratégie, s'appliquent à tous les serveurs du groupe d'administration. Si des serveurs de différents types ont été ajoutés à un groupe d'administration, il faudra peut-être prévoir des listes individuelles de règles pour le contrôle du lancement des applications sur chacun d'entre eux. Pour pouvoir restreindre l'application d'une stratégie aux serveurs d'un groupe d'administration, vous pouvez utiliser des *profils de stratégie*.

Il est recommandé d'appliquer les profils de stratégie pour la configuration des règles de contrôle du lancement des applications sur des serveurs de différents types à l'intérieur d'un même groupe d'administration géré par une même stratégie. Ceci permet d'optimiser la protection du serveur car les règles définies contrôlent le lancement des seules applications caractéristiques pour ce type de serveur (par exemple, vous pouvez autoriser le lancement uniquement des clients de messagerie via un profil configuré pour des serveurs de messagerie).

Les profils de stratégie sont appliqués à tous les serveurs du groupe d'administration conformément aux *tags* attribués à ceux-ci. Vous pouvez configurer un profil de stratégie pour tous les serveurs d'un groupe possédant le même tag.

> Pour en savoir plus sur les tags et les profils de stratégie et pour obtenir les instructions sur leur utilisation, consultez le *Manuel de l'administrateur de Kaspersky Security Center*.

► *Pour appliquer un profil de stratégie dans la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration pour lequel vous souhaitez configurer l'application de profils de stratégie.

2. Définissez les tags pour chaque serveur du groupe d'administration, en fonction des types de serveur. Pour ce faire, procédez comme suit :

   - Dans le panneau des résultats du groupe d'administration sélectionné, ouvrez l'onglet **Ordinateurs** et sélectionnez le serveur auquel vous souhaitez attribuer un tag. Dans la fenêtre **Propriétés : <Nom de l'ordinateur>** du serveur sélectionné, ouvrez la section **Balises** et composez la liste des tags. Cliquez sur **OK**.

3. Créez le profil de stratégie et configurez son application pour la protection des serveurs au sein du groupe d'administration. Pour ce faire, procédez comme suit :

   - Dans le panneau des résultats du groupe d'administration sélectionné, accédez à l'onglet **Stratégies** et sélectionnez la stratégie pour laquelle vous souhaitez configurer l'application de profils. Dans la fenêtre **Propriétés : <nom de la stratégie>** de la stratégie sélectionnée, ouvrez la section **Profil de** la stratégie, puis cliquez sur le bouton **Ajouter**, pour créer un autre profil. La fenêtre **Propriétés : <Nom du profil>** s'ouvre. Exécutez les actions suivantes :

     a. Dans la section **Règles d'activation**, configurez la zone d'application du profil et définissez les conditions dans lesquelles le profil sera activé.

     b. Dans la section **Contrôle du lancement des applications**, configurez la liste des règles de contrôle du lancement des applications pour le profil modifié.

     c. Cliquez sur **OK**.

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

Le profil configuré sera appliqué dans la stratégie pour la tâche Contrôle du lancement des applications.

Importation des règles depuis un fichier XML

Vous pouvez importer les rapports créés sur la base des résultats de l'exécution de la tâche de groupe Génération automatique des règles d'autorisation et les appliquer en guise de liste de règles d'autorisation dans la stratégie configurée.

A la fin de la tâche de groupe de génération automatique des règles d'autorisation, l'application exporte les règles d'autorisation créées dans un fichier au format XML enregistré dans le dossier réseau partagé. Chaque fichier contenant une liste de règles est créé au départ de l'analyse du lancement des fichiers et des applications sur chaque serveur distinct du réseau de l'organisation. La liste contient les règles d'autorisation du lancement pour les fichiers et les applications dont le type correspond au type repris dans les paramètres de la tâche de groupe de génération automatique des règles.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour créer des règles d'autorisation de lancement d'applications pour un groupe de serveurs sur la base de la liste des règles d'autorisation créée automatiquement, procédez comme suit.*

1. Sous l'onglet **Tâches** dans le panneau d'administration du groupe de serveur configuré, créez une tâche de groupe Génération automatique des règles d'autorisation ou choisissez une tâche existante.

2. Dans les propriétés de la tâche de groupe de génération automatique des règles d'autorisation créée ou dans l'Assistant de création de tâche, configurez les paramètres suivants :

   - Dans la section **Notifications**, configurez les paramètres de conservation du rapport sur l'exécution de la tâche.

     Les détails sur la configuration des paramètres dans cette section sont repris dans le *Manuel de l'administrateur de Kaspersky Security Center*.

   - Dans la section **Configuration**, indiquez les types d'application dont le lancement sera autorisé par les règles créées. Vous pouvez également modifier la composition du dossier dont les applications pourront être lancées : exclure les dossiers indiqués par défaut de la zone d'application de la tâche et ajouter manuellement de nouveaux dossiers.

   - Dans la section **Paramètres**, indiquez les actions de la tâche pendant son exécution et à son issue. Indiquez les critères qui seront utilisés pour créer les règles ainsi que le nom du fichier dans lequel ces règles seront créées.

   - Dans la section **Planification**, configurez les paramètres du lancement de la tâche selon la planification.

- Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel la tâche sera exécutée.
- Dans la section **Exclusions de la zone d'action de la tâche**, définissez les groupes d'ordinateurs qu'il faut exclure de la zone d'action de la tâche.

> Kaspersky Security ne créera pas de règles d'autorisation d'après les applications exécutées sur les ordinateurs exclus.

3. Sous l'onglet **Tâches** du panneau d'administration du groupe de serveurs configurés, sélectionnez la tâche de génération automatique des règles d'autorisation dans la liste des tâches de groupe, puis cliquez sur le bouton **Démarrer** pour lancer la tâche.

   A l'issue de la tâche, les listes de règles d'autorisation générées automatiquement seront enregistrées dans le dossier réseau partagé dans des fichiers XML.

4. Ajoutez les listes de règles d'autorisation créées à la tâche de contrôle du lancement des applications. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie configurée, dans les paramètres de la tâche Contrôle du lancement des applications :

   a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

   b. Cliquez sur le bouton **Ajouter** et dans la liste qui s'ouvre, choisissez l'option **Importer les règles depuis un fichier au format XML**.

   c. Sélectionnez le principe d'ajout des règles d'autorisation générées automatiquement à la liste des règles de contrôle du lancement des applications déjà créées. Il est conseillé de choisir l'option **Fusionner les règles aux règles existantes** qui ajoute uniquement les règles qui n'existent pas déjà dans la liste.

   d. Dans la fenêtre Windows standard qui s'ouvre, choisissez les fichiers au format XML créés à l'issue de la tâche de groupe Génération automatique des règles d'autorisation.

   e. Cliquez sur le bouton **OK** dans la fenêtre **Règles du contrôle du lancement des applications** et dans la fenêtre **Paramètres de la tâche**.

5. Si vous souhaitez appliquer les règles créées pour le contrôle du lancement des applications, sélectionnez le mode d'exécution **Appliquer les règles de contrôle du lancement des applications** dans les propriétés de la tâche Contrôle du lancement des applications dans la stratégie.

Les règles d'autorisation générées automatiquement sur la base des lancements de tâches sur chaque serveur distinct seront appliquées à tous les ordinateurs du réseau soumis à la stratégie configurée. Pour ces ordinateurs, l'application autorisera le lancement uniquement des applications pour lesquelles des règles d'autorisation ont été créées.

Importation des règles depuis un fichier de rapport de Kaspersky Security Center sur les applications bloquées

Vous pouvez importer les données relatives aux lancements d'application bloqués depuis le rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche Contrôle du lancement des applications en mode **Statistiques seulement** et appliquer ces données à la composition d'une liste de règles d'autorisation du lancement d'applications dans la stratégie configurée.

Lors de la création du rapport sur les événements survenus pendant l'exécution de la tâche de contrôle du lancement des applications, vous pouvez surveiller le lancement des applications qu'il faudra bloquer.

Lors de l'importation depuis le rapport des données sur les applications bloquées dans les paramètres de la stratégie, confirmez que la liste à appliquer contient uniquement les applications dont vous souhaitez autoriser le lancement.

► *Pour créer des règles d'autorisation du lancement d'application pour un groupe de serveurs sur la base d'un rapport de Kaspersky Security Center relatif aux applications bloquées, procédez comme suit :*

1. Dans les propriétés de la stratégie, accédez aux paramètres de la tâche Contrôle du lancement des applications et activez le mode **Statistiques seulement**.

2. Dans la section **Evénements** des propriétés de la stratégie, assurez-vous que :

   - La durée de conservation de l'événement est supérieure à la durée de fonctionnement prévue de la tâche en mode **Statistiques seulement** (valeur par défaut : 30 jours) sous l'onglet **Evénement critique** pour l'événement *Le lancement de l'application est interdit*.
   - La durée de conservation de l'événement est supérieure à la durée prévue de fonctionnement de la tâche en mode **Statistiques seulement** (valeur par défaut : 30 jours) sous l'onglet **Avertissement** pour l'événement *Statistiques seulement : le lancement de l'application est interdit*.

     A l'issue de la période définie dans la colonne **Durée de conservation**, les informations relatives aux événements enregistrés seront supprimées et ne figureront pas dans le fichier du rapport. Avant de lancer la tâche Contrôle du lancement des applications en mode **Statistiques seulement**, assurez-vous que la durée d'exécution de la tâche n'est pas supérieure à la durée de conservation établie pour les événements indiqués.

3. Une fois la tâche terminée, exportez les événements enregistrés dans un fichier .TXT. Pour ce faire, développez l'entrée **Rapports et notifications** et dans la sous-entrée **Evénements**, créez une sélection d'événements sur la base de la caractéristique *Interdit* afin de voir les applications dont le lancement sera bloqué par la tâche de contrôle du lancement des applications. Dans le panneau des résultats de la sélection créée, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les lancements d'application bloqués dans un fichier au format TXT.

   Avant d'importer et d'appliquer un rapport créé dans une stratégie, assurez-vous qu'il contient les données relatives uniquement aux applications dont vous souhaitez autoriser le lancement.

4. Importez les données relatives aux lancements d'application bloqués dans la tâche de contrôle du lancement des applications. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie, dans les paramètres de la tâche Contrôle du lancement des applications :

   a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel, sélectionnez l'option **Importer les données relatives aux applications bloquées depuis le rapport de Kaspersky Security Center**.

c. Sélectionnez le principe d'ajout des règles depuis la liste créée sur la base du rapport de Kaspersky Security Center à la liste des règles de contrôle du lancement des applications existantes.

d. Dans la fenêtre Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les lancements d'application bloqués ont été exportés.

e. Cliquez sur le bouton **OK** dans la fenêtre **Règles du contrôle du lancement des applications** et dans la fenêtre **Paramètres de la tâche**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les applications bloquées seront ajoutées à la liste des règles de contrôle du lancement des applications.

Création et configuration d'une tâche dans Kaspersky Security Center

Cette section contient des informations sur les tâches dans Kaspersky Security Center, ainsi que des instructions pour configurer leurs paramètres.

Dans cette section

A propos de la création de tâches dans Kaspersky Security Center

Vous pouvez créer des tâches de groupe pour des groupes d'administration et pour des sélections d'ordinateurs. Vous pouvez créer les types de tâche suivants :

- ajout d'une clé ;
- copie des mises à jour ;
- tâches de mise à jour des bases et des modules de l'application ;
- remise à l'état antérieur à la mise à jour des bases de l'application ;
- analyse à la demande ;
- vérification de l'intégrité des modules de l'application ;
- génération automatique des règles d'autorisation.

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- pour un ordinateur : dans la fenêtre **Propriétés <nom de l'ordinateur>**dans la section **Tâches** ;
- pour un groupe d'administration : dans le panneau des résultats de l'entrée du groupe d'ordinateurs sélectionné sous l'onglet **Tâches** ;
- pour une sélection d'ordinateurs : dans le panneau des résultats de l'entrée **Tâches pour des sélections d'ordinateurs**.

Les stratégies permettent de suspendre la programmation des tâches locales prédéfinies de mise à jour et d'analyse à la demande sur tous les serveurs protégés appartenant à un groupe d'administration. (cf. section “Configuration du lancement planifié des tâches locales prédéfinies” à la page 404)

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Manuel de l'administrateur Kaspersky Security Center.*

Création d'une tâche dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour créer une tâche dans la console d'administration de Kaspersky Security Center, procédez comme suit :*

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :

   - Pour créer une tâche locale :

     a. Dans l'arborescence de la console d'administration, déployez l'entrée **Ordinateurs administrés,** puis sélectionnez le groupe auquel appartient le serveur protégé.

     b. Dans le panneau des résultats, sous l'onglet **Ordinateurs**, ouvrez le menu contextuel de la ligne reprenant les informations relatives au serveur protégé, puis sélectionnez l'option **Propriétés**.

     c. Dans la section **Tâches** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   - Pour créer une tâche de groupe :

     a. Dans l'arborescence de la console d'administration, développez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe pour lequel vous souhaité créer une stratégie.

     b. Dans le panneau des résultats, ouvrez le menu contextuel de l'onglet **Tâches** et choisissez l'option **Créer → Tâche**.

   - Pour créer une tâche pour une sélection arbitraire d'ordinateurs, ouvrez, dans l'arborescence de la Console d'administration, le menu contextuel de l'entrée **Tâches pour des sélections d'ordinateurs** et choisissez l'option **Créer → Tâche**.

   La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la fenêtre **Définition du nom de la tâche**, saisissez le nom de la tâche (100 caractères maximum, ne peut contenir les caractères **I * < > ? \ / | :)**. Il est conseillé d'utiliser un nom qui évoque la tâche (par exemple, Analyse à la demande du dossier partagé).
3. Dans la fenêtre **Sélection du type de la tâche**, sous l'onglet **Kaspersky Security 10 for Windows Server**, sélectionnez le type de la tâche à créer.
4. Si vous avez choisi n'importe quel type de tâche, à l'exception de Annulation de la mise à jour des bases de l'application ou Ajout d'une clé, la fenêtre **Configuration** s'ouvre. Sélectionnez une des options suivantes :
   - **Créer**, pour créer une tâche selon les paramètres définis par défaut pour les tâches nouvellement créées du type que vous avez sélectionné ;
   - **Importer une tâche créée à l'aide de Kaspersky Anti-Virus version 6.0 ou 8.0**, pour utiliser en tant que modèle une tâche créée préalablement dans Kaspersky Anti-Virus 6.0 ou 8.0 for Windows Servers Enterprise Edition.

     Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de configuration dans lequel vous aviez enregistré la tâche existante.
5. En fonction du type de tâche créée, exécutez une des actions suivantes :
   - *Si vous créez une tâche d'analyse à la demande* :
     a. Dans la fenêtre **Zone d'analyse**, définissez la zone d'analyse.

     La zone d'analyse reprend par défaut les secteurs critiques du serveur. Les zones analysées sont accompagnées d'une coche ☑ dans le tableau.

     Vous pouvez modifier la zone d'analyse, y inclure des zones distinctes prédéfinies, des disques, des dossiers, des objets de réseaux et des fichiers et définir les paramètres particuliers de la protection pour chaque zone ajoutée.

     - Pour exclure de l'analyse toutes les zones d'analyse, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.
     - Pour inclure une zone prédéfinie, un disque, un dossier, un objet réseau ou un fichier à la zone d'analyse, cliquez avec le bouton droit de la souris dans le tableau **Zone d'analyse** et choisissez l'option **Ajouter une zone**. Dans la fenêtre **Ajout d'objets à la zone d'analyse**, sélectionnez une zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque du serveur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur **OK**.

- Pour exclure les sous-dossiers ou les sous-fichiers de l'analyse, sélectionnez le dossier (disque) ajouté dans la fenêtre **Zone d'analyse** de l'Assistant, ouvrez le menu contextuel et choisissez l'option **Personnaliser**, puis dans la fenêtre **Niveau de sécurité**, cliquez sur le bouton **Configuration** et dans la fenêtre **Configuration de l'analyse à la demande**, sous l'onglet **Général**, décochez la case **Sous-dossiers** (**Sous-fichiers**).
- Pour modifier les paramètres de sécurité de la zone d'analyse, ouvrez le menu contextuel de la zone dont vous souhaitez modifier les paramètres et choisissez l'option **Personnaliser**. Dans la fenêtre **Configuration de l'analyse à la demande**, sélectionnez un des niveaux de sécurité prédéfinis ou cliquez sur le bouton **Configuration** afin de configurer manuellement les paramètres de sécurité. La configuration se déroule de la même manière que dans la console de Kaspersky Security.
- Pour exclure les objets intégrés de la zone d'analyse ajoutée, ouvrez le menu contextuel dans le tableau **Zone d'analyse**, sélectionnez **Ajouter une exclusion** et désignez les objets que vous voulez exclure : sélectionnez une zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque du serveur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur le bouton **OK**.

  Les zones exclues de l'analyse sont accompagnées de l'icône ☐ dans le tableau.

  a. Exécutez les actions suivantes dans la fenêtre **Paramètres**.

  Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure de la zone d'analyse les objets décrits dans la zone de confiance de Kaspersky Security.

  Si vous avez l'intention d'utiliser la tâche créée en tant que tâche d'analyse des zones critiques de l'ordinateur, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide** dans la fenêtre **Paramètres**. L'application Kaspersky Security Center évaluera l'état de la sécurité du ou des serveurs sur la base des résultats de l'exécution des tâches ayant le statut *Tâche d'analyse des zones critiques*, et non seulement sur la base des résultats de l'exécution de la tâche prédéfinie **Analyse rapide**. Lors de la création d'une tâche locale d'analyse à la demande, la case n'est pas accessible.

Pour attribuer la priorité de base **Bas** (**Low**) au processus de travail dans lequel la tâche sera exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Paramètres**. Par défaut, les processus dans lesquels les tâches de Kaspersky Security sont exécutées ont la priorité **Moyenne** (**Normal**). La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

- *Si vous créez une des tâches de mise à jour*, définissez les paramètres de la tâche conformément à vos exigences:

    a. Sélectionnez la source des mises à jour dans la fenêtre **Source des mises à jour**.

    b. Cliquez sur le bouton **Configuration des paramètres du réseau local**. La fenêtre **Configuration des paramètres de connexion** s'ouvre.

    c. Sous l'onglet **Configuration des paramètres de connexion**, procédez comme suit :

    Désignez le mode du serveur FTP pour la connexion au serveur protégé.

    Le cas échéant, modifiez le délai d'attente pour la connexion au serveur de mise à jour.

    Configurez les paramètres d'accès au serveur proxy lors de la connexion à la source des mises à jour.

    Indiquez l'emplacement du serveur protégé (ou des serveurs) pour optimiser la récupération des mises à jour.

- *Si vous créez une tâche Mise à jour des modules de l'application*, configurez les paramètres requis de la mise à jour des modules de l'application dans la fenêtre **Configuration des paramètres de mise à jour des modules de l'application** :

    a. Décidez si vous souhaitez copier et installer les mises à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles.

    b. Si vous avez choisi **Copier et installer les mises à jour critiques des modules de l'application**, le redémarrage du serveur peut être requis pour terminer l'installation des modules de l'application. Pour que Kaspersky Security relance automatiquement le serveur après la fin de la tâche, cochez la case **Autoriser le redémarrage du système d'exploitation**. Pour annuler le redémarrage automatique une fois la tâche terminée, décochez la case **Autoriser le redémarrage du système d'exploitation**.

c. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour prévues des modules de Kaspersky Security, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement **Des mises à jour prévues des modules de Kaspersky Security sont disponibles**. Celle-ci reprendra l'adresse de la page de notre site d'où les mises à jour prévues peuvent être téléchargées.

- *Si vous créez la tâche Copie des mises à jour*, indiquez, dans la fenêtre **Configuration des paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de la source locale des mises à jour, dans lequel les mises à jour seront enregistrées.

- *Si vous créez une tâche Activation de l'application*, appliquez le fichier clé ou le code d'activation à l'aide duquel vous souhaitez activer l'application dans la fenêtre **Paramètres d'activation**. Cochez la case **Utiliser en tant que code d'activation additionnel ou clé additionnelle** si vous souhaitez créer une tâche pour renouveler la licence.

- *Si vous créez une tâche Génération automatique des règles d'autorisation*, désignez dans la fenêtre **Configuration** les paramètres sur la base desquels la liste des règles d'autorisation sera créée :

  a. Indiquez un préfixe pour les noms des règles et configurez les paramètres de la zone d'application des règles d'autorisation. Cliquez sur **Suivant**.

  b. Désignez les actions que la tâche exécutera pendant la génération des règles d'autorisation et à l'issue de celle-ci.

6. Configurez les paramètres de la planification de la tâche (vous pouvez configurer la planification des tâches de tous les types à l'exception de la tâche Annulation de la mise à jour). Exécutez les actions suivantes dans la fenêtre **Planification** :

   a. Pour activer la planification, cochez la case **Exécuter de manière planifiée** ;

b. Désignez la fréquence d'exécution de la tâche : choisissez une des valeurs suivantes dans la liste **Fréquence** : **Chaque heure**, **Chaque jour**, **Chaque semaine**, **Au lancement de l'application**, **À la mise à jour des bases de l'application** (dans les tâches de groupe Mise à jour des bases de l'application, Mise à jour des modules de l'application, vous avez également la possibilité de choisir la fréquence **Après réception des mises à jour par le serveur d'administration**) :

- Si vous avez sélectionné **Chaque heure**, indiquez le nombre d'heures dans le champ **Toutes les <chiffres> heure(s)** du groupe de paramètres **Configuration du démarrage des tâches** ;
- Si vous avez sélectionné **Chaque jour**, indiquez le nombre de jours dans le champ **Tous les <chiffres> jour(s)** du groupe de paramètres **Configuration du démarrage des tâches**.
- Si vous avez sélectionné **Chaque semaine**, indiquez le nombre de semaines dans le champ **Toutes les <chiffres> semaine(s)** du groupe de paramètres **Configuration du démarrage des tâches**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;

c. Dans le champ **Heure de démarrage**, indiquez l'heure de la première exécution de la tâche ; dans le champ **A partir de**, indiquez la date d'entrée en vigueur de la planification.

d. Au besoin, définissez les paramètres complémentaires de la planification : cliquez sur le bouton **Avancé** et, dans la fenêtre **Paramètres de planification avancés**, procédez comme suit :

- Définissez la durée maximale de l'exécution d'une tâche : saisissez le nombre d'heures et de minutes dans le champ **Durée** du groupe **Paramètres d'arrêt de la tâche**.
- Indiquez l'intervalle de temps au cours d'une période de 24 heures pendant lequel l'exécution de la tâche sera suspendue : dans le groupe **Paramètres d'arrêt de la tâche**, saisissez les heures de début et de fin de l'intervalle dans le champ **Suspendre à partir de … jusqu'à**.
- Indiquez la date à partir de laquelle la planification ne sera plus active : cochez la case **Suspendre la planification à partir du** et à l'aide de la fenêtre **Calendrier,** choisissez la date à partir de laquelle la planification ne sera plus active.

- Activez le lancement des tâches ignorées : cochez la case **Lancer les tâches non exécutées**.
- Activez l'utilisation du paramètre de répartition de l'heure d'exécution : cochez la case **Répartir l'exécution des tâches sur** et indiquez la valeur du paramètre en minutes.

e. Cliquez sur **OK**.

7. Si la tâche créée est une tâche pour une sélection quelconque d'ordinateurs, sélectionnez les ordinateurs du réseau (groupes) sur lesquels elle sera exécutée.

8. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte sous les autorisations duquel vous souhaitez exécuter la tâche.

9. Dans la fenêtre **Fin de la création de la tâche**, cochez la case **Lancer la tâche à la fin de l'Assistant** si vous souhaitez que la tâche soit lancée après sa création. Cliquez sur le bouton **Terminer**.

La tâche créée apparaîtra dans la liste **Tâches**.

Configuration des tâches de groupe dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer une tâche de groupe pour plusieurs serveurs, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de la tâche.

2. Dans le panneau des résultats du groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez la tâche dont vous souhaitez configurer les paramètres. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

   - double-cliquez sur le nom de la tâche dans la liste des tâches créées ;
   - sélectionnez le nom de la tâche dans la liste des tâches créées et suivez le lien **Modifier les paramètres de la tâche** ;
   - ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

4. Dans la section **Notifications**, configurez les paramètres de notification sur les événements de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Manuel de l'administrateur de Kaspersky Security Center*.

5. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :

   - Si vous configurez une tâche d'analyse à la demande :

     a. Dans la section **Configuration**, créez la zone d'analyse.

     b. Dans la section **Paramètres**, configurez l'intégration aux autres modules de l'application et le niveau de priorité de la tâche.

   - Si vous configurez l'une des tâches de mise à jour, définissez les paramètres de la tâche en fonction de vos besoins :

     a. Dans la section **Source des mises à jour**, configurez les paramètres de la source des mises à jour et l'optimisation de l'utilisation du sous-système disque.

     b. Cliquez sur le bouton **Configuration des paramètres de connexion** pour configurer les paramètres de connexion généraux et les paramètres de connexion à la source des mises à jour.

   - Si vous configurez la tâche Mise à jour des modules de l'application, sélectionnez dans la section **Configuration des paramètres de mise à jour des modules de l'application** l'action à effectuer : copier et installer les mises à jour critiques des modules de l'application ou simplement rechercher les mises à jour disponibles.

- Si vous configurez la tâche Copie des mises à jour, indiquez, dans la section **Configuration des paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de la source locale des mises à jour, dans lequel les mises à jour seront enregistrées.

- Si vous configurez la tâche Activation de l'application, appliquez le fichier clé ou le code d'activation à l'aide duquel vous souhaitez activer l'application dans la section **Paramètres d'activation**. Cochez la case **Utiliser en tant que code d'activation additionnel ou clé additionnelle** si vous souhaitez ajouter un code d'activation ou une clé pour renouveler la licence.

- Si vous configurez la tâche Génération automatique des règles d'autorisation, désignez dans la section **Configuration** les paramètres sur la base desquels la liste des règles d'autorisation sera créée.

6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour).

7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Manuel de l'administrateur de Kaspersky Security Center.*

8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Manuel de l'administrateur de Kaspersky Security Center*

9. Dans la fenêtre **Propriétés <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

Les paramètres des tâches de groupe pouvant être configurés sont décrits dans le tableau ci-dessous.

Tableau 64. Paramètres des tâches de groupe de Kaspersky Security

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
Génération automatique des règles d'autorisation	**Configuration**	Vous pouvez modifier la zone de protection en ajoutant ou en supprimant des chemins d'accès aux dossiers et en indiquant l'emplacement des dossiers et les types de fichiers dont le lancement est autorisé par les règles générées automatiquement. Lors de la création des règles d'autorisation, vous pouvez tenir compte, ou non, des applications déjà en cours d'exécution.
	Paramètres	Vous pouvez indiquer les actions lors de la création des règles d'autorisation : • **Utiliser un certificat numérique** ; Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Cette option est conseillée si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation. Cette option est sélectionnée par défaut.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
		• **Utiliser l'en-tête et l'empreinte du certificat numérique** ; La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique. Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique indiqués dans la règle. L'utilisation de cette case limite de manière plus stricte le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
		unique du certificat numérique et elle ne peut être forgée. Si la case est désélectionnée, le critère de déclenchement des règles d'autorisation du contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation. La case est accessible si vous avez choisi l'option **Utiliser un certificat numérique**. Cette case est cochée par défaut. • **En l'absence de certificat** ; Liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le contrôle du lancement des applications dans le cas où le fichier sur la base duquel est créée la règle ne dispose pas d'un certificat numérique. • **Code de hachage SHA256**. La valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
		applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée. • **Chemin du fichier**. Le chemin d'accès au fichier sur la base duquel est créée la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications par les fichiers qui se trouvent dans les dossiers indiqués sous l'onglet **Dossiers de sélection** dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**. • **Utiliser le code de hachage SHA256** ; Si cette option est sélectionnée, la valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
		applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la valeur de la somme de contrôle indiquée. • **Créer des règles pour un utilisateur ou un groupe d'utilisateurs**. Champ affichant l'utilisateur et/ou le groupe d'utilisateurs. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini. Par défaut, le groupe **Tous** est sélectionné. Vous pouvez configurer les paramètres pour le fichier de configuration à l'aide de la liste des règles d'autorisation créées que Kaspersky Security compose au terme de l'exécution de la tâche.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.
Activation de l'application	**Paramètres d'activation de l'application**	Vous pouvez ajouter un code d'activation ou une clé pour l'activation de l'application ou le renouvellement de la licence.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
Copie des mises à jour	**Source des mises à jour**	Vous pouvez indiquer le serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky Lab en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs indiqués manuellement.
	Fenêtre **Configuration des paramètres de connexion** ► *Pour ouvrir la fenêtre **Configuration des paramètres de connexion**,* cliquez sur le bouton **Configuration** des paramètres de connexion dans la section **Source des mises à jour**.	Vous pouvez activer ou désactiver l'utilisation du mode FTP passif, si possible, et indiquer le délai d'attente de la connexion. Dans le groupe **Paramètres de connexion aux sources des mises à jour** vous pouvez configurer les paramètres d'utilisation du serveur proxy pour la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs.
	Configuration des paramètres de copie des mises à jour	Vous pouvez indiquer le contenu des mises à jour à copier. Dans le champ **Dossier de conservation locale des mises à jour copiées**, indiquez le chemin d'accès au dossier dans lequel Kaspersky Security conservera les mises à jour copiées.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.
Mise à jour des bases de l'application	**Source des mises à jour**	Dans le groupe **Source des mises à jour**, vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs indiqués manuellement. Le groupe **Optimisation de l'utilisation du sous-système disque** vous permet de configurer les paramètres de la fonction réduisant la charge sur le sous-système disque. Cette fonction est disponible sous Microsoft Windows Server 2008 ainsi que les versions plus récentes du système d'exploitation : • **Réduire la charge sur le sous-système disque aux dépends de la mémoire vive**. La case active ou désactive la fonction d'optimisation du sous-système disque grâce à un placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
		Quand la case est cochée, la fonction est active. Cette case est décochée par défaut. • **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**.
	Fenêtre **Configuration des paramètres de connexion** ► *Pour ouvrir la fenêtre **Configuration des paramètres de connexion**,* cliquez sur le bouton **Configuration des paramètres de connexion** dans la section **Source des mises à jour**.	Vous pouvez activer ou désactiver l'utilisation du mode FTP passif, si possible, et indiquer le délai d'attente de la connexion. Dans le groupe **Paramètres de connexion aux sources des mises à jour** vous pouvez configurer les paramètres d'utilisation du serveur proxy pour la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.
Mise à jour des modules de l'application	**Source des mises à jour**	Vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs indiqués manuellement.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
	Fenêtre **Configuration des paramètres de connexion** ► *Pour ouvrir la fenêtre **Configuration des paramètres de connexion**,* cliquez sur le bouton **Configuration des paramètres de connexion** dans la section **Source des mises à jour**.	Vous pouvez activer ou désactiver l'utilisation du mode FTP passif, si possible, et indiquer le délai d'attente de la connexion. Dans le groupe **Paramètres de connexion aux sources des mises à jour** vous pouvez configurer les paramètres d'utilisation du serveur proxy pour la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs.
	Configuration des paramètres de mise à jour des modules de l'application	Vous pouvez indiquer les actions que Kaspersky Security effectuera si des mises à jour critiques des modules de l'application sont disponibles ou si des informations sur les mises à jour programmées sont disponibles, et configurer les actions effectuées par l'application une fois l'installation des mises à jour critiques terminée.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
Analyse à la demande	**Configuration**	Vous pouvez définir la Zone d'analyse pour la tâche d'analyse à la demande et accéder à la configuration du niveau de sécurité.
	Fenêtre **Configuration de l'analyse à la demande** ► *Pour ouvrir la fenêtre **Configuration de l'analyse à la demande**,* cliquez sur le bouton **Configurer le niveau de sécurité** dans la section **Configuration**.	Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou configurer manuellement les paramètres du niveau de sécurité personnalisé.
	Paramètres	Le groupe **Analyseur heuristique** vous permet d'activer ou de désactiver l'utilisation de l'analyseur heuristique dans la tâche d'analyse à la demande et de configurer le niveau d'analyse à l'aide du curseur. Dans le groupe **Paramètres avancés**, vous pouvez configurer les paramètres suivants : • application d'une zone de confiance dans la tâche d'analyse à la demande ; • utilisation des services du KSN dans la tâche d'analyse à la demande ; • niveau de priorité de la tâche d'analyse à la demande : effectuer la tâche en arrière-plan (priorité basse) ou considérer l'exécution de la tâche comme un tâche d'analyse rapide (priorité élevée).
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

Type de la tâche de Kaspersky Security	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
Vérification de l'intégrité des modules de l'application	**Planification**	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

Pour le type de tâche Retour à l'état antérieur à la mise à jour des bases de l'application, vous ne pouvez télécharger que les paramètres standards gérés par Kaspersky Security Center dans les sections **Notifications** et **Exclusions de la zone d'action de la tâche**. Vous trouverez plus d'informations sur la configuration des paramètres dans ces sections dans le *Manuel de l'administrateur de Kaspersky Security Center.*

Attribution de l'état Analyse rapide à la tâche d'analyse à la demande

Kaspersky Security Center attribue par défaut l'état *Avertissement* au serveur si la tâche Analyse rapide est exécutée moins souvent que la valeur du paramètre de Kaspersky Security **Seuil de déclenchement de l'événement "L'analyse des secteurs critiques n'a plus eu lieu depuis longtemps"**.

► *Pour configurer l'analyse de tous les serveurs appartenant à un groupe d'administration, procédez comme suit :*

1. Créez une tâche de groupe d'analyse à la demande. Dans la fenêtre **Paramètres** de l'Assistant de création de tâches, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide de l'ordinateur**. Les paramètres que vous aurez définis (zone d'analyse et paramètres de protection) seront identiques pour tous les serveurs du groupe. Programmez l'exécution de la tâche.

   Vous pouvez cocher la case **Considérer l'exécution de la tâche comme une analyse rapide de l'ordinateur** aussi bien lors de la création de la tâche d'analyse à la demande pour un groupe d'ordinateurs ou pour une sélection d'ordinateurs ou plus tard, dans la fenêtre **Propriétés : <nom de la tâche>**.

2. À l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez le lancement planifié des tâches prédéfinies d'analyse à la demande sur les serveurs du groupe (cf. section "Configuration du lancement planifié des tâches locales prédéfinies" à la page 404).

Dès ce moment, le Serveur d'administration de Kaspersky Security Center évalue la protection du serveur protégé et vous informe à l'issue de la dernière exécution de la tâche avec l'état *Tâche d'analyse rapide* et non pas sur la base des résultats de la tâche prédéfinie Analyse rapide.

Vous pouvez attribuer l'état *Tâche d'analyse rapide* à des tâches de groupe d'analyse à la demande ou à des tâches pour des sélections d'ordinateurs.

La console de Kaspersky Security permet de voir si la tâche d'analyse à la demande est une tâche d'analyse rapide de l'ordinateur.

Dans la console de Kaspersky Security, la case **Considérer l'exécution de la tâche comme une analyse rapide** apparaît dans la propriété des tâches mais elle ne peut être modifiée.

Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center

► *Pour configurer les tâches locales dans la fenêtre **Paramètres de l'application**, procédez comme suit :*

1. Dans l'arborescence du Serveur d'administration Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

2. Dans le panneau des résultats, choisissez l'onglet **Ordinateurs**.

3. Ouvrez la fenêtre **Propriétés : <Nom de l'ordinateur>** d'une des méthodes suivantes :

   - Double-clic sur le nom du serveur à protéger.

   - Ouvrez le menu contextuel du nom du serveur protégé et sélectionnez l'option **Propriétés**.

4. Dans la fenêtre **Propriétés : <nom de l'ordinateur>**, au départ du groupe **Applications**, ouvrez la fenêtre **Paramètres de l'application** d'une des méthodes suivantes :

   - Double-cliquez sur le nom de l'application dans la liste des applications installées.
   - Sélectionnez le nom de l'application dans la liste, puis cliquez sur le bouton **Propriétés**.
   - Ouvrez le menu contextuel du nom de l'application dans la liste des applications installées, puis choisissez l'option **Propriétés**.

   Si l'application est soumise à une stratégie de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

5. Dans la liste des tâches, sélectionnez la tâche locale dont vous souhaitez configurer les paramètres.

6. Configurez les paramètres de la tâche sélectionnée en fonction de vos besoins.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center

Si un problème survient durant l'utilisation de Kaspersky Security (par exemple, Kaspersky Security s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez activer la création de fichiers de trace et de fichier dump des processus de Kaspersky Security et envoyer ces fichiers au Service d'assistance technique de Kaspersky Lab pour l'analyse.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour configurer les paramètres de diagnostic des échecs dans Kaspersky Security Center, procédez comme suit :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center**" à la page 436).

2. Ouvrez l'onglet **Diagnostic des échecs**, puis procédez comme suit :

   - Si vous souhaitez enregistrer les informations de débogage dans un fichier, cochez la case **Consigner les informations de débogage dans le fichier de traçage**.

     - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security enregistrera les fichiers de trace.
     - Configurez le niveau de détail des informations de débogage.

     La liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Security consigne dans le fichier de trace.

     Vous avez le choix parmi les niveaux de détail suivants :

     - **Evénements critiques** : Kaspersky Security enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.

- **Erreurs** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
- **Evénements importants** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.
- **Evénements d'information** : Kaspersky Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs, aux événements importants et aux événements d'information.
- **Toutes les informations de débogage** : Kaspersky Security enregistre dans le fichier de trace toutes les informations de débogage.

Le niveau de détail à définir pour résoudre le problème qui se pose est déterminé par l'expert du Support Technique.

Le niveau de détail sélectionné par défaut est **Toutes les informations de débogage**.

La liste déroulante est accessible si la case **Consigner les informations de débogage dans le fichier de traçage** est cochée.

- Taille maximale du fichier de trace
- Indiquez les modules à déboguer.

Liste des codes de sous-systèmes de Kaspersky Security dont les informations de débogage sont enregistrées dans le fichier de trace. Les codes des sous-systèmes doivent être séparés par une virgule et en respectant la distinction entre majuscules et minuscules (cf. tableau ci-dessous).

Tableau 65. Codes des sous-systèmes de Kaspersky Security

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Security dans MMC
ak_conn	Sous-système d'intégration à l'agent d'administration de Kaspersky Security Center
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Security.

wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance de Kaspersky Security.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de protection des fichiers en temps réel.
netapp	Sous-système de protection des stockages réseau.
qb	Sous-système de la quarantaine et des sauvegardés.
scandll	Module auxiliaire d'analyse antivirus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.
prague	Sous-système des fonctions de base.
scsrv	Sous-système d'affichage de messages sur les interceptions de scripts.
script	Intercepteur de scripts.
updater	Sous-système de mise à jour des bases et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant logiciel enfichable de Kaspersky Security (gui) et du plug-in d'administration de Kaspersky Security pour Kaspersky Security Center (ak_conn) sont appliqués après le redémarrage de ces composants. Les paramètres de traçage des sous-systèmes de prise en charge du protocole SNMP (snmp) sont appliqués après le redémarrage du service SNMP. Les paramètres de traçage du sous-système des compteurs de performances (perfcount) sont appliqués après le redémarrage de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Security sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Kaspersky Security enregistre par défaut les informations de débogage du fonctionnement de tous les sous-systèmes de Kaspersky Security (recommandé).

Le champ est accessible si la case **Consigner les informations de débogage dans le fichier de traçage** est cochée

- Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump sur incident**.
  - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security enregistrera le fichier dump.

3. Cliquez sur **OK**.

Les paramètres configurés de l'application seront appliqués sur le serveur protégé.

Configuration des paramètres de déblocage automatique de l'accès des ordinateurs au serveur dans le Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security dans Kaspersky Security Center est identique à la configuration locale des paramètres de ces composants dans la Console de Kaspersky Security. Les détails de la configuration des paramètres des tâches et des fonctions de l'application figurent dans les sections respectives du Manuel de l'administrateur de Kaspersky Security 10 for Windows Server.

Vous pouvez indiquer la durée au terme de laquelle les ordinateurs bloqués seront automatiquement débloqués. Ces ordinateurs auront alors la possibilité d'accéder aux fichiers réseau.

Par défaut, la durée de blocage de l'accès des ordinateurs aux fichiers réseau est égale à 30 minutes. Cette durée est décomptée à partir de la date de blocage de l'ordinateur.

► *Pour modifier la durée de blocage de l'accès des ordinateurs aux fichiers réseau, procédez comme suit :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center**" à la page 436).
2. Présentation de la tâche **Blocage de l'accès aux fichiers réseau**.

3. Indiquez le nombre de jours, d'heures ou de minutes à décompter à partir du moment du blocage de l'ordinateur et au terme desquels les ordinateurs bloqués sont autorisés à accéder fichiers réseau.

4. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Vous pouvez restaurer l'accès aux fichiers réseau sur des ordinateurs bloqués antérieurement ou purger la liste des ordinateurs douteux.

► *Pour restaurer l'accès pour des ordinateurs bloqués antérieurement ou pour supprimer les ordinateurs de la liste des ordinateurs douteux, procédez comme suit :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center**" à la page 436).

2. Présentation de la tâche **Blocage de l'accès aux fichiers réseau**.

3. Cliquez sur **Liste des ordinateurs douteux**.

4. Exécutez une des actions suivantes :

   - Dans la fenêtre **Liste des ordinateurs douteux** qui s'ouvre, sélectionnez les modules auxquels vous souhaitez restaurer l'accès, puis cliquez sur le bouton **Supprimer de la liste**.

   - Cliquez sur le bouton **Purger toute la liste** pour supprimer les ordinateurs de la liste des ordinateurs douteux ou pour rétablir l'accès pour tous les ordinateurs bloqués.

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

Les ordinateurs sélectionnés seront débloqués ou supprimés de la liste des ordinateurs douteux.

Compteurs de Kaspersky Security

Cette section contient des informations sur les compteurs de Kaspersky Security : compteurs de performances pour l'application Moniteur système et compteurs et interruptions SNMP.

Dans cette section

Compteurs de performance pour l'application Moniteur système

Cette section fournit des informations sur les compteurs de performance pour l'application Moniteur Système de Microsoft Windows enregistrés par Kaspersky Security pendant l'installation.

Dans cette section

Présentation des compteurs de performance de Kaspersky Security

Les composants à installer de Kaspersky Security reprennent par défaut le composant **Compteurs de performance**. Pendant l'installation, Kaspersky Security enregistrer ses compteurs de performance pour l'application Moniteur système de Microsoft Windows.

Grâce aux compteurs de Kaspersky Security, vous pouvez contrôler les performances de l'application durant l'exécution des tâches de protection en temps réel. Vous pouvez identifier les goulots d'étranglement en cas d'utilisation avec d'autres applications et les manques de ressources. Vous pouvez diagnostiquer une mauvaise configuration de Kaspersky Security et les échecs de fonctionnement.

Pour consulter les compteurs de performance de Kaspersky Security, ouvrez la console **Optimisation** dans l'élément **Administration** du panneau de configuration de Windows.

Les sections suivantes abordent la définition des compteurs, les intervalles de calcul des relevés recommandés, les valeurs limites et les recommandations pour la configuration de Kaspersky Security lorsque les compteurs dépassent ces valeurs.

Total de requêtes rejetées

Tableau 66. Total de requêtes rejetées

Nom	Total de requêtes rejetées (Total number of requests denied)
Description	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de Kaspersky Security, le calcul est réalisé depuis la dernière exécution de Kaspersky Security. L'application ignore les objets dont les requêtes de traitement sont rejetées par les processus de travail de Kaspersky Security.

Fonction	Ce compteur permet d'identifier : • La réduction de la qualité de la protection en temps réel en raison d'une charge complète des processus de Kaspersky Security ; • L'interruption de la protection en temps réel en raison d'un refus du gestionnaire d'intercepteurs de fichiers.
Valeur normale / limite	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés. Les situations suivantes sont envisageables en fonction du "comportement" du compteur : • le compteur indique certains processus rejetés durant une longue période : tous les processus de Kaspersky Security étaient totalement occupés, si bien que Kaspersky Security n'a pas pu analyser les objets. Pour éviter que des objets soient ignorés, augmentez le nombre de processus de Kaspersky Anti-Virus pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security **Quantité maximale de processus actifs** et **Nombre de processus pour la protection en temps réel**. • Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : le gestionnaire d'intercepteurs de fichiers ne fonctionne plus. Kaspersky Security n'analyse plus les objets. Redémarrez Kaspersky Security.

Total de requêtes ignorées

Tableau 67. Total de requêtes ignorées

Nom	Total de requêtes ignorées (Total number of requests skipped).
Description	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par Kaspersky Security mais qui n'ont pas donné d'événement sur la fin du traitement, le calcul est réalisé depuis la dernière exécution de l'application. Si la requête de traitement d'un objet reçue par un des processus de travail n'a pas envoyé d'événement sur la fin du traitement, le pilote transmet cette requête à un autre processus et la valeur du compteur **Total des requêtes ignorées** augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a accepté la requête de traitement (ils étaient occupés) ou n'a pas envoyé d'événement sur la fin du traitement, Kaspersky Security ignore cet objet et la valeur du compteur **Total des requêtes rejetées** augmente d'une unité.
Fonction	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
Valeur normale / limite	0 / 1.
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur diffère de zéro, cela signifie qu'un ou plusieurs flux du gestionnaire d'intercepteurs de fichiers sont gelés. La valeur du compteur correspond au nombre de flux gelés en ce moment. Si la vitesse d'analyse n'est pas satisfaisante, redémarrez Kaspersky Security afin de rétablir les flux gelés.

Nombre de requêtes non traitées en raison d'un manque de ressources système

Tableau 68. Nombre de requêtes non traitées en raison d'un manque de ressources système

Nom	Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)
Description	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Security. Kaspersky Security ignore les objets dont les requêtes de traitement ne sont pas traitées par le pilote d'interception de fichiers.
Fonction	Le compteur permet de repérer et de résoudre une éventuelle baisse de la qualité de la protection en temps réel provoquée par un manque de ressources.
Valeur normale / limite	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si le compteur affiche une valeur différente de zéro, les processus de travail de Kaspersky Security ont besoin de plus de mémoire vive pour traiter les requêtes. Il se peut que les processus actifs d'autres applications utilisent toute la mémoire vive disponible.

Nombre de requêtes envoyées pour traitement

Tableau 69. Nombre de requêtes envoyées pour traitement

Nom	Nombre de requêtes envoyées pour traitement (Number of requests sent to be processed)
Description	Nombre d'objets en attente de traitement par les processus actifs.
Fonction	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Security et le niveau général de l'activité de fichiers sur le serveur.
Valeur normale / limite	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur le serveur
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	non

Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Tableau 70. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers (Average number of file interception dispatcher streams).
Description	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (moyenne pour tous les processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une éventuelle détérioration de la qualité de la protection en temps réel en raison de la charge des processus de Kaspersky Security et d'y remédier.
Valeur normale / limite	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Chaque processus actif peut accepter un maximum de 60 flux du gestionnaire d'intercepteurs de fichiers. Si la valeur du compteur approche de 60, il se peut qu'aucun des processus actifs ne puisse accepter une nouvelle requête de traitement du pilote d'intercepteurs de fichiers et Kaspersky Security ignorera l'objet. Augmentez le nombre de processus de Kaspersky Security pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security **Quantité maximale de processus actifs** et **Nombre de processus de protection en temps réel**.

Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Tableau 71. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers (Maximum number of file interception dispatcher streams)
Description	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (nombre le plus élevé de processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une réduction des performances en raison d'une répartition inégale de la charge dans les processus actifs exécutés et d'y remédier
Valeur normale / limite	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur de ce compteur dépasse en permanence et de beaucoup la valeur du compte **Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers**, Kaspersky Security répartit de manière inégale la charge sur les processus exécutés. Redémarrez Kaspersky Security.

Nombre d'éléments dans la file d'attente des objets infectés

Tableau 72. Nombre d'éléments dans la file d'attente des objets infectés

Nom	Nombre d'éléments dans la file d'attente des objets infectés et autres objets détectés (Number of items in the infected object queue).
Description	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment.
Fonction	Le compteur permet d'identifier les situations suivantes : • l'interruption de la protection en temps réel en raison d'un éventuel refus du gestionnaire d'intercepteurs de fichiers ; • la surcharge du processus suite à une répartition inégale du temps de processus entre Kaspersky Security et les autres applications exécutées ; • les épidémies de virus.
Valeur normale / limite	La valeur du compteur peut être différente de zéro tant que Kaspersky Security traite les objets probablement infectés ou infectés découverts mais elle revient sur zéro juste après le traitement / La valeur du compteur est différente de zéro pendant une longue période.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur n'est pas égale à zéro pendant une longue période : • Kaspersky Security ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Redémarrez Kaspersky Security. • Manque de temps de processus pour le traitement des objets ; Accordez à Kaspersky Security plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur.

	• Une épidémie de virus s'est déclenchée. L'émergence d'une épidémie de virus est également indiquée par le nombre élevé d'objets infectés ou probablement infectés découverts dans la tâche **Protection des fichiers en temps réel**. Vous pouvez consulter les informations relatives au nombre d'objets découverts dans les statistiques de la tâche (cf. page 127) ou dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security dans les journaux d'exécution des tâches » à la page 310).

Nombre d'objets traités par seconde

Tableau 73. Nombre d'objets traités par seconde

Nom	Nombre d'objets traités par seconde (Number of objects processed per second)
Description	Nombre d'objets traités par unité de temps pendant laquelle ces objets ont été traités ; le décompte s'opère sur des intervalles de temps égaux
Fonction	Ce compteur affiche la vitesse de traitement des objets ; il permet d'identifier une baisse des performances du serveur en raison d'un manque de temps de processus actif pour les processus de Kaspersky Security ou d'un échec de Kaspersky Security et d'y remédier.
Valeur normale / limite	Varie / non.
Intervalle de calcul des relevés recommandé	Une minute

Recommandation pour la configuration si la valeur dépasse la valeur limite	Les valeurs du compteur dépendent des paramètres de Kaspersky Security et de la charge des processus des autres applications sur le serveur. Observez le niveau moyen du compteur au cours d'une longue période. Si le niveau du compteur a diminué, c'est peut-être à cause d'une des situations suivantes : • Les processus de travail de Kaspersky Security ne disposent pas des ressources de processus suffisantes pour traiter les objets. Accordez à Kaspersky Security plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur. • Un échec s'est produit dans le fonctionnement de Kaspersky Security (plusieurs flux sont gelés). Redémarrez Kaspersky Security.

Compteurs et interruptions SNMP de Kaspersky Security

Cette section contient des informations sur les interruptions SNMP de Kaspersky Security

Dans cette section

A propos des compteurs et interruptions SNMP de Kaspersky Security

Si vous avez inclus le composant **Compteurs et pièges SNMP** dans les composants de Kaspersky Security à installer, vous pouvez consulter les compteurs et les pièges de Kaspersky Security selon le protocole Simple Network Management Protocol (SNMP).

Pour consulter les compteurs et les pièges de Kaspersky Security depuis l'ordinateur-poste de travail de l'administrateur, lancez sur le serveur protégé le service SNMP (SNMP Service) et le service de pièges SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

Compteurs SNMP de Kaspersky Security

Cette section propose un tableau contenant la description des paramètres des compteurs SNMP de Kaspersky Security.

Dans cette section

Compteurs de performance

Tableau 74. Compteurs de performance

Compteur	Description
currentRequestsAmount	Nombre de requêtes envoyées pour traitement (cf. page 448)
currentInfectedQueueLength	Nombre d'éléments dans la file d'attente des objets infectés et autres objets détectés (cf. page 451)
currentObjectProcessingRate	Nombre d'objets traités par seconde (cf. page 452)
currentWorkProcessesNumber	Nombre de processus de travail de Kaspersky Security en ce moment

Compteurs généraux

Tableau 75. Compteurs généraux

Compteur	Description
currentApplicationUptime	Durée de fonctionnement de Kaspersky Security depuis sa dernière exécution (en centièmes de secondes)
currentFileMonitorTaskStatus	Etat de la tâche Protection des fichiers en temps réel : **on** – en exécution ; **off** – arrêtée ou suspendue
currentScriptCheckerTaskStatus	Etat de la tâche Analyse des scripts : **on** – en exécution; **off** – arrêtée ou suspendue
lastCriticalAreasScanAge	Période écoulée depuis la dernière analyse des zones critiques du serveur (intervalle de temps en secondes entre la date de fin de la tâche portant le statut *Tâche d'analyse des zones critiques* et le moment actuel)
licenseExpirationDate	Date de fin de validité de la licence. Si des clés active et additionnelle ou des codes d'activation ont été ajoutés, la date affichée est la date d'échéance de la licence associée à la clé complémentaire ou au code d'activation.

Compteur de mise à jour

Tableau 76. Compteur de mises à jour

Compteur	Description
avBasesAge	"Age" des bases (intervalle de temps en centièmes de seconde entre la date de création des dernières mises à jour installées et l'heure actuelle).

Compteurs de protection en temps réel

Tableau 77. Compteurs de protection en temps réel

Compteur	Description
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalInfectedObjectsFound	Nombre d'objets infectés découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalSuspiciousObjectsFound	Nombre d'objets probablement infectés découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalVirusesFound	Nombre d'objets détectés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsQuarantined	Nombre total d'objets infectés ou probablement infectés que Kaspersky Security a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotQuarantined	Nombre total d'objets infectés ou probablement infectés que Kaspersky Security a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsDisinfected	Nombre total d'objets infectés réparés par Kaspersky Security ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

Compteur	Description
totalObjectsNotDisinfected	Nombre total d'objets infectés ou suspects que Kaspersky Security a tenté de réparer en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsDeleted	Nombre total d'objets infectés ou probablement infectés que Kaspersky Security a supprimé ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDeleted	Nombre total d'objets infectés ou probablement infectés que Kaspersky Security a dû supprimer ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsBackedUp	Nombre total d'objets infectés placés dans la sauvegarde par Kaspersky Security ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotBackedUp	Nombre total d'objets infectés ou suspects que Kaspersky Security a tenté de placer en vain dans la sauvegarde ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

Compteurs de quarantaine

Tableau 78. Compteurs de quarantaine

Compteur	Description
totalObjects	Nombre d'objets présents actuellement en quarantaine
totalSuspiciousObjects	Nombre d'objets probablement infectés présents actuellement en quarantaine
currentStorageSize	Volume de données en quarantaine (Mo)

Compteurs de sauvegarde

Tableau 79. Compteurs de sauvegarde

Compteur	Description
currentBackupStorageSize	Volume de données en sauvegarde (Mo)

Compteurs d'analyse des scripts

Tableau 80. Compteurs d'analyse des scripts

Compteur	Description
totalScriptsProcessed	Total de scripts analysés
totalInfectedIDangerousScriptsFound	Total des scripts suspects découverts.
totalSuspiciousScriptsFound	Nombre total des scripts potentiellement dangereux découverts.
totalScriptsBlocked	Total des scripts dont l'accès a été bloqué

Interruptions SNMP

Les paramètres des pièges SNMP de Kaspersky Security sont décrits dans le tableau ci-dessous.

Tableau 81. Interruptions SNMP de Kaspersky Security

Piège	Description	Paramètres
eventThreatDetected	Un objet a été détectée.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

Piège	Description	Paramètres
eventBackupStorageSizeExceeds	Dépassement de la taille maximale de la sauvegarde. Le volume total de données de la sauvegarde dépasse la valeur du paramètre **Taille maximale de sauvegarde (Mo)**. Kaspersky Security continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Le seuil d'espace libre pour la sauvegarde est atteint. La quantité d'espace disponible dans la sauvegarde, définie par le paramètre **Seuil d'espace disponible**, est revenue à la valeur indiquée. Kaspersky Security continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Dépassement de la taille maximale de la quarantaine. Le volume total de données de la quarantaine dépasse la valeur du paramètre **Taille maximale de la quarantaine**. Kaspersky Security continue à placer les objets probablement infectés en quarantaine.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Le seuil d'espace libre pour la quarantaine est atteint. La quantité d'espace libre dans la quarantaine, définie par le paramètre **Seuil d'espace libre de la quarantaine**, est revenue à la valeur indiquée. Kaspersky Security continue à placer les objets probablement infectés en quarantaine.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Erreur de placement de l'objet en quarantaine.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Erreur de conservation d'une copie de l'objet en sauvegarde.	eventSeverity eventDateAndTime

Piège	Description	Paramètres
		eventSource objectName userName computerName storageObjectNotAddedEvent Reason
eventQuarantineInternalError	Erreur de quarantaine.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Erreur de sauvegarde.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Les bases de données ne sont plus à jour. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Les bases de données sont périmées. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Security est lancé.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security est arrêté.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerform ForALongTime	L'analyse des zones critiques n'a pas été réalisée depuis longtemps. Le nombre de jours écoulés depuis la dernière tâche dont le statut est *Tâche d'analyse rapide* est compté	eventSeverity eventDateAndTime eventSource days

Piège	Description	Paramètres
eventLicenseHasExpired	La durée de validité de la clé est écoulée.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	La clé de licence arrive bientôt à échéance. Le nombre de jour restant avant la fin de la validité de la licence est compté	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Erreur d'exécution de la tâche.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Erreur d'exécution de la tâche de mise à jour.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

Le tableau suivant décrit les paramètres des interruptions et leurs valeurs possibles.

Tableau 82. Valeurs des paramètres des pièges SNMP

Paramètre	Description et valeurs possibles
eventDateAndTime	Heure à laquelle l'événement est survenu
eventSeverity	Niveau d'importance de l'événement. Le paramètre peut prendre les valeurs suivantes : • critical (1) – critique, • warning (2) – avertissement, • info (3) – informations.
UserName	Nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté)
computerName	Nom de l'ordinateur (par exemple, nom de l'ordinateur

Paramètre	Description et valeurs possibles
	dont l'utilisateur a tenté d'accéder à un fichier infecté)
eventSource	Source de l'événement : composant fonctionnel pendant le fonctionnement duquel l'événement s'est produit. Le paramètre peut prendre les valeurs suivantes : • unknown (0) – composant fonctionnel non identifié ; • quarantine (1) – Quarantaine ; • backup (2) – Sauvegarde ; • reporting (3) – Journaux d'exécution des tâches ; • updates (4) – Mise à jour ; • realTimeProtection (5) –Protection des fichiers en temps réel ; • onDemandScanning (6) – Analyse à la demande ; • product (7) – événement lié non pas au fonctionnement d'un composant particulier mais au fonctionnement de Kaspersky Security dans son ensemble ; • systemAudit (8) – Journal d'audit système. • nasProtection (10) – Protection des stockages réseau.
eventReason	Cause de l'événement. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown (0) – cause indéterminée, • reasonInvalidSettings (1) – uniquement pour les événements de la sauvegarde et de la quarantaine, s'affiche si le dossier de sauvegarde ou de quarantaine est inaccessible (privilèges d'accès insuffisants ou le chemin de réseau indiqué dans les paramètres de la quarantaine est incorrect). Dans ce cas, Kaspersky Security utilisera le dossier de sauvegarde ou de quarantaine indiqué par défaut.

Paramètre	Description et valeurs possibles
objectName	Nom de l'objet (par exemple, nom du fichier contenant la menace)
threatName	Nom de l'objet détecté selon la classification de l'Encyclopédie des virus (http://www.securelist.fr). Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Security renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche (cf. section "Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security dans les journaux d'exécution des tâches" à la page 310).
detectType	Type d'objet détecté Le paramètre peut prendre les valeurs suivantes : • undefined (0) – indéterminé ; • virware – virus et vers de réseau traditionnels ; • trojware – chevaux de Troie ; • malware – autres programmes malveillants ; • adware – programmes publicitaires ; • pornware – logiciels pornographiques ; • riskware – logiciel avec licence pouvant être utilisé à des fins malveillantes pour endommager l'ordinateur ou les données.
detectCertainty	Coefficient de certitude de la découverte d'une menace. Le paramètre peut prendre les valeurs suivantes : • Suspicion (probablement infecté) : Kaspersky Security a détecté une correspondance partielle entre un morceau de code de l'objet et un morceau de code malveillant connu.

Paramètre	Description et valeurs possibles
	• Sure (infecté) : Kaspersky Security a détecté une équivalence parfaite entre une partie du code de l'objet et une partie d'un code malveillant connu.
days	Nombre de jours (par exemple, nombre de jours d'ici la fin de la validité de la licence).
errorCode	Code erreur.
knowledgeBaseId	Adresse de l'article dans la banque de solutions (par exemple, adresse de l'article décrivant une erreur quelconque).
taskName	Nom de la tâche.
updaterErrorEventReason	Cause de la non-application de la mise à jour. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown(0) – raison inconnue ; • reasonAccessDenied – accès interdit ; • reasonUrlsExhausted – fin de la liste des sources de mise à jour ; • reasonInvalidConfig – fichier de configuration incorrect ; • reasonInvalidSignature – signature invalide ; • reasonCantCreateFolder – création du répertoire impossible ; • reasonFileOperError – erreur de fichier ; • reasonDataCorrupted – objet corrompu ; • reasonConnectionReset – arrêt de la connexion ; • reasonTimeOut – délai d’attente pour la connexion expiré ; • reasonProxyAuthError – erreur d’authentification sur le serveur proxy ;

Paramètre	Description et valeurs possibles
	• reasonServerAuthError – erreur d'authentification sur le serveur ; • reasonHostNotFound – ordinateur introuvable ; • reasonServerBusy – serveur inaccessible ; • reasonConnectionError – erreur de connexion ; • reasonModuleNotFound – objet introuvable ; • reasonBlstCheckFailed(16) – erreur de vérification de la liste noire des clés. Il se peut qu'une actualisation ait été diffusée au moment de la mise à jour des bases. Essayez à nouveau de réaliser la mise à jour dans quelques minutes. Consultez la description détaillée de ces causes et les actions que l'administrateur peut entreprendre sur le site du Support Technique, dans la section **Si l'application a renvoyé une erreur** (http://support.kaspersky.com/fr/error).
storageObjectNotAddedEventReason	Cause du non placement de l'objet en sauvegarde ou en quarantaine. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown(0) – raison inconnue. • reasonStorageInternalError – erreur dans les bases de données ; restaurez Kaspersky Security. • reasonStorageReadOnly – la base de données est uniquement accessible en lecture ; restaurez Kaspersky Security. • reasonStorageIOError – erreur d'entrée/de sortie : a) Kaspersky Security est corrompu, restaurez-le ; b) le disque sur lequel les fichiers de Kaspersky Security sont sauvegardés est abîmé.

Paramètre	Description et valeurs possibles
	• reasonStorageCorrupted – le référentiel est abîmé ; restaurez Kaspersky Security. • reasonStorageFull – la base de données est remplie ; faites de la place sur le disque. • reasonStorageOpenError – échec de l'ouverture du fichier de base de données ; restaurez Kaspersky Security. • reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigences de Kaspersky Security. • reasonObjectNotFound – l'objet placé dans le référentiel n'existe pas sur le disque. • reasonObjectAccessError – privilèges insuffisants pour l'utilisation de Backup API : le compte utilisateur sous les privilèges duquel l'opération est réalisée ne jouit pas des privilèges Backup Operator. • reasonDiskOutOfSpace – espace insuffisant sur le disque.

Contacter le Support Technique

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

Dans cette section

Modes d'obtention du Support Technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des sources d'informations relatives à l'application, contactez le Support Technique. Les employés du Support Technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Le Support Technique n'est pas proposé aux utilisateurs d'une version d'essai.

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

Voici comment contacter les experts du Support Technique de Kaspersky Lab :

- appeler le Support Technique par téléphone (http://support.kaspersky.com/fr/b2b) ;
- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Support Technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un portail à disposition des entreprises qui utilisent les applications de Kaspersky Lab. Le portail Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le portail Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky Lab des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte Kaspersky CompanyAccount. À l'aide d'un seul compte, vous pouvez centraliser l'administration des demandes électroniques envoyées par les employés à Kaspersky Lab et gérer les droits d'accès de ces employés à Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Vous pouvez également obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

Support Technique par téléphone

Vous pouvez téléphoner aux experts du Support Technique dans la plupart des régions du monde. Vous pourrez trouver des informations sur les modes d'obtention de l'assistance technique dans votre région et les coordonnées du Support Technique sur le site Internet du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/b2b).

Avant de contacter le Support Technique, prenez connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Utilisation du fichier de trace et du script AVZ

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Security à envoyer au Support Technique de Kaspersky Lab. Les experts du Support technique de Kaspersky Lab peuvent également vous demander de créer un *fichier de traçage*. Le fichier de trace permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

L'analyse des données que vous envoyez permet aux experts du Support technique de Kaspersky Lab de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus exécutés, de rechercher la présence éventuelle de menaces sur l'ordinateur, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse de l'ordinateur.

Pour une assistance plus efficace en cas de questions sur l'utilisation de l'application, les experts du Support Technique peuvent vous demander (pour la réparation) de modifier les paramètres de l'application pendant les diagnostics. Pour ce faire, l'exécution des actions suivantes peut être requise :

- Activer la fonctionnalité de conservation des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules séparés de l'application, qui n'est pas disponibles via les outils standards de l'interface d'utilisateur.
- Modifier les paramètres de conservation et d'envoi des informations diagnostiques à conserver.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Glossaire

A

Agent d'administration

Composant de Kaspersky Security Center qui assure l'interaction entre le serveur d'administration et les applications de Kaspersky Lab installées sur un nœud particulier du réseau (poste de travail ou serveur). Ce module est unique pour toutes les applications Windows du portefeuille de la société.

Archive

Fichier qui contient un ou plusieurs fichiers qui peuvent être des archives.

Analyse heuristique

Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky Lab. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.

Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état *probablement infecté*.

Analyse sur la base de signatures

Technologie d'identification des menaces qui utilise les bases de Kaspersky Security contenant les descriptions des menaces connues et les méthodes pour les éliminer. La protection selon cette méthode offre le niveau minimum de sécurité. Conformément aux recommandations des spécialistes de Kaspersky Lab, cette méthode est toujours activée.

Analyseur heuristique

Module de Kaspersky Security qui exécute l'analyse heuristique.

B

Bases antivirus

Bases de données qui contiennent les informations relatives aux menaces informatiques connues de Kaspersky Anti-Virus au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les bases antivirus sont créées par les experts de Kaspersky Lab et actualisées toutes les heures

C

Clé active

Clé utilisée actuellement par l'application.

Clé additionnelle

Clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée actuellement.

F

Faux positif

Situation où un objet sain est considéré comme infecté par une application de Kaspersky Lab car son code évoque celui d'un virus.

Fichier infecté

Fichier contenant un code malveillant (pendant l'analyse du fichier, le code d'un programme connu présentant une menace a été détectée). Les experts de Kaspersky Lab vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

Fichier potentiellement infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'insertion et d'activation de code malveillant est nettement élevé pour ces fichiers.

Fichier probablement infecté

Fichier contenant soit le code modifié d'un virus connu, soit du code évoquant un virus, mais toujours inconnu de Kaspersky Lab. Les objets probablement infectés sont identifiés à l'aide de l'analyse heuristique.

G

Groupe d'administration

Sélection d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion au sein d'un ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

M

Masque de fichier

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- ***** : remplace zéro ou plus de caractère de n'importe quel type.
- **?** : remplace n'importe quel caractère.

Il faut prendre en considération que le nom est toujours séparé de l'extension du fichier par un point.

Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases et modules de l'application) obtenus via le serveur de mises à jour de Kaspersky Lab.

O

Objet OLE

Fichier associé ou intégré à un autre fichier. Les applications de Kaspersky Lab permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Microsoft Office Excel® dans un document Microsoft Office Word, ce tableau sera analysé en tant qu'objet OLE.

Objets exécutés au démarrage du système

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur l'ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

Paramètres de l'application

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

Protection contre le chiffrement

Activité malveillante des ransomwares qui vise à chiffrer les fichiers contenant les données de l'utilisateur. Les fichiers chiffrés ne peuvent être lus ou utilisés.

Q

Quarantaine

Dossier dans lequel l'application de Kaspersky Lab déplace les objets potentiellement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

R

Réparation des objets

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être réparés.

S

Sauvegarde

Dossier spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur réparation ou leur suppression.

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction de centralisation des informations relatives aux applications de Kaspersky Lab installées sur le réseau de la société et qui permet de les administrer.

T

Tâche

Fonctions réalisées par l'application de Kaspersky Lab qui se présentent sous la forme de tâches, par exemple : Protection des fichiers en temps réel, Analyse complète de l'ordinateur, Mise à jour des bases.

V

Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs de programme malveillant pour pénétrer dans un système ou une application et nuire son intégrité. Un grand nombre de vulnérabilités dans un système rend son fonctionnement peu fiable car les virus, installés dans le système, peuvent entraîner des erreurs du système d'exploitation ou des applications installées.

Informations sur le code tiers

Les informations sur le code tiers se trouvent dans le fichier legal_notices.txt, situé dans le dossier d'installation de l'application.

AO KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre diverses menaces dont les virus et autres programmes malveillants, le courrier indésirable (spam), les attaques de réseau et les attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie ("IDC Endpoint Tracker 2014").

Kaspersky Lab a été fondée en Russie en 1997. Kaspersky Lab est devenu un groupe international qui compte 34 bureaux dans 31 pays. L'entreprise emploie plus de 3000 experts qualifiés.

PRODUITS. Les applications de Kaspersky Lab protègent les ordinateurs des particuliers comme les réseaux informatiques des entreprises.

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection de l'information sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des équipements gérés par l'automatisation industrielle et la prévention des escroqueries financières. L’utilisation de ces solutions combinée à des outils d’administration centralisés permet de mettre en place et d’exploiter une protection efficace et automatisée de toute organisation, quelle que soit sa taille, contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands organismes d'évaluation. Elles sont compatibles avec les logiciels de nombreux fournisseurs et sont optimisées pour une exécution sur de nombreuses plateformes.

Les experts antivirus de Kaspersky Lab travaillent 24 heures sur 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 ces menaces aux bases utilisées par les applications de Kaspersky Lab.

TECHNOLOGIE. De nombreuses technologies, sans lesquelles les antivirus actuels ne seraient pas ce qu'ils sont, ont justement été mises au point par Kaspersky Lab. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme 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 ou ZyXEL. Beaucoup des innovations technologiques de l'entreprise sont brevetées.

RESULTATS. Au cours de ses années de lutte contre les menaces informatiques, Kaspersky Lab a remporté de nombreux prix. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais pour Kaspersky Lab, la plus grande récompense de toutes, c'est la fidélité des utilisateurs du monde entier. Les produits et les technologies de la société protègent plus de 400 millions de personnes. Kaspersky Lab compte plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.fr/
Laboratoire de virus :	http://newvirus.kaspersky.com/fr (pour l'analyse de fichiers ou de sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

Avis de marques déposées

Les marques déposées et les marques de service appartiennent à leur propriétaire.

Citrix, Citrix Presentation Server, XenApp et XenDesktop sont de marques de commerce de Citrix Systems, Inc. et/ou de ses filiales déposées aux Etats-Unis et dans d'autres pays.

Dell, Dell Compellent - sont de marques de commerce de Dell, Inc.

Celerra, EMC, Isilon, OneFS et VNX sont des marques de commerce ou des marques déposées d'EMC Corporation aux Etats-Unis et/ou dans d'autres pays.

Hitachi - est une marque de commerce de Hitachi, Ltd.

Domino et System Storage sont des marques de commerce d'International Business Machines Corporation déposées dans de nombreuses juridictions à travers le monde.

Excel, Hyper-V, JScript, Microsoft, Outlook, Windows, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Data ONTAP et NetApp sont des marques de commerce ou des marques déposées de NetApp, Inc. aux Etats-Unis et/ou dans d'autres pays.

Oracle – est une marque de commerce de Oracle Corporation et / ou ses filiales.

Index

A

B

C

D

E

G

I

J

K

L

M

P

Q

R

S

T

Z