KASPERSKY

Kaspersky Security for Windows Server

Manuel de l'administrateur

Version du produit : 10.1.1.746

Chers utilisateurs !

Merci d'avoir choisi Kaspersky Lab en tant que fournisseur de logiciels de sécurité. Nous espérons que ce document vous aidera à utiliser nos produits.

Date de révision du document : 02.10.2018

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

Sommaire

A propos du guide

Le manuel de l'administrateur de Kaspersky Security for Windows Server 10.1.1.746 (ci-après "Kaspersky Security 10.1.1 for Windows Server") Le Manuel de l'administrateur s'adresse aux spécialistes qui installent et administrent Kaspersky Security 10.1.1 for Windows Server sur tous les périphériques protégés ainsi qu'aux spécialistes chargés de l'assistance technique des organisations qui utilisent Kaspersky Security 10.1.1 for Windows Server.

Ce manuel contient des informations sur la configuration et l'utilisation de Kaspersky Security 10.1.1 for Windows Server.

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

Contenu du chapitre

Dans ce document

Le Manuel de l'administrateur de Kaspersky Security 10.1.1 for Windows Server contient les sections suivantes.

Sources d'informations sur Kaspersky Security 10.1.1 for Windows Server

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

Kaspersky Security 10.1.1 for Windows Server

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Security 10.1.1 for Windows Server. Elle reprend la configuration matérielle et logicielle requise pour l'application.

Installation et suppression de l'application

Cette section explique pas à pas la procédure d'installation et de désinstallation de Kaspersky Security 10.1.1 for Windows Server.

Interface de l'application

Cette section contient des informations sur les éléments de l'interface de Kaspersky Security 10.1.1 for Windows Server.

Licence de l'application

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

Lancement et arrêt de Kaspersky Security 10.1.1 for Windows Server

Cette section contient les informations sur le lancement et l'arrêt du plug-in de Kaspersky Security 10.1.1 for Windows Server (ci-après plug-in d'administration) et du Service Kaspersky Security.

A propos des autorisations d'accès pour les fonctions de Kaspersky Security 10.1.1 for Windows Server

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server et des services Windows® enregistrés par l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

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 10.1.1 for Windows Server sur plusieurs serveurs.

Création et configuration d'une tâche dans Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Security 10.1.1 for Windows Server, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center.

Protection en temps réel du serveur

Cette section présente les tâches de protection en temps réel : Protection des fichiers en temps réel, Monitoring des scripts, Utilisation du KSN et Protection contre le chiffrement, ainsi que la fonctionnalité Protection contre les exploits. La section contient également les instructions relatives à la configuration des tâches de protection en temps réel et à la gestion des paramètres de sécurité d'un serveur protégé.

Contrôle de l'activité locale

Cette section fournit des informations sur la fonction de Kaspersky Security 10.1.1 for Windows Server qui contrôle les lancements des applications et les connexions de périphériques externes via USB.

Contrôle de l'activité réseau

Cette section contient des informations sur les tâches Gestion du pare-feu et Protection contre le chiffrement.

Diagnostic du système

Cette section contient des informations sur la tâche de Moniteur d'intégrité des fichiers et les possibilités d'inspection du journal système du système d'exploitation.

Intégration aux systèmes tiers

Cette section décrit l'intégration de Kaspersky Security 10.1.1 for Windows Server aux fonctionnalités et technologies tierces.

Utilisation de Kaspersky Security 10.1.1 for Windows Server depuis la ligne de commande

Cette section décrit l'utilisation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande.

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.

Kaspersky Lab

Cette section contient des informations sur Kaspersky Lab.

Information 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 bleu 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 de 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.

Exemple de texte	Description de la convention
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".
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 10.1.1 for Windows Server

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.

Contenu du chapitre

Sources de données pour des consultations indépendantes

Vous pouvez utiliser les sources suivantes pour rechercher vous-même des informations sur Kaspersky Security 10.1.1 for Windows Server :

- Page de Kaspersky Security 10.1.1 for Windows Server sur le site Internet de Kaspersky Lab.
- Page de Kaspersky Security 10.1.1 for Windows Server sur le site du Support Technique (Base de connaissances).
- Manuels.

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab https://support.kaspersky.com/fr.

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

Page de Kaspersky Security 10.1.1 for Windows Server sur le site Internet de Kaspersky Lab

La page de Kaspersky Security 10.1.1 for Windows Server page https://www.kaspersky.fr/small-to-medium-business-security/windows-server-security fournit des informations générales sur l'application, sur ses fonctionnalités et ses particularités.

La page de Kaspersky Security 10.1.1 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 10.1.1 for Windows Server dans la base des connaissances

La base des connaissances est une rubrique du site du Support Technique.

La page de Kaspersky Security 10.1.1 for Windows Server dans la Base des connaissances https://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 10.1.1 for Windows Server mais également d'autres logiciels de Kaspersky Lab. Ces articles peuvent également contenir des actualités du Support technique.

Documentation de Kaspersky Security 10.1.1 for Windows Server

Le Manuel de l'administrateur de Kaspersky Security 10.1.1 for Windows Server reprend les informations relatives à l'installation, à la désinstallation, à la configuration des paramètres et à l'utilisation de l'application.

Discussion sur les logiciels de Kaspersky Lab sur le forum

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

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

Kaspersky Security 10.1.1 for Windows Server

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Security 10.1.1 for Windows Server. Elle reprend la configuration matérielle et logicielle requise pour l'application.

Contenu du chapitre

A propos de Kaspersky Security 10.1.1 for Windows Server

Kaspersky Security 10.1.1 for Windows Server protège les serveurs tournant sous les systèmes d'exploitation Microsoft® Windows et les périphériques de stockage NAS contre les virus et autres menaces informatiques qui se propagent via l'échange de fichiers. Kaspersky Security 10.1.1 for Windows Server a été développé pour les intranets des grandes et des moyennes entreprises. Les utilisateurs de Kaspersky Security 10.1.1 for Windows Server sont les administrateurs de réseau de l'organisation et les personnes chargées de la protection antivirus de ce réseau.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur les serveurs suivants :

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

Kaspersky Security 10.1.1 for Windows Server peut être géré de la manière suivante :

- via la console d'application installée sur le même serveur que Kaspersky Security 10.1.1 for Windows Server ou sur un autre ordinateur ;
- via la ligne de commande ;
- via la Console d'administration de Kaspersky Security Center.

Vous pouvez utiliser également l'application Kaspersky Security Center pour l'administration centralisée de la protection de nombreux serveurs doté chacun de Kaspersky Security 10.1.1 for Windows Server.

Il est possible de consulter les compteurs de performance de Kaspersky Security 10.1.1 for Windows Server pour l'application « Moniteur système » ainsi que les compteurs et les interruptions SNMP.

Composants et fonctions de Kaspersky Security 10.1.1 for Windows Server

L'application intègre les modules suivants :

- **Protection en temps réel**. Kaspersky Security 10.1.1 for Windows Server analyse les objets à l'accès. Kaspersky Security 10.1.1 for Windows Server analyse les objets suivants :
  - Les fichiers ;
  - Threads alternatives des systèmes de fichiers (flux NTFS) ;
  - L'enregistrement de démarrage principal et les secteurs d'amorçage des disques durs locaux ou amovibles.
- **Analyse à la demande**. Kaspersky Security 10.1.1 for Windows Server recherche une fois des virus et autres menaces informatique dans la zone indiquée. L'application analyse les fichiers, la mémoire et les objets de démarrage sur un serveur protégé.
- **Protection RPC des stockages réseau connectés** et **Protection ICAP des stockages réseau connectés**. Kaspersky Security 10.1.1 for Windows Server installé sur un serveur tournant sous un système d'exploitation Microsoft Windows protège les périphériques de stockage NAS contre les virus et autres menaces informatiques qui s'introduisent sur les serveurs via l'échange de fichiers.
- **Contrôle du lancement des applications**. Ce composant surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus.
- **Contrôle des périphériques**. Ce composant contrôle l'enregistrement et l'utilisation des périphériques de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger l'ordinateur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou des périphériques externes d'un autre type connectés par USB.
- **Protection contre le chiffrement** et **Protection contre le chiffrement pour NetApp**. Les composants protègent les dossiers partagés sur les serveurs et les périphériques de stockage NAS contre le chiffrement malveillant en bloquant les hôtes qui affichent une activité malveillante.
- **Monitoring des scripts**. Ce composant analyse le code des scripts créés à l'aide des technologies Microsoft Windows Script Technologies.
- **Protection du trafic**. Ce module intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informations connues ou autres sur le serveur protégé.
- **Gestion du pare-feu**. Ce composant permet d'administrer le pare-feu Windows : il permet de configurer les paramètres et les règles du pare-feu du système d'exploitation et interdit toute possibilité de configuration du pare-feu externe.
- **Moniteur d'intégrité des fichiers**. Kaspersky Security 10.1.1 for Windows Server détecte les modifications introduites dans les fichiers qui appartiennent aux zones de monitoring définies dans les paramètres de la tâche. Ces modifications peuvent signaler une violation de la sécurité sur le serveur protégé.
- **Inspection des journaux**. Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.

L'application peut remplir les fonctions suivantes :

- **Mise à jour des bases de l'application** et **Mise à jour des modules de l'application**. Kaspersky Security 10.1.1 for Windows Server télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky Lab, depuis le Serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.
- **Quarantaine**. Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Probablement infecté* dans la *Sauvegarde* avant de procéder à la désinfection 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 10.1.1 for Windows Server et à l'état de la protection antivirus du serveur.
- **Importation et exportation des paramètres**. Vous pouvez exporter les paramètres de Kaspersky Security 10.1.1 for Windows Server dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security 10.1.1 for Windows Server 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 du nœud dans l'arborescence des ressources fichier de l'ordinateur et enregistrer les valeurs définies comme 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 10.1.1 for Windows Server.
- **Gestion des autorisations d'accès pour les fonctions de Kaspersky Security 10.1.1 for Windows Server**. Vous pouvez configurer les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server et des services Windows que l'application enregistre pour des utilisateurs ou des groupes d'utilisateurs.
- **Enregistrement des événements de l'application dans le journal**. Kaspersky Security 10.1.1 for Windows Server enregistre les informations relatives aux paramètres de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution des tâches, aux événements associés avec Kaspersky Security 10.1.1 for Windows Server et aux informations requises pour diagnostiquer les erreurs dans Kaspersky Security 10.1.1 for Windows Server.
- **Stockage hiérarchique**. Kaspersky Security 10.1.1 for Windows Server peut fonctionner en mode 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 10.1.1 for Windows Server appliquera aux tâches d'analyse à la demande et de protection en temps réel.
- **Protection contre les exploits**. Vous pouvez protéger la mémoire des processus contre l'exploitation des vulnérabilités à l'aide de l'Agent de protection intégré dans ce processus.
- **Liste des ordinateurs bloqués**. Vous pouvez bloquer les hôtes distants qui essaient d'accéder aux dossiers partagés du serveur si une activité malveillante est détectée de leurs côté.

Nouveautés

Kaspersky Security for Windows Server offre les nouvelles fonctionnalités et améliorations suivantes :

- Prise en charge des nouvelles versions des systèmes d'exploitation Microsoft Windows.

  Mécanismes d'auto-défense reposant sur la technologie PPL : désormais, lorsque l'application est installée, elle enregistre automatiquement un pilote ELAM qui permet de démarrer le service Kaspersky Security (kavfs.exe) avec l'attribut Protected Process Light. Cela permet de renforcer l'auto-défense de l'application et d'empêcher un large éventail d'attaques.

  La fonctionnalité est disponible lorsque l'application est installée sur des serveurs tournant sous Microsoft Windows Server 2016 et plus.

- Prise en charge de la vérification et du traitement des fichiers cloud stockés dans Microsoft OneDrive.

- Fonctionnalités étendues de contrôle de la distribution des logiciels.

  Vous pouvez désormais indiquer le paquet de distribution qui peut transmettre l'attribut de confiance pour toute la chaîne de fichiers extraits. Cela permet d'augmenter la stabilité des processus d'installation des logiciels sur un serveur avec le contrôle du lancement des applications activé. En revanche, cela étend également la zone à risque d'attaque éventuelle en augmentant le nombre de lancements d'applications autorisées. Nous vous recommandons d'utiliser le paramètre pendant les déploiements de logiciels complexes, y compris quand le serveur doit être relancé pendant le processus de distribution des logiciels.

- Intégration avec des outils WMI (Windows Management Instrumentation).

  Désormais, lorsque l'application est installée, un espace-nom Kaspersky Security est automatiquement créé dans l'espace-nom racine WMI sur l'ordinateur local. Vous pouvez utiliser des solutions clientes qui prennent en charge les requêtes WMI pour obtenir des données sur l'application et ses composants.

- Prise en charge pour AMSI.

  L'utilisation de la technologie AMSI, intégrée dans Microsoft Windows, a permis l'amélioration du mécanisme d'interception des lancements de scripts sur le serveur : la stabilité de la tâche Monitoring des scripts est améliorée, l'influence de l'application sur l'environnement est réduite lors de l'interception des scripts, ceux-ci étant bloqués si des menaces sont détectées. Enfin, la zone d'action de la tâche est considérablement étendue. Désormais, le composant Monitoring des scripts fonctionne avec les scripts aux formats JS, VBS et PS1.

  La fonctionnalité est disponible lorsque le composant Monitoring des scripts est installé sur des serveurs tournant sous Microsoft Windows Server 2016 et plus.

- Le format d'affichage d'informations sur l'application et ses composants a été étendu avec la commande KAVSHELL OMSINFO : vous pouvez désormais obtenir des informations sur l'état de la tâche Contrôle du lancement des applications ainsi que des informations sur les mises à jour critiques de modules d'applications.

- Mécanismes améliorés de détection et d'isolation des virus actifs :
  - Désormais, l'application détecte les menaces sans fichiers - logiciel malveillant qui existe exclusivement dans la RAM du serveur et n'a aucune présence sur le disque dur.
  - Les mécanismes corrigés de traitement des virus actifs lorsqu'ils sont détectés : désormais, l'application arrête correctement les processus infectés.
  - Nouvelle capacité de configuration de la liste de processus à considérer comme critiques pour le système d'exploitation ; l'application n'arrête pas ces processus lorsqu'une infection active est détectée.

  Pour plus d'informations, cf. KB14306.
- Capacité de configuration de l'utilisation de l'attribut AccessTime pour les fichiers analysés par des tâches d'analyse à la demande.

  Par défaut, l'application restaure la dernière heure d'accès au fichier (attribut AccessTime) après l'analyse. Vous pouvez désormais utiliser le registre du système d'exploitation pour désactiver la restauration de l'attribut AccessTime si ce mécanisme génère des faux positifs pour les systèmes de sauvegarde.

  Pour plus d'informations, cf. KB14306.

Kit de distribution

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

- lancer l'assistant Installation de Kaspersky Security 10.1.1 for Windows Server ;
- lancer l'assistant Installation de la console de Kaspersky Security 10.1.1 for Windows Server ;
- lancer l'assistant d'installation du plug-in de Kaspersky Security 10.1.1 for Windows Server pour gérer l'application via Kaspersky Security Center ;
- lancer l'assistant d'installation du plug-in de Kaspersky Security 10.1.1 Microsoft Outlook® ;
- Lire le Manuel de l'administrateur ;
- lire le Manuel de l'utilisateur ;
- lire le Manuel d'implantation pour la Protection des stockages réseau ;
- consultez la page de Kaspersky Security 10.1.1 for Windows Server https://www.kaspersky.fr/small-to-medium-business-security/windows-server-security sur le site Internet de Kaspersky Lab ;
- visitez le site Internet du Support technique https://support.kaspersky.com/fr ;
- lire les informations relatives à la version actuelle de Kaspersky Security 10.1.1 for Windows Server.

Le dossier \client contient les fichiers d'installation de la console d'application (ensemble des composants "Outils d'administration de Kaspersky Security 10.1.1 for Windows Server").

Le dossier \server contient :

- les fichiers d'installation des composants de Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server via Kaspersky Security Center ;
- l'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 et de la Politique de confidentialité.

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

Le dossier \email_plugin contient le paquet d'installation du plug-in de Kaspersky Security 10.1.1 pour Microsoft Outlook.

Les fichiers du kit de distribution s'installent dans différents dossiers en fonction de leur rôle (cf. tableau ci-après).

Tableau 2. Fichiers u kit de distribution de Kaspersky Security 10.1.1 for Windows Server

Fichier	Fonction
autorun.inf	Fichier de démarrage automatique de l'Assistant d'installation de Kaspersky Security 10.1.1 for Windows Server pour l'installation de l'application depuis un support amovible.
ks4ws_admin_guide_fr.pdf	"Manuel de l'administrateur".
ks4ws_user_guide_fr.pdf	Manuel de l'utilisateur.
ks4ws_netstorage_guide_fr.pdf	Manuel d'implantation pour la Protection des stockages réseau.
release_notes.txt	Ce fichier contient les informations relatives à la version.
setup.exe	Fichier d'accueil de lancement de l'application (lance setup.hta).
\client\ks4wstools_x86(x64).msi	Paquet d'installation du service Windows Installer ; installe la console d'application sur le serveur protégé.
\client\setup.exe	Fichier de lancement de l'Assistant d'installation de l'ensemble des composants "Outils d'administration" (contient la console d'application) ; lance le fichier du paquet d'installation ks4wstools.msi selon les paramètres d'installation définis dans l'Assistant.
\server\bases.cab	Archive contenant les bases antivirus d'actualité au moment de l'édition de l'application.
\server\setup.exe	Fichier de lancement de l'assistant d'installation de Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server sur le serveur protégé.
\server\ks4ws.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center.

Fichier	Fonction
\server\klcfginst.exe	Programme d'installation du plug-in d'administration de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center. Installez le plug-in d'administration sur chacun des serveurs dotés de la Console d'administration Kaspersky Security Center si vous avez l'intention de l'utiliser pour administrer Kaspersky Security 10.1.1 for Windows Server.
\server\license.txt	Texte du Contrat de licence utilisateur final et de la Politique de confidentialité.
\server\migration.txt	Ce fichier décrit la migration à partir des précédentes versions de l'application.
\setup\setup.hta	Fichier pour le lancement de l'application d'accueil.
\email_plugin\ksmail_x86(x64).msi	Paquet d'installation de Windows Installer ; installe le plug-in de Kaspersky Security 10.1.1 for Windows Server Microsoft Outlook sur le serveur protégé.

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

Configurations logicielle et matérielle requises

Cette section décrit toutes les configurations logicielle et matérielle requises pour le serveur protégé et les périphériques de stockage NAS.

Configuration requise pour le serveur sur lequel Kaspersky Security 10.1.1 for Windows Server est installé

Avant d'installer Kaspersky Security 10.1.1 for Windows Server, il convient de supprimer du serveur tout autre logiciel antivirus qui serait installé.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sans supprimer la version de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition ou de Kaspersky Security 10 for Windows Server 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 objets en quarantaine et dans la sauvegarde : 400 Mo (recommandé) ;
  - pour l'enregistrement des journaux : 1 Go (recommandé).

Configuration minimale :

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

Configuration recommandée :

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

Configuration logicielle requise pour le serveur

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server requièrent Microsoft Windows Installer 3.1 sur le serveur.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur un serveur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server® 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Server 2008 Core / Standard / Enterprise / Datacenter SP1 ou suivant.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur un serveur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Small Business Server 2008 Standard / Premium ;
- Windows Server 2008 R2 Core / 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 ;
- Microsoft Small Business Server 2011 Essentials / Standard ;
- Microsoft Windows MultiPoint™ Server 2011 ;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server ;
- Windows Server 2012 Core Standard / Datacenter ;
- Windows Storage Server 2012 ;
- Windows Hyper-V Server 2012 ;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2012 R2 Core / Standard / Datacenter ;
- Windows Storage Server 2012 R2 ;
- Windows Hyper-V Server 2012 R2 ;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server ;
- Windows Server 2016 Core / Standard / Datacenter ;
- Windows Storage Server 2016 ;
- Windows Hyper-V Server 2016 ;
- Windows Server 2019 (toutes éditions).

Les systèmes d'exploitation suivants ne sont plus pris en charge par Microsoft Windows : Windows Server 2003 Standard/Enterprise/Datacenter SP2, Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 32 bits, 64 bits. Des limitations risquent d'affecter l'assistance technique des serveurs exécutant ces systèmes d'exploitation du côté de Kaspersky Lab.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur un des serveurs de terminaux suivants :

- Microsoft Remote Desktop Services sur la base de Windows Server 2008 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2008 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2016 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2019 ;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15 ;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

Kaspersky Security 10.1.1 for Windows Server est compatible avec les versions suivantes de Kaspersky Security Center :

- Kaspersky Security Center 10.4
- Kaspersky Security Center 10.5
- Kaspersky Security Center 11

Configuration requise pour le périphérique de stockage NAS protégé

Kaspersky Security 10.1.1 for Windows Server peut être utilisé pour la protection des périphériques de stockage NAS 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
- Dell™ 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 plus
- Dell 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
- 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 d'application 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 d'application 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 d'application sur l'ordinateur requièrent Microsoft Windows Installer 3.1.

Vous pouvez installer la Console de Kaspersky Security 10.1.1 sur un ordinateur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista® Editions ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8,1 ;
- Microsoft Windows 10.

Vous pouvez installer la Console de Kaspersky Security 10.1.1 sur un ordinateur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Small Business Server 2008 Standard / Premium ;
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter SP1 ou suivant ;

- Microsoft Small Business Server 2011 Essentials / Standard ;
- Microsoft Windows MultiPoint Server 2011 ;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server ;
- Windows Storage Server 2012 ;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Storage Server 2012 R2 ;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server ;
- Windows Storage Server 2016 ;
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8,1 ;
- Microsoft Windows 10.

Installation et suppression de l'application

Cette section explique pas à pas la procédure d'installation et de désinstallation de Kaspersky Security 10.1.1 for Windows Server.

Contenu du chapitre

Composants logiciels de Kaspersky Security 10.1.1 for Windows Server et leurs codes pour le service Windows Installer

Par défaut, les fichiers \server\ks4ws_x86(x64).msi installent tous les composants de Kaspersky Security 10.1.1 for Windows Server. Vous pouvez activer l'installation du composant lors de l'installation personnalisée de l'application.

Les fichiers \client\ks4wstools_x86(x64).msi installent tous les composants logiciels de la sélection "Outils d'administration".

Les rubriques suivantes indiquent les codes des composants logiciels de Kaspersky Security 10.1.1 for Windows Server pour le service Windows Installer. Vous pouvez utiliser ces codes dans le but de définir la liste des composants à installer lors de l'installation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande.

Dans cette section

Composants logiciels de Kaspersky Security 10.1.1 for Windows Server

Le tableau ci-après contient les codes et la description des composants logiciels de Kaspersky Security 10.1.1 for Windows Server.

Tableau 3. Description des composants logiciels de Kaspersky Security 10.1.1 for Windows Server

Composant	Code	Fonction exécutée
Fonction principale	Core	Ce composant contient une sélection de fonctions de base de l'application et garantit leur fonctionnement.
Contrôle du lancement des applications	AppCtrl	Ce composant surveille les tentatives de lancement des applications par les utilisateurs et autorise ou interdit le lancement des applications conformément aux règles du contrôle du lancement des applications indiquées. Le composant intervient dans la tâche Contrôle du lancement des applications.
Contrôle des périphériques	DevCtrl	Ce composant surveille les tentatives de connexion de périphérique de stockage de masse sur un serveur protégé et autorise ou non leur utilisation en fonction des règles de contrôle des périphériques. Le composant intervient dans la tâche Contrôle des périphériques.
Protection du trafic	WebGW	Ce composant traite le trafic Internet (y compris le trafic obtenu via les services de messagerie) et intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informatiques connues et autres sur le serveur protégé.

Composant	Code	Fonction exécutée
Protection antivirus	AVProtection	Ce composant garantit la protection antivirus et reprend les composants suivants : • Analyse à la demande ; • Protection des fichiers en temps réel.
Analyse à la demande	Ods	Ce composant installe les fichiers système de Kaspersky Security 10.1.1 for Windows Server et les tâches d'analyse à la demande (analyse des objets du serveur protégé exécutée à la demande). Si lors de l'installation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande vous désignez d'autres composants de Kaspersky Security 10.1.1 for Windows Server sans le composant Core, celui-ci sera installé automatiquement.
Protection des fichiers en temps réel	Oas	Ce composant réalise l'analyse antivirus des fichiers sur le serveur protégé lorsque ces fichiers sont sollicités. Le composant exécute la tâche Protection des fichiers en temps réel.
Utilisation de Kaspersky Security Network	Ksn	Ce module offre une protection sur la base des technologies cloud de Kaspersky Lab. Le composant exécute la tâche Utilisation du KSN (envoi de requêtes au Service Kaspersky Security Network et réception des conclusions de ce même Service Kaspersky Security Network).
Moniteur d'intégrité des fichiers	Fim	Ce composant permet de consigner les opérations réalisées sur les fichiers dans la zone de monitoring sélectionnée. Le composant intervient dans la tâche Moniteur d'intégrité des fichiers.
Protection contre les exploits	AntiExploit	Ce composant garantit l'administration des paramètres de la protection des processus dans la mémoire du serveur protégé.
Gestion du pare-feu	Pare-feu	Ce composant permet d'administrer le pare-feu Windows via l'interface utilisateur graphique de Kaspersky Security 10.1.1 for Windows Server. Le composant intervient dans la tâche Gestion du pare-feu.

Composant	Code	Fonction exécutée
Module d'intégration de l'Agent d'administration de Kaspersky Security Center	AKIntegration	Garantit la connexion entre Kaspersky Security 10.1.1 for Windows Server et l'Agent d'administration Kaspersky Security Center. Vous pouvez installer ce composant sur le serveur protégé si vous avez l'intention d'administrer l'application via Kaspersky Security Center.
Inspection des journaux	LogInspector	Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.
Protection RPC des stockages réseau connectés	RPCProt	Ce composant protège les périphériques de stockage NAS connectés via RPC (par exemple les périphériques de stockage NAS de NetApp) contre les virus et autres menaces informatiques qui se propagent dans le serveur via l'échange de fichiers.
Protection ICAP des stockages réseau connectés	ICAPProt	Ce composant protège les périphériques de stockage NAS connectés via ICAP (par exemple EMC Isilon) contre les virus et autres menaces informatiques qui se propagent dans le serveur via l'échange de fichiers.
Protection contre le chiffrement pour NetApp	AntiCryptorNAS	Ce composant protège les dossiers des périphériques de stockage NAS contre le chiffrement malveillant. En cas de détection d'un chiffrement malveillant, Kaspersky Security 10.1.1 for Windows Server interdit l'accès aux dossiers du périphérique de stockage NAS protégé.
Sélection de compteurs de performance de l'application "System Monitor"	PerfMonCounters	Le composant installe la sélection de compteurs de performance de l'application "System Monitor". Ces compteurs de performance permettent de mesurer les performances de Kaspersky Security 10.1.1 for Windows Server et de localiser les éventuels goulots d'étranglement lors de l'utilisation de Kaspersky Security 10.1.1 for Windows Server avec d'autres applications.
Prise en charge du protocole SNMP	SnmpSupport	Le composant publie les compteurs et les pièges de Kaspersky Security 10.1.1 for Windows Server via le service Simple Network Management Protocol (SNMP) de Microsoft Windows. Vous pouvez installer ce composant sur le serveur protégé uniquement si Microsoft SNMP est déjà installé.

Composant	Code	Fonction exécutée
Icône de Kaspersky Security 10.1.1 for Windows Server dans la zone de notification	TrayApp	Le composant affiche l'icône de Kaspersky Security 10.1.1 for Windows Server dans la zone de notification de la barre des tâches du serveur protégé. L'icône de Kaspersky Security 10.1.1 for Windows Server affiche l'état de la protection du serveur, permet d'ouvrir la Console de Kaspersky Security 10.1.1 for Windows Server dans Microsoft Management Console (si elle est installée) et la fenêtre A propos de l'application.
Utilitaire de la ligne de commande	Shell	Permet d'administrer Kaspersky Security 10.1.1 for Windows Server via la ligne de commande du serveur protégé.

Ensemble des "Outils d'administration" des composants logiciels

Le tableau suivant contient les codes et la description des composants logiciels de la sélection "Outils d'administration".

Tableau 4. Description des composants logiciels de la sélection "Outils d'administration"

Composant	Code	Fonctions du composant
Composant logiciel enfichable de Kaspersky Security 10.1.1 for Windows Server	MmcSnapin	Le composant installe le composant logiciel enfichable Microsoft Management Console pour l'administration via la Console de Kaspersky Security 10.1.1 for Windows Server. Si lors de l'installation de la sélection "Outils d'administration" via la ligne de commande vous désignez d'autres composants de la sélection sans le composant MmcSnapin, celui-ci sera installé automatiquement.
Aide	Help	Fichier chm de l'aide ; il est enregistré dans le dossier qui contient les fichiers des outils d'administration de Kaspersky Security 10.1.1 for Windows Server. Vous pouvez ouvrir le fichier d'aide via le menu **Démarrer** ou via la touche **F1** de la fenêtre ouverte de la console d'application.
Documentation	Help	Kaspersky Security 10.1.1 for Windows Server ajoute un raccourci à la ressource Internet Kaspersky Lab ou le Manuel d'implantation de la Protection des stockages réseau, le Manuel de l'administrateur et le Manuel de l'utilisateur sont disponibles au format PDF. Vous pouvez ouvrir tous les manuels via le menu **Démarrer**.

Modifications introduites dans le système après l'installation de Kaspersky Security 10.1.1 for Windows Server

Lors de l'installation de Kaspersky Security 10.1.1 for Windows Server et de la console d'application (sélection "Outils d'administration"), le service Windows Installer procède aux modifications suivantes sur le serveur protégé :

- création des dossiers de Kaspersky Security 10.1.1 for Windows Server sur le serveur protégé et sur le serveur sur lequel la console d'application est installée ;
- enregistrement des services de Kaspersky Security 10.1.1 for Windows Server ;
- création d'un groupe d'utilisateurs Kaspersky Security 10.1.1 for Windows Server ;
- enregistrement des clés de Kaspersky Security 10.1.1 for Windows Server dans la base de registres système.

Ces modifications sont décrites dans le tableau ci-dessous.

Dossier de Kaspersky Security 10.1.1 for Windows Server

Tableau 5. Dossier de Kaspersky Security 10.1.1 for Windows Server sur un serveur protégé

Dossier	Fichiers de Kaspersky Security 10.1.1 for Windows Server
Dossier d'installation par défaut de Kaspersky Security 10.1.1 for Windows Server : Dans la version 32 bits de Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ Dans la version 64 bits de Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Security for Windows Server\	Fichiers exécutable de Kaspersky Security 10.1.1 for Windows Server (dossier de destination défini pendant l'installation).
Dossier %Kaspersky Security for Windows Server%\mibs	Les fichiers Management Information Base (MIB) ; contiennent une description des compteurs et des pièges publiés par Kaspersky Security 10.1.1 for Windows Server selon le protocole SNMP.
Dossier %Kaspersky Security for Windows Server%\x64	Version 64 bits des fichiers exécutables de Kaspersky Security 10.1.1 for Windows Server (le dossier est créé uniquement en cas d'installation de Kaspersky Security 10.1.1 for Windows Server sur une version 64 bits de Microsoft Windows).

Dossier	Fichiers de Kaspersky Security 10.1.1 for Windows Server
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Security for Windows Server\10.1\Dskm\	Fichiers de service de Kaspersky Security 10.1.1 for Windows Server.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\	Fichiers contenant les paramètres des sources des mises à jour.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\Distribution\	Mises à jour des bases de données et des modules logiciels récupérés à l'aide de la tâche Copie des mises à jour (le dossier est créé à la première réception des mises à jour à l'aide de la tâche Copie des mises à jour).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\	Journaux d'exécution de la tâche et journal d'audit système.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Current\	Sélection des bases utilisées à l'heure actuelle.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Backup\	Copie de sauvegarde des bases ; écrasée à chaque mise à jour des bases de données.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Temp\	Fichiers temporaires créés lors de l'exécution des tâches de mise à jour.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\	Objets en quarantaine (dossier par défaut).

Dossier	Fichiers de Kaspersky Security 10.1.1 for Windows Server
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\	Objets dans la sauvegarde (dossier par défaut).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\	Objets restaurés de la sauvegarde ou de la quarantaine (dossier par défaut pour les objets restaurés).

Tableau 6. Dossiers créés lors de l'installation de la console d'application

Dossier	Fichiers de la console de Kaspersky Security 10.1.1 for Windows Server
Dossier d'installation par défaut de la Console de l'application : • Dans la version 32 bits de Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Outils d'administration de Kaspersky Security 10.1.1 for Windows Server\ • Dans la version 64 bits de Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Outils d'administration de Kaspersky Security 10.1.1 for Windows Server\	Fichiers de la sélection "Outils d'administration" (dossier de destination indiqué lors de l'installation de la console de Kaspersky Security 10.1.1 for Windows Server).

Services de Kaspersky Security 10.1.1 for Windows Server

Les services de Kaspersky Security 10.1.1 for Windows Server sont lancés sous le compte utilisateur Système local (SYSTEM).

Tableau 7. Services de Kaspersky Security 10.1.1 for Windows Server

Service	Fonction
Service Kaspersky Security (KAVFS)	Service essentiel de Kaspersky Security 10.1.1 for Windows Server qui gère les tâches et les flux de travail de Kaspersky Security 10.1.1 for Windows Server.
Service Kaspersky Security Management Service (KAVFSGT)	Ce service est destiné à l'administration de l'application Kaspersky Security 10.1.1 for Windows Server via la console d'application.
Service Protection contre les exploits de Kaspersky Security (KAVFSSLP)	Service jouant le rôle d'intermédiaire pour transmettre les paramètres de protection aux agents externes de protection, ainsi que pour recevoir les données sur les événements de sécurité.
Kaspersky Security Script Checker (KAVFSSCS)	Le service est démarré avec la tâche Monitoring des script et permet de contrôler l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies.

Groupes Kaspersky Security 10.1.1 for Windows Server

Groupes Kaspersky Security 10.1.1 for Windows Server

Tableau 8. Groupes Kaspersky Security 10.1.1 for Windows Server

Groupe	Fonction
KAVWSEE Administrators	Groupe sur le serveur protégé dont les utilisateurs ont un accès complet au service Kaspersky Security Management ainsi qu'un accès total à toutes les fonctions de Kaspersky Security 10.1.1 for Windows Server.

Clés de la base de registres système

Tableau 9. Clés de la base de registres système

Clé	Fonction
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Propriétés du Service Kaspersky Security 10.1.1 for Windows Server.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Paramètres du journal des événements de Kaspersky Security 10.1.1 for Windows Server (journal des événements de Kaspersky).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Propriétés du service d'administration de Kaspersky Security 10.1.1 for Windows Server.
Dans la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] Dans la version 64 bits de Microsoft Windows : [[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Paramètres des compteurs de performance.
Dans la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\SnmpAgent] Dans la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]	Paramètres du composant « prise en charge du protocole SNMP ».

Dans la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump] Dans la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump]	Paramètres d'écriture du fichier dump.
Dans la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1.1\Trace] Dans la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Trace]	Paramètres du fichier de trace.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment]	Configuration des tâches et des fonctions de l'application.

Processus de Kaspersky Security 10.1.1 for Windows Server

Kaspersky Security 10.1.1 for Windows Server lance les processus décrits dans le tableau ci-dessous.

Tableau 10. Processus de Kaspersky Security 10.1.1 for Windows Server

Nom du fichier	Fonction
kavfswp.exe	Flux de travail de Kaspersky Security 10.1.1 for Windows Server
kavtray.exe	Processus de l'icône dans la barre d'état système
kavshell.exe	Processus de l'utilitaire de la ligne de commande
kavfsrcn.exe	Processus d'administration à distance Kaspersky Security 10.1.1 for Windows Server
kavfs.exe	Processus du Service Kaspersky Security
kavfsgt.exe	Processus du Service Kaspersky Security Management
kavfswh.exe	Processus du service Protection contre les exploits de Kaspersky Security Management
kavfsscs.exe	Service Kaspersky Security Script Checker

Paramètres d'installation et de désinstallation et options de ligne de commande correspondantes pour le service Windows Installer

Les tableaux suivants offrent une description des paramètres d'installation et de désinstallation de Kaspersky Security 10.1.1 for Windows Server ainsi que leur valeur par défaut. Ils indiquent également les arguments pour modifier les valeurs des paramètres d'installation et leurs valeurs possibles. Vous pouvez utiliser ces arguments avec les arguments standard de l'instruction msiexec du service Windows Installer lors de l'installation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande.

Tableau 11. Paramètres d'installation et options de ligne de commande dans Windows Installer

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Acceptation des termes du Contrat de licence utilisateur final	EULA=<valeur> 0 : vous n'acceptez pas les termes du Contrat de licence utilisateur final. 1 : vous acceptez les termes du Contrat de licence utilisateur final.	0	Vous devez accepter les termes du Contrat de licence utilisateur final pour pouvoir installer Kaspersky Security 10.1.1 for Windows Server.
Acceptation des termes de la Politique de confidentialité	PRIVACYPOLICY=<valeur> 0 : vous n'acceptez pas les termes de la Politique de confidentialité. 1 : vous acceptez les termes de la Politique de confidentialité.	0	Vous devez accepter les termes de la Politique de confidentialité pour installer Kaspersky Security 10.1.1 for Windows Server.
Dossier de destination	INSTALLDIR=<chemin d'accès complet au répertoire>	Kaspersky Security 10.1.1 for Windows Server : %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Outils d'administration : %ProgramFiles%\Kaspersky Lab\Outils d'administration de Kaspersky Security for Windows Server Dans la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%.	Dossier dans lequel les fichiers de Kaspersky Security 10.1.1 for Windows Server vont être enregistrés lors de son installation. Vous pouvez indiquer un autre dossier.

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Lancement de la Protection des fichiers en temps réel au démarrage de Kaspersky Security 10.1.1 for Windows Server (**Activer la protection en temps réel après l'installation de l'application**)	RUNRTP=<valeur> 1 : démarrer ; 0 : ne pas démarrer.	1	Activez ce paramètre pour lancer la Protection des fichiers en temps réel et le Monitoring des scripts au lancement de Kaspersky Security 10.1.1 for Windows Server (recommandé).
Exclusions de l'analyse, recommandées par Microsoft Corporation (**Ajouter les exclusions recommandées par Microsoft**)	ADDMSEXCLUSION=<valeur> 1 : exclure ; 0 : ne pas exclure.	1	Dans la tâche Protection des fichiers en temps réel sont exclus de la zone de protection les objets du serveur dont l'exclusion est recommandée par Microsoft Corporation. Certains programmes sur le serveur peuvent devenir instables lorsque les logiciels antivirus interceptent ou modifient les fichiers auxquels ces applications font appel. Ainsi, Microsoft Corporation inclus certains logiciels chargés du contrôle des domaines dans cette catégorie.

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Objets exclus de la zone d'analyse selon les recommandations de Kaspersky Lab (**Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions**)	ADDKLEXCLUSION=<valeur> 1 : exclure ; 0 : ne pas exclure.	1	Dans la tâche Protection des fichiers en temps réel, les objets du serveur dont l'exclusion est recommandée par Kaspersky Lab sont exclus de la zone de protection.
Autoriser les connexions à distance à la console d'application.	ALLOWREMOTECON= <valeur> 1 : autoriser ; 0 : interdire.	0	Par défaut, la connexion à distance à la console d'application installée sur le serveur protégé n'est pas autorisée. Vous pouvez autoriser cette connexion pendant l'installation. Kaspersky Security 10.1.1 for Windows Server créé les règles d'autorisation pour le processus kavfsgt.exe sur le protocole TCP pour tous les ports.

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Chemin d'accès au fichier clé (**Clé**)	LICENSEKEYPATH=<nom_fichier_clé>	Dossier \server dans le kit de distribution	Par défaut, le programme d'installation tente de trouver le fichier avec l'extension .key dans le dossier \server du kit de distribution. Si le dossier \server contient plusieurs fichiers clé, le programme d'installation choisit le fichier clé qui possède la date de fin de validité la plus lointaine. Vous pouvez enregistrer au préalable le fichier clé dans le répertoire \server ou indiquer un autre chemin d'accès au fichier clé à l'aide du paramètre **Ajouter une clé**. Vous pouvez ajouter une clé après l'installation de Kaspersky Security 10.1.1 for Windows Server à l'aide de l'outil d'administration que vous aurez choisi, par exemple via la console d'application. Si vous n'ajoutez pas la clé de l'application lors de son installation, Kaspersky Security 10.1.1 for Windows Server ne fonctionnera pas.

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Chemin d'accès au fichier de configuration	CONFIGPATH=<nom_fichier_configuration>	Désactivé	Kaspersky Security 10.1.1 for Windows Server importe les paramètres depuis le fichier de configuration indiqué et créé dans l'application. Kaspersky Security 10.1.1 for Windows Server n'importe pas les mots de passe contenus dans le fichier de configuration tels que les mots de passe des comptes utilisateur de lancement de tâches ou les mots de passe de connexion au serveur proxy. Après l'importation des paramètres, vous devrez saisir tous les mots de passe manuellement. Si vous ne désignez pas le fichier de configuration, Kaspersky Security fonctionnera après l'installation selon les paramètres par défaut.

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Autorisation des connexions de réseau pour la Console de Kaspersky Security	ADDWFEXCLUSION=<valeur> **1** : autoriser ; **0** : interdire.	0	Cette option permet d'installer Kaspersky Security 10.1.1 for Windows Server sur un autre serveur. Grâce à la console de Kaspersky Security 10.1.1 for Windows Server installée sur un autre ordinateur, vous pourrez administrer la protection d'un serveur à distance. Le port TCP 135 est ouvert dans le pare-feu de Microsoft Windows, les connexions réseau sont autorisées pour le fichier exécutable du processus d'administration à distance de Kaspersky Security 10.1.1 for Windows Server kavfsrcn.exe et l'accès aux applications DCOM est ouvert. Une fois l'installation terminée, ajoutez les utilisateurs au groupe KAVWSEE Administrators pour leur permettre d'administrer l'application à distance, si le serveur tourne sous Microsoft Windows Server 2008, et autorisez les connexions au Service Kaspersky Security Management (kavfsgt.exe) sur le serveur. Vous pouvez lire des informations complémentaires

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut	Description
Désactivation de la recherche d'une application non compatible	SKIPINCOMPATIBLESW = <valeur> 0 : la recherche d'applications non compatibles a lieu ; 1 : la recherche d'applications non compatibles n'a pas lieu.	0	Ce paramètre permet d'activer ou de désactiver la recherche en arrière-plan d'une application incompatible lors de l'installation de l'application sur un périphérique. Quelle que soit la valeur de ce paramètre, Kaspersky Security 10.1.1 for Windows Server signale toujours, lors de l'installation, la présence d'autres versions de l'application installée sur ce même appareil.

Tableau 12. Paramètres de désinstallation et options de ligne de commande dans Windows Installer

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut
Restauration du contenu de la quarantaine	RESTOREQTN =<valeur> **0** : supprimer le contenu de la quarantaine ; **1** : restaurer le contenu de la quarantaine dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \Quarantine.	0 – Supprimer
Restauration du contenu de la Sauvegarde	RESTOREBCK =<valeur> **0** : supprimer le contenu de la Sauvegarde ; **1** : restaurer le contenu de la Sauvegarde dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \Backup.	0 – Supprimer

Paramètre	Options de la ligne de commande du programme d'installation Windows Installer et leurs valeurs possibles	Valeur par défaut
Saisie du mot de passe en cours pour la confirmation de l'opération de suppression (lorsque la fonction d'application du mot de passe est active)	UNLOCK_PASSWORD = <mot de passe indiqué>	Désactivé
Dossier pour la restauration des objets	RESTOREPATH=<chemin d'accès complet au dossier> Les objets restaurés seront enregistrés dans le dossier spécifié.	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1.1\Restored

Journal d'installation et de désinstallation de Kaspersky Security 10.1.1 for Windows Server

Si vous installez ou désinstallez Kaspersky Security 10.1.1 for Windows Server à l'aide de l'Assistant d'installation (Désinstallation), le service Windows Installer crée le journal d'installation (de désinstallation). Le fichier journal ks4ws_install_<uid>.log (où <uid> est un identifiant unique à 8 caractères) est enregistré dans le répertoire %temp% de l'utilisateur sous les privilèges duquel le fichier setup.exe a été lancé.

Si vous exécutez l'option **Modify or Remove** de la console d'application ou Kaspersky Security 10.1.1 for Windows Server à partir du menu **Démarrer**, le journal ks4ws_10.1.1_maintenance.log est automatiquement créé dans le dossier %temp%.

Si vous installez ou désinstallez Kaspersky Security 10.1.1 for Windows Server via la ligne de commande, le journal d'installation n'est pas créé par défaut.

► *Pour installer Kaspersky Security 10.1.1 for Windows Server avec le fichier journal créé sur le disque C:\, exécutez l'instruction suivante :*

- msiexec /i ks4ws_x86.msi /l*v ks4ws /qn EULA=1 PRIVACYPOLICY=1
- msiexec /i ks4ws_x64.msi /l*v ks4ws /qn EULA=1 PRIVACYPOLICY=1

Planification de l'installation

Cette section décrit les outils d'administration de Kaspersky Security 10.1.1 for Windows Server, les particularités de l'installation et de la suppression de Kaspersky Security 10.1.1 for Windows Server à l'aide d'un assistant (cf. section "Installation et suppression de l'application à l'aide de l'assistant" à la page 50), via la ligne de commande (cf. section "Installation et suppression de l'application via la ligne de commande" à la page 64), via Kaspersky Security Center (cf. section "Installation et suppression de l'application via Kaspersky Security Center" à la page 70) et via une stratégie de groupe Active Directory® (cf. section "Installation et suppression via les stratégies de groupe Active Directory" à la page 76).

Avant de lancer l'installation de Kaspersky Security 10.1.1 for Windows Server, planifiez les principales étapes de celle-ci.

1. Définissez les outils d'administration que vous utiliserez pour administrer et configurer Kaspersky Security 10.1.1 for Windows Server.
2. Déterminez les composants d'application requis à installer (cf. section "Composants logiciels de Kaspersky Security 10.1.1 for Windows Server et leurs code pour le service Windows Installer" à la page 30).
3. Sélectionnez le mode d'installation.

Dans cette section

Sélection des outils d'administration

Définissez les outils d'administration que vous utiliserez pour la configuration des paramètres de Kaspersky Security 10.1.1 for Windows Server et son administration. En guise d'outils d'administration de Kaspersky Security 10.1.1 for Windows Server, vous pouvez choisir la console d'application, l'utilitaire de ligne de commande ou la console d'administration de Kaspersky Security Center.

Console de Kaspersky Security 10.1.1 for Windows Server

La console de Kaspersky Security 10.1.1 for Windows Server est un composant logiciel enfichable isolé qui est ajouté à la console Microsoft Management Console. Il est possible d'administrer Kaspersky Security 10.1.1 for Windows Server via la console d'application installée sur le serveur protégé ou sur tout autre ordinateur du réseau de l'organisation.

Dans une des consoles Microsoft Management Console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants logiciels enfichables Kaspersky Security 10.1.1 for Windows Server afin de pouvoir administrer ainsi la protection de plusieurs serveurs sur lesquels Kaspersky Security 10.1.1 for Windows Server est installé.

La console d'application fait partie des composants d'application "Outils d'administration".

Utilitaire de la ligne de commande

Vous pouvez administrer Kaspersky Security 10.1.1 for Windows Server via la ligne de commande du serveur protégé.

L'utilitaire de ligne de commande fait partie des composants logiciels de Kaspersky Security 10.1.1 for Windows Server.

Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center afin de centraliser l'administration de la protection antivirus des ordinateurs de votre entreprise, vous pourrez administrer Kaspersky Security 10.1.1 for Windows Server via la Console d'administration Kaspersky Security Center.

Il faudra installer les composants suivants :

- **Module d'intégration de l'Agent d'administration de Kaspersky Security Center**. Ce composant fait partie des composants logiciels de Kaspersky Security 10.1.1 for Windows Server. Il garantit la communication entre Kaspersky Security 10.1.1 for Windows Server et l'Agent d'administration. Installez le module d'intégration à l'Agent d'administration Kaspersky Security Center sur le serveur protégé.
- **Agent d'administration Kaspersky Security Center** Installez-le sur chaque serveur protégé. Ce composant garantit l'interaction entre la copie de Kaspersky Security 10.1.1 for Windows Server sur le serveur et la Console d'administration Kaspersky Security Center. Le fichier d'installation de l'Agent d'administration fait partie du kit de distribution de Kaspersky Security Center.
- **Plug-in d'administration de Kaspersky Security 10.1.1 for Windows Server**. De plus, sur le serveur où est installé le Serveur d'administration Kaspersky Security Center, installez le plug-in de Kaspersky Security 10.1.1 for Windows Server via la Console d'administration. Il assure l'interface d'administration de l'application via Kaspersky Security Center. Le fichier d'installation du plug-in d'administration, \server\klcfginst.exe, fait partie du kit de distribution de Kaspersky Security 10.1.1 for Windows Server.

Sélection du type d'installation

Après avoir sélectionné les composants logiciels pour l'installation de Kaspersky Security 10.1.1 for Windows Server (cf. section "Composants logiciels de Kaspersky Security 10.1.1 for Windows Server et leurs code pour le service Windows Installer" à la page 30), sélectionnez la méthode d'installation de l'application.

Sélectionnez le mode d'installation en fonction de l'architecture du réseau et des conditions suivantes :

- Recours à des paramètres d'installation spéciaux pour Kaspersky Security 10.1.1 for Windows Server ou aux paramètres recommandés (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page 40).
- Paramètres d'installation identiques pour tous les serveurs ou propres à chaque serveur ?

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server à l'aide d'un assistant Installation ou en mode silencieux en exécutant le package d'installation selon les paramètres d'installation via la ligne de commande. Vous pouvez réaliser une installation centralisée à distance de Kaspersky Security 10.1.1 for Windows Server via les stratégies de groupe Active Directory ou à l'aide d'une tâche d'installation à distance de Kaspersky Security Center.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur un serveur, le configurer et enregistrer ses paramètres dans un fichier de configuration en vue d'utiliser le fichier créé ultérieurement pour installer Kaspersky Security 10.1.1 for Windows Server sur d'autres serveurs (cette possibilité n'est pas offerte en cas d'installation de l'application via des stratégies de groupe Active Directory).

Lancement de l'Assistant d'installation

Grâce à l'Assistant d'installation, vous pouvez installer :

- Les composants de Kaspersky Security 10.1.1 for Windows Server (cf. section "Kaspersky Security 10.1.1 for Windows Server software components" à la page 31) sur un serveur protégé depuis le fichier \server\setup.exe inclus dans le kit de distribution.
- La Console de Kaspersky Security 10.1.1 for Windows Server (cf section "Installation de la console de Kaspersky Security 10.1.1 for Windows Server" à la page 54) à l'aide du fichier \client\setup.exe du kit de distribution sur le serveur protégé ou sur un autre hôte LAN.

Lancement du package d'installation via la ligne de commande selon les paramètres d'installation requis

Si vous lancez le fichier du package d'installation sans les options de la ligne de commande, Kaspersky Security 10.1.1 for Windows Server sera installé selon les paramètres par défaut. Grâce aux arguments de Kaspersky Security 10.1.1 for Windows Server, vous pouvez modifier les paramètres d'installation.

Vous pouvez installer la console d'application sur le serveur protégé et/ou sur le poste de travail de l'administrateur.

Vous pouvez aussi utiliser des exemples de commande pour l'installation de Kaspersky Security 10.1.1 for Windows Server et de la Console de l'application (cf. Section « Installation et suppression de l'application via la ligne de commande » à la page 64).

Installation centralisée du logiciel via Kaspersky Security Center

Si vous utilisez Kaspersky Security Center pour administrer la protection antivirus des ordinateurs du réseau, vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur plusieurs serveurs à l'aide d'une tâche d'installation à distance de Kaspersky Security Center.

Les serveurs sur lesquels vous souhaitez installer Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center (cf. section "Installation et suppression de l'application via Kaspersky Security Center" à la page 70) peuvent soit se trouver dans le même domaine que Kaspersky Security Center, soit dans un autre domaine. Ils peuvent également n'appartenir à aucun domaine.

Installation centralisée via les stratégies de groupe Active Directory

Les stratégies de groupe Active Directory permettent d'installer Kaspersky Security 10.1.1 for Windows Server sur un serveur protégé. Vous pouvez également installer la console d'application sur le serveur protégé ou sur le poste de travail de l'administrateur.

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server uniquement avec les paramètres par défaut.

Les serveurs sur lesquels Kaspersky Security 10.1.1 for Windows Server est installé à l'aide des stratégies de groupe Active Directory (cf. section "Installation et suppression de l'application à l'aide de stratégies de groupe Active Directory" à la page 76) doivent se trouver dans le même domaine et dans la même unité organisationnelle. L'installation a lieu lors du démarrage du serveur avant la connexion à Microsoft Windows.

Installation et suppression de l'application à l'aide de l'assistant

Cette section décrit les procédures d'installation et de suppression de Kaspersky Security 10.1.1 for Windows Server et de la console d'application via l'assistant d'installation. Elle fournit également des informations sur la configuration complémentaire de Kaspersky Security 10.1.1 for Windows Server et sur les actions à réaliser lors de l'installation.

Dans cette section

Installation à l'aide de l'Assistant d'installation

Les sections suivantes contiennent des informations sur l'installation de Kaspersky Security 10.1.1 for Windows Server et de la console d'application.

► *Pour installer et utiliser Kaspersky Security 10.1.1 for Windows Server, procédez comme suit :*

1. Installez Kaspersky Security 10.1.1 for Windows Server sur un serveur protégé.
2. Installez la console d'application sur les ordinateurs sur lesquels vous avez l'intention d'administrer Kaspersky Security 10.1.1 for Windows Server.
3. Si vous avez installé la console d'application sur tout ordinateur du réseau autre que le serveur protégé, procédez à une configuration complémentaire afin que les utilisateurs de la console d'application puissent administrer Kaspersky Security 10.1.1 for Windows Server à distance.
4. Réalisez ces actions après l'installation de Kaspersky Security 10.1.1 for Windows Server.

Dans cette section

Installation de Kaspersky Security 10.1.1 for Windows Server

Avant d'installer Kaspersky Security 10.1.1 for Windows Server, suivez ces étapes :

- Assurez-vous qu'aucun autre logiciel antivirus n'est installé sur le serveur. Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sans supprimer Kaspersky Antivirus 8.0 for Windows Servers Enterprise Edition ou Kaspersky Security 10 for Windows Server.
- Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté est enregistré dans le groupe des administrateurs sur le serveur protégé.

Lorsque les actions décrites ci-dessus ont été effectuées, passez à la procédure d'installation. Définissez les paramètres d'installation de Kaspersky Security 10.1.1 for Windows Server en suivant les instructions de l'Assistant. Vous pouvez interrompre l'installation de Kaspersky Security 10.1.1 for Windows Server à n'importe quelle étape de l'assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'Assistant d'installation.

Vous pouvez obtenir de plus amples informations sur les paramètres d'installation (de désinstallation) (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page 40).

► *Pour installer Kaspersky Security 10.1.1 for Windows Server à l'aide de l'Assistant d'installation :*

1. Lancez le fichier d'accueil setup.exe sur le serveur.
2. Dans la section **Installation** de la fenêtre qui s'ouvre, cliquez sur le lien **Installer Kaspersky Security 10.1.1 for Windows Server**.
3. Dans la fenêtre d'accueil de l'Assistant d'installation de Kaspersky Security 10.1.1 for Windows Server, appuyez sur le bouton **Suivant**.

   La fenêtre **Contrat de licence utilisateur final et Politique de confidentialité** s'ouvre.
4. Révisez le Contrat de licence et la Politique de confidentialité.
5. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **les termes de ce Contrat de licence utilisateur final Politique de confidentialité décrivant la manipulation des données** afin de poursuivre l'installation.

   Si vous n'acceptez pas le Contrat de licence utilisateur final et/ou la Politique de confidentialité, l'installation sera interrompue.
6. Cliquez sur **Suivant**.

   Si une version compatible est installée sur le serveur, la fenêtre **Découverte d'une version antérieure de l'application** s'ouvre.

   Si aucune version antérieure de l'application n'est détectée, passez à l'étape 8 de ces instructions.
7. Pour mettre à niveau une version antérieure de l'application, cliquez sur **Installer**. L'assistant Installation réalise la mise à niveau de l'application jusqu'à Kaspersky Security 10.1.1 for Windows Server et enregistre les paramètres compatibles dans la nouvelle version. Lorsque la mise à jour de l'application est terminée, la fenêtre **Installation complète** s'ouvre (passez à l'étape 15 des présentes instructions).

   La fenêtre **Analyse rapide de l'ordinateur avant l'installation** s'ouvre.
8. Dans la fenêtre **Analyse rapide de l'ordinateur avant l'installation**, cochez la case **Rechercher la présence éventuelle de virus sur l'ordinateur** afin de rechercher la présence éventuelle de menaces dans les secteurs d'amorçage des disques locaux du serveur et dans la mémoire système. Ensuite, cliquez sur **Suivant**. À la fin de l'analyse, les résultats s'affichent dans une fenêtre.

   Vous pourrez y consulter les informations relatives aux objets analysés sur le serveur : nombre total d'objets analysés, nombre de types de menaces découvertes, nombre d'objets infectés et probablement infectés découverts, nombre de processus dangereux ou suspects que Kaspersky Security 10.1.1 for Windows Server a supprimés de la mémoire et nombre de processus dangereux ou suspects que l'application n'a pas réussi à supprimer.

   Pour voir exactement les fichiers qui ont été analysés, cliquez sur le bouton **Liste des objets traités**.
9. Dans la fenêtre **Analyse rapide de l'ordinateur avant l'installation**, cliquez sur le bouton **Suivant**.

   La fenêtre **Installation personnalisée** s'ouvre.

10. Sélectionnez les composants que vous souhaitez installer.

    La liste recommandée des composants à installer reprend par défaut tous les composants de Kaspersky Security 10.1.1 for Windows Server, à l'exception des composants Gestion du pare-feu et Monitoring des scripts.

    > Le composant Prise en charge du protocole SNMP de Kaspersky Security 10.1.1 for Windows Server apparaît dans la liste des composants à installer uniquement si le service SNMP Microsoft Windows est installé sur le serveur.

11. Pour annuler toutes les modifications de la fenêtre **Installation personnalisée**, cliquez sur le bouton **Réinitialiser**. Cliquez sur **Suivant**.
12. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :

    - Le cas échéant, désignez un dossier pour la copie des fichiers de Kaspersky Security 10.1.1 for Windows Server.
    - Le cas échéant, consultez les informations concernant l'espace disponible sur les disques durs locaux en cliquant sur **Disque**.

    Cliquez sur **Suivant**.
13. Dans la fenêtre **Paramètres avancés d'installation** qui s'ouvre, définissez les paramètres d'installation suivants :

    - **Activer la protection en temps réel après l'installation de l'application**.
    - **Ajouter les exclusions recommandées par Microsoft**.
    - **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions**.

      Cliquez sur **Suivant**.
14. Dans la fenêtre **Importation des paramètres du fichier de configuration** qui s'ouvre, procédez comme suit :

    a. Désignez le fichier de configuration pour importer les paramètres de Kaspersky Security 10.1.1 for Windows Server depuis un fichier de configuration existant créé dans n'importe quelle version précédente compatible de l'application.

    b. Ensuite, cliquez sur **Suivant**.

15. Dans la fenêtre **Activation de l'application** qui s'ouvre, exécutez l'une des actions suivantes :
    - Si vous souhaitez activer l'application, sélectionnez un fichier clé de Kaspersky Security 10.1.1 for Windows Server.
    - Si vous souhaitez activer l'application plus tard, cliquez sur **Suivant**.
    - si vous aviez enregistré le fichier clé dans le dossier \server du kit de distribution, le nom de ce fichier apparaît dans le champ **Clé**.
    - Si vous souhaitez ajouter une licence à l'aide d'un fichier clé qui se trouve dans un autre dossier, spécifiez le fichier clé.

      Vous ne pouvez pas activer l'application à l'aide d'un code d'activation dans l'Assistant d'installation. Si vous souhaitez activer l'application à l'aide d'un code d'activation, vous pourrez en ajouter un après l'installation de l'application.

      Après l'ajout du fichier clé, la fenêtre affiche les informations concernant la licence. Kaspersky Security 10.1.1 for Windows Server affiche la date d'expiration de la licence calculée. La date de validité de la licence est calculée à partir de l'ajout de la clé mais elle ne dépasse jamais la date limite de validité du fichier clé.

      Cliquez sur **Suivant** pour appliquer la clé dans l'application.
16. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**. L'assistant lance l'installation des composants de Kaspersky Security 10.1.1 for Windows Server.
17. La fenêtre **Installation terminée** s'ouvre à la fin de l'installation.
18. Cochez la case **Lire les notes de publication** afin de consultez les informations relatives à la version après la fin de l'Assistant d'installation.
19. Cliquez sur le bouton **OK**.

La fenêtre de l'Assistant d'installation se ferme. Une fois l'installation terminée, Kaspersky Security 10.1.1 for Windows Server est prêt à être utilisé si vous avez ajouté la clé d'activation.

Installation de la console de Kaspersky Security 10.1.1 for Windows Server

Définissez les paramètres d'installation de la console d'application en suivant les instructions de l'Assistant d'installation. Vous pouvez interrompre l'installation à n'importe quelle étape de l'Assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'Assistant d'installation.

► *Pour installer la console d'application, procédez comme suit :*

1. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté est enregistré dans le groupe des administrateurs sur l'ordinateur.
2. Exécutez le fichier d'accueil setup.exe.

   La fenêtre de bienvenue de l'application s'ouvre.
3. Cliquez sur le lien **Installer la console de Kaspersky Security 10.1.1 for Windows Server**.

   La fenêtre d'accueil de l'Assistant d'installation s'ouvre. Cliquez sur **Suivant**.

4. Révisez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité dans la fenêtre ouverte et sélectionnez **les termes de ce Contrat de licence utilisateur final** et **Politique de confidentialité décrivant la manipulation des données** afin de poursuivre l'installation. Cliquez sur **Suivant**.

   La fenêtre **Paramètres avancés d'installation** s'ouvre.

5. Dans la fenêtre **Paramètres avancés d'installation**, procédez comme suit :

   - Si vous avez l'intention d'administrer Kaspersky Security 10.1.1 for Windows Server distant à l'aide de la console d'application, cochez la case **Autoriser l'accès à distance**.
   - Pour ouvrir la fenêtre **Installation personnalisée** et sélectionner des composants, procédez comme suit :

     a. Cliquez sur le bouton **Avancé**.

        La fenêtre **Installation personnalisée** s'ouvre.

     b. Sélectionnez les composants "Outils d'administration" définis à partir d'une liste.

        Par défaut, tous les composants sont installés.

     c. Cliquez sur **Suivant**.

   > Vous pouvez obtenir de plus amples informations sur les composants de Kaspersky Security 10.1.1 for Windows Server (cf Section "Composants logiciels de Kaspersky Security 10.1.1 for Windows Server et leurs code pour le service Windows Installer" à la page 30).

6. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :

   a. Le cas échéant, désignez un autre dossier pour la conservation des fichiers installés.

   b. Cliquez sur **Suivant**.

7. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**.

   L'Assistant lance l'installation des composants sélectionnés.

8. Cliquez sur le bouton **OK**.

La fenêtre de l'Assistant d'installation se ferme. La console d'application sera installée sur le serveur protégé.

Si un ensemble d'"outils d'administration" a été installé sur n'importe quel ordinateur du réseau autre que le serveur protégé, réglez les paramètres avancés (cf. section "Configuration avancée après l'installation de la console d'application sur un autre ordinateur" à la page 55).

Configuration avancée après l'installation de la console d'application sur un autre ordinateur

Si vous avez installé la console d'application sur tout ordinateur du réseau autre que le serveur protégé, réalisez les actions décrites ci-dessous afin que les utilisateurs puissent administrer Kaspersky Security 10.1.1 for Windows Server à distance :

- Sur le serveur protégé, ajoutez les utilisateurs de Kaspersky Security 10.1.1 for Windows Server au groupe KAVWSEE Administrators.
- Autorisez les connexions réseau pour le Service Kaspersky Security Management (kavfsgt.exe) (voir section "A propos des autorisations d'accès au Service Kaspersky Security Management" à la page 101) si le pare-feu Windows ou un pare-feu tiers est utilisé sur le serveur protégé.
- Si lors de l'installation de la console d'application sur un ordinateur tournant sous Microsoft Windows vous n'avez pas coché la case **Autoriser l'accès à distance**, vous devez autoriser manuellement les connexions réseau pour la console d'application via le pare-feu de cet ordinateur.

Autorisation des connexions de réseau pour la console d'application

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

La console d'application sur l'ordinateur distant utilise le protocole DCOM pour obtenir les informations sur les événements de Kaspersky Security 10.1.1 for Windows Server (objets analysés, tâches terminées, etc.) fournies par le Service Kaspersky Security Management sur le serveur protégé. Vous devez autoriser les connexions réseau pour la console d'application dans le pare-feu Windows pour la console d'application afin d'établir une connexion entre la console d'application et le Service Kaspersky Security Management.

Sur l'ordinateur distant où l'application est installée, procédez comme suit :

- 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 réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Security 10.1.1 for Windows Server.

  L'ordinateur sur lequel la console d'application est installée utilise le port TCP 135 pour accéder au serveur protégé et pour recevoir une réponse.
- Configurez la règle de trafic sortant du pare-feu Windows pour autoriser la connexion.

  Contrairement aux services TCP/IP et UDP/IP classiques où un seul protocole est associé à un port fixe, le service DCOM affecte des ports de manière dynamique pour les objets COM qu'il supprime. Si un pare-feu existe entre le client (ou la console d'application est installée) et le point limite DCOM (le serveur protégé), un grand éventail de ports doivent être ouverts.

La même étape doit être appliquée pour configurer tout autre pare-feu logiciel ou matériel.

Si la console d'application était ouverte lorsque vous configuriez la connexion entre le serveur protégé et le serveur sur lequel la console d'application est installée, fermez la console d'application, attendez la fin du processus d'administration à distance kavfsrcn.exe de Kaspersky Security 10.1.1 for Windows Server et relancez la console d'application. 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 distant sur lequel la console de Kaspersky Security 10.1.1 for Windows Server est installée, ouvrez la console du Service des composants.
2. Choisissez **Démarrer** > **Exécuter**.
3. Saisissez la commande `dcomcnfg`.
4. Cliquez sur le bouton **OK**.
5. Dans la console du **Service des composants** du serveur, développez le nœud **Ordinateurs**.
6. Ouvrez le menu contextuel du nœud **Poste de travail**.
7. Choisissez l'option **Propriétés**.
8. Dans l'onglet **Sécurité COM** de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les limites** du groupe de paramètres **Autorisations d'accès**.
9. Dans la fenêtre **Autoriser l'accès à distance**, vérifiez que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur ANONYMOUS LOGON.
10. Cliquez sur le bouton **OK**.

► *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 10.1.1 for Windows Server, procédez comme suit :*

1. Sur l'ordinateur distant, fermez la console de Kaspersky Security 10.1.1 for Windows Server.
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 **Démarrer** > **Panneau de configuration** > **Pare-feu Windows** et, dans la fenêtre **Pare-feu Windows**, cliquez sur **Modifier les paramètres**.

     b. Dans la fenêtre Pare-feu Windows (ou Paramètres du pare-feu Windows), cliquez sur le bouton **Ajouter un port** sous l'onglet **Exclusions**.

     c. Dans le champ **Nom**, indiquez le nom du port RPC (TCP/135) ou entrez un autre nom, par exemple DCOM Kaspersky Security 10.1.1 for Windows Server et dans le champ **Nom de port**, indiquez le numéro du port : 135.

     d. Sélectionnez le protocole **TCP**.

     e. Cliquez sur le bouton **OK**.

     f. Sous l'onglet **Exclusions**, cliquez sur le bouton **Ajouter**.

- Dans Microsoft Windows 7 et suivants :
  a. Sélectionnez 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 de destination lors de l'installation de la console de Kaspersky Security 10.1.1 for Windows Server à l'aide de Microsoft Management Console.
4. Cliquez sur le bouton **OK**.
5. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu Windows (Paramètres du pare-feu Windows)**.

► *Ajout de la règle de trafic sortant du pare-feu Windows :*

1. Sélectionnez Démarrer > Panneau de configuration > Pare-feu Windows.
2. Dans la fenêtre **Pare-feu Windows**, cliquez sur le lien **Paramètres avancés**.

   La fenêtre **Pare-feu Windows avec sécurité avancée** s'ouvre.
3. Cochez le nœud enfant **Règles de trafic sortant**.
4. Dans le panneau **Actions**, cliquez sur l'option **Nouvelle règle**.
5. Dans la fenêtre de l'**assistant de création de nouvelle règle de sortie**, sélectionnez l'option **Port** et cliquez sur **Suivant**.
6. Sélectionnez le protocole **TCP**.
7. Dans le champ **Ports distants spécifiques** spécifiez la plage de ports suivante pour autoriser les connexions sortantes : 1024-65535.
8. Dans la fenêtre **Action**, sélectionnez l'option **Autoriser la connexion**.
9. Enregistrez la nouvelle règle et fermez la fenêtre **Pare-feu Windows avec fonctions avancées de sécurité**.

Le pare-feu Windows autorise désormais les connexions réseau entre la console d'application et le Service Kaspersky Security Management.

Actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server

Kaspersky Security 10.1.1 for Windows Server lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si l'option **Activer la protection en temps réel après l'installation de l'application** (option par défaut) a été sélectionnée lors de l'installation de Kaspersky Security 10.1.1 for Windows Server, l'application analyse les objets du système de fichiers de serveur lorsqu'ils sont sollicités. Si le composant Monitoring des scripts a été installé dans le cadre de l'installation personnalisée, Kaspersky Security 10.1.1 for Windows Server analyse le code de programme de tous les scripts lorsqu'ils sont exécutés Chaque vendredi à 20h00, Kaspersky Security 10.1.1 for Windows Server lance la tâche Analyse des zones critiques.

Après l'installation de Kaspersky Security 10.1.1 for Windows Server, il est conseillé de réaliser les actions suivantes :

- Lancez la tâche Mise à jour des bases de l'application. Une fois installé, Kaspersky Security 10.1.1 for Windows Server analyse les objets à l'aide des bases livrées avec le kit de distribution de l'application.

  Nous recommandons de mettre à jour immédiatement les bases de Kaspersky Security 10.1.1 for Windows Server car elles peuvent être obsolètes.

  Par la suite, l'application mettra à jour les bases toutes les heures conformément à la planification définie dans la tâche par défaut.
- Lancer une analyse des zones critiques du serveur si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur le serveur protégé avant l'installation de Kaspersky Security 10.1.1 for Windows Server.
- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security 10.1.1 for Windows Server.

Dans cette section

Lancement et configuration de la tâche de mise à jour des bases de l'application de Kaspersky Security 10.1.1 for Windows Server

► *Pour mettre à jour les bases de l'application après l'installation, procédez comme suit :*

1. Configurer la connexion avec la source des mises à jour, les serveurs HTTP ou FTP de mise à jour de Kaspersky Lab, dans les propriétés de la tâche Mise à jour des bases de l'application.
2. Lancer la tâche Mise à jour des bases de l'application.

► *Pour configurer la connexion aux serveurs de mise à jour de Kaspersky Lab dans la tâche Mise à jour des bases de l'application, effectuez les actions suivantes :*

1. Lancez la console d'application d'une des manières suivantes :
   - Ouvrez la console d'application sur le serveur protégé. Pour cela, cliquez sur **Démarrer** > **Tous les programmes** > **Kaspersky Security 10.1.1 for Windows Server** > **Outils d'administration** > **Console de Kaspersky Security 10.1.1 for Windows Server**.
   - Si vous avez lancé la console d'application sur un serveur non protégé, connectez-vous au serveur protégé :
     a. Ouvrez le menu contextuel du nœud **Kaspersky Security** dans l'arborescence de la console d'application.
     b. Sélectionnez l'option **Se connecter à un autre ordinateur**.

c. Dans la fenêtre **Sélection d'ordinateur** qui s'ouvre, choisissez **Autre ordinateur** et saisissez le nom de réseau du serveur protégé dans le champ textuel.

> Si le compte utilisateur employé pour se connecter à Microsoft Windows ne possède pas les autorisations d'accès au Service Kaspersky Security Management (cf. section "A propos des autorisations d'accès au Service Kaspersky Security Management" à la page 101), indiquez un compte utilisateur doté de ces autorisations.

La fenêtre Console d'application s'ouvre.

2. Dans l'arborescence de la console d'application, développez le nœud **Mise à jour**.
3. Sélectionnez le nœud enfant **Mise à jour des bases de l'application**.
4. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.
5. Dans la fenêtre **Paramètres de la tâche** qui s'ouvre, ouvrez l'onglet **Paramètres de connexion**.
6. Exécutez les actions suivantes :
   a. Si le protocole Web Proxy Auto-Discovery Protocole (WPAD) pour la reconnaissance automatique des paramètres du serveur proxy par le réseau local n'est pas configuré, définissez les paramètres du serveur proxy : dans la section **Paramètres du serveur proxy**, cochez la case **Utiliser les paramètres du serveur proxy indiqué** et saisissez l'adresse dans le champ **Adresse** et le numéro de port du serveur proxy dans le champ **Port**.
   b. Si votre réseau requiert une authentification au moment de l'accès au serveur proxy, sélectionnez la méthode requise dans la liste déroulante de la section **Paramètres d'authentification du serveur proxy** :
      - **Utiliser l'authentification NTLM** si le serveur proxy prend en charge l'analyse intégrée de l'authenticité dans Microsoft Windows (NTLM authentification). Kaspersky Security 10.1.1 for Windows Server accède alors au serveur proxy à l'aide du compte utilisateur indiqué dans les paramètres de la tâche (la tâche est exécutée par défaut sous le compte utilisateur **Système local** (**SYSTEM**)).
      - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** si le serveur prend en charge l'authentification NTLM Microsoft Windows intégrée. Kaspersky Security 10.1.1 for Windows Server utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy. Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
      - **Utiliser le nom d'utilisateur et le mot de passe** pour choisir l'authentification traditionnelle (Basic authentification). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
7. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres de connexion à la source des mises à jour dans la tâche Mise à jour des bases de l'application sont sauvegardés.

► *Pour lancer la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Dans l'arborescence de la console d'application, développez le nœud **Mise à jour**.
2. Dans le menu contextuel du nœud enfant **Mise à jour des bases de l'application**, sélectionnez l'option **Démarrer**.

La tâche de Mise à jour des bases de l'application démarre.

Une fois la tâche terminée, vous pouvez consulter la date de publication des dernières mises à jour des bases de l'application installées dans le panneau de détails du nœud **Kaspersky Security**.

Analyse des zones critiques

Une fois que les bases de Kaspersky Security 10.1.1 for Windows Server ont été mises à jour, recherchez la présence éventuelle d'applications malveillantes sur le serveur à l'aide de la tâche Analyse des zones critiques.

► *Pour lancer la tâche Analyse des zones critiques, procédez comme suit :*

1. Dans l'arborescence de la console d'application, développez le nœud **Analyse à la demande**.
2. Dans le menu contextuel du nœud enfant **Analyse des zones critiques**, sélectionnez la commande **Démarrer**.

La tâche est lancée et l'état **Exécution en cours** apparaît dans l'espace de travail.

► *Pour consulter le journal d'exécution de la tâche,*

dans le panneau de détails **Analyse des zones critiques**, cliquez sur le lien **Ouvrir le journal**.

Modification de la sélection de composants et récupération de Kaspersky Security 10.1.1 for Windows Server

Vous pouvez ajouter ou supprimer des composants de Kaspersky Security 10.1.1 for Windows Server. Vous devez d'abord arrêter la tâche Protection des fichiers en temps réel si vous souhaitez supprimer le composant Protection des fichiers en temps réel. Dans tous les autres cas, il n'est pas nécessaire d'arrêter la Protection des fichiers en temps réel ou le Service Kaspersky Security.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Security 10.1.1 for Windows Server requiert la saisie du mot de passe lors de toute tentative de suppression ou de modification de la liste des composants de l'application dans une étape supplémentaire de l'assistant.

► *Pour modifier la sélection de composants de Kaspersky Security 10.1.1 for Windows Server :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes > Kaspersky Security 10.1.1 for Windows Server > Modification ou suppression**.

   La fenêtre **Modification, réparation ou suppression** de l'Assistant d'installation s'ouvre.
2. Sélectionnez **Modification de la liste des composants**. Cliquez sur **Suivant**.

   La fenêtre **Installation personnalisée** s'ouvre.

3. Dans la liste des composants disponibles de la fenêtre **Installation personnalisée**, sélectionnez les composants que vous souhaitez ajouter à Kaspersky Security 10.1.1 for Windows Server ou que vous souhaitez supprimer de l'application. Pour ce faire, procédez comme suit :

   - Pour modifier la composition des composants, cliquez sur le bouton situé près du nom du composant sélectionné, et, dans le menu contextuel, sélectionnez :
     - L'option **Le composant sera installé sur un disque dur local** si vous souhaitez installer un composant ;
     - L'option **Le composant et ses sous-composants seront installés sur le disque dur local** si vous souhaitez installer un groupe de composants.
   - Pour supprimer des composants installés, cliquez sur le bouton situé en regard du nom du composant sélectionné et, dans le menu contextuel, sélectionnez l'option **Ce composant ne sera plus disponible.**

   Cliquez sur **Installer**.

4. Dans la fenêtre **Prêt pour l'installation**, confirmez la modification de la liste des composants en cliquant sur le bouton Installer.
5. Dans la fenêtre qui s'ouvre lorsque l'installation est terminée, cliquez sur le bouton **OK**.

La liste des composants de Kaspersky Security 10.1.1 for Windows Server sera modifiée conformément aux paramètres définis.

Si des problèmes se présentent durant l'utilisation de Kaspersky Security 10.1.1 for Windows Server (Kaspersky Security 10.1.1 for Windows Server s'arrête, les tâches se soldent par un échec ou ne sont pas lancées), vous pouvez tenter de restaurer Kaspersky Security 10.1.1 for Windows Server. Vous pouvez procéder à la restauration en conservant les valeurs actuelles des paramètres de Kaspersky Security 10.1.1 for Windows Server ou en sélectionnant le mode qui rétablira toutes les valeurs par défaut des paramètres de Kaspersky Security 10.1.1 for Windows Server.

► *Pour rétablir Kaspersky Security 10.1.1 for Windows Server après une erreur de l'application ou d'une tâche, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes > Kaspersky Security 10.1.1 for Windows Server > Modification ou suppression**.

   La fenêtre **Modification, restauration ou suppression** de l'Assistant d'installation s'ouvre.

2. Sélectionnez **Réparation des composants installés**. Cliquez sur **Suivant**.

   La fenêtre **Réparation des composants installés** s'ouvre.

3. Dans la fenêtre **Réparation des composants installés**, cochez la case **Rétablir les paramètres recommandés de l'application** si vous souhaitez annuler les paramètres configurés et restaurer les paramètres par défaut de Kaspersky Security 10.1.1 for Windows Server. Cliquez sur **Installer**.
4. Dans la fenêtre **Prêt pour la réparation**, confirmez la réparation de l'application en cliquant sur le bouton **Installer**.
5. Dans la fenêtre qui s'ouvre lorsque la restauration est terminée, cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server sera restauré conformément aux paramètres définis.

Suppression à l'aide de l'Assistant d'installation

Cette section contient des instructions pour supprimer Kaspersky Security 10.1.1 for Windows Server et la console d'application d'un serveur protégé à l'aide de l'Assistant d'installation.

Dans cette section

Désinstallation de Kaspersky Security 10.1.1 for Windows Server

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

Vous pouvez désinstaller Kaspersky Security 10.1.1 for Windows Server du serveur protégé à l'aide de l'Assistant d'installation/de désinstallation.

Il faudra peut-être redémarrer le serveur sur lequel Kaspersky Security 10.1.1 for Windows Server a été désinstallé. Il est possible de reporter le redémarrage à plus tard.

La suppression, la réparation et l'ajout d'une application via le panneau d'administration Windows sont impossible si le système d'exploitation utilise la fonction Contrôle des comptes utilisateurs (User Account Control) ou si l'accès à l'administration de l'application est protégé par un mot de passe.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Security 10.1.1 for Windows Server requiert la saisie du mot de passe lors de toute tentative de suppression ou de modification de la liste des composants de l'application dans une étape supplémentaire de l'assistant.

► *Pour désinstaller Kaspersky Security 10.1.1 for Windows Server :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes > Kaspersky Security 10.1.1 for Windows Server > Modification ou suppression**.

   La fenêtre **Modification, réparation ou suppression** de l'Assistant d'installation s'ouvre.
2. Sélectionnez **Suppression des composants de l'application**. Cliquez sur **Suivant**.

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

3. Si nécessaire, dans la fenêtre **Paramètres avancés de désinstallation de l'application**, procédez comme suit :

   a. Cochez la case **Exporter les objets de la quarantaine** pour que Kaspersky Security 10.1.1 for Windows Server exporte les objets qui ont été mis en quarantaine. Cette case est décochée par défaut.

   b. Cochez la case **Exporter les objets de la sauvegarde** pour exporter les objets de la sauvegarde de Kaspersky Security 10.1.1 for Windows Server. Cette case est décochée par défaut.

   c. Cliquez sur le bouton **Enregistrer dans** et indiquez le dossier vers lequel vous souhaitez exporter les objets restaurés. Par défaut, les objets sont exportés vers le dossier %ProgramData%\Kaspersky Lab\Kaspersky Security 10.1.1 for Windows Server\Uninstall.

   Cliquez sur **Suivant**.

4. Dans la fenêtre **Prêt pour la désinstallation**, confirmez l'opération de désinstallation en cliquant sur **Désinstaller**.
5. Dans la fenêtre qui s'ouvre lorsque la suppression est terminée, cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server est désinstallé du serveur protégé.

Désinstallation de la console de Kaspersky Security 10.1.1 for Windows Server

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

Vous pouvez désinstaller la console d'application sur l'ordinateur à l'aide de l'Assistant d'installation/de désinstallation.

Il n'est pas nécessaire de redémarrer le serveur après la désinstallation de la console d'application.

► *Pour désinstaller la console d'application, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes > Kaspersky Security 10.1.1 for Windows Server > Outils d'administration > Modification ou suppression**.
2. La fenêtre **Modification, restauration ou suppression** de l'Assistant s'ouvre.

   Choisissez l'option **Suppression des composants de l'application**, puis cliquez sur **Suivant**.
3. La fenêtre **Prêt pour la désinstallation** s'ouvre. Cliquez sur le bouton **Supprimer**.

   La fenêtre **Désinstallation terminée** s'ouvre.
4. Cliquez sur le bouton **OK**.

L'opération de suppression se termine ; la fenêtre de l'Assistant se ferme.

Installation et suppression de l'application via la ligne de commande

Cette section décrit les particularités de l'installation et de la désinstallation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande. Elle fournit également des exemples de commande pour l'installation et la désinstallation de Kaspersky Security 10.1.1 for Windows Server et des exemples de commandes pour l'ajout et la suppression de composants de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande.

Dans cette section

A propos de l'installation et de la désinstallation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande

Vous pouvez installer et désinstaller Kaspersky Security 10.1.1 for Windows Server, ajouter ou supprimer des composants en exécutant les fichiers du package d'installation \server\ks4ws_x86(x64).msi via la ligne de commande et en précisant les paramètres d'installation à l'aide d'arguments.

Vous pouvez installer la sélection "Outils d'administration" sur le serveur protégé ou sur un autre ordinateur du réseau afin d'utiliser la console d'application localement ou à distance. Pour ce faire, utilisez le paquet d'installation \client\ks4wstools.msi.

Réalisez l'installation sous un compte utilisateur appartenant au groupe d'administrateurs du serveur sur lequel vous souhaitez installer le composant.

Si vous exécutez l'un des fichiers \product\ks4ws_x86(x64).msi sur le serveur protégé sans clés additionnelles, Kaspersky Security 10.1.1 for Windows Server est installé avec les paramètres d'installation recommandés.

Vous pouvez définir la sélection des composants à installer à l'aide de l'argument ADDLOCAL en utilisant en guise de valeur le code des composants sélectionnés ou de la sélection de composants.

Exemple de commande pour l'installation de Kaspersky Security 10.1.1 for Windows Server

Cette rubrique présente des exemples de commandes pour l'installation de Kaspersky Security 10.1.1 for Windows Server.

Sur les serveurs fonctionnant sous Microsoft Windows 32 bits, exécutez les fichiers du kit de distribution dont le suffixe est x86. Sur les serveurs fonctionnant sous Microsoft Windows 64 bits, exécutez les fichiers du kit de distribution dont le suffixe est x64.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des instructions et des clés standard de Windows Installer.

Exemples pour l'installation de Kaspersky Security 10.1.1 for Windows Server depuis le fichier setup.exe

► *Pour installer Kaspersky Security 10.1.1 for Windows Server avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande :*

```
\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

► *Pour installer Kaspersky Security 10.1.1 for Windows Server avec les paramètres suivants :*

- Installer uniquement les composants Protection des fichiers en temps réel et Analyse à la demande ;
- Ne pas lancer la Protection en temps réel au démarrage de Kaspersky Security 10.1.1 for Windows Server ;
- Ne pas exclure de l'analyse les fichiers dont l'exclusion est recommandée par Microsoft Corporation ;

saisissez l'instruction suivante :

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Exemples de commandes pour l'installation : exécution du fichier msi du paquet d'installation

► *Pour installer Kaspersky Security 10.1.1 for Windows Server avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande :*

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Pour installer Kaspersky Security 10.1.1 for Windows Server selon les paramètres recommandés en affichant l'interface d'installation, saisissez la commande :*

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

► *Pour installer Kaspersky Security 10.1.1 for Windows Server avec activation à l'aide du fichier clé C:\0000000A.key :*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

- *Pour installer Kaspersky Security 10.1.1 for Windows Server avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux, saisissez la commande :*

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Pour installer Kaspersky Security 10.1.1 for Windows Server en enregistrant ses fichiers dans le dossier de destination C:\WSEE, saisissez la commande suivante :*

```
msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1
```

- *Pour installer Kaspersky Security 10.1.1 for Windows Server, enregistrer le fichier journal sous le nom ks4ws.log dans le répertoire où se trouve le fichier msi du package d'installation de Kaspersky Security 10.1.1 for Windows Server, saisissez la commande suivante :*

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Pour installer la console de Kaspersky Security 10.1.1 for Windows Server, exécutez la commande suivante :*

```
msiexec /i ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Pour installer Kaspersky Security 10.1.1 for Windows Server avec activation à l'aide du fichier clé C:\0000000A.key ; configurer Kaspersky Security 10.1.1 for Windows Server conformément aux paramètres du fichier de configuration C:\settings.xml, saisissez la commande suivante :*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- *Pour installer les correctifs de l'application lorsque Kaspersky Security 10.1.1 for Windows Server est protégé par mot de passe, exécutez la commande suivante :*

```
msiexec /p "<nom de fichier msp avec le chemin>" UNLOCK_PASSWORD=<mot de passe>
```

Actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server

Kaspersky Security 10.1.1 for Windows Server lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si vous avez choisi l'option **Activer la protection en temps réel après l'installation de l'application** lors de l'installation de Kaspersky Security 10.1.1 for Windows Server, Kaspersky Security 10.1.1 for Windows Server analyse les objets du système de fichiers de serveur lorsqu'ils sont sollicités. Si le composant Monitoring des scripts a été installé dans le cadre de l'installation personnalisée, Kaspersky Security 10.1.1 for Windows Server analyse le code de tous les scripts lorsqu'ils sont exécutés. Chaque vendredi à 20h00, Kaspersky Security 10.1.1 for Windows Server lance la tâche Analyse des zones critiques.

Après l'installation de Kaspersky Security 10.1.1 for Windows Server, il est conseillé de réaliser les actions suivantes :

- Lancer la tâche de mise à jour des bases de l'application de Kaspersky Security 10.1.1 for Windows Server. Une fois installé, Kaspersky Security 10.1.1 for Windows Server analyse les objets à l'aide des bases livrées avec le kit de distribution. Nous conseillons de réaliser une mise à jour immédiate des bases de Kaspersky Security 10.1.1 for Windows Server. Pour ce faire, vous devez lancer la tâche Mise à jour des bases de l'application. Par la suite, la mise à jour des bases de données sera exécutée toutes les heures selon la planification définie par défaut.

  Par exemple, vous pouvez lancer la tâche Mise à jour des bases de l'application à l'aide de l'instruction suivante :

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456 :

  Dans ce cas, les mises à jour des bases de données de Kaspersky Security 10.1.1 for Windows Server sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab. La connexion à la source des mises à jour s'opère via le serveur proxy (adresse du proxy : proxy.company.com, port : 8080) et utilise l'authentification intégrée de Microsoft Windows pour accéder au serveur (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser ; mot de passe : 123456).
- Lancez une analyse des zones critiques du serveur si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur le serveur protégé avant l'installation de Kaspersky Security 10.1.1 for Windows Server.

► *Pour réaliser la tâche Analyse des zones critiques à l'aide d'une ligne de commande, exécutez la commande suivante :*

KAVSHELL SCANCRITICAL /W:scancritical.log

Cette instruction conserve le journal d'exécution de la tâche dans le fichier scancritical.log du dossier actif.

- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security 10.1.1 for Windows Server.

Ajout et suppression de composants. Exemples de commandes

Le composant "Analyse à la demande" est installé automatiquement. Il n'est pas nécessaire de l'indiquer dans la liste des valeurs de la clé ADDLOCAL lors de la suppression ou de l'ajout de composants de Kaspersky Security 10.1.1 for Windows Server.

► *Pour ajouter le composant Contrôle du lancement des applications aux composants déjà installés, exécutez la commande suivante :*

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn
```

ou

```
\server\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Si vous renseignez non seulement les composants que voulez installer, mais également ceux qui sont déjà installés, Kaspersky Security 10.1.1 for Windows Server installe à nouveau les composants indiqués installés.

► *Pour supprimer les composants installés, exécutez la commande suivante :*

```
msiexec /i ks4ws.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,Fim,LogInsp
ector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection
,RamDisk REMOVE=AppCtrl,ScriptMonitoring" /qn
```

Désinstallation de Kaspersky Security 10.1.1 for Windows Server. Exemples de commandes

► *Pour désinstaller Kaspersky Security 10.1.1 for Windows Server sur le serveur protégé, saisissez la commande suivante :*

```
msiexec /x ks4ws.msi /qn
```

ou

- Sous un système d'exploitation 32 bits :

```
msiexec /x {6B19338E-C525-492C-92C3-1DFEAE5CC3ED} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {BD9BD9FC-F4D1-498E-8091-740925B2ACB2} /qn
```

► *Pour désinstaller la console de Kaspersky Security 10.1.1 for Windows Server, saisissez la commande suivante :*

```
msiexec /x ks4wstools.msi /qn
```

ou

- Sous un système d'exploitation 32 bits :

```
msiexec /x {FBB703C9-7F99-4023-B5E4-1E2B5A4E6509} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {29F4E82D-BB68-49A1-959E-928D02F8B028} /qn
```

► *Pour désinstaller Kaspersky Security 10.1.1 for Windows Server d'un serveur protégé sur lequel la protection par mot de passe est activée, saisissez la commande suivante :*

- Sous un système d'exploitation 32 bits :

```
msiexec.exe /x {6B19338E-C525-492C-92C3-1DFEAE5CC3ED} UNLOCK_PASSWORD=***
/qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec.exe /x {BD9BD9FC-F4D1-498E-8091-740925B2ACB2} UNLOCK_PASSWORD=***
/qn
```

► *Pour désinstaller le plug-in de Kaspersky Security 10.1.1 Microsoft Outlook, saisissez la commande suivante :*

- Sous un système d'exploitation 32 bits :

```
msiexec /x {99BD32C3-D305-4201-AD3E-3B2A94FDCB5E} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {D17EA574-ACA5-471E-B904-AD2835452047} /qn
```

Codes de retour

Le tableau ci-dessous décrit les codes de retour de la ligne de commande.

Tableau 13. Codes de retour

Code	Description
1324	Le nom du dossier d'installation contient des caractères interdits.
25001	Privilèges insuffisants pour installer Kaspersky Security 10.1.1 for Windows Server. Afin d'installer l'application, lancez l'Assistant d'installation avec les privilèges d'administrateur local.
25003	Impossible d'installer Kaspersky Security 10.1.1 for Windows Server sur des ordinateurs tournant sous cette version de Microsoft Windows. Veuillez lancer l'Assistant d'installation de l'application prévu pour la version 64 bits de Microsoft Windows.
25004	Une application incompatible a été détectée. Avant de poursuivre l'installation, supprimez les applications suivantes de l'ordinateur à protéger : <liste des applications incompatibles>.
25010	Le chemin d'accès indiqué ne peut être utilisé pour conserver des objets en quarantaine.
25011	Le nom du dossier de conservation des objets en quarantaine contient des caractères interdits.
26251	Echec du chargement de la DLL pour les Compteurs de performance.
26252	Echec du chargement de la DLL pour les Compteurs de performance.
27300	Impossible d'installer le pilote.
27301	Impossible de supprimer le pilote.
27302	Impossible d'installer le composant réseau. Le seuil maximum d'appareils de filtrage pris en charge a été atteint.
27303	Les bases antivirus sont introuvables.

Installation et suppression de l'application via Kaspersky Security Center

Cette section contient des informations générales sur l'installation de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center. Elle décrit également la procédure d'installation et de désinstallation de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center et les actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server.

Dans cette section

Informations générales sur l'installation via Kaspersky Security Center

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center à l'aide d'une tâche d'installation à distance.

Une fois que cette tâche a été exécutée, Kaspersky Security 10.1.1 for Windows Server est installé selon les mêmes paramètres sur plusieurs serveurs.

Vous pouvez rassembler les serveurs dans un groupe d'administration unique et créer une tâche de groupe pour l'installation de Kaspersky Security 10.1.1 for Windows Server sur les serveurs de ce groupe.

Vous pouvez créer une tâche d'installation à distance de Kaspersky Security 10.1.1 for Windows Server pour une sélection de serveurs qui n'appartiennent pas à un groupe d'administration. Lors de la création de cette tâche, vous devrez constituer la liste des serveurs distincts sur lesquels il faut installer Kaspersky Security 10.1.1 for Windows Server.

Le *Système d'aide de Kaspersky Security Center* contient des informations supplémentaires sur la tâche d'installation à distance.

Privilèges pour l'installation ou la désinstallation de Kaspersky Security 10.1.1 for Windows Server

Le compte utilisateur que vous spécifiez dans la tâche d'installation (de suppression) à distance doit appartenir au groupe d'administrateurs sur chacun des serveurs protégés dans tous les cas, sauf dans les situations suivantes.

- Les ordinateurs sur lesquels vous souhaitez installer Kaspersky Security 10.1.1 for Windows Server sont déjà dotés de l'Agent d'administration Kaspersky Security Center (quel que soit le domaine où se trouvent les ordinateurs et de leur appartenance à un domaine quelconque).

  Si l'Agent d'administration n'est pas encore installé sur les serveurs, vous pouvez l'installer en même temps que Kaspersky Security 10.1.1 for Windows Server à l'aide d'une tâche d'installation à distance. Avant d'installer l'Agent d'administration, assurez-vous que le compte utilisateur indiqué dans la tâche appartient au groupe d'administrateurs sur chacun des serveurs.

- Tous les ordinateurs sur lesquels vous souhaitez installer Kaspersky Security 10.1.1 for Windows Server se trouvent dans le même domaine que le Serveur d'administration et celui-ci est enregistré sous le compte Administrateur de domaine (**Domain Admin**) (si le compte jouit des privilèges d'administrateur local sur les ordinateurs du domaine).

Par défaut, la tâche d'installation à distance selon la méthode **Installation forcée** s'exécute sous le compte sous les privilèges duquel le Serveur d'administration fonctionne.

Dans les tâches de groupe, ainsi que dans les tâches pour une sélection d'ordinateurs, où l'installation (la suppression) forcée a été choisie, le compte utilisateur doit posséder les autorisations suivantes sur l'ordinateur client :

- autorisation pour l'exécution à distance des applications ;
- autorisations sur la ressource **Admin$** ;
- autorisation **Entrée en tant que service**.

Procédure d'installation de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center

Le Manuel d'implantation de Kaspersky Security Center contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

Si vous comptez administrer plus tard Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center, assurez-vous que les conditions suivantes sont remplies :

- Le plug-in d'administration (fichier \server\klcfginst.exe du kit de distribution de Kaspersky Security for Windows Server) est également installé sur le serveur sur lequel est installé le Serveur d'administration de Kaspersky Security Center.
- Sur les serveurs protégés, l'Agent d'administration de Kaspersky Security Center est installé. Si les serveurs protégés ne sont pas dotés de l'Agent d'administration de Kaspersky Security Center, vous pouvez l'installer en même temps que Kaspersky Security 10.1.1 for Windows Server via une tâche d'installation à distance.

Vous pouvez également réunir au préalable les serveurs dans un groupe d'administration afin de pouvoir ultérieurement administrer les paramètres de la protection à l'aide de stratégies ou des tâches de groupe de Kaspersky Security Center.

► *Pour installer Kaspersky Security 10.1.1 for Windows Server à l'aide d'une tâche d'installation à distance, procédez comme suit :*

1. Lancement de la console d'administration de Kaspersky Security Center
2. Dans Kaspersky Security Center, développez le nœud **Installation à distance** et, dans le nœud enfant **Paquets d'installation**, sélectionnez l'option **Créer un paquet d'installation pour une application Kaspersky Lab**.
3. Entrez le nom du paquet d'installation.
4. Spécifiez le fichier ks4ws.kud à partir du kit de distribution de Kaspersky Security 10.1.1 for Windows Server comme fichier du paquet d'installation.

   La fenêtre **Contrat de licence utilisateur final et Politique de confidentialité** s'ouvre.
5. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **les termes de ce Contrat de licence utilisateur final Politique de confidentialité décrivant la manipulation des données** afin de poursuivre l'installation.

   Vous devez accepter le Contrat de licence et la Politique de confidentialité.
6. Pour modifier la sélection des composants de Kaspersky Security 10.1.1 for Windows Server à installer (cf.Section « Modification de la sélection de composants et récupération de Kaspersky Security 10.1.1 for Windows Server » à la page 61) et les paramètres d'installation par défaut (cf. Section « Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer » à la page 40) dans le paquet d'installation :
   a. Dans Kaspersky Security Center, développez le nœud **Installation à distance**.
   b. Dans l'espace de travail du nœud enfant **Paquets d'installation**, ouvrez le menu contextuel du paquet d'installation créé pour Kaspersky Security 10.1.1 for Windows Server et l'option **Propriétés**.
   c. Dans la section **Configuration** de la fenêtre **Propriétés : <nom du paquet d'installation>**, réalisez les opérations suivantes :
      a. Dans le groupe de paramètres **Composants installés**, cochez les cases en regard des noms des composants de Kaspersky Security 10.1.1 for Windows Server que vous souhaitez installer.
      b. Pour désigner un répertoire de destination différent du répertoire sélectionné par défaut, indiquez le nom du dossier et son chemin d'accès dans le champ **Dossier de destination**.

         Le chemin d'accès au répertoire cible peut contenir des variables système. Si le répertoire indiqué n'existe pas sur le serveur, il sera créé.

c. Dans le groupe **Paramètres avancés d'installation**, définissez les valeurs suivantes :

- Réaliser l'analyse antivirus sur le serveur avant l'installation.
- Activer la protection en temps réel après l'installation de l'application.
- Ajouter les exclusions recommandées par Microsoft.
- Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions.

d. Si vous souhaitez importer les paramètres depuis le fichier de configuration créé dans la version antérieure de Kaspersky Security 10.1.1 for Windows Server, renseignez le fichier de configuration requis.

d. Dans la boîte de dialogue **Propriétés : <nom du paquet d'installation>**, cliquez sur le bouton **OK**.

7. Dans le nœud **Paquets d'installation**, créez une tâche pour installer à distance Kaspersky Security 10.1.1 for Windows Server sur les serveurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

   Le *Système d'aide de Kaspersky Security Center* contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.

8. Lancez la tâche d'installation à distance pour Kaspersky Security 10.1.1 for Windows Server.

Kaspersky Security 10.1.1 for Windows Server est installé sur les serveurs indiqués dans la tâche.

Actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server

Après l'installation de Kaspersky Security 10.1.1 for Windows Server, il est conseillé d'actualiser les bases de Kaspersky Security 10.1.1 for Windows Server sur les serveurs et de lancer l'analyse des zones critiques des serveurs si ceux-ci n'étaient pas dotés d'un logiciel antivirus avec Protection en temps réel active avant l'installation de Kaspersky Security 10.1.1 for Windows Server.

Si les serveurs sur lesquels vous avez installé Kaspersky Security 10.1.1 for Windows Server sont réunis dans un groupe d'administration de Kaspersky Security Center, vous pouvez exécuter ces tâches de la manière suivante :

1. Créez une tâche de mise à jour des bases de l'application pour le groupe de serveurs sur lesquels vous avez installé Kaspersky Security 10.1.1 for Windows Server. Désignez le Serveur d'administration Kaspersky Security Center comme source des mises à jour.
2. Créez une tâche de groupe d'analyse à la demande avec l'état Tâche d'analyse des zones critiques. Kaspersky Security Center évaluera l'état de la protection de chaque ordinateur du groupe sur la base des résultats de cette tâche et non pas sur la base de la tâche système Analyse des zones critiques.
3. Créez une stratégie pour le groupe de serveurs. Sous l'onglet **Tâches système** des propriétés de la stratégie créée, désactivez l'exécution programmée des tâches système d'analyse à la demande et de mise à jour des bases de l'application sur les serveurs du groupe d'administration.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security 10.1.1 for Windows Server.

Installation de la console d'application via Kaspersky Security Center

Le *Manuel d'implantation de Kaspersky Security Center* contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

► *Pour installer la console d'application à l'aide d'une tâche d'installation à distance, procédez comme suit :*

1. Dans la console d'administration de Kaspersky Security Center, développez le nœud **Installation à distance** et dans le nœud enfant **Paquets d'installation**, créez un nouveau paquet d'installation à partir du fichier client\setup.exe. Création d'un paquet d'installation :
   - Dans la fenêtre **Sélection du paquet de distribution pour l'installation**, sélectionnez le fichier client\setup.exe du dossier du kit de distribution de Kaspersky Security 10.1.1 for Windows Server et cochez la case **Copier les mises à jour du référentiel dans le paquet d'installation**.
   - Le cas échéant, modifiez la liste des composants à installer dans le champ **Paramètres de lancement du fichier exécutable (facultatif)** à l'aide de l'argument ADDLOCAL et modifiez le dossier cible.

     Par exemple, pour installer la console d'application seul dans le dossier C:\KasperskyConsole sans le fichier d'aide et la documentation, procédez comme suit :

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
     ```
2. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la console d'application sur les ordinateurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

   Le *Système d'aide de Kaspersky Security Center* contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.
3. Lancez la tâche créée d'installation à distance.

La console d'application est installée sur les ordinateurs désignés dans la tâche.

Désinstallation de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center

Si l'accès à l'administration de Kaspersky Security 10.1.1 for Windows Server sur les ordinateurs du réseau est protégé par un mot de passe, introduisez le mot de passe lors de la création de la tâche de suppression de plusieurs applications. Si la protection par mot de passe n'est pas gérée centralement par une stratégie de Kaspersky Security Center, Kaspersky Security 10.1.1 for Windows Server est supprimé sur les serveurs dont l'accès est protégé par mot de passe si le mot de passe saisi correspond à la valeur définie. Kaspersky Security 10.1.1 for Windows Server n'est pas désinstallé sur les autres ordinateurs.

► *Pour supprimer Kaspersky Security 10.1.1 for Windows Server, procédez comme suit dans la Console d'administration de Kaspersky Security Center :*

1. Dans la Console d'administration Kaspersky Security Center, créez et lancez une tâche de suppression de l'application.
2. Dans la tâche, sélectionnez la méthode de suppression (comme vous aviez choisi la méthode d'installation, cf. section précédente) et désignez le compte utilisateur sous les privilèges duquel le Serveur d'administration communiquera avec les serveurs. Vous pouvez désinstaller Kaspersky Security 10.1.1 for Windows Server uniquement selon les paramètres de désinstallation par défaut (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page 40).

Installation et suppression via les stratégies de groupe Active Directory

Cette section décrit l'installation et la désinstallation de Kaspersky Security 10.1.1 for Windows Server via des stratégies de groupe d'Active Directory. Elle fournit également des informations sur les actions requises après l'installation de Kaspersky Security 10.1.1 for Windows Server via des stratégies de groupe.

Dans cette section

Installation de Kaspersky Security 10.1.1 for Windows Server via des stratégies de groupe d'Active Directory

Vous pouvez installer Kaspersky Security 10.1.1 for Windows Server sur plusieurs serveurs à l'aide d'une stratégie de groupe Active Directory. Vous pouvez, de la même manière, installer la console d'application.

Les serveurs sur lesquels vous souhaitez installer Kaspersky Security 10.1.1 for Windows Server ou la console d'application doivent appartenir au même domaine et à la même unité d'organisation.

Les systèmes d'exploitation des serveurs sur lesquels vous souhaitez installer Kaspersky Security 10.1.1 for Windows Server à l'aide de la stratégie doivent tous être de la même version (32 ou 64 bits).

Vous devez posséder les autorisations d'administrateur de domaine.

Pour installer Kaspersky Security 10.1.1 for Windows Server, utilisez les paquets d'installation ks4ws_x86(x64).msi. Pour installer la console d'application, utilisez le paquet d'installation ks4wstools.msi.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

► *Pour installer Kaspersky Security 10.1.1 for Windows Server (ou la console d'application) :*

1. Enregistrez-le fichier msi du paquet d'installation de la version correspondante du système d'exploitation de Microsoft Windows (32 ou 64 bits) dans un dossier partagé sur le contrôleur de domaine.
2. Sur le contrôleur de domaine, créez une stratégie pour groupe auquel appartiennent les serveurs.
3. A l'aide du **Group Policy Object Editor**, créez un nouveau paquet d'installation dans le nœud **Configuration ordinateur**. Saisissez le chemin d'accès au fichier msi du paquet d'installation de Kaspersky Security 10.1.1 for Windows Server (de la console d'application) au format UNC (Universal Naming Convention).
4. Cochez la case **Toujours installer avec des droits élevés** du service Windows Installer aussi bien dans le nœud **Configuration ordinateur** que dans le nœud **Configuration utilisateur** du groupe sélectionné.
5. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Security 10.1.1 for Windows Server est installé sur les ordinateurs du groupe après leur redémarrage, avant d'entrer dans Microsoft Windows.

Actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server

Après l'installation de Kaspersky Security 10.1.1 for Windows Server sur les serveurs protégés, il est conseillé de procéder immédiatement à la mise à jour des bases de l'application et de lancer une analyse des zones critiques. Vous pouvez réaliser ces actions (cf. section "Actions à réaliser après l'installation de Kaspersky Security 10.1.1 for Windows Server" à la page 58) depuis la console de l'application.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security 10.1.1 for Windows Server.

Désinstallation de Kaspersky Security 10.1.1 for Windows Server via des stratégies de groupe d'Active Directory

Si vous avez installé Kaspersky Security 10.1.1 for Windows Server (ou la console d'application) sur les serveurs du groupe à l'aide de la stratégie de groupe Active Directory, vous pouvez utiliser cette stratégie pour désinstaller Kaspersky Security 10.1.1 for Windows Server (ou la console d'application).

La suppression de l'application n'est possible que selon les paramètres de suppression par défaut.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

Si l'accès à l'administration de l'application est protégé par un mot de passe, la suppression de Kaspersky Security 10.1.1 for Windows Server via des stratégies de groupe Active Directory est impossible.

► *Pour désinstaller Kaspersky Security 10.1.1 for Windows Server (ou la console d'application) :*

1. Sur le contrôleur de domaine, choisissez l'unité d'organisation reprenant les serveurs desquels vous souhaitez supprimer Kaspersky Security 10.1.1 for Windows Server ou la console d'application.
2. Sélectionnez la stratégie créée pour l'installation de Kaspersky Security 10.1.1 for Windows Server et dans **Editeur des stratégies de groupe**, nœud **Installation des logiciels** (**Configuration ordinateur** > **Configuration des programmes** > **Installation des logiciels**) ouvrez le menu contextuel du paquet d'installation de Kaspersky Security 10.1.1 for Windows Server (de la console d'application) et sélectionnez la commande **Toutes les tâches > Supprimer**.
3. Sélectionnez la méthode de suppression **Immediately uninstall the software from users and computers**.
4. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Security 10.1.1 for Windows Server est supprimé des serveurs après leur redémarrage et avant l'ouverture de session dans Microsoft Windows.

Vérification des fonctions de Kaspersky Security 10.1.1 for Windows Server. Utilisation du virus d'essai EICAR

Cette section décrit le virus de test EICAR et la procédure de vérification des fonctions Protection en temps réel et Analyse à la demande de Kaspersky Security 10.1.1 for Windows Server à l'aide du virus de test EICAR.

Dans cette section

A propos du virus d'essai EICAR

Le virus d'essai vise à vérifier le fonctionnement des logiciels antivirus. Il a été développé par l'organisation The European Institute for Computer Antivirus Research (EICAR).

Le virus d'essai n'est pas un virus et il ne contient pas un code logiciel qui pourrait nuire à votre ordinateur mais les logiciels antivirus de la majorité des éditeurs le considèrent comme une menace.

Le fichier qui contient le virus d'essai s'appelle eicar.com. Vous pouvez le télécharger depuis le site Internet du projet EICAR http://www.eicar.org/anti_virus_test_file.htm.

Avant d'enregistrer le fichier dans un répertoire sur le disque dur de l'ordinateur, assurez-vous que la Protection des fichiers en temps réel de ce répertoire est désactivée.

Le fichier eicar.com contient une ligne de texte. Pendant l'analyse, Kaspersky Security 10.1.1 for Windows Server découvre la menace test dans cette ligne de texte, attribue l'état **infecté** au fichier et le supprime. Les informations sur la menace découverte dans le fichier apparaissent dans la console d'application, dans le journal d'exécution de la tâche.

Vous pouvez également utiliser le fichier eicar.com afin de voir comment Kaspersky Security 10.1.1 for Windows Server désinfecte les objets infectés et comment il découvre les objets probablement infectés. Pour ce faire, ouvrez le fichier à l'aide d'un éditeur de texte, ajoutée au début de la ligne de texte un des préfixes repris au tableau ci-après et enregistrez le fichier sous un nouveau nom, par exemple eicar_cure.com.

Pour que Kaspersky Security 10.1.1 for Windows Server traite le fichier eicar.com avec un préfixe, dans la section des paramètres de sécurité **Protection des objets**, indiquez la valeur **Tous les objets** pour la tâche Protection des fichiers en temps réel de Kaspersky Security 10.1.1 for Windows Server et pour la tâche d'analyse à la demande.

Tableau 14. Préfixe des fichiers EICAR

Préfixe	Etat du fichier après l'analyse et l'action de Kaspersky Security 10.1.1 for Windows Server
Sans préfixe	Kaspersky Security 10.1.1 for Windows Server attribue l'état **Infecté** à l'objet et le supprime.
SUSP–	Kaspersky Security 10.1.1 for Windows Server attribue l'état **probablement infecté** à l'objet (découvert à l'aide de l'analyse heuristique) et le supprime (les objets probablement infectés ne sont pas désinfectés).
WARN–	Kaspersky Security 10.1.1 for Windows Server attribue l'état **probablement infecté** à l'objet (le code de l'objet correspond en partie à un code malveillant connu) et le supprime (les objets probablement infectés ne sont pas désinfectés).
CURE–	Kaspersky Security 10.1.1 for Windows Server attribue l'état **Infecté** à l'objet et le désinfecte. Si la désinfection a réussi, tout le texte du fichier est remplacé par le mot "CURE".

Test de la Protection en temps réel et de l'Analyse à la demande

Après l'installation de Kaspersky Security 10.1.1 for Windows Server, vous pouvez confirmer que Kaspersky Security 10.1.1 for Windows Server trouve les objets qui contiennent du code malveillant. Pour la vérification, vous pouvez utiliser un virus d'essai EICAR (cf. la section "A propos du virus d'essai EICAR" à la page 78).

► *Pour vérifier la fonction Protection en temps réel, procédez comme suit :*

1. Téléchargez le fichier eicar.com du site de EICAR http://www.eicar.org/anti_virus_test_file.htm. Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel ordinateur du réseau.

   Avant d'enregistrer le fichier dans un répertoire sur le disque de l'ordinateur, assurez-vous que la Protection des fichiers en temps réel de ce répertoire est désactivée.

2. Si vous souhaitez également vérifier le fonctionnement des notifications des utilisateurs du réseau, assurez-vous que le service Windows Messenger de Microsoft est activé sur le serveur protégé et sur l'ordinateur sur lequel vous avez enregistré le fichier eicar.com.
3. Ouvrez la console d'application.
4. Copiez le fichier eicar.com enregistré sur le disque local du serveur protégé selon une des méthodes suivantes :
   - Pour vérifier le fonctionnement des notifications via la fenêtre du service des terminaux, copiez le fichier eicar.com sur le serveur connecté à la console à l'aide du programme "Connexion au poste de travail distant" (Remote Desktop Connection).
   - Pour vérifier le fonctionnement des notifications via le service Windows Messenger, copiez le fichier eicar.com depuis l'ordinateur sur lequel vous l'avez enregistré via l'environnement de réseau de cet ordinateur.

La Protection des fichiers en temps réel fonctionne comme il se doit si les événements suivants se produisent :

- Le fichier eicar.com est supprimé du serveur protégé.
- Dans la console d'application, le journal d'exécution de la tâche a reçu l'état **Critique**. Le journal reprend une ligne d'information sur la menace contenue dans le fichier eicar.com. (Pour consulter le journal d'exécution de la tâche dans l'arborescence de la console d'application, développez le nœud **Protection en temps réel du serveur**, sélectionnez la tâche Protection des fichiers en temps réel et, dans le panneau de détails du nœud, cliquez sur le lien **Ouvrir le journal**).
  - Un message du service Windows Messenger sur l'ordinateur d'où vous avez copié le fichier (service de terminal dans la session terminal sur le serveur) dont le texte est : "`Kaspersky Security 10.1.1 for Windows Server a interdit l'accès à <chemin d'accès au fichier eicar.com sur l'ordinateur>\eicar.com sur l'ordinateur <nom réseau de l'ordinateur> à <heure de l'événement>. Cause : menace détectée. Virus : EICAR-Test-File. Nom d'utilisateur : <nom d'utilisateur>. Nom de l'ordinateur : <nom réseau de l'ordinateur d'où vous avez copié le fichier>.`

  Assurez-vous que le service Windows Messenger fonctionne sur l'ordinateur d'où vous avez copié le fichier eicar.com.

► *Pour vérifier la fonction Analyse à la demande, procédez comme suit :*

1. Téléchargez le fichier eicar.com du site Internet d'EICAR http://www.eicar.org/anti_virus_test_file.htm. Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel ordinateur du réseau.

   Avant d'enregistrer le fichier dans un répertoire sur le disque de l'ordinateur, assurez-vous que la Protection des fichiers en temps réel de ce répertoire est désactivée.

2. Ouvrez la console d'application.
3. Exécutez les actions suivantes :
   a. Dans l'arborescence de la console d'application, développez le nœud **Analyse à la demande**.
   b. Sélectionnez le nœud enfant **Analyse des zones critiques**.
   c. Sous l'onglet **Configuration de la zone d'analyse**, ouvrez le menu contextuel du nœud **Réseau**, puis choisissez **Ajouter un fichier de réseau**.
   d. Saisissez le chemin d'accès au fichier eicar.com sur l'ordinateur distant au format UNC (Universal Naming Convention).
   e. Cochez la case afin d'inclure le chemin de réseau dans la zone d'analyse.
   f. Lancez la tâche Analyse des zones critiques.

L'analyse à la demande fonctionne correctement si les conditions suivantes sont remplies :

- Le fichier eicar.com est supprimé du disque dur de l'ordinateur.
- Dans la console d'application, le journal d'exécution de la tâche a reçu l'état **Critique** ; le journal d'exécution de la tâche Analyse des zones critiques reprend une ligne d'information sur la menace dans le fichier eicar.com. (Pour consulter le journal d'exécution de la tâche dans l'arborescence de la console d'application, développez le nœud **Analyse à la demande**, sélectionnez la tâche Analyse des zones critiques et dans le panneau de détails du nœud, cliquez sur le lien **Ouvrir le journal**).

Interface de l'application

Vous pouvez contrôler Kaspersky Security 10.1.1 for Windows Server via la console d'application locale et le plug-in d'administration. Les actions avec la console d'application locale sont décrites dans le *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*. L'interface de la console d'administration de Kaspersky Security Center sert à effectuer des actions avec le plug-in d'administration. L'*aide de Kaspersky Security Center* fournit des informations détaillées sur l'interface de Kaspersky Security Center.

Licence de l'application

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

Contenu du chapitre

A propos du Contrat de licence utilisateur final

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

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

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final, en utilisant les moyens suivants :

- Lors de l'installation de Kaspersky Security 10.1.1 for Windows Server
- En lisant le document license.txt. Ce document est inclus dans le kit de distribution de l'application.

Vous acceptez les conditions du Contrat de licence utilisateur final, 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

Un *certificat de licence* est un document qui vous est remis avec le fichier clé ou le code d'activation (le cas échéant).

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

- Numéro de la commande ;
- Informations sur l'utilisateur qui a obtenu la licence ;
- Informations sur l'application qui peut être activée à l'aide de la licence octroyée ;
- Limite du nombre d'unités sous licence (par exemple, les appareils sur lesquels l'application peut être utilisée sous les termes de la licence fournie) ;
- Date de début de validité de la licence ;
- Date d'expiration de la licence ou dispositions 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.

Une licence *commerciale* est une 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 l'application n'est plus disponible). Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky Security 10.1.1 for Windows Server, il faut renouveler la validité de la licence commerciale.

La fonctionnalité disponible de l'application dans le cadre de la licence commerciale dépend du choix du produit. Le produit sélectionné est indiqué dans le certificat de licence (cf. section "A propos du certificat de licence" à la page 84). Vous trouverez des informations sur les produits disponibles sur le site Internet de Kaspersky Lab à l'adresse https://www.kaspersky.fr/small-to-medium-business-security/windows-server-security.

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.

Assurez-vous que la clé additionnelle que vous ajoutez expire après la clé active.

Vous ne pouvez pas utiliser d'abonnement comme clé additionnelle.

A propos de l'abonnement

Un *abonnement* donne le droit d'utiliser l'application en respectant les paramètres sélectionnés (date de fin de l'abonnement, nombre d'appareils protégés). Un abonnement Kaspersky Security 10.1.1 for Windows Server peut être enregistré auprès du fournisseur de services (par exemple, votre fournisseur d'accès à 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.

Un abonnement peut être *limité* ou *illimité*.

L'abonnement limité est soumis à une licence réduit et n'est pas renouvelé automatiquement.

L'abonnement illimité est renouvelé automatiquement sans votre intervention après le paiement en temps opportuns et il ne possède pas de date d'échéance fixe.

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

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

A propos du code d'activation

Un *code d'activation* est une séquence unique de 20 lettres et nombres. Vous devez entrer un code d'activation afin d'ajouter une clé d'activation de Kaspersky Security 10.1.1 for Windows Server. Vous recevez le code d'activation à l'adresse email indiquée lors de l'achat de Kaspersky Security 10.1.1 for Windows Server.

Pour activer l'application avec un code d'activation, vous avez besoin d'un accès à Internet afin de vous connecter aux serveurs d'activation de Kaspersky Lab.

Si vous avez perdu votre code d'activation après avoir installé l'application, vous pouvez le récupérer. Vous pouvez avoir besoin du code d'activation pour enregistrer un compte d'entreprise Kaspersky par exemple. Pour récupérer votre code d'activation, contactez le Support Technique de Kaspersky Lab.

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 en utilisant un fichier clé. 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 utilisateur final. Si la clé est bloquée, il faudra en ajouter une autre pour pouvoir utiliser l'application.

Une clé peut être active ou additionnelle.

Clé active est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour 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.

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.

Vous recevez un fichier clé à l'adresse email indiquée lors de l'achat de Kaspersky Security 10.1.1 for Windows Server.

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 https://support.kaspersky.com/fr.
- Obtenir un fichier clé sur le site Internet de Kaspersky Lab sur la base du code d'activation en votre possession.

A propos de la collecte des données

Le contrat de licence de Kaspersky Security 10.1.1 for Windows Server, et plus spécifiquement le paragraphe intitulé "Conditions du traitement des données", spécifie les conditions, la responsabilité et la procédure d'envoi et de traitement des données indiquées dans ce Guide. Avant d'accepter le contrat de licence, révisez attentivement ses conditions, ainsi que tous les documents liés au contrat de licence.

Les données que vous envoyez à Kaspersky Lab lorsque vous utilisez l'application sont protégées et traitées conformément à la Politique de confidentialité disponible à l'adresse www.kaspersky.com/Products-and-Services-Privacy-Policy.

En acceptant les conditions du contrat de licence, vous acceptez d'envoyer automatiquement les données suivantes à Kaspersky Lab :

- Pour prendre en charge le mécanisme de réception de mises à jour : informations sur l'application installée et son activation : identifiant de l'application en cours d'installation et version complète, y compris le numéro de version, le type et l'identifiant de licence, identifiant d'installation, identifiant unique de la tâche de mise à jour.
- Pour accéder aux articles de la base de connaissances en cas d'erreurs de l'application (service de redirection) : informations sur le type d'application et de lien, notamment le nom, l'environnement local et le numéro de version complète de l'application, type de lien de redirection et identifiant d'erreur.
- Pour gérer les confirmations du traitement des données : informations sur l'état d'acceptation des contrats de licence et des autres documents, qui stipulent les conditions de transfert des données : identifiant et version du contrat de licence ou autre document, comprenant les conditions acceptées ou refusées du traitement des données, attribut désignant l'action de l'utilisateur (confirmation ou rappel de l'acceptation des conditions) ; date et heure des changements d'état de l'acceptation des conditions de traitement des données.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final, en utilisant les moyens suivants :

- Pendant l'installation de l'application, l'assistant d'installation de Kaspersky Security 10.1.1 for Windows Server affiche le texte complet du contrat de licence lors de la demande d'acceptation des conditions de ce contrat.
- A tout moment dans le fichier TXT (license.txt) contenant le texte intégral du Contrat de licence. Le fichier est inclut dans le kit de distribution de Kaspersky Security 10.1.1 for Windows Server, accompagné des fichiers d'installation de l'application.

Traitement des données locales

Tout en exécutant les fonctions principales de l'application décrites dans ce Guide, Kaspersky Security 10.1.1 for Windows Server traite et stocke en local une séquence de données sur le serveur protégé :

- informations sur les fichiers analysés et les objets détectés, par exemple les noms et attributs des fichiers traités et les chemins d'accès complets à ces derniers sur les supports analysés, types de fichiers, actions effectuées sur les fichiers analysés, comptes des utilisateurs effectuant des actions sur le réseau protégé ou sur le serveur protégé, noms et données sur les périphériques analysés, informations sur les processus exécutés sur le système, sommes de contrôle, horodatages, attributs de certificat numérique, données sur les scripts exécutés ;
- informations sur l'activité et les paramètres du système d'exploitation, par exemple, paramètres du pare-feu Windows, entrées du journal des événements Windows, noms des comptes utilisateur, démarrages des fichiers exécutables démarrés et types, noms, sommes de contrôle et attributs de ces fichiers ;
- informations sur l'activité du réseau local, y compris les adresses IP des ordinateurs clients bloqués ;
- Informations sur les adresses Internet analysées, par exemple les adresses URL et IP ou le téléchargement a démarré, page Internet de téléchargement, identifiant du protocole et numéro du port de connexion, attribut de nocivité d'une adresse et taille de fichier, ses sommes de contrôle (MD5, SHA-256), informations sur un processus qui a téléchargé le fichier (sommes de contrôle MD5, SHA-256), attribut qui indique la détection effectuée pendant le débogage, sommes de contrôle des fichiers analysés (MD5), identification du protocole de connexion, numéro de port utilisé, adresse URL analysée, nom d'un fichier analysé, données du certificat Internet.

Kaspersky Security 10.1.1 for Windows Server traite et stocke les données, ce qui fait partie de la fonctionnalité de base de l'application, notamment pour enregistrer dans le journal les événements de l'application et recevoir des données de diagnostic. Les données traitées en local sont protégées conformément aux paramètres configurés et appliqués de l'application.

Kaspersky Security 10.1.1 for Windows Server vous permet de configurer le niveau de protection des données traitées en local : vous pouvez modifier les droits d'accès des utilisateurs aux données du processus, modifier les périodes de conservation de ces données, désactiver entièrement ou partiellement la fonctionnalité qui implique l'enregistrement des événements dans le journal des données et modifier le chemin et les attributs du dossier sur le lecteur où les données sont enregistrées.

Vous trouverez des informations détaillées sur la configuration des fonctionnalités de l'application qui impliquent le traitement des données et les paramètres par défaut du stockage des données traitées dans les sections correspondantes de ce Guide.

Par défaut, toutes les données stockées sur un ordinateur local sont supprimées après la désinstallation Kaspersky Security 10.1.1 for Windows Server sauf les fichiers avec des informations de diagnostics (fichiers de trace et fichiers dump). Vous devez supprimer manuellement ces fichiers. Vous trouverez des informations détaillées sur la configuration des processus de diagnostic dans les sections correspondantes de ce guide.

Activation de l'application à l'aide d'une clé

Vous pouvez activer Kaspersky Security 10.1.1 for Windows Server en appliquant une clé.

Si Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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 activées dans Kaspersky Security 10.1.1 for Windows Server et que vous ajoutez une nouvelle clé en tant que clé active, cette nouvelle clé remplace la clé active antérieure et la clé additionnelle n'est pas supprimée.

► *Pour activer Kaspersky Security 10.1.1 for Windows Server :*

1. Dans l'arborescence de la console d'application, développez le nœud **Licence**.
2. Dans le panneau de détails du nœud **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.

   Vous pouvez aussi ajouter une clé à titre complémentaire. Pour ce faire, cochez la case **Utiliser en tant que clé additionnelle**.

4. Cliquez sur le bouton **OK**.

La clé sélectionnée sera appliquée. L'information sur la clé ajoutée s'affiche dans le panneau des résultats du nœud **Licence**.

Consultation des informations sur la licence active

Consultation des informations sur la licence

Les informations sur la licence active s'affichent dans le panneau de détails du nœud **Kaspersky Security** de la console d'application. L'état de la clé peut prendre une des valeurs suivantes :

- **Vérification de l'état de la clé** : Kaspersky Security 10.1.1 for Windows Server analyse le fichier clé ajouté et le code d'activation appliqué, puis attend une réponse concernant l'état actuel de la clé.
- **Date d'expiration de la licence** : Kaspersky Security 10.1.1 for Windows Server est actif jusqu'à la date et l'heure indiquées. L'état de la clé est mis en évidence en jaune dans les cas suivants :
  - Il reste 14 jours avant l'expiration de la licence et aucune clé additionnelle ou code d'activation 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 10.1.1 for Windows Server n'a pas été activé car aucune clé n'a été ajoutée ou aucun code d'activation n'a été appliqué. L'état est mis en évidence en rouge.
- **Licence expirée** : Kaspersky Security 10.1.1 for Windows Server n'est pas actif car la licence a expiré. L'état est mis en évidence en rouge.
- **Violation du Contrat de licence utilisateur final** : Kaspersky Security 10.1.1 for Windows Server 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 83). L'état est mis en évidence en rouge.
- **Clé placée dans 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 d'une clé par des tiers pour l'activation illicite d'une application. L'état est mis en évidence en rouge.
- **Abonnement suspendu** : l'abonnement a été temporairement suspendu. L'état est mis en évidence en rouge. Vous pouvez rétablir l'abonnement à tout moment.

Consultation des informations sur la licence active

► *Pour voir les informations sur la licence valide,*

Dans l'arborescence de la console d'application, développez le nœud **Licence**.

Les informations générales relatives à la licence active apparaissent dans le panneau de détails du nœud **Licence** (cf. tableau ci-dessous).

Tableau 15. Informations générales sur la licence dans le nœud 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. Les informations de la colonne Etat de l'activation dans le panneau d'administration du nœud 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'application 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 de détails du nœud. • **Erreur d'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 de la tâche.
Clé	Numéro de la clé que vous avez utilisée pour activer l'application.
Type de licence	Type de licence : commerciale.
Date d'expiration	Date de fin de validité de la licence associée à la clé active.
Etat du code d'activation ou de la clé	Etat du code d'activation ou de la clé : actif ou complémentaire.

► *Pour consulter les informations détaillées sur la licence.*

Dans le panneau des résultats du nœud **Licence** dans le menu contextuel de la ligne des informations sur la licence que vous voulez examiner, choisissez l'option **Propriétés**.

Dans la fenêtre **Propriétés : <Etat du code d'activation ou de la clé>**, l'onglet **Général** reprend les détails relatifs à la licence active et 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 10.1.1 for Windows Server (cf. tableau ci-dessous).

Tableau 16. Détails sur la licence dans la fenêtre Propriétés <Etat du code d'activation ou de la 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.
Expire dans (jours)	Nombre de jours restants avant la date de fin de validité de la licence associée selon la clé active.

Champ	Description
Date d'expiration	Date de fin de validité de la licence associée à la clé active. Si vous activez l'application selon un abonnement illimité, la valeur *Illimité* apparaît dans le champ. Si Kaspersky Security 10.1.1 for Windows Server ne parvient pas à déterminer la date de fin de validité de la licence, la valeur *Inconnue* apparaît dans le champ.
Application	Le nom de l'application pour laquelle une clé ou un code d'activation a été ajouté.
Restrictions d'utilisation de la clé	Restriction prévue sur l'utilisation de la clé (le cas échéant).
Accès à l'assistance 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 a été achetée.

Restriction des fonctions à l'expiration de la licence

Quand la licence active arrive à son échéance, les restrictions suivantes sont appliquées aux composants fonctionnels :

- Toutes les tâches sont arrêtées, à l'exception des tâches Protection des fichiers en temps réel, Analyse à la demande et Vérification de l'intégrité de l'application.
- Lancement de toutes les tâches, à l'exception des tâches Protection en temps réel, Analyse à la demande et Vérification de l'intégrité de l'application. Ces tâches sont toujours opérationnelles, mais font intervenir les anciennes bases antivirus.
- La fonction Protection contre les exploits est limitée :
  - Les processus sont protégés jusqu'à leur redémarrage.
  - Il est impossible d'ajouter de nouveaux processus à la zone de protection.

Les autres fonctions (stockage, journaux, informations de diagnostic) sont toujours disponibles.

Renouvellement de la licence

Par défaut Kaspersky Security 10.1.1 for Windows Server signale l'échéance prochaine de la validité de la licence 14 jours avant la date d'expiration de la licence. Dans ce cas, l'état **Date d'expiration de la licence** dans le panneau de détails du nœud **Kaspersky Security** est mis en évidence en jaune.

Vous pouvez renouveler une licence avant son expiration grâce à l'ajout d'un code d'activation ou d'une clé additionnelle. 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 d'application, développez le nœud **Licence**.
3. Dans le panneau de détails du nœud **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.
     c. Cochez la case **Utiliser en tant que clé additionnelle**.
   - Si vous souhaitez renouveler la licence à l'aide d'un code d'activation :
     a. Cliquez sur le lien **Ajouter un code d'activation**.
     b. Dans la fenêtre qui s'ouvre, saisissez le code d'activation.
     c. Cochez la case **Utiliser en tant que clé additionnelle**.

   L'application d'un code d'activation requiert une connexion à Internet.
4. Cliquez sur le bouton **OK**.

La clé additionnelle ou le code d'activation est ajouté et est appliqué automatiquement à l'expiration de la clé ou du code d'activation de Kaspersky Security 10.1.1 for Windows Server utilisé.

Suppression d'une clé

Vous pouvez supprimer une clé que vous avez ajoutée.

Si Kaspersky Security 10.1.1 for Windows Server possède une clé additionnelle et que vous supprimez la clé active, la clé additionnelle devient automatiquement la clé active.

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

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

1. Dans l'arborescence de la console d'application, sélectionnez le nœud **Licence**.
2. Dans le tableau contenant les informations relatives aux clés ajoutées qui figure dans le panneau de détails du nœud **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.

Lancement et arrêt du plug-in Kaspersky Security 10.1.1 for Windows Server

Cette section contient les informations sur le lancement et l'arrêt du plug-in de Kaspersky Security 10.1.1 for Windows Server, et du service Kaspersky Security.

Contenu du chapitre

Lancement et arrêt du plug-in de Kaspersky Security 10.1.1 for Windows Server

Aucune action supplémentaire n'est requise pour lancer le plug-in de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center. Après l'installation du plug-in sur l'ordinateur de l'administrateur, le lancement s'opère en même temps que le lancement de Kaspersky Security Center. Vous trouverez toutes les informations détaillées sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center.*

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 dans lesquels les tâches Protection en temps réel du serveur, Contrôle de l'activité locale, Protection des stockages réseau, Analyse à la demande et Mise à jour sont exécutées.

Le lancement de Kaspersky Security 10.1.1 for Windows Server marque par défaut le lancement des tâches Protection des fichiers en temps réel, Monitoring des scripts (si ce module est installé) et Analyse au démarrage du système d'exploitation 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 relancé le Service Kaspersky Security, l'application lance automatiquement uniquement les tâches dont la planification reprend la fréquence **Au lancement de l'application**, alors que les autres tâches doivent être lancées manuellement.

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

Vous pouvez lancer et arrêter Kaspersky Security 10.1.1 for Windows Server uniquement si vous faites partie du groupe d'administrateurs sur le serveur protégé.

► *Pour arrêter ou lancer l'application via la console d'application, procédez comme suit :*

1. Dans l'arborescence de la console d'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Choisissez une des commandes suivantes :
   - **Arrêter le service**
   - **Lancer le service**

Le Service Kaspersky Security sera lancé ou arrêté.

Autorisations d'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server et des services Windows enregistrés par l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

Contenu du chapitre

A propos des autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server

Par défaut, l'accès à toutes les fonctions de Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server et aussi aux utilisateurs du groupe SYSTEM.

Les utilisateurs qui ont accès à la fonction **Modifier** les privilèges de Kaspersky Security 10.1.1 for Windows Server peuvent offrir l'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server, il ne pourra pas ouvrir la console d'application.

Vous pouvez attribuer à l'utilisateur ou au groupe d'utilisateurs un des niveaux prédéfinis d'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server :

- **Contrôle complet** : accès à toutes les fonctions de l'application : consultation et modification des paramètres généraux de fonctionnement de Kaspersky Security 10.1.1 for Windows Server, des paramètres des composants, des autorisations des utilisateurs de Kaspersky Security 10.1.1 for Windows Server ainsi que la consultation des statistiques de Kaspersky Security 10.1.1 for Windows Server.
- **Modifier** : accès à l'ensemble des fonctions de l'application, sauf la modification des autorisations des utilisateurs : possibilité de consulter et de modifier les paramètres généraux et les paramètres des composants de Kaspersky Security 10.1.1 for Windows Server.
- **Lire** : consultation des paramètres généraux de Kaspersky Security 10.1.1 for Windows Server, des paramètres des composants de Kaspersky Security 10.1.1 for Windows Server, des statistiques de Kaspersky Security 10.1.1 for Windows Server et des autorisations d'utilisateur de Kaspersky Security 10.1.1 for Windows Server.

Vous pouvez également configurer les autorisations d'accès avancé (cf. section "Configuration des autorisations d'accès à Kaspersky Security 10.1.1 for Windows Server et au service Kaspersky Security" à la page 101) es : autoriser ou interdire l'accès aux fonctions spécifiques de Kaspersky Security 10.1.1 for Windows Server.

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 17. A propos des autorisations d'accès pour les fonctions de Kaspersky Security 10.1.1 for Windows Server

Autorisations d'accès	Description
Administration des tâches	Lancement/arrêt/suspension/reprise d'une tâche de Kaspersky Security 10.1.1 for Windows Server.
Création et suppression des tâches Analyse à la demande	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilités : • Importation des paramètres de Kaspersky Security 10.1.1 for Windows Server depuis un fichier de configuration. • Modifiez les paramètres de l'application.
Lire les paramètres	Possibilités : • Consultation des paramètres généraux de Kaspersky Security 10.1.1 for Windows Server et des paramètres des tâches. • Exportation des paramètres de Kaspersky Security 10.1.1 for Windows Server vers un fichier de configuration. • Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Gérer les stockages	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 d'Anti-Virus dans les journaux d'exécution des tâches et le journal d'audit système.
Consultation des statistiques	Consultation des statistiques de chacune des tâches de Kaspersky Security 10.1.1 for Windows Server.
Licence de l'application	Vous pouvez activer ou désactiver Kaspersky Security 10.1.1 for Windows Server.
Suppression de l'application	Fonction de désinstallation de Kaspersky Security 10.1.1 for Windows Server.
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Security 10.1.1 for Windows Server 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 pour les fonctions de Kaspersky Security 10.1.1 for Windows Server.

A propos des autorisations d'administration du Service Kaspersky Security

Lors de l'installation, Kaspersky Security 10.1.1 for Windows Server enregistre le Service Kaspersky Security (KAVFS) dans Windows et autorise en interne le lancement des composants au lancement 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 d'application ou depuis le plug-in d'administration.

Par défaut, l'accès à l'administration du Service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe "Administrateurs" 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.

Il est impossible de supprimer le compte utilisateur SYSTEM ou de modifier les autorisations de ce compte. En cas de modification des autorisations du compte utilisateur SYSTEM, les autorisations maximales sont rétablies pour ce compte lors de l'enregistrement des modifications.

Les utilisateurs qui disposent d'un accès aux fonctions du niveau (cf. section "A propos des autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server" à la page 96) Modification des autorisations peuvent octroyer l'accès à l'administration du Service Kaspersky Security à d'autres utilisateurs enregistrés sur le serveur protégé ou appartenant au domaine.

Vous pouvez attribuer à l'utilisateur ou à un groupe d'utilisateurs de Kaspersky Security 10.1.1 for Windows Server un des niveaux prédéfinis d'administration du Service Kaspersky Security :

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

Vous pouvez également réaliser une configuration étendue des autorisations d'accès : autoriser ou interdire l'accès à des fonctions particulières de Kaspersky Security 10.1.1 for Windows Server (voir 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 18. Restriction des autorisations d'accès pour les fonctions de Kaspersky Security 10.1.1 for Windows Server

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

Enregistrement du Service Kaspersky Security

La technologie *Protected Process Light* (également appelée "PPL") fait en sorte que le système d'exploitation charge uniquement les services et les processus de confiance. Pour qu'un service puisse fonctionner comme un service protégé, un pilote *à lancement anticipé anti-application malveillante* doit être installé sur le serveur protégé.

Lorsqu'un processus est démarré en tant que PPL, il ne peut être administré par un utilisateur, quels que soient les privilèges accordés à ce dernier. L'enregistrement du Service Kaspersky Security comme PPL avec le pilote ELAM est prise en charge sur les systèmes d'exploitation Microsoft Windows Server 2016 et plus. Si vous installez Kaspersky Security 10.1.1 for Windows Server sur un serveur exécutant un système d'exploitation prenant en charge la technologie PPL, la gestion des privilèges pour le Service Kaspersky Security (KAVFS) ne sera pas disponible.

Un pilote *à lancement anticipé anti-application malveillante* (également appelé "ELAM") fournit une protection aux ordinateurs de votre réseau lors de leur démarrage et avant l'initialisation des pilotes tiers.

Le pilote ELAM est automatiquement installé lors de l'installation de Kaspersky Security 10.1.1 for Windows Server et sert à enregistrer le Service Kaspersky Security comme PPL lors du démarrage du système d'exploitation. Lorsque le Service Kaspersky Security (kavfs.exe) est démarré en tant que processus protégé par le système, d'autres processus non protégés sur le système ne peuvent pas injecter de threads, écrire dans la mémoire virtuelle du processus protégé ou arrêter le service.

Le Service Kaspersky Security démarre l'ensemble des tâches enfants comme des PPL.

Remarque : vous pouvez utiliser le protocole TLS dans la configuration de la tâche Protection du trafic uniquement sur les serveurs fonctionnant sous le système d'exploitation Microsoft Windows Server 2016 ou plus.

A propos des autorisations d'accès au Service Kaspersky Security Management

Vous pouvez passer en revue la liste des services de Kaspersky Security 10.1.1 for Windows Server.

Lors de l'installation, Kaspersky Security 10.1.1 for Windows Server enregistre le Service Kaspersky Security Management (KAVFSGT). Pour administrer l'application via la console d'application installée sur un autre ordinateur, il faut que le compte sous les autorisations duquel la connexion à Kaspersky Security 10.1.1 for Windows Server s'opère possède un accès complet au service Kaspersky Security Management sur le serveur protégé.

Par défaut, l'accès au service Kaspersky Security Management 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 10.1.1 for Windows Server.

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

Il est impossible d'autoriser ou d'interdire l'accès de l'utilisateur au Service Kaspersky Security Management en configurant Kaspersky Security 10.1.1 for Windows Server.

Vous pouvez vous connecter à Kaspersky Security 10.1.1 for Windows Server 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 Kaspersky Security 10.1.1 for Windows Server et au service Kaspersky Security

Vous pouvez modifier la liste des utilisateurs et groupes d'utilisateurs ayant accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server 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 d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Complémentaire**, exécutez une des actions suivantes :
   - Choisissez l'option **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs ayant accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server.
   - Choisissez l'option **Autorisations d'accès de l'utilisateur pour l'administration du service Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du service Kaspersky Security.

     La fenêtre de groupe **Autorisations pour Kaspersky Security 10.1.1 for Windows Server** s'ouvre.
4. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Pour ajouter un utilisateur ou un groupe à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez octroyer 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**.
5. Cliquez sur le bouton **Appliquer**.

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

► *Pour modifier les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server ou du Service Kaspersky Security d'un utilisateur ou d'un groupe d'utilisateurs, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Complémentaire**, exécutez une des actions suivantes :
   - Choisissez l'option **Modifier les droits de l'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 10.1.1 for Windows Server.
   - Choisissez l'option **Modifier les droits d'utilisateurs pour l'administration du Service Kaspersky Security** 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 de groupe **Autorisations pour Kaspersky Security** s'ouvre.
4. 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.
5. 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 10.1.1 for Windows Server ou du Service Kaspersky Security.
   - **Lire** :
     - Autorisations suivantes sur l'administration de Kaspersky Security 10.1.1 for Windows Server : **Récupérer les statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lire les privilèges**.
     - Autorisations suivantes pour l'administration du service Kaspersky Security : **Lire les paramètres du service**, **Solliciter l'état du service auprès du Gestionnaire de contrôle des services**, **Solliciter le statut auprès du service**, **Lire la liste des services dépendants**, **Lire les privilèges**.

- **Modifier** :
  - Toutes les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server, à l'exception de **Modifier les privilèges**.
  - Autorisations suivantes sur l'administration du service Kaspersky Security : **Modifier les 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**.

6. Si vous souhaitez réaliser une configuration étendue 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 10.1.1 for Windows Server** qui s'ouvre, sélectionnez l'utilisateur ou le groupe requis.
   b. Cliquez sur le bouton **Modifier**.
   c. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).
   d. 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.
   e. Cliquez sur le bouton **OK**.
   f. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Security 10.1.1 for Windows Server**, cliquez sur **OK**.
7. Dans la fenêtre de groupe **Autorisations pour Kaspersky Security**, cliquez sur le bouton **Appliquer**.

Les autorisations d'administration de Kaspersky Security 10.1.1 for Windows Server ou du Service Kaspersky Security configurées sont enregistrées.

Accès protégé par mot de passe aux fonctions de Kaspersky Security 10.1.1 for Windows Server

Vous pouvez limiter l'accès à l'administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs (cf. section "Autorisations d'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server" à la page 96). Vous pouvez renforcer la protection de l'accès à l'exécution des opérations critiques grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Security 10.1.1 for Windows Server.

Kaspersky Security 10.1.1 for Windows Server requiert alors la saisie du mot de passe lors des tentatives d'accès aux fonctions suivantes de l'application :

- connexion à la console d'application ;
- désinstallation de Kaspersky Security 10.1.1 for Windows Server ;
- modification des composants de Kaspersky Security 10.1.1 for Windows Server;
- exécution des commandes de la ligne de commande.

L'interface de Kaspersky Security 10.1.1 for Windows Server masque le mot de passe désigné à l'écran. Kaspersky Security 10.1.1 for Windows Server conserve le mot de passe spécifié sous la forme d'une somme de contrôle calculée à la création du mot de passe.

Vous pouvez exporter et importer les paramètres d'une application protégée par un mot de passe. Le fichier de configuration obtenu à l'issue de l'exportation des paramètres de l'application protégée contient la valeur de la somme de contrôle du mot de passe et la valeur du modificateur utilisé pour l'extension de la ligne du mot de passe.

Ne modifiez pas la valeur de la somme de contrôle ou du modificateur dans le fichier de configuration. L'importation d'une configuration protégée par mot de passe qui a été modifiée manuellement peut entraîner le blocage complet de l'accès à l'application.

► *Pour protéger l'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**. Développez le groupe d'administration reprenant les serveurs pour lesquels vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres d'une stratégie pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez **<Nom de la stratégie> > Propriétés**.
   - Si vous souhaitez configurer les paramètres de l'application (cf. section "**Configuration des tâches locales dans la fenêtre Paramètres de l'application de Kaspersky Security Center**" à la page 123) pour un seul serveur, ouvrez les paramètres requis dans la fenêtre **Paramètres de l'application** de Kaspersky Security Center.
3. Dans le groupe **Sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Paramètres de sécurité** s'ouvre.
4. Dans le groupe **Paramètres de protection par mot de passe**, cochez la case **Utiliser la protection par mot de passe**.

   Les champs **Mot de passe** et **Confirmer mot de passe** deviennent actifs.
5. Saisissez dans le champ **Mot de passe** le mot de passe que vous voulez utiliser pour protéger l'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server.
6. Dans le champ **Confirmer mot de passe**, saisissez à nouveau le mot de passe.
7. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés. Kaspersky Security 10.1.1 for Windows Server requiert la saisie du mot de passe défini pour accéder aux fonctions protégées.

Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pouvez plus contrôler l'application. Il devient également impossible de désinstaller l'application depuis le serveur protégé.

Vous pouvez modifier ou annuler le mot de passe défini dans les paramètres de l'application à tout moment.

► *Pour réinitialiser le mot de passe,*

décochez la case **Utiliser la protection par mot de passe** dans les paramètres de la stratégie ou de l'application.

La protection par mot de passe sera désactivée. Kaspersky Security 10.1.1 for Windows Server supprime la somme de contrôle de l'ancien mot de passe dans les paramètres de l'application.

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 protégé, procédez comme suit :*

1. Sur le serveur protégé administré tournant sous Microsoft Windows Server, sélectionnez **Démarrer > Panneau de configuration > Sécurité > Pare-feu Windows.**
2. Dans la fenêtre **Paramètres du pare-feu Windows**, sélectionnez **Modifier les paramètres**.
3. Sous 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 dossier que vous avez indiqué en tant que dossier de destination lors de l'installation de la console d'application.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres du pare-feu Windows**.

Les connexions réseau pour le service Kaspersky Security Management sont alors autorisées sur le serveur protégé.

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 10.1.1 for Windows Server sur plusieurs serveurs.

Contenu du chapitre

A propos des stratégies

Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs serveurs sur lesquels Kaspersky Security 10.1.1 for Windows Server est installé.

Une stratégie applique les paramètres de Kaspersky Security 10.1.1 for Windows Server, 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 *actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Security 10.1.1 for Windows Server. Vous pouvez les consulter dans la console d'application 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 10.1.1 for Windows Server applique aux ordinateurs locaux les valeurs des paramètres en regard desquels vous avez sélectionné l'icône 🔒 dans les propriétés de la stratégie au lieu de la valeur des paramètres en vigueur 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 10.1.1 for Windows Server.

Si une stratégie est active, les paramètres dans la console d'application qui sont accompagnés de l'icône 🔒 dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres (accompagnés de l'icône 🔓 dans la stratégie) peuvent être modifiées dans la console d'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône 🔒 empêchent également la modification des paramètres dans Kaspersky Security Center pour un ordinateur depuis la fenêtre **Propriétés : <Nom de l'ordinateur>**.

Les paramètres configurés et transmis à l'ordinateur local à l'aide de la stratégie active sont enregistrés dans les paramètres des tâches locales après la désactivation de la stratégie active.

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 des tâches de protection en temps réel des serveurs dans les boîtes de dialogue 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 des tâches de protection en temps réel des serveurs, les paramètres généraux de Kaspersky Security 10.1.1 for Windows Server, les paramètres de la quarantaine et les paramètres de la Sauvegarde, le niveau de détail des journaux d'exécution de la tâche ainsi que les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Security 10.1.1 for Windows Server.

► *Pour créer une stratégie pour un groupe de serveurs sur lesquels Kaspersky Security 10.1.1 for Windows Server est installé, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, déployez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration contenant les serveurs pour lesquels vous souhaitez créer une stratégie.
2. Dans le panneau de détails du groupe d'administration sélectionné, choisissez l'onglet **Stratégies** et cliquez sur le lien **Créer une stratégie** pour démarrer l'assistant et créer une stratégie.

   La fenêtre **Assistant de nouvelle stratégie** s'ouvre.
3. Dans la fenêtre **Sélectionnez l'application pour laquelle vous souhaitez créer une stratégie de groupe**, sélectionnez Kaspersky Security 10.1.1 for Windows Server et cliquez sur **Suivant**.
4. **Saisissez un nom de stratégie de groupe** dans le champ **Nom**.

   Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ | .`
5. Pour appliquer une configuration de stratégie utilisée dans une version précédente de l'application :
   a. Cochez la case **Utiliser les paramètres d'une stratégie pour des versions précédentes de l'application**.
   b. Cliquez sur le bouton **Parcourir** et sélectionnez la stratégie que vous souhaitez appliquer.
   c. Cliquez sur **Suivant**.
6. Sélectionnez une des options suivantes dans la fenêtre **Sélection du type d'opération** :
   - **Nouvelle**, pour créer une nouvelle stratégie avec les paramètres par défaut.
   - **Importer une stratégie créée avec des versions précédentes de Kaspersky Security for Windows Server** pour utiliser la stratégie de cette version en tant que modèle.
   - Cliquez sur le bouton **Parcourir** et sélectionnez un fichier de configuration où une stratégie existante est stockée.

7. Dans la fenêtre **Protection en temps réel**, configurez les paramètres des tâches Protection des fichiers en temps réel, les tâches d'Utilisation du KSN et la fonction de Protection contre les exploits 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 ordinateurs du réseau et interdire l'application des paramètres de la tâche configurés dans la stratégie.
   - Cliquez sur le bouton pour interdire la configuration des paramètres d'une tâche sur les ordinateurs du réseau et autoriser l'application des paramètres de la tâche configurés dans la stratégie.

   La stratégie récemment créée utilise les paramètres par défaut des tâches de protection en temps réel des serveurs.

   - Si vous souhaitez modifier les paramètres d'une tâche Protection des fichiers en temps réel définis par défaut, cliquez sur le bouton **Configuration** dans la section **Protection des fichiers en temps réel**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos besoins. Cliquez sur le bouton **OK**.
   - Si vous souhaitez modifier les paramètres par défaut d'une tâche Utilisation du KSN, cliquez sur le bouton **Configuration** dans la section **Utilisation du KSN**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos besoins. Cliquez sur le bouton **OK**.

     Pour démarrer la tâche d'Utilisation du KSN, vous devez accepter la Déclaration KSN dans la fenêtre Traitement des données (cf. Section « Configuration du traitement des données » à la page 200).

   - Si vous souhaitez modifier les paramètres par défaut du composant Protection contre les exploits, cliquez sur le bouton **Configuration** dans la section **Protection contre les exploits**. Dans la fenêtre qui s'ouvre, configurez la fonctionnalité en fonction de vos besoins. Cliquez sur le bouton **OK**.

8. Sélectionnez un des états suivants de la stratégie suivants dans la fenêtre **Créer la stratégie de groupe pour l'application** :

   - **Stratégie active** si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si une stratégie active existe déjà dans le groupe, celle-ci est désactivée et la nouvelle stratégie est appliquée.
   - **Stratégie inactive**, si vous ne voulez pas appliquer immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.
   - Cochez la case **Ouvrir les propriétés de la stratégie immédiatement après leur création** pour fermer automatiquement l'**Assistant de nouvelle stratégie** et configurer la nouvelle stratégie après avoir cliqué sur le bouton **Suivant**.

9. 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 10.1.1 for Windows Server.

Configuration de stratégies

La fenêtre **Propriétés :<Nom de la stratégie>** d'une stratégie existante permet de configurer les paramètres généraux de Kaspersky Security 10.1.1 for Windows Server, les paramètres de la quarantaine et de la Sauvegarde, les paramètres de la zone de confiance, les paramètres de la Protection en temps réel, les paramètres du Contrôle de l'activité locale, le niveau de détail des journaux d'exécution de la tâche, les notifications des utilisateurs et des administrateurs relatives aux événements de Kaspersky Security 10.1.1 for Windows Server, les privilèges d'accès à l'administration de l'application et du service Kaspersky Security et les paramètres d'application des profils de stratégie.

► *Pour configurer les paramètres d'une stratégie, procédez comme suit :*

1. Développez l'entrée **Appareils administrés** dans l'arborescence de la Console d'administration de Kaspersky Security Center.
2. Développez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de la stratégie associée et ouvrez le nœud enfant **Stratégies** dans le panneau de détails.
3. Sélectionnez la stratégie que vous souhaitez configurer et ouvrez la fenêtre **Propriétés : <nom de la stratégie>** d'une des manières suivantes :
   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.
   - Dans le panneau de droite des détails du nœud sélectionné, cliquez sur le lien **Configurer la stratégie**.
   - Double-cliquez sur la stratégie sélectionnée.
4. Activez ou désactivez l'application de la stratégie dans la section **Etat de la stratégie** de l'onglet **Général**. 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.

   Le paramètre **Stratégie hors du bureau** n'est pas disponible dans le cadre de la gestion de Kaspersky Security 10.1.1 for Windows Server.
5. Dans les sections **Notifications sur les événements**, **Paramètres de l'application**, **Journaux et notifications**, **Complémentaire** et **Historique des révisions**, vous pouvez modifier la configuration de l'application (cf. tableau ci-dessous).

6. Dans les sections **Protection en temps réel du serveur**, **Contrôle de l'activité locale**, **Contrôle de l'activité réseau** et **Diagnostic du système**, configurez les paramètres de l'application et 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 ordinateurs du réseau pour chaque composant distinct de l'application.

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

Les paramètres définis seront appliqués dans la stratégie.

Les instructions relatives à la configuration des paramètres des tâches et des fonctions de l'application dans la console d'application figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

Sections contenant les paramètres de stratégie de Kaspersky Security 10.1.1 for Windows Server

Général

La section **Général** permet de configurer les paramètres de stratégie suivants :

- Indiquez l'état de la stratégie.
- Héritage des paramètres des stratégies parent pour les stratégies fille.

Notifications sur les événements

La section **Notifications sur les événements** 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 :

- Définir l'emplacement et la durée de conservation des informations sur l'événement enregistré ;
- Sélection du mode de notification sur les événements enregistrés.

Paramètres de l'application

Tableau 19. Paramètres de la section Paramètres de l'application

Section	Options
Montée en puissance et interface	Le bouton **Configuration** de la sous-section **Montée en puissance et interface** permet de configurer les paramètres suivants : • choisir la configuration automatique ou manuelle des paramètres de montée en puissance ; • configurer l'affichage de l'icône de l'application.
Sécurité	Le bouton **Configuration** de la sous-section **Sécurité** permet de configurer les paramètres suivants : • Configurez les paramètres de lancement de la tâche. • Actions de l'application en cas de passage à l'alimentation du serveur via un onduleur. • Activation ou désactivation de la protection par mot de passe des fonctions de l'application.
Connexions	Le bouton **Configuration** de la sous-section **Connexions** 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 du serveur proxy ; • définition des paramètres d'authentification sur le serveur proxy.
Lancer les tâches système	Le bouton **Configuration** de la sous-section **Lancer les tâches système** permet d'interdire ou d'autoriser le lancement des tâches système planifiées suivantes, configurées sur les ordinateurs locaux : • Tâche Analyse à la demande. • Tâches de mise à jour et de copie des mises à jour.

Complémentaire

Tableau 20. Paramètres de la section Complémentaire

Section	Options
Zone de confiance	Le bouton **Configuration** de la sous-section **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 une liste des processus de confiance.
Analyse des disques amovibles	La section **Analyse des disques amovibles** contient le bouton **Configuration** qui permet de configurer les paramètres d'analyse des disques USB amovibles.

Autorisations d'accès de l'utilisateur pour l'administration de l'application	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** permet de configurer les paramètres des droits des utilisateurs et des groupes d'utilisateurs à l'administration de Kaspersky Security 10.1.1 for Windows Server.
Autorisations d'accès de l'utilisateur pour l'administration du service Security	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Security** permet de configurer les droits des utilisateurs et des groupes d'utilisateurs à l'administration du service Kaspersky Security.
Stockages	Dans la sous-section **Stockages**, cliquez sur le bouton **Configuration** pour configurer les paramètres suivants de la quarantaine, de la Sauvegarde et de la liste des ordinateurs douteux : • 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. • Configurez les paramètres du blocage des hôtes.

Protection en temps réel du serveur

Tableau 21. Paramètres de la section Protection en temps réel du serveur

Section	Options
Protection des fichiers en temps réel	Le bouton **Configuration** de la sous-section **Protection des fichiers en temps réel** permet de configurer les paramètres suivants d'exécution de la tâche : • Indiquez le mode de protection. • Configurez l'utilisation de l'analyse heuristique. • Configurez l'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 sécurité ; • Configurez les paramètres de lancement de la tâche.
Utilisation du KSN	Le bouton **Configuration** de la sous-section **Utilisation du KSN** permet de configurer les paramètres suivants d'exécution de la tâche : • actions à réaliser sur les objets considérés comme douteux par KSN ; • Configurez le transfert de données et l'utilisation de Kaspersky Security Center comme serveur proxy KSN. Cliquez sur le bouton **Traitement des données** pour accepter ou rejeter la Déclaration de KSN et la Déclaration de KMP, et pour configurer des paramètres d'échanges de données fiables.

Protection du trafic	Le bouton **Configuration** de la sous-section **Protection du trafic** permet de configurer les paramètres suivants d'exécution de la tâche : • Configurez le mode de fonctionnement de la tâche. • Configurez la protection contre les applications malveillantes. • Activez la protection contre les menaces par emails, l'antiphishing et le traitement des URL. Cliquez sur la **liste de règles** pour configurer le contrôle Internet ou pour appliquer des règles prédéfinies de définition des catégories.
Protection contre les exploits	Le bouton **Configuration** de la sous-section **Protection contre les exploits** permet de configurer les paramètres suivants d'exécution de la tâche : • sélection du mode de protection de la mémoire des processus ; • définition de l'action de réduction de l'impact de l'exploitation des vulnérabilités ; • enrichissement et modification de la liste des processus à protéger.
Monitoring des scripts	Le bouton **Configuration** de la sous-section **Monitoring des scripts** permet de configurer les paramètres suivants d'exécution de la tâche : • Autorisation ou interdiction de l'exécution de scripts potentiellement dangereux. • Configurez l'utilisation de l'analyse heuristique. • Configurez l'application de la zone de confiance. • Configurez les paramètres de lancement de la tâche.

Contrôle de l'activité locale

Tableau 22. Paramètres de la section Contrôle de l'activité locale

Section	Options
Contrôle du lancement des applications	Le bouton **Configuration** de la sous-section **Contrôle du lancement des applications** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • Configuration des paramètres du contrôle du nouveau lancement des applications ; • Indiquez la zone d'application des règles du contrôle du lancement des applications. • Configuration de l'utilisation du KSN ; • Configurez les paramètres de lancement de la tâche.
Contrôle des périphériques	Le bouton **Configuration** de la sous-section **Contrôle des périphériques** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • Configurez les paramètres de lancement de la tâche.

Contrôle de l'activité réseau

Tableau 23. Paramètres de la section Contrôle de l'activité réseau

Section	Options
Gestion du pare-feu	Le bouton **Configuration** de la sous-section **Gestion du pare-feu** permet de configurer les paramètres suivants d'exécution de la tâche : • Règles du pare-feu ; • Configurez les paramètres de lancement de la tâche.
Protection contre le chiffrement	Le bouton **Configuration** de la sous-section **Protection contre le chiffrement** permet de configurer les paramètres suivants d'exécution de la tâche : • Zone de protection du composant Protection contre le chiffrement ; • Configurez les paramètres de lancement de la tâche.

Diagnostic du système

Tableau 24. Paramètres de la section Diagnostic du système

Section	Options
Moniteur d'intégrité des fichiers	La sous-section **Moniteur d'intégrité des fichiers** permet de configurer le contrôle sur les modifications dans les fichiers qui peuvent indiquer un cas d'atteinte à la sécurité sur un serveur protégé.
Inspection des journaux	La section **Inspection des journaux** permet de configurer le contrôle de l'intégrité d'un serveur protégé sur la base des résultats de l'analyse du journal des événements Windows.

Journaux et notifications

Tableau 25. Paramètres de la section Journaux et notifications

Section	Options
Journaux d'exécution de la tâche	Le bouton **Configuration** de la sous-section **Journaux d'exécution de la tâche** 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. • Spécifiez l'intégration de SIEM avec les paramètres de Kaspersky Security Center.
Notifications sur les événements	Le bouton **Configuration** de la sous-section **Notifications sur les événements** permet de configurer les paramètres suivants : • paramètres de notification des utilisateurs pour l'événement *Objet détecté* ; • paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements du groupe **Configuration des notifications**.
Interaction avec le Serveur d'administration	Le bouton **Configuration** de la section **Interaction avec le Serveur d'administration** permet de choisir les types d'objets que Kaspersky Security 10.1.1 for Windows Server va signaler au Serveur d'administration.

Protection des stockages réseau

Tableau 26. Paramètres de la section Protection des stockages réseau

Section	Options
Protection des fichiers en temps réel (RPC)	Le bouton **Configuration** de la sous-section **Protection des fichiers en temps réel (RPC)** permet de configurer les paramètres suivants : • Configuration de l'analyse heuristique • Paramètres de connexion au périphérique de stockage NAS. • Zone de protection de la tâche.
Protection des fichiers en temps réel (ICAP)	Le bouton **Configuration** de la sous-section **Protection des fichiers en temps réel (ICAP)** permet de configurer les paramètres suivants : • Paramètres de connexion du service ICAP. • Intégration aux autres composants. • Niveau de sécurité.
Protection contre le chiffrement pour NetApp	Le bouton **Configuration** de la sous-section **Protection contre le chiffrement pour NetApp** permet de configurer les paramètres suivants : • Mode de tâche ; • Configuration de l'analyse heuristique ; • Paramètres d'authentification au serveur proxy ; • Précisez les exclusions de la zone de protection.

Pour en savoir plus sur les tâches Protection des stockages réseau, consultez le *Manuel d'implantation pour la Protection des stockages réseau de Kaspersky Security 10.1.1 for Windows Server*.

Historique des révisions

La section **Historique des révisions** permet d'administrer les révisions : comparer à la révision actuelle ou à une autre stratégie, ajouter des descriptions de révisions, enregistrer les révisions dans un fichier ou revenir à l'état antérieur à la révision.

Configuration du lancement planifié des tâches locales du système prédéfinies

Les stratégies permettent d'autoriser ou d'interdire le lancement des tâches locales du système d'analyse à la demande et de mise à jour programmée localement sur chaque serveur du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'ordinateur local selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.
- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Le lancement des tâches locales du système est interdit par défaut par la stratégie.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont régies via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de groupe de mise à jour ou d'analyse à la demande, autorisez le lancement des tâches locales du système dans la stratégie : Kaspersky Security 10.1.1 for Windows Server réalise la mise à jour des bases de données et des modules de l'application et lance également toutes les tâches locales du système d'analyse à la demande conformément à la programmation par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâches d'analyse à la demande : Analyse des zones critiques, Analyse de la 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 système prédéfinies sera automatiquement activée.

► *Pour autoriser ou interdire le lancement planifié des tâches système de Kaspersky Security 10.1.1 for Windows Server dans une stratégie, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Appareils administrés**, déployez ensuite le groupe requis, puis sélectionnez l'onglet **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 système de Kaspersky Security 10.1.1 for Windows Server sur le groupe de serveurs et choisissez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés : <nom de la stratégie>**, ouvrez la section **Paramètres de l'application**. Cliquez sur le bouton **Configuration** dans le groupe **Lancer les tâches système** et réalisez les opérations 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.

   L'activation ou la désactivation des cases n'a aucun impact sur les paramètres de lancement des tâches locales définies par l'utilisateur du type indiqué.
4. Assurez-vous que la stratégie (cf. section "A propos des stratégies" à la page 107) que vous configurez est active et appliquée au groupe de serveurs d'administration.
5. Cliquez sur le bouton **OK**.

Les paramètres définis du lancement planifié sont appliqués aux tâches sélectionnées.

Création et configuration d'une tâche dans Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Security 10.1.1 for Windows Server, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

Contenu du chapitre

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 :

- Activation de l'application ;
- Copie des mises à jour ;
- Mise à jour des bases de l'application ;
- Mise à jour des modules de l'application ;
- Annulation de la mise à jour des bases de l'application ;
- Analyse à la demande ;
- Vérification de l'intégrité de l'application ;
- Génération des règles du Contrôle du lancement des applications ;
- Génération des règles du Contrôle des périphériques.

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 de détails du nœud du groupe d'ordinateurs sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'ordinateurs : dans le panneau de détails du nœud **Sélection de périphériques**.

Les stratégies permettent de désactiver les planifications pour la mise à jour et les tâches système locale d'analyse à la demande (cf. section "Configuration du lancement planifié des tâches locales du système prédéfinies" à la page 116) sur tous les serveurs protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

Création d'une tâche dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 du Serveur d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
     b. Dans le panneau de détails, sous l'onglet **Périphériques**, ouvrez le menu contextuel de la ligne du serveur protégé et sélectionnez **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 de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe pour lequel vous souhaitez créer une tâche.
     b. Dans le panneau de détails, ouvrez l'onglet **Tâches** et choisissez l'option **Créer une tâche**.
   - Pour créer une tâche pour une sélection arbitraire d'ordinateurs, choisissez l'option **Créer une tâche** dans le nœud **Sélection de périphériques** de la console d'administration de Kaspersky Security Center.

   La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la fenêtre **Sélectionnez le type de tâche**, sous le titre **Kaspersky Security 10.1.1 for Windows Server**, sélectionnez le type de la tâche à créer.
3. Si vous avez choisi n'importe quel type de tâche, sauf Annulation de la mise à jour des bases de l'application ou Activation de l'application, la fenêtre **Configuration** s'ouvre. 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 d'analyse sont accompagnées de l'icône ☑ 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 critiques, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.
     - Pour inclure une zone d'analyse prédéfinie, un disque, un dossier, un objet réseau ou un fichier à la zone d'analyse, cliquez-droit dans le tableau **Zone d'analyse** et choisissez l'option Ajouter une zone. Dans la fenêtre **Ajouter des objets à la zone d'analyse**, sélectionnez la zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque de l'ordinateur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur le bouton **OK**.
     - Pour exclure des sous-dossiers ou des 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 **Configurer**, puis dans la fenêtre Niveau de sécurité, cliquez sur le bouton **Configuration** et dans la fenêtre **Paramètres de l'analyse à la demande** de l'onglet **Général**, décochez les cases **Sous-dossiers** et **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 **Configurer**. Dans la fenêtre **Paramètres 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 des paramètres de sécurité se déroule de la même manière que dans la console de Kaspersky Security 10.1.1 for Windows Server.
     - 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 de l'ordinateur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau et cliquez sur le bouton **OK**.
     - Les zones d'analyse exclues sont accompagnées de l'icône ☐ dans le tableau.

     b. Exécutez les actions suivantes dans la fenêtre **Options**.

     Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure les objets repris dans la zone d'analyse de Kaspersky Security 10.1.1 for Windows Server.

     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 **Exécuter la tâche en arrière-plan** dans la fenêtre **Options**. 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 système **Analyse des zones critiques**. 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 **faible** (Low) au processus de travail dans lequel la tâche va être exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Options**. Par défaut, les processus dans lesquels les tâches de Kaspersky Security 10.1.1 for Windows Server sont exécutées ont la priorité **Moyenne** (Normale). 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 **Paramètres de connexion**. La fenêtre **Paramètres de connexion** s'ouvre.

  c. A la fenêtre **Paramètres de connexion** :

     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 **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 sans installation.

  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 10.1.1 for Windows Server 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 des modules de Kaspersky Security 10.1.1 for Windows Server, 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 mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Il est possible de configurer une notification pour l'administrateur au sujet de l'événement **Nouvelle mise à jour prévue des modules de l'application disponible**. Cette notification reprend l'adresse Internet de notre site depuis lequel il est possible de télécharger les mises à jour planifiées.

- *Pour créer la tâche Copie des mises à jour*, indiquez, dans la fenêtre **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.

- *Pour créer 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 fenêtre **Paramètres d'activation**. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez créer une tâche pour renouveler la licence.

- *Si vous créez la tâche Génération des règles du Contrôle des périphériques ou la tâche Génération des règles du Contrôle du lancement des applications*, définissez dans la fenêtre **Configuration** les paramètres sur la base desquels la liste des règles d'autorisation sera composée :

  a. Désignez le préfixe pour les noms des règles (seulement pour la tâche de génération des règles du Contrôle du lancement des applications).

  b. Configurez les paramètres de la zone d'application des règles d'autorisation (seulement pour la tâche de génération des règles du Contrôle du lancement des applications). Cliquez sur **Suivant**.

  c. Indiquez les actions que la tâche exécutera pendant la composition des règles d'autorisation (seulement pour la tâche Génération des règles du Contrôle du lancement des applications) et à la fin de celle-ci.

4. 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 des bases de l'application). Exécutez les actions suivantes dans la fenêtre **Planification** :

   a. Pour activer la planification, cochez la case **Exécuté selon la programmation** ;

   b. Désignez la fréquence de démarrage de la tâche : choisissez une des valeurs suivantes dans la liste **Fréquence** : **Toutes les heures**, **Tous les jours**, **Toutes les semaines**, **Au lancement de l'application**, **A la mise à jour des bases de l'application** (dans les tâches de groupe Mise à jour des bases de l'application et 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 **Toutes les heures**, indiquez le nombre d'heures dans le champ **Toutes les <nombre> heure(s)** du groupe de configuration **Paramètres du lancement de la tâche**.
      - Si vous avez sélectionné **Tous les jours**, indiquez le nombre de jours dans le champ **Tous les <nombre> jour(s)** du groupe de configuration **Paramètres du lancement de la tâche**.
      - Si vous avez sélectionné **Toutes les semaines**, indiquez le nombre de semaines dans le champ **Toutes les <nombre> semaine(s)** du groupe de configuration **Paramètres du lancement de la tâche**. Précisez les jours de la semaine où la tâche sera lancées (par défaut les tâches sont exécutées le lundi).

   c. Dans le champ **Démarrer à**, indiquez l'heure de lancement 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 de configuration **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 de configuration **Paramètres d'arrêt de la tâche**, saisissez les heures de début et de fin de l'intervalle dans les champs **Pause à partir de** et **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 le paramètre de distribution de l'heure d'exécution : cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur en minutes.

   e. Cliquez sur le bouton **OK**.

5. Si la tâche créée est une tâche pour une sélection quelconque d'ordinateurs, sélectionnez les ordinateurs du réseau (groupes) sur lesquels elle sera exécutée.
6. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte sous les autorisations duquel vous souhaitez exécuter la tâche.
7. Dans la fenêtre **Définition du nom de la tâche**, saisissez le nom de la tâche (100 caractères maximum) qui ne peut pas contenir les caractères **" * < > ? \ | :**. Il est conseillé d'indiquer le type de tâche dans son nom (par exemple, Analyse à la demande du dossier partagé).
8. 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 apparaît dans la liste **Tâches**.

Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center

► *Pour configurer les tâches locales ou les paramètres généraux de l'application pour un seul serveur du réseau, ouvrez la fenêtre Paramètres de l'application et procédez comme suit :*

1. Dans l'arborescence du Serveur d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau de détails, choisissez l'onglet **Périphériques**.
3. Ouvrez la fenêtre **Propriétés : <Nom de l'ordinateur>** à l'aide d'une des méthodes suivantes :
   - Double-clic sur le nom du serveur protégé.
   - Ouvrez le menu contextuel du nom du serveur protégé et sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : <Nom de l'ordinateur>** s'ouvre.
4. Pour configurer les paramètres de la tâche locale, procédez comme suit :
   a. Passez à la section **Tâches**.
      - Dans la liste des tâches, sélectionnez une tâche locale à configurer.
      - Double-cliquez sur le nom de la tâche dans la liste des tâches.
      - Sélectionnez le nom de la tâche et cliquez sur le bouton **Propriétés**.
      - Puis, choisissez l'option **Propriétés** dans le menu contextuel de la tâche choisie.
5. Pour configurer les paramètres de l'application, procédez comme suit :
   a. Passez à la section **Applications**.
      - Dans la liste des applications installées, sélectionnez une application à configurer.
      - 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**.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

Configuration des tâches de groupe dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, 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 *Système d'aide 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 **Zone d'analyse**, créez une zone d'analyse.
     b. Dans la section **Options**, 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 **Configuration**, 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 **Paramètres de connexion** pour configurer les paramètres de connexion de la source des mises à jour.
   - Pour configurer la tâche Mise à jour des modules de l'application, sélectionnez dans la section **Paramètres de mise à jour des modules de l'application** une action à effectuer : copier et installer les mises à jour critiques des modules de l'application ou simplement les rechercher.
   - Pour configurer la tâche Copie des mises à jour, indiquez, dans la section **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.
   - Pour configurer 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 ou de clé additionnels** si vous souhaitez ajouter un code d'activation ou une clé pour renouveler la licence.
   - Si vous configurez une des tâches de création automatique des règles d'autorisation du contrôle du serveur, désignez dans la section **Configuration** les paramètres qui vont servir de base à la création de la règle d'autorisation.
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 des bases de l'application).
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 *Système d'aide 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 *Système d'aide de Kaspersky Security Center*.
9. Dans la fenêtre **Propriétés**, 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 27. Paramètre de tâches de groupe de Kaspersky Security 10.1.1 for Windows Server

Types de tâche de Kaspersky Security 10.1.1 for Windows Server	Section dans la fenêtre Propriétés : <Nom de la tâche>	Paramètres de la tâche
Génération automatique de règle (cf. section "Tâches Génération des règles du Contrôle du lancement des applications et Génération des règles du Contrôle des périphériques" à la page 129).	**Configuration**	Lors de la configuration des paramètres de la tâche Génération des règles du Contrôle du lancement des applications, vous pouvez : • Modifier la zone de protection en ajoutant ou en supprimant des chemins d'accès aux dossiers et en indiquant les types de fichiers dont le lancement est autorisé par les règles générées automatiquement. • Tenir compte ou non des applications lancées.
	Options	Vous pouvez indiquer les actions lors de la création des règles d'autorisation du contrôle du lancement des applications : • **Utiliser un certificat numérique** • **Utiliser l'objet et l'empreinte du certificat numérique** • **En cas d'absence de certificat, utiliser** • **Utiliser le hash SHA256** • **Créer des règles pour un utilisateur ou un groupe d'utilisateurs** Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security 10.1.1 for Windows Server crée à la fin des tâches.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Activation de l'application (cf. section "Tâche Activation de l'application" à la page 131)	**Paramètres d'activation**	Vous pouvez ajouter un code d'activation ou une clé pour l'activation de l'application ou le renouvellement de la date d'expiration.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Copie des mises à jour (cf. section "Tâches de mise à jour" à la page 132)	**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 personnalisés manuellement.
	Fenêtre **Paramètres de connexion**	La zone de groupe **Paramètres de connexion à la source des mises à jour** permet d'indiquer s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.
	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 10.1.1 for Windows Server va conserver les mises à jour copiées.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Mise à jour des bases de l'application (cf. section "Tâche de mise à jour" à la page 132)	**Configuration**	Dans la zone de 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 personnalisés manuellement. Le groupe Optimisation de l'utilisation du sous-système de disque vous permet de configurer les paramètres de la fonction de réduction de la charge sur le sous-système disque : • **Réduire la charge sur les I/O du disque** • **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**
	Fenêtre **Paramètres de connexion**	La zone de groupe **Paramètres de connexion à la source des mises à jour** permet d'indiquer s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Mise à jour des modules de l'application (cf. section "Tâche de mise à jour" à la page 132)	**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 personnalisés manuellement.
	Fenêtre **Paramètres de connexion**	La zone de groupe **Paramètres de connexion à la source des mises à jour** permet d'indiquer s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.
	Configuration des paramètres de mise à jour des modules de l'application	Vous pouvez indiquer les actions que Kaspersky Security 10.1.1 for Windows Server va réaliser si des mises à jour critiques des modules de l'application sont disponibles ou ont déjà été installées et si Kaspersky Security 10.1.1 for Windows Server doit obtenir des informations sur les mises à jour planifiées.
	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Analyse à la demande (cf. section "Création d'une tâche d'analyse à la demande" à la page 135)	**Zone d'analyse**	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 **Paramètres de l'analyse à la demande**	Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser manuellement les paramètres du niveau de sécurité.
	Options	La zone de groupe **Analyse heuristique** vous permet d'activer ou de désactiver l'utilisation de l'analyseur heuristique pour la tâche d'analyse à la demande et de configurer le niveau d'analyse à l'aide d'un curseur. Vous pouvez configurer les paramètres suivants dans la zone de groupe **Intégration aux autres composants** : • Appliquer la zone de confiance pour les tâches d'analyse à la demande. • Utilisation du KSN pour les tâches d'analyse à la demande. • Niveau de priorité de la tâche d'analyse à la demande : exécuter la tâche en arrière-plan (priorité basse) ou considérer l'exécution de la tâche comme un tâche d'analyse des zones critiques.

	Planification	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
érification de l'intégrité des modules de l'application (à la page 134)	**Planification**	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Pour les tâches, par exemple Annulation de la mise à jour des bases de l'application, vous ne pouvez configurer que les paramètres de tâche standard dans les sections **Notification** et **Exclusions de la zone d'action de la tâche** gérées par Kaspersky Security Center. Vous trouverez plus d'informations sur la configuration des paramètres dans ces sections dans le *Système d'aide de Kaspersky Security Center*.

Dans cette section

Tâches de Génération des règles du Contrôle des périphériques et Génération des règles du Contrôle du lancement des applications

► *Pour configurer la tâche Génération des règles du Contrôle des périphériques ou la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, configurez les paramètres de notification sur les événements de la tâche.
5. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

6. La section **Configuration** permet de configurer les paramètres suivants :
   - 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.
   - Tenir compte ou non des applications lancées.
7. Vous pouvez indiquer les actions à réaliser lors de la création des règles d'autorisation du Contrôle du lancement des applications dans la section **Configuration** :
   - **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.
   - **Utiliser l'objet 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. Kaspersky Security 10.1.1 for Windows Server autorise 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 active 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.

     - **Hash 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 via les fichiers qui se trouvent dans les dossiers indiqués sous l'onglet dans le tableau Créer des règles d'autorisation pour les applications des dossiers.

- **Utiliser le hash 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.

  Il est conseillé d'appliquer cette option lorsque les règles générées doivent répondre au niveau de sécurité le plus fiable : la somme de contrôle SHA256 peut être appliquée comme seul identifiant du fichier. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle réduit la zone d'application des règles à un fichier.

  Cette option est sélectionnée par défaut.

- **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 les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security 10.1.1 for Windows Server crée à la fin des tâches.

8. 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 des bases de l'application).
9. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
10. 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 de ces sections dans le *Système d'aide de Kaspersky Security Center*.

11. Dans la fenêtre **Propriétés**, cliquez sur le bouton **OK**.

    Les paramètres des tâches de groupe définis seront enregistrés.

Tâche Activation de l'application

► *Pour configurer la tâche Activation de l'application, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, configurez les paramètres de notification sur les événements de la tâche.
5. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.
6. Dans la section **Paramètres d'activation** de l'application, appliquez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter une clé pour renouveler la licence.
7. 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 des bases de l'application).
8. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
9. 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 de ces sections dans le *Système d'aide de Kaspersky Security Center*.
10. Dans la fenêtre **Propriétés**, cliquez sur le bouton **OK**.

    Les paramètres des tâches de groupe définis seront enregistrés.

Tâches de mise à jour

Pour configurer la tâche Copie des mises à jour, Mise à jour des bases de l'application ou Mise à jour des modules de l'application, procédez comme suit :

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, 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 *Système d'aide de Kaspersky Security Center*.

5. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :

   - 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.

     a. 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 personnalisés manuellement.

     b. Le groupe **Optimisation de l'utilisation des I/O du disque** permet de configurer les paramètres de la fonction réduisant la charge sur le sous-système disque pour la tâche Mise à jour des bases de l'application :

     - **Réduire la charge sur les I/O du 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.

       Si la case est cochée, la fonction est active.

       Cette case est décochée par défaut.

     - **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**

       Volume de mémoire vive (en mégaoctets) que l'application utilisera pour le placement des fichiers de mises à jour. Le volume de mémoire vive défini par défaut est de 512 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

     c. Cliquez sur le bouton **Paramètres de connexion** et, dans la fenêtre **Paramètres de connexion** qui s'ouvre, configurez les paramètres d'utilisation du serveur proxy pour la connexion avec les serveurs de mise à jour de Kaspersky Lab et d'autres serveurs.

   - La section **Paramètres de mise à jour des modules de l'application** pour la tâche Mise à jour des modules de l'application permet de désigner les actions que Kaspersky Security 10.1.1 for Windows Server va effectuer 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. Elle permet également de configurer les actions effectuées par Kaspersky Security 10.1.1 for Windows Server une fois l'installation des mises à jour critiques terminée.

   - Dans la section **Paramètres de copie des mises à jour** de la tâche **Copie des mises à jour**, désignez la composition des mises à jour et le dossier de destination.

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 des bases de l'application).
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 de ces sections dans le *Système d'aide de Kaspersky Security Center*.

8. Dans la fenêtre **Propriétés**, cliquez sur le bouton **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

S'agissant de la tâche Annulation de la mise à jour des bases de l'application, vous pouvez configurer uniquement les paramètres de tâche standard contrôlée par Kaspersky Security Center dans les sections **Notifications** et **Exclusions** de la zone d'analyse. Vous trouverez plus d'informations sur la configuration des paramètres dans ces sections dans le *Système d'aide de Kaspersky Security Center*.

Vérification de l'intégrité des modules de l'application

► *Pour configurer la tâche de mise à jour de groupe des modules de l'application, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, 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 *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Périphériques**, choisissez les périphériques pour lesquels vous souhaitez configurer la tâche de vérification de l'intégrité des modules de l'application.
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 des bases de l'application).

7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
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 de ces sections dans le *Système d'aide de Kaspersky Security Center*.

9. Dans la fenêtre **Propriétés**, cliquez sur le bouton **OK**.

   Les paramètres des tâches de groupe définis seront enregistrés.

Création d'une tâche d'analyse à la demande

► *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 du Serveur d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
     b. Dans le panneau de détails, sous l'onglet **Périphériques**, 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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe pour lequel vous souhaitez créer une stratégie.
     b. Dans le panneau de détails, ouvrez le menu contextuel de l'onglet **Tâches** et choisissez l'option **Créer > Tâche**.
   - Pour créer une tâche pour une sélection arbitraire d'ordinateurs, choisissez l'option **Créer tâche** dans le nœud **Sélection de périphériques** de la Console d'administration Kaspersky Security Center.

   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**l * < > ? \ / | :)**. Il est conseillé d'indiquer le type de tâche dans son nom (par exemple, Analyse à la demande du dossier partagé).
3. Sous l'onglet **Kaspersky Security 10.1.1 for Windows Server** de la fenêtre **Type de tâche**, sélectionnez la tâche **Analyse à la demande**, puis cliquez sur **Suivant**.

4. 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 d'analyse sont accompagnées de l'icône ☑ dans le tableau. Les zones d'analyse exclues sont accompagnées de l'icône ☐ 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 critiques, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.
   - Pour inclure une zone d'analyse, un disque, un dossier, un objet réseau ou un fichier prédéfini dans la zone d'analyse :
     a. Cliquez avec le bouton droit de la souris dans le tableau **Zone d'analyse** et choisissez l'option **Ajouter une zone** ou cliquez sur le bouton **Ajouter**.
     b. Dans la fenêtre **Ajouter des objets à la zone d'analyse**, sélectionnez la zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque de l'ordinateur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur le bouton **OK**.
   - Pour exclure des sous-dossiers ou des fichiers de l'analyse, sélectionnez le dossier (le disque) ajouté dans la fenêtre **Zone d'analyse** de l'assistant :
     a. Ouvrez le menu contextuel et sélectionnez l'option **Configurer**.
     b. Cliquez sur le bouton **Configuration** afin d'ouvrir la fenêtre **Niveau de sécurité**.
     c. Sous l'onglet **Général** de la fenêtre **Paramètres de l'analyse à la demande**, décochez les cases **Sous-dossiers** et **Sous-fichiers**.
   - Pour modifier les paramètres de sécurité de la zone d'analyse :
     a. Ouvrez le menu contextuel de la zone dont vous souhaitez modifier les paramètres et choisissez l'option **Configurer**.
     b. Dans la fenêtre **Paramètres 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.

     Les paramètres de sécurité sont configurés de la même manière que pour la tâche Protection des fichiers en temps réel (cf. section "Configuration manuelle des paramètres de sécurité" à la page 187).

   - Pour ignorer les objets joints dans la zone d'analyse ajoutée :
     a. Ouvrez le menu contextuel du tableau **Zone d'analyse** et sélectionnez **Ajouter** une exclusion.
     b. Désignez les objets à exclure : sélectionnez une zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque de l'ordinateur, le dossier, l'objet réseau ou le dossier sur le serveur ou tout autre ordinateur du réseau.
     c. Cliquez sur le bouton **OK**.

5. Dans la section **Options**, configurez l'analyse heuristique et l'intégration aux autres modules :

   - Configurez l'utilisation de l'analyse heuristique (cf. section "Utilisation de l'analyse heuristique" à la page 181).
   - 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 10.1.1 for Windows Server.

     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 10.1.1 for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne prend pas en compte les opérations sur les 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 la case **Utiliser KSN pour l'analyse** si vous souhaitez utiliser les services cloud de Kaspersky Security Network pour la tâche.

     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 d'analyse à la demande n'utilise pas les services du KSN.

     Cette case est cochée par défaut.

   - Pour attribuer la priorité de base **faible** (Low) au processus de travail dans lequel la tâche va être exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Options**.

     La case modifie la priorité de la tâche.

     Si 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 le système de fichiers du serveur par les autres tâches de Kaspersky Security 10.1.1 for Windows Server ou les autres applications. Par conséquent la vitesse d'exécution de la tâche diminue quand la charge augmente et inversement.

     Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security 10.1.1 for Windows Server et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

     Cette case est décochée par défaut.

   Par défaut, les processus dans lesquels les tâches de Kaspersky Security 10.1.1 for Windows Server sont exécutées ont la priorité **Moyenne** (Normale).

- Pour utiliser la tâche créée en tant que tâche d'analyse des zones critiques, cochez la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** dans la fenêtre **Options**.

  La case modifie la priorité de la tâche : active ou désactive l'enregistrement des événements dans le journal *Analyse des zones critiques* et l'actualisation de l'état de la protection du serveur. Kaspersky Security Center évalue la sécurité du ou des serveurs sur la base des résultats des performances des tâches portant l'état *Analyse des zones critiques*. La case n'est pas accessible dans les propriétés des tâches locales du système ou définies par l'utilisateur dans Kaspersky Security 10.1.1 for Windows Server. Vous pouvez modifier ce paramètre uniquement du côté de Kaspersky Security Center.

  Si la case est cochée, le Serveur d'administration consigne l'événement Analyse des zones critiques réalisée et actualise l'état de la protection du serveur sur la base des résultats de 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 des zones critiques.

6. Cliquez sur **Suivant**.
7. Dans la fenêtre **Planification**, définissez une planification (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 143) pour la tâche.
8. Indiquez le compte utilisateur sous lequel vous souhaitez exécuter la tâche, puis définissez le nom de celle-ci.
9. Cliquez sur **Terminer**.

Une tâche Analyse à la demande est créée pour un serveur ou un groupe de serveurs sélectionnés.

Configuration d'une tâche d'analyse à la demande

► *Pour configurer une tâche d'analyse à la demande existante, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. 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 cliquez sur le lien **Configurer 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 **Notification**, 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 *Système d'aide de Kaspersky Security Center*.

5. La section **Configuration** permet de réaliser les opérations suivantes :

   a. Dans le groupe **Zone d'analyse**, cochez les cases en regard des ressources fichier que vous souhaitez inclure dans la zone d'analyse.

   b. Cliquez sur le bouton **Configurer** et choisissez le niveau de sécurité.

      Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser manuellement les paramètres du niveau de sécurité.

   c. Pour configurer manuellement le niveau de sécurité, cliquez sur le bouton **Configuration** dans la fenêtre **Paramètres de l'analyse à la demande**.

6. La section **Options** permet de réaliser les opérations suivantes :

   a. Activez ou désactivez l'utilisation du bouton **Analyse heuristique** et configurez le niveau d'analyse à l'aide du curseur dans le groupe **Analyse heuristique**.

   b. Configurez les paramètres avancés (cf. section "Création d'une tâche d'analyse à la demande" à la page 135).

7. 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 des bases de l'application).

8. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.

9. 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 de ces sections dans le *Système d'aide de Kaspersky Security Center*.

10. Dans la fenêtre **Propriétés**, cliquez sur le bouton **OK**.

    Les paramètres des tâches de groupe définis seront enregistrés.

Attribution de l'état "Analyse des zones critiques" à la tâche d'analyse à la demande

Kaspersky Security Center attribue par défaut l'état *Avertissement* au serveur si la tâche Analyse des zones critiques est exécutée moins souvent que ne l'indique le paramètre du seuil de génération d'événement de Kaspersky Security 10.1.1 for Windows Server **Analyse des zones critiques non réalisée 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.
2. Dans la fenêtre **Options** de l'Assistant de création de tâches, cochez la case **Considérer l'exécution de la tâche comme une analyse des zones critiques**. 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 des zones critiques** aussi bien lors de la création de la tâche d'analyse à la demande pour un groupe de serveurs ou pour une sélection de serveurs que plus tard, dans la fenêtre **Propriétés : <nom de la tâche>**.

3. A l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez le lancement planifié des tâches prédéfinies (cf. section "Configuration du lancement planifié des tâches locales du système" à la page 116).

Dès ce moment, le Serveur d'administration de Kaspersky Security Center évalue la protection du serveur protégé et vous en informe sur la base de la dernière exécution de la tâche portant l'état tâche Analyse des zones critiques et non sur la base des résultats de la tâche système *Analyse des zones critiques*.

Vous pouvez attribuer l'état *Tâche d'analyse des zones critiques* à des tâches de groupe d'analyse à la demande ou à des tâches pour des sélections d'ordinateurs.

La console d'application permet de voir si la tâche d'analyse à la demande est une tâche d'analyse des zones critiques.

Dans la console d'application, la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** apparaît dans la propriété des tâches mais elle ne peut pas être modifiée.

Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center

Si un problème survient durant l'utilisation de Kaspersky Security 10.1.1 for Windows Server (par exemple, Kaspersky Security 10.1.1 for Windows Server s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez activer la création de fichiers de trace et du fichier dump des processus de Kaspersky Security 10.1.1 for Windows Server et envoyer ces fichiers au Support Technique de Kaspersky Lab pour l'analyse.

Kaspersky Security 10.1.1 for Windows Server n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par l'utilisateur avec les droits correspondants.

Kaspersky Security 10.1.1 for Windows Server consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Security 10.1.1 for Windows Server. Vous pouvez configurer les autorisations d'accès (cf. section "Autorisations d'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server" à la page 96) et autoriser l'accès aux journaux, aux fichiers de trace et aux fichiers dump pour les utilisateurs requis uniquement.

► *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 123).
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 trace**.
     - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security 10.1.1 for Windows Server va enregistrer les fichiers de trace.
     - Configurez le niveau de détail des informations de débogage.

       Cette liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Security 10.1.1 for Windows Server consigne dans le fichier de trace.

       Vous avez le choix parmi les niveaux de détail suivants :

       - **Evénements critiques** : Kaspersky Security 10.1.1 for Windows Server enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.
       - **Erreurs** : Kaspersky Security 10.1.1 for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
       - **Evénements importants** : Kaspersky Security 10.1.1 for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.
       - **Evénements d'information** : Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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 trace** est cochée.
     - Taille maximale du fichier de trace
     - Indiquez les modules à déboguer. Les codes des composants doivent être séparés par un point-virgule. Les codes sont sensibles à la case (cf. tableau ci-dessous).

Tableau 28. Codes de sous-système de Kaspersky Security 10.1.1 for Windows Server

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Security 10.1.1 for Windows Server dans Microsoft Management Console.
ak_conn	Sous-système d'intégration à l'Agent d'administration de Kaspersky Security Center
bl	Processus de contrôle, met en œuvre les tâches de contrôle de Kaspersky Security 10.1.1 for Windows Server.
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance Kaspersky Security 10.1.1 for Windows Server.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de Protection des fichiers en temps réel.
qb	Sous-système de la Quarantaine et de la Sauvegarde.
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.
updater	Sous-système de mise à jour des bases de données 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 10.1.1 for Windows Server (gui) et du plug-in d'administration de 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 relancement du service SNMP. Les paramètres de traçage du sous-système des compteurs de performance (perfcount) sont appliqués après le relancement de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Security 10.1.1 for Windows Server sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Par défaut, Kaspersky Security 10.1.1 for Windows Server consigne les informations de débogage pour tous les composants de Kaspersky Security 10.1.1 for Windows Server.

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

- Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump**.
  - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security 10.1.1 for Windows Server enregistrera le fichier dump.

3. Cliquez sur le bouton **OK**.

Les paramètres configurés de l'application seront appliqués sur le serveur protégé.

Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Security 10.1.1 for Windows Server et configurer les paramètres de la planification.

Dans cette section

Configuration des paramètres de planification du lancement des tâches

La console d'application permet de planifier le lancement des tâches locales du système et définies par l'utilisateur. Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

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

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et réalisez les opérations suivantes :
   - Si vous voulez configurer les paramètres d'une stratégie, sélectionnez dans le groupe d'ordinateur **Stratégies > <om de la stratégie> > <section> > Configuration > Administration des tâches**.
   - Si vous souhaitez configurer les paramètres de l'application pour un seul serveur, ouvrez la fenêtre **Paramètres de la tâche** dans Kaspersky Security Center (cf. section "**Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center**" à la page 123).

     La fenêtre **Configuration** s'ouvre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la programmation**.

   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.
3. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
   a. Choisissez une des options suivantes dans la liste **Fréquence** :
      - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
      - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
      - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. 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 10.1.1 for Windows Server.
      - **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 l'application.

b. Indiquez, dans le champ **Démarrer à**, l'heure du premier lancement 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, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres** de la tâche sous l'onglet **Planification**.
> La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est interdit par les paramètres d'une stratégie en vigueur de Kaspersky Security Center (cf. section "Configuration de la planification de l'exécution programmée des tâches locales du système" à la page 116).

4. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification 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 tâche.

     b. Cochez la case **Pause à partir de**, puis saisissez les heures de début et de fin pour spécifier un intervalle de temps de moins de 24 heures pendant lequel l'exécution de la tâche sera suspendue.

   - 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 le lancement des tâches ignorées.

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

5. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

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 de la tâche, procédez comme suit :*

1. Dans l'arborescence de la console d'application, ouvrez le menu contextuel du nom de la tâche dont vous souhaitez planifier le 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 **Exécuté selon la programmation** si vous souhaitez activer l'exécution planifiée d'une tâche.
   - Décochez la case **Exécuté selon la programmation** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

     Les paramètres de la planification du lancement de la tâche ne sont pas supprimés. Ils sont appliqué au prochain lancement planifié de la tâche.
4. Cliquez sur le bouton **Appliquer**.

Les paramètres configurés du lancement planifié de la tâche sont enregistrés.

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center.

Contenu du chapitre

Analyse des fichiers de stockage dans le cloud

A propos du fichier clé

Vous pouvez activer ou désactiver Kaspersky Security 10.1.1 for Windows Server. L'application prend en charge la nouvelle fonction OneDrive Files On-Demand.

> Kaspersky Security 10.1.1 for Windows Server ne prend pas en charge les autres stockages dans le cloud.

OneDrive Files On-Demand permet d'accéder à tous les fichiers de OneDrive sans avoir à les télécharger tous et à utiliser de l'espace de stockage sur votre appareil. Vous pouvez télécharger des fichiers sur votre disque dur lorsque vous en avez besoin.

Lorsque la fonction OneDrive Files On-Demand est activée, des icônes d'état apparaissent en regard de chaque fichier dans la colonne **Etat** de l'Explorateur de fichiers. Vous avez le choix entre les modes suivants de fonctionnement de la tâche :

Cette icône d'état indique que le fichier est *uniquement disponible en ligne*. Les fichiers uniquement disponibles en ligne ne sont pas stockés sur le disque dur. Vous ne pouvez pas les ouvrir lorsque votre appareil n'est pas connecté à Internet.

Cette icône d'état indique qu'un fichier est *disponible en local*. Ce cas se produit lorsque vous ouvrez un fichier uniquement disponible en ligne et qu'il se télécharge sur votre appareil. Vous pouvez ouvrir un fichier disponible en local à tout moment même sans accès Internet. Pour gagner de l'espace, vous pouvez redéfinir l'état du fichier sur uniquement en ligne.

Cette icône d'état indique qu'un fichier est *stocké sur le disque dur et toujours disponible*.

Analyse des fichiers de stockage dans le cloud

Kaspersky Security 10.1.1 for Windows Server analyse les fichiers sur la base de leur extension. Ces fichiers OneDrive ont les états et . Les fichiers sont ignorés pendant l'analyse car ils ne sont pas physiquement situés sur le serveur protégé.

Kaspersky Security 10.1.1 for Windows Server ne télécharge pas automatiquement les fichiers depuis le cloud lors de l'analyse, même s'ils

Pour être reconnu par Kaspersky Security 10.1.1 for Windows Server, le fichier doit répondre aux paramètres suivants :

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone de protection de la tâche Protection des fichiers en temps réel. Le fichier est analysé lorsque l'utilisateur y accède. Si l'utilisateur accède à un fichier , celui-ci est téléchargé, devient disponible en local et a désormais l'état . Pour confirmer l'optimisation de la tâche Protection des fichiers en temps réel.
- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone d'analyse de la tâche Analyse à la demande. La tâche analyse les fichiers avec les états et . Si des fichiers sont trouvés dans la zone, ils seront ignorés pendant l'analyse et un événement d'information sera enregistré dans le journal d'exécution de la tâche. Il indiquera que le fichier analysé n'est qu'une marque de réservation pour un fichier cloud et n'existe pas sur un disque local.
- Création de règles de contrôle des applications et utilisation : vous pouvez créer des règles d'autorisation et d'interdiction pour les fichiers et à l'aide de la tâche Génération des règles du Contrôle du lancement des applications. La tâche Contrôle du lancement des applications applique le principe d'interdiction par défaut et des règles créées pour traiter et interdire les fichiers cloud.

  La tâche Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Security 10.1.1 for Windows Server. Les fichiers ne sont pas inclus dans la zone de génération de règles par l'application car ils ne sont pas physiquement stockés sur un disque dur. Aucune règle d'autorisation ne peut être créée pour ces fichiers. Par conséquent, ils sont soumis au principe d'interdiction par défaut.

Lorsqu'une menace est détectée sur un fichier cloud OnDrive, l'application exécute l'action spécifiée dans les paramètres de la tâche effectuant l'analyse. Ainsi, le fichier peut être supprimé, désinfecté, placé en quarantaine ou sauvegardé.

Les modifications apportées aux fichiers locaux sont synchronisées avec les copies stockées sur OneDrive conformément aux principes exposés dans la documentation Microsoft OneDrive correspondante.

Gestion de Kaspersky Security 10.1.1 for Windows Server à partir de Kaspersky Security Center

Vous pouvez réaliser l'administration centralisée de plusieurs serveurs dotés de Kaspersky Security 10.1.1 for Windows Server et inclus dans un groupe d'administration via le plug-in de Kaspersky Security 10.1.1 for Windows Server. Kaspersky Security Center permet également de configurer séparément les paramètres de fonctionnement de chaque serveur au sein 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 10.1.1 for Windows Server 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 *Système d'aide de Kaspersky Security Center*.

Les paramètres de l'application pour un ordinateur ne peuvent être configurés si le fonctionnement de Kaspersky Security 10.1.1 for Windows Server sur ce serveur est contrôlé par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Security 10.1.1 for Windows Server 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 la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la console d'application ou à distance dans la fenêtre **Propriétés : <nom de l'ordinateur>** de Kaspersky Security Center.

  Les stratégies permettent de configurer les paramètres généraux de fonctionnement de l'application, les paramètres des tâches Protection en temps réel, Contrôle de l'activité locale, Protection des stockages réseau, tâche système planifiée et usage du profil.

- **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 des règles du Contrôle du lancement des applications.

- **A l'aide de tâches pour une sélection de périphériques**. Les tâches pour une sélection de périphériques permettent de configurer à distance des paramètres de tâches communs 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 propriétés d'un ordinateur unique**. La fenêtre **Propriétés : <nom de l'ordinateur>** permet de configurer à distance les paramètres d'une tâche pour un serveur unique 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 10.1.1 for Windows Server, si le serveur sélectionné n'est pas contrôlé par une stratégie active de Kaspersky Security Center.

Kaspersky Security Center permet de configurer les paramètres de l'application, les possibilités additionnelles et le fonctionnement des journaux. Vous pouvez configurer ces paramètres aussi bien pour un groupe de serveur que pour un seul.

Configuration des paramètres généraux de l'application dans Kaspersky Security Center

Vous pouvez configurer les paramètres généraux de Kaspersky Security 10.1.1 for Windows Server depuis Kaspersky Security Center pour un groupe de serveurs ou pour un serveur individuel.

Dans cette section

Configuration de la montée en puissance et de l'interface dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

► *Pour configurer les paramètres de la montée en puissance et de l'interface de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Paramètres de l'application** du groupe **Montée en puissance et interface**, cliquez sur **Configuration**.

4. Sous l'onglet **Général** de la fenêtre **Montée en puissance et interface**, configurez les paramètres suivants :

   - La section **Paramètres d'optimisation** permet de configurer les paramètres qui définissent le nombre de processus utilisés par Kaspersky Security 10.1.1 for Windows Server.

     - **Détecter automatiquement les paramètres d'optimisation**.

       Kaspersky Security 10.1.1 for Windows Server régit automatiquement le nombre de processus utilisés.

       Cette valeur est définie par défaut.

     - **Indiquer manuellement le nombre de processus actifs**.

       Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server. 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 composants des tâches de protection en temps réel. 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.

   - Dans le groupe **Interaction avec l'utilisateur**, configurez l'affichage de l'icône de la barre d'état de l'application dans la zone de notification : décochez ou cochez la case **Afficher l'icône de la barre d'état dans la barre des tâches**.

5. Sous l'onglet **Stockage hiérarchique**, sélectionnez une des options d'accès au stockage hiérarchique :

   - **Aucun système HSM**

     Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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**

  Kaspersky Security 10.1.1 for Windows Server utilise des attributs de fichiers étendus pour analyser les fichiers dans le stockage distant lors de l'exécution de la tâche d'analyse à la demande.

- **Système HSM non identifié**

  Kaspersky Security 10.1.1 for Windows Server 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 le bouton **OK**.

Les paramètres d'application définis seront enregistrés.

Configuration des paramètres de sécurité dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

► *Pour configurer les paramètres de sécurité manuellement, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

   Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Paramètres de l'application** du groupe **Sécurité et fiabilité**, cliquez sur le bouton **Configuration**.

4. Configurez les paramètres suivants dans la fenêtre **Paramètres de sécurité** :

   - Le groupe **Paramètres de fiabilité** permet de configurer les paramètres de restauration des tâches de Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server après un échec de l'application ou un arrêt forcé de celle-ci.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server restaure automatiquement ses tâches après un échec de l'application ou un arrêt forcé de celle-ci.

       Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server. Le champ de saisie est accessible si la case **Réaliser la restauration des tâches** a été cochée.

   - Le groupe **Action lors du passage à une source d'alimentation continue** permet de limiter la charge de Kaspersky Security 10.1.1 for Windows Server sur le serveur dans le cadre de l'alimentation de secours :

     - **Ne pas lancer les tâches d'analyse programmée**

       Cette case active ou désactive le lancement d'une tâche d'analyse programmée entre l'entrée en action de l'alimentation de secours du serveur et le rétablissement de l'alimentation normale.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ne lance pas les tâches d'analyse programmée entre l'entrée en action de l'alimentation de secours du serveur et le rétablissement de l'alimentation standard.

       Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server lance les tâches d'analyse programmée 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 du serveur à une source d'alimentation de secours.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server arrête l'exécution des tâches d'analyse en cours lors du passage du serveur à une source d'alimentation de secours.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server poursuit l'exécution des tâches d'analyse en cours après que le serveur est passé à une source d'alimentation de secours.

  Cette case est cochée par défaut.

  Le serveur passe à une alimentation de secours uniquement si le niveau de charge de la batterie passe au-dessous de 90 %.

- Dans le groupe **Paramètres de protection par mot de passe**, définissez le mot de passe de protection de l'accès aux fonctions de Kaspersky Security 10.1.1 for Windows Server.

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

Les paramètres définis de sécurité et de fiabilité sont enregistrés.

Configuration des paramètres de connexion dans Kaspersky Security Center

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Security 10.1.1 for Windows Server et les serveurs de mise 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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Paramètres de l'application** du groupe **Serveur proxy**, cliquez sur le bouton **Configuration**.

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

4. Configurez les paramètres suivants dans la fenêtre **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 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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 10.1.1 for Windows Server.

       Si la case est cochée, les échanges avec les autres ordinateurs du réseau auquel appartient l'ordinateur disposant de Kaspersky Security 10.1.1 for Windows Server se font directement. Le serveur proxy n'est pas utilisé.

       Si la case est décochée, les ordinateurs locaux sont sollicités via le serveur proxy.

       Cette case est cochée par défaut.

   - Définissez les paramètres d'authentification dans le groupe **Paramètres d'authentification du serveur proxy** :

     - Sélectionnez les paramètres d'authentification dans la liste déroulante.

       - **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.

- Dans le groupe **Licence**, cochez ou décochez la case **Utiliser Kaspersky Security Center comme serveur proxy pour l'activation de l'application**.

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

Les paramètres de la connexion définis seront enregistrés.

Configuration des possibilités complémentaires de l'application

Vous pouvez configurer les possibilités complémentaires de Kaspersky Security 10.1.1 for Windows Server depuis Kaspersky Security Center pour un groupe de serveurs ou pour un serveur individuel.

Dans cette section

Configuration des paramètres de la zone de confiance dans Kaspersky Security Center

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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** du groupe de paramètres **Zone de confiance**.

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

4. Sous l'onglet **Exclusions**, indiquez les objets qui seront ignorés par Kaspersky Security 10.1.1 for Windows Server lors de l'analyse :

   - Pour ajouter les exclusions recommandées, cliquez sur le bouton **Ajouter les exclusions recommandées**.

     Quand vous cliquez sur ce bouton, les exclusions recommandées par Microsoft Corporation et celles recommandées par Kaspersky Lab sont ajoutées 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 10.1.1 for Windows Server va considérer 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**

       Ajoute un fichier, un dossier, un disque ou un fichier script à une exclusion.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore la zone, le fichier, le dossier, le disque ou le fichier script prédéfini(e) spécifié(e) lors de l'analyse à l'aide du composant Kaspersky Security 10.1.1 for Windows Server sélectionné dans la section **Zone d'application des exclusions**.

       Cette case est cochée par défaut.

     - **Objets à détecter**

       Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

       Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server détecte tous les objets indiqués par défaut dans l'application.

       Cette case est décochée par défaut.

- **Zone d'application des exclusions**

  Nom de la tâche de Kaspersky Security 10.1.1 for Windows Server 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 que Kaspersky Security 10.1.1 for Windows Server va ignorer 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.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les opérations de lecture de fichiers réalisées par les outils de copie de sauvegarde installés sur le serveur.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server ignore les opérations des processus de confiance sur les fichiers lors de l'analyse.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse les opérations des processus de confiance sur les fichiers.

     Cette case est décochée par défaut.

6. Le cas échéant, ajoutez les processus pour lesquels vous ne souhaitez pas analyser l'activité sur les fichiers (cf. section "Ajout de processus de confiance" à la page 157) en cliquant sur le bouton **Ajouter**.
7. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance** pour enregistrer les modifications.

Ajout de processus de confiance

► *Pour ajouter un ou plusieurs processus à la liste des processus de confiance :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

> Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** du groupe de paramètres **Zone de confiance**.

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

4. Sous l'onglet **Processus de confiance** et cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés**.
5. Cliquez sur **Ajouter**.
6. Sélectionnez une des options suivantes dans le menu contextuel du bouton :

   - **Processus multiples**.

     Configurez les paramètres suivants dans la fenêtre **Ajout de processus de confiance** qui s'ouvre :

     a. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

        Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

        Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

        Cette case est cochée par défaut.

     b. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

        Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

        Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

        Cette case est cochée par défaut.

     c. Cliquez sur le bouton **Parcourir** pour ajouter des données sur la base de processus exécutables.

     d. Dans la fenêtre qui s'ouvre, sélectionnez un fichier exécutable.

        > Vous pouvez ajouter un seul fichier exécutable à la fois. Répétez les étapes c-d pour ajouter d'autres fichiers exécutables.

     e. Cliquez sur le bouton **Processus** pour ajouter des données sur la base de processus en cours.

     f. Dans la fenêtre qui s'ouvre, sélectionnez des processus. Pour sélectionner plusieurs processus, maintenez le bouton **CTRL** enfoncé.

     g. Cliquez sur le bouton **OK**.

Le compte utilisateur sous les privilèges duquel la tâche Protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur le serveur où Kaspersky Security 10.1.1 for Windows Server 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 le serveur local. Vous pouvez sélectionner des processus dans la liste des processus en cours d'exécution en cliquant sur le bouton **Processus** uniquement si vous utilisez la console de d'application sur un serveur local ou dans les paramètres de l'hôte indiqué via Kaspersky Security Center.

- **Un processus sur la base du nom et du chemin d'accès.**

  Configurez les paramètres suivants dans la fenêtre **Ajouter les processus de confiance manuellement** qui s'ouvre :

  a. Saisissez un chemin d'accès au fichier exécutable (y compris le nom du fichier).

  b. Cliquez sur le bouton **OK**.

- **Un processus sur la base des propriétés de l'objet.**

  Configurez les paramètres suivants dans la fenêtre **Ajouter un processus de confiance** qui s'ouvre :

  a. Cliquez sur le bouton **Parcourir** et sélectionnez un processus.

  b. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

     Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

     Cette case est cochée par défaut.

  c. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

     Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

     Cette case est cochée par défaut.

  d. Cliquez sur le bouton **OK**.

  Pour ajouter le processus sélectionné à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

7. Dans la fenêtre **Ajouter un processus de confiance**, cliquez sur le bouton **OK**.

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

Application du masque not-a-virus

Le masque not-a-virus permet d'ignorer les fichiers logiciels et les ressources internet légitimes, qui peuvent être considérés comme nuisibles pendant l'analyse. Le masque concerne les tâches suivantes :

- Protection des fichiers en temps réel
- Analyse à la demande.
- Monitoring des scripts.
- Protection RPC des stockages réseau connectés.
- Protection du trafic.

Si le masque n'est pas ajouté à la liste d'exclusions, Kaspersky Security 10.1.1 for Windows Server applique les actions spécifiées dans les paramètres d'exécution de la tâche pour les ressources logicielles ou Internet qui entrent dans cette catégorie.

► *Pour appliquer le masque not-a-virus, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** du groupe de paramètres **Zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
4. Sous l'onglet **Exclusions**, faites défiler la liste et sélectionnez la ligne avec la valeur **not-a-virus:*** si la case est décochée.
5. Cliquez sur le bouton **OK**.

Une nouvelle configuration est appliquée.

Analyse des disques amovibles

Vous pouvez configurer l'analyse des disques amovibles connectés via USB au serveur protégé.

Kaspersky Security 10.1.1 for Windows Server analyse le disque amovible à l'aide de la tâche Analyse à la demande. L'application crée automatiquement une tâche Analyse à la demande lors de la connexion du disque amovible et supprime cette tâche à la fin de l'analyse. La tâche créée est exécutée selon le niveau de sécurité prédéfini pour l'analyse des disques amovibles. Vous ne pouvez pas configurer les paramètres de la tâche temporaire Analyse à la demande.

Si vous avez installé Kaspersky Security 10.1.1 for Windows Server sans bases antivirus, l'analyse des disques amovibles n'est pas disponible.

Kaspersky Security 10.1.1 for Windows Server lance l'analyse des disques amovibles connectés via USB lorsque ces derniers sont enregistrés dans le système d'exploitation en tant que périphérique de stockage de masse (USB Mass Storage Device). L'application n'analyse pas le disque amovible si la tâche Contrôle des périphériques a bloqué la connexion de ce dernier. L'application ne lance pas l'analyse des périphériques mobiles MTP.

Kaspersky Security 10.1.1 for Windows Server autorise l'accès aux disques amovibles durant l'analyse.

Les résultats de l'analyse de chaque disque amovible peuvent être consultés dans le journal d'exécution de la tâche Analyse à la demande créée lors de la connexion de ce disque.

Vous pouvez modifier les valeurs des paramètres du composant Analyse des disques amovibles (cf. tableau ci-dessous).

Tableau 29. Paramètres d'analyse des disques amovibles

Paramètre	Valeur par défaut	Description
Analyser les disques amovibles à la connexion via USB	Case décochée	Vous pouvez activer ou désactiver l'analyse des disques amovibles lors de leur connexion au serveur protégé via USB.
Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)	1024 Mo	Vous pouvez réduire la plage de déclenchement du composant en indiquant le volume de données maximum sur le disque amovible. Kaspersky Security 10.1.1 for Windows Server ne lance pas l'analyse du disque amovible si le volume des données qu'il contient est supérieur à la valeur indiquée.

Analyser avec le niveau de sécurité	Protection maximale	Vous pouvez configurer les paramètres des tâches d'analyse à la demande créées en choisissant un de trois niveaux de sécurité suivants : • Protection maximale • Recommandé • Performance maximale L'algorithme des actions à effectuer lors de la détection d'objets infectés, probablement infectés et autres, ainsi que d'autres paramètres d'analyse pour chaque niveau de sécurité correspondent aux niveaux de sécurité préétablis dans les tâches d'analyse à la demande.

Pour configurer les paramètres d'analyse des disques amovibles à la connexion, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Complémentaire**, cliquez sur **Configuration** dans le groupe **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.

4. Dans le groupe **Analyse à la connexion**, procédez comme suit :
   - Cochez la case **Analyser les disques amovibles à la connexion via USB** si vous souhaitez que Kaspersky Security 10.1.1 for Windows Server lance automatiquement l'analyse des disques amovibles à la connexion.
   - Le cas échéant, cochez la case **Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.
5. Cliquez sur le bouton **OK**.

   Les paramètres définis seront enregistrés et appliqués.

Configuration des autorisations d'accès dans Kaspersky Security Center

Vous pouvez configurer les autorisations d'accès pour l'administration de l'application et 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 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Ouvrez la section **Complémentaire** et réalisez les opérations suivantes :
   - Si vous souhaitez configurer les autorisations d'accès pour l'administration de Kaspersky Security 10.1.1 for Windows Server pour un utilisateur ou un groupe d'utilisateurs, cliquez sur le bouton **Configuration** dans la section **Autorisations d'accès de l'utilisateur 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 la section **Autorisations d'accès de l'utilisateur pour l'administration du service Security**.
4. Dans la fenêtre qui s'ouvre, configurez les autorisations d'accès (cf. section "Autorisations d'accès pour les fonctions de Kaspersky Security 10.1.1 for Windows Server" à la page 96) en fonction de vos exigences.

Les paramètres 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 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans le groupe **Stockages**.

4. Sous l'onglet **Sauvegarde** de la fenêtre paramètres des **Stockages**, configurez les paramètres de la **Sauvegarde** suivants :
   - Si vous souhaitez définir le **Dossier de 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.
   - Pour indiquer un dossier de restauration, dans le groupe Paramètres de restauration, sélectionnez le dossier requis sur le disque local du serveur protégé ou saisissez le nom du dossier et son chemin d'accès complet dans le champ **Dossier cible pour la restauration des objets**.
5. Dans la fenêtre Paramètres des **stockages**, 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 **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 cible pour la restauration des objets**.
6. Cliquez sur le bouton **OK**.

Les paramètres configurés de la Quarantaine et de la Sauvegarde seront enregistrés.

Interdire l'accès et désinfecter. Liste des ordinateurs bloqués

Cette section décrit comment bloquer les ordinateurs douteux et configurer les paramètres du Stockage des ordinateurs bloqués.

Dans cette section

A propos du Stockage des ordinateurs bloqués

Le stockage des ordinateurs bloqués est installé par défaut si un des composants suivants est installé : Protection des fichiers en temps réel, Protection contre le chiffrement pour NetApp, Protection contre le chiffrement. Les tâches surveillent les tentatives d'accès aux dossiers réseau partagés du serveur protégé ou du périphérique de stockage NAS conformément à la liste des ordinateurs douteux. Les informations relatives aux hôtes bloqués de tous les serveurs protégés sont envoyées au Kaspersky Security Center. Kaspersky Security 10.1.1 for Windows Server bloque l'accès aux dossiers réseau partagés ou aux dossiers de périphériques de stockage NAS pour tous les ordinateurs distants dans la liste des ordinateurs douteux.

Le Stockage des ordinateurs bloqués est rempli quand au moins une des tâches suivantes est lancée en mode actif et quand les conditions indiquées sont remplies :

- En cas de détection d'une activité malveillante émanant d'un ordinateur qui tente d'accéder aux ressources de fichier réseau pendant l'exécution de la tâche Protection des fichiers en temps réel et si la case du paramètre **Ajouter les hôtes à l'origine d'une activité malveillante à la liste des ordinateurs douteux** a été cochée lors de la configuration de la tâche Protection des fichiers en temps réel.

  La case est uniquement disponible dans les paramètres de la stratégie de Kaspersky Security Center

- En cas de détection d'un chiffrement malveillant réalisé par un ordinateur qui accède aux ressources de fichier réseau pendant l'exécution de la tâche Protection contre le chiffrement.
- En cas de détection d'une attaque de ransomware contre le périphérique de stockage NAS pendant l'exécution de la tâche Protection contre le chiffrement pour NetApp.

Après la détection d'une activité ou d'une tentative de chiffrement malveillant, la tâche envoie les informations relatives à l'hôte à l'origine de l'attaque au stockage des ordinateurs bloqués et l'application génère un événement critique pour le blocage de l'hôte. Toutes les tentatives d'accès aux dossiers réseau partagés réalisées au départ de cet hôte seront bloquées.

Par défaut, Kaspersky Security 10.1.1 for Windows Server supprime les ordinateurs douteux de la liste 30 minutes après leur ajout. L'accès de l'ordinateur aux ressources de fichier réseau est rétabli automatiquement après sa suppression de la liste des ordinateurs douteux. Vous pouvez indiquer la durée au terme de laquelle les ordinateurs bloqués sont automatiquement débloqués.

Remarque : lorsque vous limitez l'accès pour la gestion des stockages pour n'importe quel compte utilisateur, le stockage des ordinateurs bloqués reste disponible. Les paramètres Liste des ordinateurs bloqués ne sont pas modifiables, uniquement si le compte utilisateur ne bénéficie pas des droits **Modifier les privilèges** pour l'administration de Kaspersky Security 10.1.1 for Windows Server (cf. section "Configuration des autorisations d'accès à Kaspersky Security 10.1.1 for Windows Server et au service Kaspersky Security" à la page 101).

Activation du blocage des hôtes douteux

Pour ajouter des hôtes qui affichent une activité malveillante ou de chiffrement malveillant au stockage **Liste des ordinateurs bloqués** et bloquer l'accès aux ressources de fichier réseau pour ces hôtes, au moins une des tâches suivantes doit être exécutée en mode actif :

- Protection des fichiers en temps réel
- Protection contre le chiffrement
- Protection contre le chiffrement pour NetApp

► *Configuration de la tâche Protection des fichiers en temps réel :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Sélectionnez l'onglet **Stratégies**, puis ouvrez **<Nom de la stratégie>** > **Protection en temps réel du serveur** > **Configuration** dans le groupe **Protection des fichiers en temps réel**.

   La fenêtre **Protection en temps réel du serveur** s'ouvre.
3. Dans le groupe **Intégration aux autres composants**, cochez la case **Ajouter les hôtes à l'origine d'une activité malveillante à la liste des ordinateurs douteux**, si vous souhaitez que Kaspersky Security 10.1.1 for Windows Server empêche les hôtes pour lesquels une activité malveillante a été détectée lors de l'exécution de la tâche Protection des fichiers en temps réel d'accéder aux ressources de fichier réseau.
4. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la programmation**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
5. Dans la fenêtre **Protection en temps réel du serveur**, cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

► *Configurez la tâche Protection contre le chiffrement :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Sous l'onglet **Stratégies**, ouvrez **<Nom de la stratégie>** > **Contrôle de l'activité réseau** > **Configuration** dans le groupe **Protection contre le chiffrement**.

   La fenêtre **Protection contre le chiffrement** s'ouvre.
3. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la programmation**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
4. Dans la fenêtre **Protection contre le chiffrement**, cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

► *Configurez la tâche Protection contre le chiffrement pour NetApp :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Sous l'onglet **Stratégies**, ouvrez **<Nom de la stratégie>** > **Protection des stockages réseau** > **Configuration** dans le groupe **Protection contre le chiffrement pour NetApp**.

   La fenêtre **Protection contre le chiffrement pour NetApp** s'ouvre.
3. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la programmation**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
4. Dans la fenêtre **Protection contre le chiffrement pour NetApp**, cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server bloque l'accès aux ressources de fichier réseau pour les hôtes qui affichent une activité malveillante ou de chiffrement.

Configuration des paramètres de la Liste des ordinateurs bloqués

► *Pour configurer le Stockage des ordinateurs bloqués :*

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 123).
2. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans le groupe **Stockages**.

   La fenêtre **Paramètres des stockages** s'ouvre.

   > Vous pouvez configurer le paramètre de blocage des hôtes pour le groupe de serveurs administrés via les paramètres de la stratégie. Pour configurer les paramètres de blocage de l'hôte, ouvrez **<Nom de la stratégie>** > **Avancé** et cliquez sur le bouton **Configuration**. Sous l'onglet **Liste des ordinateurs bloqués**, réglez la condition de blocage des hôtes. La Liste des ordinateurs bloqués n'est pas disponible dans les paramètres de la stratégie.
3. Ouvrez l'onglet **Liste des ordinateurs bloqués**.
4. Dans la section **Paramètres du blocage des hôtes**, indiquez le nombre de jours, d'heures et de minutes à décompter à partir du moment du blocage des hôtes et au terme desquels les hôtes de la liste des ordinateurs douteux sont autorisés à accéder aux ressources de fichier réseau.
5. Cliquez sur le bouton **Liste des ordinateurs bloqués**.

6. Exécutez une des actions suivantes :
   - Dans la fenêtre **Liste des ordinateurs douteux** qui s'ouvre, sélectionnez les hôtes 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 hôtes de la liste des ordinateurs douteux et pour rétablir l'accès pour tous les hôtes de la liste des ordinateurs douteux.
7. Cliquez sur le bouton **OK**.

   Les ordinateurs sélectionnés sont débloqués et supprimés de la liste des ordinateurs douteux.
8. Cliquez sur **OK** dans la fenêtre **Paramètres des stockages**.

Les nouveaux paramètres des hôtes de la liste des ordinateurs douteux sont enregistrés.

A propos de la configuration des journaux

La Console d'administration de Kaspersky Security Center permet de configurer les notifications adressées à l'administrateur et aux utilisateurs relatives aux événements liés à l'utilisation de Kaspersky Security 10.1.1 for Windows Server et à l'état de la protection antivirus du serveur protégé :

- 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 10.1.1 for Windows Server pour un ordinateur dans la fenêtre **Propriétés :<nom de l'ordinateur>** ou pour un groupe d'ordinateurs dans la fenêtre **Propriétés : <nom de la stratégie>** du groupe d'administration sélectionné.

L'onglet **Evénements** ou la fenêtre **Configuration des notifications** permettent de configurer les types de notification suivants :

- 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 *Système d'aide de Kaspersky Security Center*.
- La fenêtre **Configuration 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 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 **Configuration des notifications**, l'administrateur système recevra les notifications relatives à ces événements via la méthode indiquée deux fois.

Dans cette section

Configuration des paramètres du journal

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 for Windows Server*.

► *Pour configurer les journaux de Kaspersky Security 10.1.1 for Windows Server, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans le groupe **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Journaux d'exécution de la tâche**.
4. Dans la fenêtre **Paramètres des journaux**, configurez les paramètres suivants de Kaspersky Security 10.1.1 for Windows Server conformément à vos exigences :
   - 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 10.1.1 for Windows Server pour lequel vous souhaitez indiquer le niveau de détails.
     b. Pour définir le niveau de détails dans les journaux d'exécution de la tâche et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Niveau d'importance**.
   - Pour modifier l'emplacement par défaut des journaux, 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 le bouton **OK**.

Les paramètres des journaux configurés sont conservés.

Journaux de sécurité

Kaspersky Security 10.1.1 for Windows Server tient un journal des événement liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le serveur protégé. Ce journal enregistre les événements suivants :

- Evénements de Protection contre les exploits.
- Les événements critiques du composant Inspection des journaux.
- Les événements critiques qui indiquent une tentative de violation de la sécurité (pour les tâches Protection en temps réel du serveur, Analyse à la demande, Moniteur d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez purger les journaux de sécurité ainsi que le journal d'audit système. Dans ce cas, Kaspersky Security 10.1.1 for Windows Server enregistre l'événement d'audit système sur la purge du journal de sécurité.

Configuration des paramètres d'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des volumes des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il récolte et analyse les événements reçus et réalise également d'autres actions d'administration des journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : ce mode suppose que tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'ordinateur local même après avoir été envoyés à SIEM.

  Il est recommandé d'utiliser ce mode pour réduire au maximum la charge sur le serveur protégé.

- Supprimer les copies locales des événements : ce mode suppose que tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans SIEM soient supprimés de l'ordinateur local.

  L'application ne supprime jamais les versions locales des journaux de sécurité.

Kaspersky Security 10.1.1 for Windows Server peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus pas le SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Pour réduire le risque d'erreur d'envoi des événements à SIEM, vous pouvez indiquer les paramètres de connexion au serveur syslog de miroir.

Le serveur syslog de miroir est un serveur syslog complémentaire vers lequel l'application passe automatiquement si la connexion au serveur principal syslog ou son utilisation sont impossibles.

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres de fonctionnement (cf. tableau ci-dessous).

Tableau 30. Paramètres d'intégration à SIEM

Paramètre	Valeur par défaut	Description
Envoyer les événements à un serveur syslog externe via le protocole syslog	Pas appliqué	Vous pouvez activer et désactiver l'intégration à SIEM en cochant ou décochant la case.
Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi à SIEM en cochant ou décochant la case.

Paramètre	Valeur par défaut	Description
Format des événements	Données structurées	Vous pouvez choisir un de deux formats sous lesquels l'application convertit les événements avant de les envoyer au serveur syslog pour mieux les reconnaître au niveau du SIEM.
Protocole de connexion	TCP	Vous pouvez utiliser la liste déroulante pour configurer la connexion au serveur syslog principal via les protocoles UPD ou TCP et au serveur syslog miroir via le protocole TCP.
Paramètres de connexion au serveur syslog principal	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.
Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible	Pas appliqué	Vous pouvez activer et désactiver l'application du serveur syslog de miroir à l'aide de la case.
Paramètres de connexion au serveur syslog complémentaire	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.

► *Pour configurer les paramètres d'intégration à SIEM, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

   Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans le groupe **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Journaux d'exécution de la tâche**.

   La fenêtre **Paramètres des journaux et des notifications** s'ouvre.

4. Sélectionnez l'onglet **Intégration à SIEM**.

5. Dans le groupe **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.

   La case active ou désactive l'utilisation de la fonction d'envoi des événements publiés au serveur syslog externe.

   Si la case est cochée, l'application exécute l'envoi des événements publiés sur SIEM conformément à la configuration des paramètres d'intégration à SIEM.

   Si la case est décochée, l'application n'exécute pas l'intégration à SIEM. Vous ne pouvez pas configurer les paramètres d'intégration à SIEM si la case est décochée.

   Cette case est décochée par défaut.

6. Si besoin, dans le groupe **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe**.

   La case active ou désactive la suppression des copies locales des journaux au moment de leur envoi à SIEM.

   Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le SIEM. Il est recommandé d'utiliser ce mode sur les ordinateurs de faible puissance.

   Si la case est décochée, l'application envoie uniquement les événements à SIEM. Les copies des journaux continuent d'être conservées localement.

   Cette case est décochée par défaut.

   L'état de la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe** n'influence pas les paramètres de conservation des événements des journaux sécurité : l'application ne supprime jamais automatiquement les événement des journaux de sécurité.

7. Dans le groupe **Format des événements**, indiquez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi à SIEM.

   Par défaut, l'application exécute la conversion au format de données structurées.

8. Dans le groupe **Paramètres de connexion**, procédez comme suit :
   - Indiquez le protocole de connexion à SIEM.
   - Indiquez les paramètres de connexion au serveur syslog principal.

     Vous pouvez indiquer l'adresse IP uniquement au format IPv4.
   - Si besoin, cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n'est pas disponible.
     - Définissez les paramètres suivants de connexion au serveur syslog de miroir : **Adresse IP** et **Port**.

       Les champs **Adresse IP** et **Port** pour le serveur syslog de miroir ne peuvent pas être modifiés si la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible** est décochée.

       Vous pouvez indiquer l'adresse IP uniquement au format IPv4.
9. Cliquez sur le bouton **OK**.

Les paramètres d'intégration à SIEM configurés seront appliqués.

Configuration des paramètres des notifications

► *Pour configurer les notifications de Kaspersky Security 10.1.1 for Windows Server, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans le groupe **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Notifications sur les événements**.

4. Dans la fenêtre **Configuration des notifications**, configurez les paramètres suivants de Kaspersky Security 10.1.1 for Windows Server conformément à vos exigences :

   - Sélectionnez le type de notification dont vous souhaitez configurer les paramètres dans la liste **Configuration des notifications**.
   - Configurez le mode de notification de l'utilisateur dans le groupe **Informer les utilisateurs**. Le cas échéant, rédigez le texte de la notification.
   - Configurez le mode de notification de l'administration 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 supplémentaires des notifications.
   - Définissez dans le groupe **Seuils de déclenchement des événements** les intervalles à l'issue desquels Kaspersky Security 10.1.1 for Windows Server enregistre les événements *Bases de l'application dépassées, Bases de l'application fortement dépassées* et *Analyse des zones critiques non réalisée depuis longtemps*.

     - **Les bases de l'application sont dépassées (jours)**

       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 (jours)**

       Nombre de jours écoulés depuis la dernière mise à jour des bases de l'application.

       La valeur par défaut est de 14 jours.

     - **Analyse des zones critiques non réalisée depuis longtemps (jours)**

       Nombre de jours depuis la dernière exécution réussie de la tâche d'analyse des zones critiques.

       La valeur par défaut est de 30 jours.

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

Les paramètres de la notification définis seront enregistrés.

Configuration de l'interaction avec le Serveur d'administration

► *Pour sélectionner les types des objets au sujet desquels Kaspersky Security 10.1.1 for Windows Server va envoyer des informations au serveur d'administration de Kaspersky Security Center :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Cliquez sur **le bouton Configuration** dans le bloc Interaction **avec** le Serveur d'administration **de la section** Journaux et notifications.

   La fenêtre **Listes réseau du Serveur d'administration** s'ouvre.
4. Dans la fenêtre **Listes réseau du Serveur d'administration**, choisissez les types d'objets au sujet desquels Kaspersky Security 10.1.1 for Windows Server va transmettre des informations au serveur d'administration de Kaspersky Security Center :
   - Objets de la quarantaine.
   - Objets sauvegardés.
   - Liste des ordinateurs douteux.
5. Cliquez sur le bouton **OK**.

   Kaspersky Security 10.1.1 for Windows Server transmet les informations relatives aux types d'objets choisis au Serveur d'administration.

Protection en temps réel du serveur

Cette section présente la tâche Protection en temps réel du serveur : la tâche Protection des fichiers en temps réel, Utilisation du KSN, Monitoring des scripts et Protection contre les exploits. Cette section contient également des instructions relatives à la configuration des tâches de protection en temps réel et à la gestion des paramètres de sécurité d'un serveur protégé.

Contenu du chapitre

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 10.1.1 for Windows Server analyse les objets du serveur protégé suivants lorsqu'ils sont sollicités :

- Les fichiers,
- 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.
- Fichiers conteneurs Windows Server 2016 et Windows Server 2019.

Lorsqu'un programme quelconque enregistre un fichier sur le serveur ou tente de le lire, Kaspersky Security 10.1.1 for Windows Server intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace, il exécute les actions que vous avez définies dans les paramètres de la tâche ou par défaut : il tente de désinfecter le fichier, le place en quarantaine ou il le supprime. Kaspersky Security 10.1.1 for Windows Server rend le fichier à l'application uniquement s'il est sain ou si sa désinfection a réussi.

Kaspersky Security 10.1.1 for Windows Server intercepte s opérations sur les fichiers exécutées dans les conteneurs Windows Server 2016.

Un *conteneur* est un environnement isolé qui permet aux applications de s'exécuter sans interaction directe avec le système d'exploitation. Si le conteneur se trouve dans la zone de protection de la tâche, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers du conteneur lorsqu'ils sont sollicités par les utilisateurs à la recherche de menaces informatiques. En cas de détection d'une menace, l'application tente de désinfecter le conteneur. Si la tentative réussit, le conteneur continue à fonctionner. Si la désinfection échoue, il est arrêté.

Kaspersky Security 10.1.1 for Windows Server détecte également les applications malveillantes pour les processus exécutés dans le sous-système Windows pour Linux®. Pour ces processus, la tâche Protection des fichiers en temps réel applique l'action définie par la configuration actuelle.

Configuration de la tâche Protection des fichiers en temps réel

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

Tableau 31. Paramètres par défaut de la tâche Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
Zone de protection	L'ensemble de l'ordinateur, à l'exception des disques virtuels.	Vous pouvez limiter la zone de protection.
Niveau de sécurité	Identique pour toute la zone de protection ; correspond au niveau de sécurité **Recommandé**.	Pour les entrées sélectionnées dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez : • Appliquer un autre niveau de sécurité prédéfini ; • Modifier manuellement le niveau de sécurité ; • Enregistrer la configuration des paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud.
Mode de protection des objets	A l'accès et à la modification.	Vous pouvez sélectionner le mode de protection, c'est-à-dire définir le type d'accès auquel Kaspersky Security 10.1.1 for Windows Server va analyser l'objet.
Analyse 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.
Appliquer la zone de confiance	Appliquée.	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.

Paramètre	Valeur par défaut	Description
Utiliser KSN pour la protection	Appliquée.	Vous pouvez améliorer l'efficacité de la protection du serveur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Planification du lancement de la tâche	Au lancement de l'application.	Vous pouvez configurer le lancement de la tâche planifiée.
Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante	Pas appliqué.	Vous pouvez ajouter les ordinateurs qui manifestent une activité malveillante à la liste des ordinateurs douteux.

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

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection des fichiers en temps réel**, cliquez sur le bouton **Configuration** du groupe **Protection des fichiers en temps réel**.

   La fenêtre **Protection des fichiers en temps réel** s'ouvre.
4. Configurez les paramètres de la tâche suivants :
   - Sous l'onglet **Général** :
     - Mode de protection (cf. section "Sélection du mode de protection" à la page 182)
     - Utilisation de l'analyse heuristique (à la page 181)
     - Paramètres d'intégration aux autres composants de Kaspersky Security 10.1.1 for Windows Server.
   - Sous l'onglet **Administration des tâches** :
     - Paramètres de lancement de la tâche planifiée (cf. section "Configuration des paramètres de la planification du lancement des tâches" à la page 143).

5. Sélectionnez l'onglet **Zone de protection**, puis réalisez les opérations suivantes :
   - Cliquez sur le bouton **Ajouter** ou **Modifier** pour modifier la zone de protection (cf. section "Zone de protection dans la tâche Protection des fichiers en temps réel" à la page 183).
     - Dans la fenêtre qui s'ouvre, sélectionnez les éléments que vous souhaitez inclure dans la zone de protection de la tâche :
       - **Zone prédéfinie**
       - **Disque, dossier ou objet réseau**
       - **Fichier**
     - Sélectionnez un des niveaux de sécurité prédéfinis (cf. section "Sélection des niveaux de sécurité prédéfinis" à la page 185) ou configurez manuellement les paramètres de protection (cf. section "Configuration manuelle des paramètres de sécurité" à la page 187).
6. Cliquez sur le bouton **OK** dans la fenêtre **Protection des fichiers en temps réel**.

Kaspersky Security 10.1.1 for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

Utilisation de l'analyse heuristique

Vous pouvez utiliser l'analyse heuristique et configurer le niveau d'analyse pour les tâches de Kaspersky Security 10.1.1 for Windows Server.

► *Pour configurer l'analyse heuristique :*

1. Ouvrez les paramètres de l'application (cf. Section "Gestion de Kaspersky Security 10.1.1 for Windows Server à partir de Kaspersky Security Center" à la page 148) ou ceux de la stratégie (cf. section "Configuration d'une stratégie" à la page 109) pour laquelle vous souhaitez configurer l'Analyse heuristique.
2. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

   La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

   Si la case est cochée, l'analyse heuristique est activée.

   Si la case est décochée, l'analyse heuristique est désactivée.

   Cette case est cochée par défaut.

3. 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'analyse 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'analyse heuristique** est cochée.

4. Cliquez sur le bouton **OK**.

Les paramètres configurés de la tâche seront appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Sélection du mode de protection

La tâche Protection des fichiers en temps réel permet de sélectionner le mode de protection. Le groupe **Mode de protection d'objets** permet de définir le type d'accès aux objets déclenchant une analyse par Kaspersky Security 10.1.1 for Windows Server.

Le paramètre **Mode de protection d'objets** possède une valeur unique pour toute la zone de protection reprise dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les entrées particulières de la zone de protection.

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

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du bloc **Protection des fichiers en temps réel**.

   La fenêtre **Protection des fichiers en temps réel** s'ouvre.

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

   - **Mode intelligent**

     Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server analyse à nouveau cet objet uniquement après la dernière sauvegarde effectuée par ce processus.

   - **A l'accès et à la modification**

     Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

   - **A l'exécution**

     Kaspersky Security 10.1.1 for Windows Server analyse le fichier uniquement en cas d'ouverture pour exécution.

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

Le mode de protection des objets sélectionné sera adopté.

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

Zones de protection prédéfinies

Les ressources fichiers du serveur protégé s'affichent dans les paramètres de la tâche **Protection des fichiers en temps réel** sous l'onglet **Zone de protection**.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Security 10.1.1 for Windows Server couvre les zones de protection définies suivantes :

- **Disques durs locaux**. Kaspersky Security 10.1.1 for Windows Server protège les fichiers sur les disques durs du serveur.
- **Disques amovibles**. Kaspersky Security 10.1.1 for Windows Server 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.
- **Réseau**. Kaspersky Security 10.1.1 for Windows Server protège les fichiers qui sont enregistrés dans les dossiers réseau ou qui y sont lus par les applications exécutées sur le serveur. Kaspersky Security 10.1.1 for Windows Server ne protège pas les fichiers dans les répertoires réseau lorsqu'ils sont sollicités par des applications depuis d'autres ordinateurs.
- **Disques virtuels**. 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.

Par défaut, vous pouvez afficher et configurer des zones de protection prédéfinies dans la liste de zones ; vous pouvez également ajouter des zones prédéfinies à la liste au moment de sa création dans les paramètres de la zone de protection.

La zone de protection inclut par défaut tous les secteurs prédéfinis, à l'exception des disques virtuels.

Les disques virtuels créés à l'aide de la commande SUBST ne figurent pas dans l'arborescence des ressources fichier du serveur dans la console d'application. Pour inclure les objets d'un disque virtuel 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 affichés dans la liste des ressources fichier du serveur. Pour inclure les objets d'un disque réseau dans la zone de protection, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

Sélection des niveaux de sécurité prédéfinis

Pour les entrées sélectionnées dans la liste des ressources de fichiers de l'ordinateur, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité prédéfinie (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si des mesures de sécurité du serveur complémentaires ont été adoptées dans votre réseau, telles que des pare-feu ou des stratégies de sécurité, en plus de Kaspersky Security 10.1.1 for Windows Server.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre 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 dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité informatique élevé.

Tableau 32. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Options	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Protection des objets	Selon l'extension	En fonction du format	En fonction du format
Protection uniquement des nouveaux fichiers et des fichiers modifiés	Activée	Activée	Désactivée

Options	Niveau de sécurité		
Actions à exécuter sur les objets infectés et autres	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible
Actions à exécuter sur les objets probablement infectés	Interdire l'accès et placer en quarantaine	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et placer en quarantaine
Exclure les fichiers	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 configuré
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
Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré	Oui	non	Oui

Les paramètres **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si, après avoir choisi un des niveaux de sécurité prédéfinis, vous modifiez les paramètres de sécurité **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique**, le niveau de sécurité 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 d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du bloc **Protection des fichiers en temps réel**.

   La fenêtre **Protection des fichiers en temps réel** s'ouvre.
4. Sous l'onglet **Zone de protection**, choisissez le nœud dont vous souhaitez configurer les paramètres de sécurité, puis cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de la protection des fichiers en temps réel** s'ouvre.
5. Choisissez le niveau de sécurité requis dans la liste déroulante :
   - **Protection maximale**
   - **Recommandé**
   - **Performance maximale**
6. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Kaspersky Security 10.1.1 for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont 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 toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé** (cf. section "Sélection des niveaux de sécurité prédéfinis" à la page 185).

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 différentes entrées dans l'arborescence ou la liste des ressources de fichiers du serveur.

Lorsque vous utilisez l'arborescence des ressources du fichier serveur, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

► *Pour configurer manuellement les paramètres de sécurité du nœud sélectionnée :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du bloc **Protection des fichiers en temps réel**.

   La fenêtre **Protection des fichiers en temps réel** s'ouvre.
4. Sous l'onglet **Zone de protection**, choisissez le nœud dont vous souhaitez configurer les paramètres de sécurité, puis cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de la protection des fichiers en temps réel** s'ouvre.
5. Sous l'onglet **Niveau de sécurité**, vous pouvez sélectionner tout nouveau existant ou cliquer sur le bouton **Configuration** pour définir une configuration personnalisée.
6. Vous pouvez configurer les paramètres de sécurité personnalisés du nœud sélectionné en fonction de vos exigences.
   - Paramètres généraux (cf. section "Configuration des règles prédéfinies d'une tâche" à la page 188)
   - Actions (cf. section "Configuration des actions" à la page 191)
   - Optimisation (cf. section "Configuration de l'optimisation" à la page 193)
7. Cliquez sur **Enregistrer** dans la fenêtre **Configuration de la zone de protection**.

Les paramètres de la nouvelle zone de protection sont enregistrés.

Configuration des paramètres de tâche généraux

► *Configuration des paramètres généraux de sécurité de la tâche Protection des fichiers en temps réel*

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "Configuration manuelle des paramètres de sécurité" à la page 187).
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Protection des objets**, indiquez les types d'objets que vous souhaitez inclure à la zone de protection :
   - **Tous les objets**

     Kaspersky Security 10.1.1 for Windows Server analyse tous les objets.
   - **Objets analysés en fonction du format**

     Kaspersky Security 10.1.1 for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

     Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security 10.1.1 for Windows Server.
   - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

     Kaspersky Security 10.1.1 for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

     Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security 10.1.1 for Windows Server.
   - **Objets analysés en fonction de la liste d'extensions indiquée**

     Kaspersky Security 10.1.1 for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.
   - **Analyser les secteurs d'amorçage et la partition MBR**

     Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les secteurs et les zones d'amorce sur les disques durs et les disques amovibles du serveur.

     Cette case est cochée par défaut.
   - **Analyser les flux NTFS alternatifs**

     Analyse des flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

     Si la case est cochée, l'application analyse un objet probablement infecté et tous les flux NTFS associés à cet objet.

     Si la case est décochée, l'application analyse uniquement l'objet qui a été détecté et considéré comme probablement infecté.

     Cette case est cochée par défaut.

4. Dans la section **Optimisation**, cochez ou décochez la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés**.

   La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security 10.1.1 for Windows Server a identifiés comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

   Si la case est décochée, vous pouvez décider si vous souhaitez analyser et protéger uniquement les nouveaux fichiers ou tous les fichiers, quel que soit leur état de modification.

   La case est cochée par défaut pour le niveau de sécurité **Performance maximale** et **Recommandé**. Si le niveau de sécurité sélectionné est **Protection maximale**, la case est décochée.

   Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous**/**Nouveaux** uniquement de chacun des types d'objets composés.

5. Dans le groupe **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :

   - **Toutes les/ uniquement les nouvelles archives**

     Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les archives.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 auto-extractibles.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les archives SFX.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 d'emails**

     Analyse des fichiers des bases de données de messagerie de Microsoft Outlook et Microsoft Outlook Express.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers des bases de données de messagerie.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers aux formats de messagerie.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server analyse les objets intégrés au fichier.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration des actions

► *Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "Configuration manuelle des paramètres de sécurité" à la page 187).
2. Sélectionnez l'onglet **Actions**.

3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

   - **Informer uniquement**.

     En cas de détection de ce mode, Kaspersky Security 10.1.1 for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'écran suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté*. *Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

     Le mode **Informer uniquement** doit être configuré séparément pour chaque zone de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security 10.1.1 for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

   - **Bloquer l'accès**.

     Lorsque cette option est sélectionnée, Kaspersky Security 10.1.1 for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.

   - **Exécuter une action supplémentaire**.

     Sélectionnez l'action dans la liste déroulante.

     - **Désinfecter**.
     - **Désinfecter. Supprimer si la désinfection est impossible**.
     - **Supprimer**.
     - **Recommandé**.

4. Sélectionnez l'action à exécuter sur les objets probablement infectés :

   - **Informer uniquement**.

     En cas de détection de ce mode, Kaspersky Security 10.1.1 for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'écran suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté*. *Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

     Le mode **Informer uniquement** doit être configuré séparément pour chaque zone de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security 10.1.1 for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

   - **Bloquer l'accès**.

     Lorsque cette option est sélectionnée, Kaspersky Security 10.1.1 for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.

   - **Exécuter une action supplémentaire**.

     Sélectionnez l'action dans la liste déroulante.

     - **Quarantaine**.
     - **Supprimer**.
     - **Recommandé**.

5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
   a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

      Si la case est cochée, vous pouvez définir une action principale et secondaire pour chaque type d'objet détecté en cliquant sur le bouton **Configuration** en regard de la case.

      Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server exécute les actions sélectionnées dans les sections **Actions à exécuter sur les objets infectés et autres** et **Actions à exécuter sur les objets probablement infectés** des types d'objets nommés, respectivement.

      Cette case est décochée par défaut.

   b. Cliquez sur le bouton **Configuration**.
   c. Dans la fenêtre qui s'ouvre, choisissez la première action et l'action secondaire (si la première échoue) pour chaque type de l'objet détecté.
   d. Cliquez sur le bouton **OK**.
6. Choisissez l'action à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**.

   La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

   Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security 10.1.1 for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

   Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security 10.1.1 for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.

   La case est cochée par défaut pour le niveau de sécurité **Protection maximale** et décochée pour les niveaux de sécurité **Recommandé** et **Performance maximale**.
7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'optimisation

► *Pour confirmer l'optimisation de la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "Configuration manuelle des paramètres de sécurité" à la page 187).
2. Sélectionnez l'onglet **Optimisation**.

3. Dans le groupe **Exclusions** :
   - Cochez ou décochez la case **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 10.1.1 for Windows Server ignore les objets indiqués pendant l'analyse.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse tous les objets.

     Cette case est décochée par défaut.
   - Cochez ou décochez la case **Ne pas détecter**.

     Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus https://securelist.fr/.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server détecte tous les objets indiqués par défaut dans l'application.

     Cette case est décochée par défaut.
   - Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.
4. 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 limitée 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 dont la taille est supérieure à la valeur indiquée.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore pour la recherche de virus les objets composés dont la taille est supérieure à la valeur indiquée.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse les objets composés sans tenir compte de la taille.

     La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- **Utiliser la technologie iSwift**

  iSwift compare l'identifiant NTFS du fichier, identifiant stocké dans une base de données, avec un identifiant en cours. L'analyse est effectuée uniquement pour les fichiers dont les identifiant ont changé (nouveaux fichiers et fichiers modifiés depuis la dernière analyse des objets système NTFS).

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse des objets système NTFS.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers du système NTFS en ignorant la date de création ou de modification.

  Cette case est cochée par défaut.

- **Utiliser la technologie iChecker**

  iChecker calcule et enregistre les sommes de contrôle des fichiers analysés. Si un objet est modifié, la somme de contrôle change. L'application compare toutes les sommes de contrôle pendant la tâche d'analyse et analyse uniquement les fichiers nouveaux et modifiés depuis la dernière analyse de fichiers.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers nouveaux et modifiés.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers en ignorant leur date de création ou de modification.

  Cette case est cochée par défaut.

5. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

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

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 10.1.1 for Windows Server face aux nouvelles menaces, augmente l'efficacité de certains modules de la protection et réduit la possibilité de faux positifs.

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Kaspersky Security 10.1.1 for Windows Server 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.

Pour de plus amples informations sur le transfert, le traitement, le stockage et la destruction des informations sur l'utilisation de l'application, vous pouvez consulter la fenêtre Traitement des données de la tâche Utilisation du KSN et la Politique de confidentialité sur le site Internet de Kaspersky Lab.

La participation au Kaspersky Security Network est volontaire. La décision de participer à Kaspersky Security Network est prise pendant ou après l'installation de Kaspersky Security 10.1.1 for Windows Server. Vous pouvez changer d'avis quant à votre décision de participer au Kaspersky Security Network à n'importe quel moment.

Le réseau Kaspersky Security Network peut être utilisé dans les tâches suivantes de Kaspersky Security 10.1.1 for Windows Server :

- Protection des fichiers en temps réel
- Analyse à la demande.
- Contrôle du lancement des applications.
- Protection du trafic.
- Protection RPC des stockages réseau connectés.
- Protection ICAP des stockages réseau connectés.

Kaspersky Private Security Network

Vous trouverez toutes les informations détaillées sur la configuration de Private Security Network (ci-après "KSN privé") dans l'*aide de Kaspersky Security Center*.

Si vous utilisez le KSN privé sur l'ordinateur protégé, dans la fenêtre **Traitement des données** (cf. section "Configuration du traitement des données" à la page 200) de la tâche Utilisation du KSN, vous pouvez lire la Déclaration de KPSN et activer la tâche à tout moment en cochant la case **J'accepte les conditions de participation au programme Kaspersky Private Security Network**. En acceptant les conditions, vous acceptez d'envoyer tous types de données mentionnées dans la Déclaration de KSN (demandes de sécurité, données statistiques) aux services KSN.

Quand vous avez accepté les conditions du KSN privé, les cases qui règlent l'utilisation du KSN global sont indisponibles.

Si vous désactivez le KSN privé lorsque la tâche Utilisation du KSN est en cours d'exécution, l'erreur *Violation de la licence* se produit et la tâche s'arrête. Pour continuer à protéger le serveur, vous devez accepter manuellement la Déclaration du KSN global dans la fenêtre **Traitement des données** et relancer la tâche.

Annulation de l'acceptation de la Déclaration de KSN

Vous pouvez annuler l'acceptation et arrêter tout échange de données avec Kaspersky Security Network à n'importe quel moment. Les actions suivantes sont considérées comme l'annulation complète ou partielle de la Déclaration de KSN :

- Si vous décochez la case **Envoyer des données sur les fichiers analysés**, l'application arrête d'envoyer des sommes de contrôle des fichiers analysés au service KSN pour analyse.
- Si vous décochez la case **Envoyer les données relatives aux URL sollicitées**, l'application arrête d'envoyer des URL pour analyse.
- Si vous décochez la case **Envoyer les statistiques de Kaspersky Security Network**, l'application arrête de traiter des données avec des statistiques KSN supplémentaires.
- Si vous décochez la case **J'accepte les conditions de la Déclaration de Kaspersky Security Network**, l'application arrête le traitement de toutes les données liées à KSN et la tâche Utilisation du KSN s'arrête.
- Si vous décochez la case **'accepte les conditions de la Déclaration de Kaspersky Managed Protection**, les services KMP sont désactivés.
- Désinstallation du composant Utilisation du KSN : le traitement de toutes les données liées à KSN s'arrête.
- Désinstallation de Kaspersky Security 10.1.1 for Windows Server via Kaspersky Security Center : le traitement de toutes les données liées à KSN s'arrête.

Configuration de la tâche Utilisation du KSN

Vous pouvez modifier les paramètres de la tâche Utilisation du KSN précisés par défaut (cf. tableau ci-dessous).

Tableau 33. Paramètres par défaut de la tâche Utilisation du KSN

Paramètre	Valeur par défaut	Description
Actions à exécuter sur les objets douteux selon KSN	Supprimer	Vous pouvez préciser les actions que Kaspersky Security 10.1.1 for Windows Server va exécuter sur les objets réputés comme douteux par KSN.
Transfert de données	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 10.1.1 for Windows Server calcule les hash MD5 pour les fichiers de n'importe quelle taille.
Déclaration de KSN	La case **J'accepte les conditions de la Déclaration de Kaspersky Security Network** est décochée.	Décidez de participer ou non à KSN après l'installation. Vous pouvez modifier votre choix concernant l'utilisation du KSN à tout moment.
Envoyer les statistiques de Kaspersky Security Network	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les statistiques de KSN seront envoyées automatiquement, sauf si vous décochez la case.
Envoyer des données sur les fichiers analysés	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les données sur les fichiers précédemment analysés depuis le démarrage de la tâche sont envoyées. Il est possible de décocher la case à tout moment.
Envoyer les données relatives aux URL sollicitées	Décochée	Si la Déclaration de KSN, l'application envoie des informations relatives aux URL consultées à Kaspersky Lab.
J'accepte les conditions de la Déclaration de Kaspersky Managed Protection	Décochée	Vous pouvez activer et désactiver l'application de n'importe quelle heuristique. Le service est disponible uniquement si l'accord séparé a été signé pendant le processus d'achat de l'application.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	Vous pouvez lancer la tâche manuellement ou planifier son exécution.
Utiliser Kaspersky Security Center en tant que serveur proxy du KSN	Sélectionné	Par défaut, les données sont envoyées à KSN via Kaspersky Security Center.

► *Pour configurer les paramètres de la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud

Appareils administrés, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du groupe **Utilisation du KSN**.

   La fenêtre **Utilisation du KSN** s'ouvre.

4. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :

   - Dans le groupe **Actions à exécuter sur les objets douteux selon KSN**, indiquez l'action que Kaspersky Security 10.1.1 for Windows Server doit exécuter en cas de détection d'un objet identifié comme infecté par le KSN :
     - **Supprimer**

       Kaspersky Security 10.1.1 for Windows Server supprime l'objet considéré comme douteux selon les données du KSN et place une copie de celui-ci dans la sauvegarde.

       Cette option est sélectionnée par défaut.

     - **Consigner les informations**

       Kaspersky Security 10.1.1 for Windows Server consigne dans le journal d'exécution de la tâche les informations sur l'objet considéré comme douteux selon les données du KSN. Kaspersky Security 10.1.1 for Windows Server ne supprime pas l'objet douteux.
   - Dans le groupe **Transfert de données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :
     - Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi à KSN si la taille du fichier est supérieure à (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 10.1.1 for Windows Server 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 10.1.1 for Windows Server calcule la somme de contrôle pour les fichiers de n'importe quelle taille.

Cette case est cochée par défaut.

- Le cas échéant, modifiez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Security 10.1.1 for Windows Server calcule la somme de contrôle.

- Dans la section **Serveur proxy du KSN**, cochez ou décochez la case **Utiliser Kaspersky Security Center en tant que serveur proxy du KSN**.

  La case permet d'administrer le transfert de données entre les serveurs protégés et KSN.

  Si la case est décochée, les données du serveur d'administration et des serveurs protégés sont envoyées à KSN directement (et non via Kaspersky Security Center). La stratégie active définit le type de données qui peut être envoyé directement à KSN.

  Si la case est cochée, toutes les données sont envoyées à KSN via Kaspersky Security Center.

  Cette case est cochée par défaut.

  Pour activer le proxy KSN, la Déclaration de KSN doit être acceptée et Kaspersky Security Center correctement configuré. Cf. *Système d'aide de Kaspersky Security Center* pour plus de détails.

5. Le cas échéant, configurez la planification du lancement de la tâche sous l'onglet **Administration des tâches**. Par exemple, vous pouvez démarrer la tâche planifiée et choisir la fréquence **Au lancement de l'application** si vous souhaitez que la tâche soit lancée automatiquement au redémarrage du serveur.

   L'application lancera la tâche Utilisation du KSN selon la planification.

6. Configurez le traitement des données (cf. section "Configuration du traitement des données" à la page 200) avant de lancer la tâche.

7. Cliquez sur le bouton **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.

Configuration du traitement des données

► *Pour configurer les données qui seront traitées par les services KSN et accepter la déclaration de KSN, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Traitement des données** du bloc **Utilisation du KSN**.

   La fenêtre **Traitement des données** s'ouvre.
4. Sous l'onglet**Statistiques et services**, lisez la Déclaration et cochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Security Network**.
5. Pour augmenter le niveau de protection, les cases suivantes sont automatiquement cochées :
   - **Envoyer des données sur les fichiers analysés**.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server envoie la somme de contrôle des fichiers analysés à Kaspersky Lab. La conclusion sur la sécurité de chaque fichier est basée sur la réputation reçue de KSN.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server n'envoie pas la somme de contrôle des fichiers à KSN.

     Remarque : les demandes concernant la réputation du fichier peuvent être envoyées en mode limité. Les limitations servent à la protection des serveurs de réputation Kaspersky Lab contre les DDoS. Dans ce scénario, les paramètres des demandes de réputation des fichiers, en cours d'envoi, sont définis par les règles et méthodes établies par les experts de Kaspersky Lab. L'utilisateur ne peut pas les configurer sur un ordinateur protégé. Les mises à jour de ces règles et méthodes sont reçues avec les mises à jour des bases de données de l'application. Si les limitations sont appliquées, l'état *Activé par Kaspersky Lab pour protéger les serveurs de KSN contre les attaques DDoS* apparaît dans les statistiques de la tâche Utilisation du KSN.

     Cette case est cochée par défaut.

- **Envoyer les données relatives aux URL sollicitées**.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server envoie les données des ressources Internet demandées, y compris des adresses Internet à Kaspersky Lab. La conclusion sur la sécurité des ressources Internet demandées est basée sur la réputation reçue de KSN.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server n'obtient pas les informations relatives à la réputation des adresses Internet depuis le KSN.

  Cette case est cochée par défaut.

  La case a une influence sur la configuration de la tâche Protection du trafic.

Vous pouvez décocher ces cases et arrêter d'envoyer des données supplémentaires à tout moment.

6. La case **Envoyer les statistiques de Kaspersky Security Network** est cochée par défaut. Vous pouvez décocher la case à tout moment si vous ne souhaitez pas que Kaspersky Security 10.1.1 for Windows Server envoie des statistiques complémentaires à Kaspersky Lab.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server envoie des statistiques supplémentaires qui peuvent contenir des données personnelles. La liste de toutes les données envoyées comme des statistiques KSN sont spécifiées dans la Déclaration de KSN. Les données reçues par Kaspersky Lab servent à améliorer la qualité des applications et le niveau des taux de détection des menaces.

   Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server n'envoie pas de statistiques supplémentaires.

   Cette case est cochée par défaut.

7. Sous l'onglet **Kaspersky Managed Protection**, lisez la Déclaration et cochez la case **J'accepte les conditions de la Déclaration de Kaspersky Managed Protection**.

   Si la case est cochée, vous acceptez d'envoyer les statistiques sur l'activité du serveur protégé aux spécialistes de Kaspersky Lab. Les données reçues sont utilisées pour l'analyse et la génération de rapports 24h/24 requises afin d'éviter les incidents liées à une violation de sécurité.

   Cette case est décochée par défaut.

Les changements d'état de la case **j'accepte les conditions de la Déclaration de Kaspersky Managed Protection** ne démarrent ou n'arrêtent pas immédiatement le traitement des données. Pour appliquer les changements, vous devez redémarrer Kaspersky Security 10.1.1 for Windows Server.

Pour utiliser le service KMP, vous devez signer le contrat de services et exécuter les fichiers de configuration sur un serveur protégé.

Pour utiliser le service KMP, vous devez accepter les conditions du traitement des données de la Déclaration de KSN sur les onglets **Services** et Statistiques.

8. Cliquez sur le bouton **OK**.

La configuration du traitement des données sera enregistrée.

Configuration du transfert de données supplémentaires

Kaspersky Security 10.1.1 for Windows Server peut être configuré pour envoyer à Kaspersky Lab les données suivantes :

- Sommes de contrôle des fichiers analysés (case **Envoyer des données sur les fichiers analysés**).
- Données sur les adresses Internet demandées et sur les emails traités (**Envoyer les données relatives aux URL sollicitées**).
- Statistiques additionnelles, y compris des données personnelles (case **Envoyer les statistiques de Kaspersky Security Network**).

Consultez la section « Traitement des données locales » de ce guide pour plus d'information sur les données envoyées à Kaspersky Lab.

Les cases correspondantes peuvent être cochées ou décochées uniquement si la case **J'accepte les conditions de la Déclaration de Kaspersky Security Network** est cochée.

Par défaut, Kaspersky Security 10.1.1 for Windows Server calcule les sommes de contrôle des fichiers et des statistiques supplémentaires après l'acceptation de la Déclaration de KSN.

Tableau 34. Etats possibles de la case à cocher et conditions correspondante

Etat de la case	Conditions pour l'état de la case Envoyer des données relatives sur les fichiers analysés.	Conditions de l'état de la case Envoyer les statistiques de Kaspersky Security Network
☑	• Des demandes sur la réputation sont envoyées • Case modifiable	• Des statistiques supplémentaires sont envoyées • Case modifiable
☑	• Aucune demande sur la réputation n'est envoyée • Case non modifiable	• Aucune statistique supplémentaire n'est envoyée • Case non modifiable
☐	• Aucune demande sur la réputation n'est envoyée • Case modifiable	• Aucune statistique supplémentaire n'est envoyée • Case modifiable
☐	• Aucune demande sur la réputation n'est envoyée • Case non modifiable	• Aucune statistique supplémentaire n'est envoyée • Case non modifiable

Protection contre les exploits

Cette section contient les instructions de configuration des paramètres de la protection de la mémoire des processus contre l'exploitation des vulnérabilités.

Contenu du chapitre

A propos de la protection contre les exploits

Kaspersky Security 10.1.1 for Windows Server permet de protéger la mémoire des processus contre les exploits. Cette fonction est mise en œuvre via le module Protection contre les exploits. Vous pouvez modifier l'état de l'activité du composant, ainsi que configurer les paramètres de protection des processus contre l'exploitation des vulnérabilités.

Le composant protège la mémoire des processus contre les Exploits à l'aide de l'Agent de protection des processus (ci après Agent) externe intégré au processus protégé.

L'Agent de protection de processus est un module de Kaspersky Security 10.1.1 for Windows Server chargé dynamiquement qui s'intègre aux processus protégés en vue de contrôler leur intégrité et de réduire l'impact de l'exploitation des vulnérabilités.

Le fonctionnement de l'Agent à l'intérieur du processus protégé dépend des itérations de lancement et d'arrêt de ce processus : le chargement primaire de l'Agent dans le processus ajouté à la liste des processus protégés est possible seulement au relancement du processus. Le déchargement de l'Agent de processus une fois supprimé de la liste est possible seulement après le relancement du processus.

Il convient d'arrêter l'Agent avant de le décharger des processus protégés : lors de la suppression du composant Protection contre les exploits, l'application gèle l'environnement et force le déchargement de l'Agent des processus protégés. Si, au cours de la désinstallation du composant, l'agent est inséré dans un des processus protégés, vous devez arrêter le processus affecté. Un redémarrage du serveur peut être nécessaire (par exemple, si le processus système est protégé).

En cas de détection de signes d'une attaque de l'Exploit sur le processus protégé, Kaspersky Security 10.1.1 for Windows Server exécute une des actions suivantes :

- termine le processus lors de la tentative d'exploitation de la vulnérabilité ;
- informe que le processus a été compromis .

Vous pouvez arrêter la protection des processus d'une des manières suivantes :

- supprimer le composant ;
- supprimer le processus de la liste des processus protégés et le relancer.

Service de protection contre les exploits de Kaspersky Security

Pour garantir l'efficacité du composant Protection contre les exploits, le service contre les exploits de Kaspersky Security est requis sur le serveur protégé. Ce service et le module Protection contre les exploits font partie de l'installation recommandée. Lors de l'installation du service sur le serveur protégé, le processus kavfswh est créé et lancé. Celui-ci transmet les informations relatives aux processus protégés depuis le module vers l'Agent de sécurité.

Après l'arrêt du service de protection contre les exploits de Kaspersky Security, Kaspersky Security 10.1.1 for Windows Server continue de protéger les processus qui ont été ajoutés à la liste des processus protégés, puis il est également chargé dans les nouveaux processus ajoutés et applique toutes les techniques disponibles de réduction de l'impact pour protéger la mémoire des processus.

En cas d'arrêt du service de protection contre les exploits de Kaspersky Security Broker Host, l'application ne reçoit pas les données sur les événements qui se produisent avec les processus protégés (y compris, les données sur les attaques des exploits et l'achèvement des processus). L'Agent ne pourra pas non plus recevoir les données sur les nouveaux paramètres de protection et sur l'ajout des nouveaux processus à la liste des processus protégés.

Mode de protection contre les exploits

Vous pouvez configurer les actions de réduction de l'impact de l'exploitation des vulnérabilités dans les processus protégés, en sélectionnant un de deux modes :

- **Terminer en cas d'exploit** : appliquez ce mode pour terminer le processus en cas de tentative d'exploitation d'une vulnérabilité.

  En cas de détection d'une tentative d'exploitation d'une vulnérabilité dans un processus du système d'exploitation critique protégé, Kaspersky Security 10.1.1 for Windows Server ne termine pas ce processus quel que soit le mode indiqué dans les paramètres du module Protection contre les exploits.

- **Seulement signaler les processus exploités** : appliquez ce mode pour recevoir des informations sur les instances d'exploits dans les processus protégés à l'aide des événements dans l'audit de sécurité filtré.

  Si ce mode est sélectionné, Kaspersky Security 10.1.1 for Windows Server consigne toutes les tentatives d'exploitation des vulnérabilités en créant des événements.

Configuration des paramètres de protection de la mémoire des processus

► *Pour configurer les paramètres de protection des Exploits pour les processus ajoutés à la liste des processus protégés, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du groupe **Protection contre les exploits**.

   La fenêtre **Protection contre les exploits** s'ouvre.

4. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :

   - **Empêcher l'exploit des processus vulnérables**.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server réduit les risques d'exploitation des vulnérabilités dans les processus dans la liste des processus protégés.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne protège pas les processus du serveur contre les exploits.

     Cette case est décochée par défaut.

   - **Terminer en cas d'exploit**.

     Si ce mode est sélectionné, Kaspersky Security 10.1.1 for Windows Server termine un processus protégé en cas de détection d'une tentative d'exploit si une technique de réduction de l'impact active a été appliquée au processus.

   - **Seulement signaler les processus exploités**.

     Si ce mode est sélectionné, Kaspersky Security 10.1.1 for Windows Server signale les exploits en affichant la fenêtre de terminal à l'écran. Le processus exploité continue d'être exécuté.

     Si lors du fonctionnement de l'application sous le mode **Terminer en cas d'exploit**, Kaspersky Security 10.1.1 for Windows Server détecte un exploit dans un processus critique, le composant force le passage au mode **Seulement signaler les processus exploités**.

5. Configurez les paramètres suivants dans la section **Actions de prévention** :

   - **Signaler les processus exploités via le service de terminal.**

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server affiche à l'écran la fenêtre de terminal qui décrit le motif de déclenchement de la protection et indique le processus dans lequel la tentative d'exploit a été détectée.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server n'affiche pas à l'écran la fenêtre de terminal lors de la détection d'une tentative d'exploitation de la vulnérabilité ou d'achèvement du processus exploités. La fenêtre de terminal s'affiche quel que soit l'état de fonctionnement du service de protection contre les exploits de Kaspersky Security. Cette case est cochée par défaut.

- **Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé**.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server réduit le risque d'exploitation de vulnérabilités des processus déjà lancés quel que soit l'état d'exécution du Service Kaspersky Security. Kaspersky Security 10.1.1 for Windows Server ne protège pas les processus ajoutés après l'arrêt du Service Kaspersky Security. Une fois le service lancé, la réduction de l'impact de l'exploitation des vulnérabilités de tous les processus sera arrêtée.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne protège pas les processus contre l'exploitation des vulnérabilités quand le Service Kaspersky Security est arrêté.

  Cette case est cochée par défaut.

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

Kaspersky Security 10.1.1 for Windows Server enregistre les paramètres de protection de processus configurés et les applique.

Ajout d'un processus protégé

Le composant Protection contre les exploits protège un certain nombre de processus par défaut. Vous pouvez exclure les processus de la zone de protection en décochant les cases correspondantes dans la liste.

► *Pour ajouter un processus à la liste des processus protégés :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

   Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** du groupe **Protection contre les exploits**.

   La fenêtre **Protection contre les exploits** s'ouvre.
4. Cliquez sur le bouton **Parcourir** sous l'onglet **Processus protégés**.

   La fenêtre standard de l'Explorateur Microsoft Windows s'ouvre.
5. Choisissez le processus que vous voulez ajouter à la liste.

6. Cliquez sur le bouton **Ouvrir**.

   Le nom du processus apparaît dans la ligne.

7. Cliquez sur **Ajouter**.

   Le processus indiqué est ajouté à la liste des processus protégés.

8. Choisissez le processus ajouté et cliquez sur **Définir les techniques de protection contre les exploits**.

   La fenêtre **Technique de réduction de l'impact** s'ouvre.

9. Choisissez une des options d'application de la technique de réduction de l'impact :

   - **Appliquer toutes les techniques de protection contre les exploits disponibles**.

     Quand cette option a été sélectionnée, il est impossible de modifier la liste. Toutes les techniques disponibles pour un processus sont appliquées par défaut.

   - **Appliquer les techniques de protection contre les exploits pour le processus**.

     Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :

     a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.

     b. Cochez ou décochez la case **Appliquer la technique Attack Surface Reduction**.

10. Configurez les paramètres de la technique Attack Surface Reduction :

    - Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
    - Dans le champ **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :
      - Internet
      - Intranet local
      - Sites de confiance
      - Sites limités
      - Ordinateur

      Ces paramètres sont applicables uniquement à Internet Explorer®.

11. Cliquez sur le bouton **OK**.

Le processus est ajouté à la zone de protection de la tâche.

Techniques de réduction de l'impact

Tableau 35. Techniques de réduction de l'impact

Technique de réduction de l'impact	Description
Data Execution Prevention (DEP)	Prévention de l'exécution des données, à savoir l'interdiction de l'exécution d'un code aléatoire dans un secteur protégé de la mémoire.
Address Space Layout Randomization (ASLR)	Modification de la disposition des structures de données dans l'espace d'adresse du processus.
Structured Exeption Handler Overwrite Protection (SEHOP)	Substitution de l'enregistrement dans la structure des exclusions ou substitution du processeur d'exclusions.
Null Page Allocation	Prévention de la réorientation de l'index nul.
LoadLibrary Network Call Check (Anti ROP)	Protection contre le chargement des bibliothèques dynamiques depuis les chemins de réseau.
Executable Stack (Anti ROP)	Interdiction de l'exécution non autorisée des zones de la pile.
Anti RET Check (Anti ROP)	Contrôle de l'invocation sûre d'une fonction via l'instruction CALL.
Anti Stack Pivoting (Anti ROP)	Protection contre le déplacement de l'index de pile ESP vers l'adresse exploitée.
Simple Export Adress Table Access Moitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection de l'accès en lecture du tableau d'exportation des adresses (Export Address Table) pour les modules kernel32.dll, kernelbase.dll et ntdll.dll
Heap Spray Allocation (Heapspray)	Protection contre l'attribution de mémoire en cas d'exécution d'un code malveillant.
Execution Flow Simulation (Anti Return Oriented Programming)	Détection de chaînes d'instructions suspectes (gadget ROP possible) dans le composant Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection contre l'élévation de privilèges via une vulnérabilité dans le pilote AFD (exécution du code arbitraire sur le cercle nul dans l'appel QueryIntervalProfile).
Attack Surface Reduction (ASR)	Interdiction du lancement de modules vulnérables via le processus protégé.
Anti Process Hollowing (Hollowing)	Protection contre la création et l'exécution des copies malveillantes des processus douteux.
Anti AtomBombing (APC)	Exploit global atom table via des appels APC.
Anti CreateRemoteThread (RThreadLocal)	Un autre processus a créé une thread dans un processus protégé.
Anti CreateRemoteThread (RThreadRemote)	Un autre processus a créé une thread de contrôle dans un processus protégé.

Protection du trafic

Cette section contient des informations sur la tâche Protection du trafic et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Protection du trafic

Le module Protection du trafic traite le trafic Internet (y compris le trafic obtenu via les services de messagerie) et intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informations connues ou autres sur le serveur protégé. Le service ICAP analyse le trafic entrant à la recherche de menaces et bloque ou autorise le trafic en fonction des résultats de l'analyse et des paramètres définis.

Kaspersky Security 10.1.1 for Windows Server détecte aussi le trafic demandé par les processus exécutés sous Windows Subsystem for Linux. Pour ces processus, la tâche Protection du trafic applique l'action définie par la configuration de la tâche en cours.

La Protection du trafic est installée par défaut. Quand l'installation est terminée, les services suivants sont enregistrés et lancés :

- Protection contre les exploits de Kaspersky Security (KAVFSWH)
- Kaspersky Traffic Security (KAVFSPROXY)

Le module offre les types de protection suivants :

- Protection contre les menaces emails :
  - Anti-phishing
  - Protection contre les applications malveillantes transmises par messagerie
- Protection contre les menaces Internet :
  - Anti-phishing
  - Analyse des adresses Internet malveillante
  - Protection contre les applications malveillantes sur Internet
  - Contrôle Internet :

- Contrôle des URL
- Contrôle des certificats
- Contrôle Internet basé sur les catégories

Il est fortement recommandé d'utiliser les services KSN lors du démarrage de la tâche Protection du trafic pour améliorer la détection des menaces. Les bases de données cloud KSN contiennent davantage de données réelles sur les menaces Internet que les bases antivirus locales. L'analyse d'un certain nombre de catégories de contrôle Internet est uniquement basée sur les conclusions reçues des services KSN.

Modes de la Protection du trafic

Protection du trafic peut fonctionner dans un des modes suivants :

- **Intercepteur de pilote :** l'application intercepte le trafic à l'aide d'un pilote réseau. Elle utilise un pilote noyau réseau pour intercepter et analyser tout le trafic entrant sur les ports indiqués.
- **Redirection :** l'application redirige le trafic en configurant les navigateurs. Le trafic entrant est redirigé depuis les navigateurs vers un proxy interne dans une session de terminal ouverte. Kaspersky Security 10.1.1 for Windows Server est désigné comme proxy interne.
- **Proxy externe :** l'application traite le trafic depuis un serveur proxy externe. Le trafic est transmis depuis le serveur proxy externe vers Kaspersky Security 10.1.1 for Windows Server. L'application analyse le trafic et recommande une action au serveur proxy. Kaspersky Security 10.1.1 for Windows Server est compatible uniquement avec les proxys qui transfèrent le trafic via le protocole ICAP.

A propos des règles de protection du trafic

Kaspersky Security 10.1.1 for Windows Server permet d'ajouter et de configurer des règles d'autorisation ou d'interdiction pour les certificats et les adresses Internet. Il prend également en charge l'utilisation de catégories prédéfinies pour bloquer le contenu indésirable. Vous pouvez appliquer des règles pour les certificats si la tâche est exécutée dans le mode **Intercepteur de pilote** ou **Redirection**.

Contrôle Internet

Ce type de contrôle est réalisé en appliquant des règles d'autorisation ou d'interdiction pour les adresses Internet et les certificats. Les règle d'autorisation ont priorité sur les conclusions du KSN et sur l'analyse à l'aide des signatures.

Il est possible d'autoriser ou d'interdire une adresse Internet ou un certificat sur la base de conclusions par ordre de priorité (de la priorité la plus haute à la plus basse) :

1. Règles d'autorisation ou d'interdiction.
2. Bases antivirus ou d'Anti-phishing.
3. KSN.
4. Catégorie.

Contrôle Internet basé sur les catégories

Kaspersky Security 10.1.1 for Windows Server permet de bloquer des adresses Internet en fonction de catégories. Vous pouvez définir le niveau d'analyse heuristique qui intervient dans la définition des catégories. Le contrôle Internet basé sur les catégories repose sur une liste prédéfinie de catégories pour l'analyse. Alors que la liste en elle-même ne peut pas être modifiée, il est possible de sélectionner les catégories des ressources Internet à autoriser ou à interdire, voire de désactiver le contrôle sur la base de catégorie. La catégorie Autre reprend toutes les ressources Internet qui n'appartiennent à aucune des autres catégories de la liste. Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server autorise toutes les ressources Internet qui n'appartiennent pas à une catégorie. Si la case est décochée, aucune ressource Internet n'est autorisée.

La définition de catégorie possède la priorité la plus faible.

Kaspersky Security 10.1.1 for Windows Server applique seulement une règle par défaut : la règle d'interdiction pour les certificats TOR. Vous pouvez décocher la règle dans les paramètres de règle pour autoriser les connexions TOR. Si la règle est appliquée, toutes les connexions TOR entrantes et sortantes sont bloquées. Si la règle est appliquée, toutes les connexions TOR entrantes et sortantes sont bloquées.

La Protection du trafic considère également les conclusions pour un masque `not-a-virus` qui portent sur les ressources ou les objets qui ne sont pas des virus en tant que tels mais qui sont capables de nuire au serveur protégé. Par défaut, Kaspersky Security 10.1.1 for Windows Server n'applique pas le masque `not-a-virus` aux catégories (cf. section "Configuration du Contrôle Internet basé sur les catégories" à la page 232).

Protection contre les menaces emails

Le module Protection du trafic analyse le courrier dans Microsoft Outlook (2010, 2013 et 32 bits et 64 bits). La protection contre les menaces email est garantie via le plug-in de Kaspersky Security 10.1.1 pour Microsoft Outlook qui est installé séparément des modules de Kaspersky Security 10.1.1 for Windows Server.

Vous pouvez installer le plug-in de Kaspersky Security 10.1.1 Microsoft Outlook sur le serveur protégé seulement si Kaspersky Security 10.1.1 for Windows Server et le client de messagerie Microsoft Outlook sont installés.

► *Pour installer ce plug-in, exécutez le package ksmail_x86(x64).msi depuis le dossier \email_plugin.*

Protection contre les menaces emails inclut les fonctions suivantes :

- Analyse des emails entrants et sortants.
- Recherche de virus dans les emails.
- Recherche de virus dans les pièces jointes (objets compactés compris).
- Analyse anti-phishing des emails.
- Analyse anti-phishing des objets compactés.

En cas de détection d'une menace, Kaspersky Security 10.1.1 for Windows Server :

- Suppression de pièces jointes.
- Modifie le corps de l'email infecté.
- Enregistre un événement *Détection de menace*.

Kaspersky Security 10.1.1 for Windows Server analyse les emails à l'ouverture de ceux-ci et non pas lorsqu'ils sont reçus par le serveur. L'analyse est réalisée une fois seulement à la première ouverture. Les emails et les objets compactés analysés sont stockés dans le cache jusqu'au redémarrage d'Outlook. Après le redémarrage, tous les emails sont à nouveau analysés à l'ouverture.

► *Le Complément est chargé dans le client de messagerie Microsoft Outlook lors du démarrage. Si vous installez le plug-in de Kaspersky Security 10.1.1 pour Microsoft Outlook tandis qu'Outlook est en cours d'exécution :*

1. Ouvrez **Fichier** > **Options** > **Compléments**.
2. Assurez-vous que le plug-in de Kaspersky Security 10.1.1 pour Microsoft Outlook a été ajouté à une des listes (actif ou inactif).
3. Relancez Microsoft Outlook.
4. Vérifiez l'état du plug-in de Kaspersky Security 10.1.1 pour Microsoft Outlook (doit devenir Actif).

Configuration de la tâche Protection du trafic

Vous pouvez modifier les paramètres de la tâche Protection du trafic par défaut (cf. tableau ci-dessous).

Tableau 36. Paramètres par défaut de la tâche Protection du trafic

Paramètre	Valeur par défaut	Description
Mode de tâche	**Proxy externe**	Le service ICAP traite le trafic depuis un serveur proxy externe.
Numéro de port réseau	1345	Le numéro de port par défaut pour le service ICAP.
Identification du service	Analyse Web	Identifiant du service ICAP pour l'adresse du serveur antivirus installé.
Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes	Appliquée.	Activez ou désactivez l'analyse de chaque adresse Internet à l'aide des signatures.
Analyser les pages Internet à l'aide de la base de données anti-phishing	Appliquée.	Activez ou désactivez l'analyse anti-phishing des adresses Internet à l'aide de l'analyse heuristique.

Paramètre	Valeur par défaut	Description
Utiliser KSN pour la protection	Appliquée.	Vous pouvez utiliser les données relatives à la réputation des applications de KSN pour garantir la protection lors de l'exécution de la tâche.
Appliquer la zone de confiance	Appliquée.	Vous pouvez appliquer la Zone de confiance si nécessaire.
Niveau de sécurité	Recommandé	Pour les entrées sélectionnées dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez : • Appliquer un autre niveau de sécurité prédéfini ; • Modifier manuellement le niveau de sécurité ; • Enregistrer la configuration des paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche de protection du trafic sera lancée ou arrêtée. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer la tâche Protection du trafic :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.
4. Sous l'onglet **Mode de tâche**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section "Sélection du mode de fonctionnement de la tâche" à la page 215).
5. Sous l'onglet **Traitement des adresses et des sites Internet**, configurez l'analyse des adresses Internet (cf. section "Configuration du traitement des adresses et des sites Internet" à la page 226) contre le phishing et les virus.

6. Sous l'onglet **Protection contre les applications malveillantes**, configurez l'analyse heuristique et le niveau de sécurité (cf. section "Configuration de la protection contre les applications malveillantes sur Internet" à la page 220).
7. Sous l'onglet **Administration des tâches**, lancez la tâche sur la base d'une planification (cf. section "Programmation des tâches" à la page 143).
8. Cliquez sur le bouton **OK**.

La configuration de la tâche est enregistrée.

Sélection du mode de fonctionnement de la tâche

► *Pour configurer le mode de fonctionnement d'une tâche :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.
4. Sous l'onglet **Général**, sélectionnez un des modes disponibles dans la liste déroulante **Mode de tâche** :
   - **Intercepteur de pilote** (cf. section "**Configuration du mode Intercepteur de pilote**" à la page 216)
   - **Redirection** (cf. section "**Configuration du mode Redirection**" à la page 218)
   - **Proxy externe**

5. Définissez les paramètres de connexion du service ICAP (requis pour les trois modes) :
   - **Numéro de port réseau**

     Le numéro de port du service ICAP pour Kaspersky Security 10.1.1 for Windows Server.
   - **Identification du service**

     Identifiant qui fait partie du paramètre RESPMOD URI du protocole ICAP (cf. document RFC 3507). RESPMOD URI désigne l'adresse du serveur ICAP antivirus installé pour le stockage réseau.

     Par exemple, si l'adresse IP du serveur protégé est 192.168.10.10, que le numéro de port est 1345 et que l'identification du service ICAP est webscan, l'adresse RESPMOD URI correspondante est : icap://192.168.10.10/webscan:1345
6. Configurez le mode de fonctionnement de tâche sélectionné.

   Aucune configuration complémentaire n'est requise pour le mode **Proxy externe**. La configuration est réalisée sur le serveur proxy externe.
7. Cliquez sur le bouton **OK**.

La configuration est enregistrée.

Configuration du mode Intercepteur de pilote

► *Dans la fenêtre **Protection du trafic** :*

1. Sélectionnez l'onglet **Général**.
2. Sélectionnez le mode **Intercepteur de pilote**.
3. Dans le groupe **Paramètres du mode de tâche**, définissez les valeurs suivantes :
   - **Analyser le trafic HTTPS**.

     Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

     Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

     Cette case est cochée par défaut.

     L'analyse est disponible uniquement si le port HTTPS est ouvert.
   - Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
     - **HNAS 1.0**
     - **HNAS 1.1**
     - **HNAS 1.2**

       La case **TLS 1.0** est sélectionnée par défaut et ne peut pas être modifiée.

- **Ne pas faire confiance aux serveurs Internet dotés d'un certificat non valide**.

  La case peut être cochée uniquement si la case **Analyser le trafic HTTPS** est cochée.

  Si la case est cochée, une page Internet dotée d'un certificat non valide est bloquée (le certificat a expiré, erreur de vérification de la signature, certificat révoqué, etc.).

- **Port de sécurité**.

  Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security 10.1.1 for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Analyser le trafic HTTPS**.

4. Pour ajouter ou exclure des ports depuis la zone d'interception, cliquez sur le bouton **Configurer la zone d'interception**.

   La fenêtre **Zone d'interception** s'ouvre.

5. Sélectionnez une des options suivantes sous l'onglet **Intercepter les ports** :

   - **Tout intercepter**
   - **Intercepter les ports indiqués** :

     a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.

     b. Cliquez sur **Ajouter**.

     Le port est inclus dans la zone d'interception.

   Par défaut, Kaspersky Security 10.1.1 for Windows Server intercepte le trafic transféré via les ports suivants : 80, 8080, 3128, 443.

6. Pour désigner les ports que vous souhaitez exclure de la zone d'interception sous l'onglet **Exclure les ports** :

   a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.

   b. Cliquez sur **Ajouter**.

   Le port est exclu de la zone.

   Par défaut Kaspersky Security 10.1.1 for Windows Server exclut les ports utilisés par d'autres applications et risque de générer des problèmes lors de la tentative de lecture des données transférées par connexion chiffrée : 3389, 1723, 13291.

7. Pour exclure des adresses IP de la zone d'interception sous l'onglet **Exclure les adresses IP** :

   a. Entrez les adresses IP au format IPv4 (sous forme abrégée ou en spécifiant une adresse avec un masque de sous-réseau).

   b. Cliquez sur **Ajouter**.

   c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

8. Pour exclure le processus ou le fichier exécutable qui requiert un échange de trafic sous l'onglet **Exclure les processus** :
   a. Cochez la case **Appliquer les exclusions pour les processus**
   b. Pour exclure un fichier :
      1. Cliquez sur le bouton **Fichiers exécutables**.
         La fenêtre standard **Ouvrir** s'ouvre.
      2. Sélectionnez le fichier exécutable que vous souhaitez exclure, puis cliquez sur **Ouvrir**.
   c. Chemin d'accès au fichier du processus sur l'ordinateur local
      1. Cliquez sur le bouton **Processus en cours d'exécution**.
         La fenêtre **Processus actifs** s'affiche.
      2. Sélectionnez le fichier exécutable du processus, puis cliquez sur le bouton **OK**.

   > Vous ne pouvez pas sélectionner les processus dans Kaspersky Security Center.

9. Dans la fenêtre **Protection du trafic**, cliquez sur le bouton **OK**.

La configuration du mode de tâche est enregistrée.

Configuration du mode Redirection

► *Dans la fenêtre **Protection du trafic** :*

1. Sélectionnez l'onglet **Général**.
2. Sélectionnez le mode de tâche **Redirection**.
3. Dans le groupe **Paramètres du mode de tâche**, définissez les valeurs suivantes :
   - **Analyser le trafic HTTPS**.
     Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.
     Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.
     Cette case est cochée par défaut.

     > L'analyse est disponible uniquement si le port HTTPS est ouvert.

   - Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
     - **HNAS 1.0**
     - **HNAS 1.1**
     - **HNAS 1.2**

       > La case **TLS 1.0** est sélectionnée par défaut et ne peut pas être modifiée.

- **Rediriger le trafic vers un proxy externe après la vérification**.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server redirige le trafic qui a déjà été analysé vers un proxy externe, par exemple un serveur proxy d'entreprise qui est utilisé au sein du réseau de l'entreprise.

  Si la case est décochée, le trafic est envoyé directement à un proxy interne.

  - **Adresse du serveur proxy**.

    L'adresse du serveur proxy interne intervient dans la redirection. Saisissez l'adresse au format IPv4.

  - **Port**.

    Le numéro de port du proxy Interne.

- **Port de sécurité**.

  Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security 10.1.1 for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Analyser le trafic HTTPS**.

Dans le mode **Redirection**, le système d'exploitation doit être configuré de telle sorte que le trafic chiffré est transmis via le port indiqué par Kaspersky Security 10.1.1 for Windows Server.

4. Cliquez sur le bouton **OK**.

La configuration du mode de tâche est enregistrée.

Paramètres de niveau de sécurité prédéfini

Pour le nœud sélectionné dans l'arborescence des ressources de fichiers du serveur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : Performance maximale, Recommandé et Protection maximale. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité prédéfinie (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si des mesures de sécurité du serveur complémentaires ont été adoptées dans votre réseau, telles que des pare-feu ou des stratégies de sécurité, en plus de Kaspersky Security 10.1.1 for Windows Server.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre 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 dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité informatique élevé.

Tableau 37. Niveaux de sécurité prédéfinis et paramètres correspondants

Options	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Analyser les objets	Conformément à la liste des extensions dans la base de données	En fonction du format	Tous les objets
Actions à exécuter sur les objets infectés et autres	Interdire	Interdire	Interdire
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 de plus de (Mo)	20 Mo	20 Mo	non
Analyse des objets composés	• Objets compactés* * uniquement les objets nouveaux et modifiés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * uniquement les objets nouveaux et modifiés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * Tous les objets

Configuration de la protection contre les applications malveillantes sur Internet

Les paramètres de protection suivants affectent également tout le trafic entrant. Cependant, les actions sélectionnées sur les objets infectés et les autres objets détectés sont effectuées uniquement pour les pièces jointes de l'email.

► *Pour configurer l'analyse heuristique en vue de détecter les virus et autres menaces contre la sécurité informatique transmises via le trafic Internet :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.
4. Sous l'onglet **Protection contre les applications malveillantes** :
   - Cochez la case **Utiliser l'analyse heuristique**.
   - Définissez le niveau requis d'analyse heuristique pour la recherche d'applications malveillantes.
   - Choisissez le niveau de sécurité (cf. section "Paramètres de niveau de sécurité prédéfini" à la page 219) requis dans la liste déroulante :
     - **Recommandé**
     - **Protection maximale**
     - **Performance maximale**
     - **Personnalisé**
5. L'onglet **Description** de la partie inférieure permet de consulter les paramètres du niveau de sécurité sélectionné.

6. Ouvrez l'onglet **Général**, puis, dans le groupe **Protection d'objet**, indiquez les objets que vous souhaitez inclure à la zone d'analyse :

   - **Tous les objets**

     Kaspersky Security 10.1.1 for Windows Server analyse tous les objets.

   - **Objets analysés en fonction du format**

     Kaspersky Security 10.1.1 for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

     Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security 10.1.1 for Windows Server.

   - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

     Kaspersky Security 10.1.1 for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

     Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security 10.1.1 for Windows Server.

   - **Objets analysés en fonction de la liste d'extensions indiquée**

     Kaspersky Security 10.1.1 for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

     a. Cliquez sur le bouton **Modifier** pour modifier la liste des extensions.

     b. Indiquez une extension dans la fenêtre qui s'ouvre.

     c. Cliquez sur **Ajouter**.

     Cliquez sur le bouton **Par défaut** pour remplir la liste à l'aide de la liste prédéfinie des extensions exclues.

7. Dans le groupe **Protection d'objet composé**, indiquez les objets composés que vous souhaitez inclure à la zone d'analyse :

   - **Archives**

     Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les archives.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ignore les archives lors de l'analyse.

     La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Archives SFX**

  Analyse des archives auto-extractibles.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les archives SFX.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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.

- **Objets compactés**

  Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Objets OLE intégrés**

  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 10.1.1 for Windows Server analyse les objets intégrés au fichier.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

8. Sous l'onglet **Actions**, sélectionnez l'action à exécuter sur les objets infectés et autres détectés.

   - **Interdire**

     Kaspersky Security 10.1.1 for Windows Server interdit le chargement de toute page Internet sur laquelle du contenu malveillant a été détecté. La raison de l'interdiction est affichée au lieu de la page.

   - **Autoriser**

     Kaspersky Security 10.1.1 for Windows Server n'interdit pas le chargement de la page sollicitée, mais consigne dans le journal la détection du contenu malveillant.

9. Sous l'onglet **Optimisation**, configurez les paramètres suivants :

   - Dans la section **Exclusions**, cochez ou décochez la case **Ne pas détecter**. Pour configurer la liste des objets à exclure :

     Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus https://securelist.fr/.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server détecte tous les objets indiqués par défaut dans l'application.

     Cette case est décochée par défaut.

     a. Cliquez sur le bouton **Modifier**.

     b. Dans la fenêtre qui s'ouvre, indiquez le nom de l'objet ou le masque.

     c. Cliquez sur **Ajouter**.

   - Dans la section **Paramètres avancés**, limitez l'intervalle d'analyse et la taille de l'objet :

     - **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 limitée 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 de plus de (Mo)**

       Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore pour la recherche de virus les objets dont la taille est supérieure à la valeur indiquée.

       Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server analyse les objets sans tenir compte de la taille.

       La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

10. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de protection contre les applications malveillantes**.

La configuration du niveau de sécurité est enregistrée.

Configuration de la protection contre les menaces emails

Pour utiliser la protection contre les menaces email, le plug-in de Kaspersky Security 10.1.1 Microsoft Outlook doit être installé et le serveur protégé correctement configuré (cf. section "Protection contre les menaces email" à la page 212).

► *Pour activer la protection contre les menaces emails :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.
4. Sous l'onglet **Protection contre les menaces email**, cochez la case **Activer la protection contre les menaces email**.

   Si cette case est cochée, Kaspersky Security 10.1.1 for Windows Server utilise le plug-in de Kaspersky Security 10.1.1 Microsoft Outlook afin de procéder à une analyse antiphishing et antivirus de tout le courrier entrant et sortant.

   Si la case est décochée, le courrier n'est pas analysé.

   Cette case est cochée par défaut.

   Si vous activez ou désactivez la protection contre les menaces email, les modifications sont appliquées après un bref délai (5 minutes) ou immédiatement après le redémarrage de Microsoft Outlook.
5. Cliquez sur le bouton **OK**.

Les modifications sont enregistrées.

Configuration du traitement des adresses et des sites Internet

► *Pour rechercher la présence éventuelle de menaces de phishing sur des ressources Internet et identifier les adresses Internet considérées comme malveillantes par les bases antivirus et la réputation des adresses Internet de KSN :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.
4. Sous l'onglet **Mode de tâche**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section "Sélection du mode de fonctionnement de la tâche" à la page 215).
5. Sous l'onglet **Traitement des adresses et des sites Internet** :
   - Décochez ou cochez la case **Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes**.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse chaque adresse Internet selon les signatures.

     Si la case est décochée, les bases antivirus n'interviennent pas dans l'analyse des adresses Internet.

     Cette case est cochée par défaut.
   - Décochez ou cochez la case **Analyser les pages Internet à l'aide de la base de données anti-phishing**.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server analyse chaque adresse Internet à l'aide des bases anti-phishing. L'analyse anti-phishing repose sur l'analyse heuristique.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne détecte pas les attaques de phishing.

     Cette case est cochée par défaut.

     Sachez que quand vous configurez l'analyse anti-phishing des adresses Internet, l'anti-phishing est appliqué automatiquement aux emails.

- Cochez ou décochez la case **Utiliser 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 10.1.1 for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne prend pas en compte les opérations sur les 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 KSN pour la protection**.

  Cette case active ou désactive l'utilisation des services KSN.

  Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs.

  Si la case est décochée, la tâche n'utilise pas les services du KSN.

  Cette case est cochée par défaut.

  La réputation KSN d'une adresse Internet est disponible uniquement si toutes les conditions suivantes sont remplies :
  a. La case **Utiliser KSN pour la protection** a été cochée dans les paramètres de la Protection du trafic
  b. La Déclaration de KSN a été acceptée.
  c. La case **Envoyer les données relatives aux URL sollicitées** (cf. section "**Configuration de la tâche Utilisation du KSN**" à la page 198) est cochée.
  d. La tâche Utilisation du KSN sera lancée.

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

La configuration du traitement des adresses et des sites Internet est enregistrée.

Ajout de règles en fonction des adresses Internet

Vous pouvez ajouter une règle en fonction d'une adresse Internet pour autoriser ou interdire une adresse Internet en particulier. Ces règles ont une priorité supérieure à celle de n'importe quelle autre conclusion.

► *Pour créer une règle sur la base d'une adresse Internet :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans le groupe **Protection du trafic**, cliquez sur le bouton **Règles**.

   La fenêtre **Règles de contrôle Internet** s'ouvre.

4. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles basées sur l'URL** pour appliquer les règles.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

   Si la case est décochée, les règles ne sont pas appliquées.

   Cette case est décochée par défaut.

   La case est disponible uniquement si la case **Analyser le trafic HTTPS** est cochée.

5. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
6. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon l'adresse Internet**.
7. Dans la fenêtre **Règle selon l'adresse Internet** qui s'ouvre :
   a. Saisissez le nom de la règle.
   b. Sélectionnez le **Type** de règle : **Interdit** ou **Autorisé**.
   c. Cochez la case **Appliquer la règle**
   d. Renseignez l'**Adresse Internet** dans le champ ci-dessous.
   e. Cliquez sur le bouton **OK**.
8. Pour modifier une règle, sélectionnez la règle en question dans la liste, puis cliquez sur **Modifier**.
9. Dans la fenêtre **Règles de contrôle Internet**, cliquez sur le bouton **OK**.

Les nouvelles règles sont appliquées.

Configuration du Contrôle Internet

Gérez les paramètres de traitement des adresses et des sites Internet, les règles et l'analyse des certificats et le contrôle Internet basé sur les catégories.

Dans cette section

Configuration de l'analyse des certificats

Kaspersky Security 10.1.1 for Windows Server permet d'analyser les certificats et d'interdire les ressources Internet dont les certificats sont non valides ou expirés. Pour configurer l'analyse des certificats, il faut réaliser les opérations suivantes :

a. Sélectionnez le mode **Intercepteur de pilote** ou **Redirection**.

b. Configurez la tâche Protection du trafic (cf. section "Sélection et configuration du mode de " à la page 229).

c. Appliquez les règles du Contrôle Internet.

d. Ajoutez et appliquez des règles pour les certificats (cf. section "Ajout de règles pour les certificats" à la page 230).

Les règles pour les certificats peuvent uniquement être utilisées dans les modes **Intercepteur de pilote** ou **Redirection**. Kaspersky Security 10.1.1 for Windows Server crée uniquement des règles d'interdiction pour les certificats.

Sélection et configuration du mode de tâche

► *Pour sélectionner et configurer le mode d'utilisation des certificats :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Protection en temps réel du serveur** du groupe **Protection du trafic**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection du trafic** s'ouvre.

4. Sous l'onglet **Général**, sélectionnez un des modes qui prend en charge l'analyse de certificats dans la liste déroulante **Mode de tâche** :

   - **Intercepteur de pilote** (cf. section "**Configuration du mode Intercepteur de pilote**" à la page 216)
   - **Redirection** (cf. section "Configuration du mode Redirection" à la page 218)

5. Dans le groupe **Paramètres du mode de tâche**, définissez les valeurs suivantes :

   - **Analyser le trafic HTTPS**.

     Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

     Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

     Cette case est cochée par défaut.

     L'analyse est disponible uniquement si le port HTTPS est ouvert.

   - Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
     - **HNAS 1.0**
     - **HNAS 1.1**
     - **HNAS 1.2**

       La case **TLS 1.0** est sélectionnée par défaut et ne peut pas être modifiée.

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

La configuration de la tâche est enregistrée.

Ajout de règles pour les certificats

Les règles pour les certificats peuvent uniquement être utilisées dans les modes **Intercepteur de pilote** ou **Redirection**. Kaspersky Security 10.1.1 for Windows Server crée uniquement des règles d'interdiction pour les certificats.

► *Pour ajouter ou configurer une règle pour un certificat :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans le groupe **Protection du trafic**, cliquez sur le bouton **Règles**.

   La fenêtre **Règles de contrôle Internet** s'ouvre.
4. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles selon le certificat** pour appliquer les règles.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

   Si la case est décochée, les certificats ne sont pas analysés par l'application.

   Cette case est décochée par défaut.

   La case est disponible uniquement si la case **Analyser le trafic HTTPS** est cochée.
5. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
6. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon le certificat**.
7. Dans la fenêtre **Règle selon le certificat** qui s'ouvre :
   a. Saisissez le nom de la règle.
   b. Cochez la case **Appliquer la règle**
   c. Sélectionnez le **Type d'opérateur** : **Masque** ou **Expression régulière**.
   d. Définissez le masque ou l'expression dans le champ **Opérateur**.
   e. Cliquez sur le bouton **OK**.
8. Pour modifier une règle, sélectionnez la règle en question dans la liste, puis cliquez sur **Modifier**.
9. Dans la fenêtre **Règles de contrôle Internet**, cliquez sur le bouton **OK**.

Les nouvelles règles sont appliquées.

Configuration du Contrôle Internet basé sur les catégories

► *Pour ajouter ou modifier une règle de la Protection du trafic basée sur les catégories :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans le groupe **Protection du trafic**, cliquez sur le bouton **Règles**.

   La fenêtre **Règles de contrôle Internet** s'ouvre.
4. Ouvrez l'onglet **Catégories**.
5. Cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server définit les catégories des ressources Internet et interdit celles qui appartiennent aux catégories sélectionnées.

   Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne définit pas les catégories.

   Cette case est décochée par défaut.

   Les paramètres du contrôle de catégorie deviennent disponibles.
6. Cochez ou décochez les cases suivantes :
   - **Autoriser l'accès si la page Internet ne peut pas être classée dans une catégorie**.
   - **Autoriser l'accès aux ressources Internet légitimes qui peuvent servir à nuire au serveur**.
   - **Autoriser l'accès aux publicités légitimes**.

7. Dans la liste des catégories disponibles (cf. section "Liste des catégories" à la page 233) :
   - Cochez la case correspondante pour autoriser une catégorie.

     La colonne **Type** change et devient **Autorisé**.
   - Décochez la case correspondante pour interdire une catégorie.

     La colonne **Type** change et devient **Interdit**.

   La liste des catégories est prédéfinie et ne peut être modifiée (il est impossible d'ajouter ou de supprimer des catégories).
8. Cliquez sur le bouton **OK**.

La configuration des règles est enregistrée.

Utilisation du masque not-a-virus

► *Pour utiliser le masque* `not-a-virus` *dans le cadre de l'analyse d'une catégorie :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez les paramètres de la tâche Utilisation du KSN (cf. section "Configuration de la tâche Utilisation du KSN" à la page 198).
2. Cochez la case **Envoyer les données relatives aux URL sollicitées**.
3. Lancez tâche Utilisation du KSN.
4. Dans la fenêtre des paramètres de la Protection du trafic (cf. section "Configuration de la tâche Protection du trafic" à la page 213), cochez la case **Utiliser KSN pour la protection**.
5. Dans la fenêtre **Règles de contrôle Internet**, sous l'onglet **Catégories**, cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.
6. Dans la liste des catégories, sélectionnez les catégories pour lesquelles vous souhaitez appliquer le masque `not-a-virus`.

   Les objets des catégories sélectionnées qui correspondent au masque ne seront pas détectés par la tâche Protection du trafic.

L'utilisation du masque `not-a-virus` est configurée dans les paramètres **Zone de confiance** (cf. section "Application du masque not-a-virus" à la page 160)

Liste des catégories

Les ressources Internet sont analysées et classées en catégories selon des tags. Le tag peut être appliqué à un certain nombre de catégorie (cf. tableau ci-dessous).

Tableau 38. Tags pour les catégories de ressources Internet

Tag	Description	Liste des catégories
18+ (adulte)	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu pour adultes (plus de 18 ans) comme des descriptions d'actes violents, de la pornographie ou du langage vulgaire.	Avortement, Rencontres entre adultes, Anorexie, Mécontentement, Discrimination, Erotique, Drogues illicites, Logiciels illicites, LGBT, Lingerie, Rencontres entre jeunes non adultes, Nudisme, Décision de police (JP), Porno, Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Education sexuelle, Réseaux sociaux, Suicide, Vocabulaire obscène, Violence, Armes.
enfants	Ces catégories peuvent contenir des ressources qui pourraient proposer du contenu pour les enfants. Par exemple, des sites Internet d'éducation, des sites de divertissements pour enfants, des forums et des blogs sur l'éducation des enfants.	Enfants, Limité par la Loi fédérale 436 (Féd. de Russie), Pages d'écoles et d'universités.
drogue	Ces catégories peuvent contenir des ressources qui pourraient proposer des informations sur les stupéfiants et autres substances licites ou illicites. Par exemple, des informations sur la distribution de drogues illicites ou d'alcool ou les sites Internet de sociétés pharmaceutiques enregistrées.	Avortement, Alcool, Anorexie, Drogue, Santé et beauté, Drogues illicites, Médecine, Pharmacie, Tabac.
éducation	Ces catégories peuvent contenir des ressources qui pourraient proposer du contenu pédagogique. Par exemple, des encyclopédies en ligne, des bases de connaissances, des sites wiki et des pages Internet de ressources éducatives ou des pages Internet consacrées à l'éducation sexuelle.	Livres et littérature, Enseignement, Enfants, Technologies de l'information, Encyclopédies en ligne, Pages d'écoles et d'universités, Moteurs de recherche, Education sexuelle.

Tag	Description	Liste des catégories
Loisirs	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux loisirs, aux hobbys et aux activités récréatives. Par exemple, divers jeux en ligne, dont des sites de pari et les réseaux sociaux, des pages Internet sur la littérature ou la chasse, des blogs sur la santé et la beauté et des fils d'informations.	Rencontres pour adultes, Loisirs, Tous les supports de communication, Astrologie et ésotérisme, Audio, vidéo et logiciels, Paris, Blogs, Casinos, Jeux de cartes, Jeux occasionnels, Chats et forums, Jeux, Culture et société, Erotique, Mode, Partage de fichiers, Pêche et chasse, Enfants, Paris, Santé et beauté, Loisirs, Maison et famille, Humour, LGBT, Lingerie, Loteries, Hébergement et diffusion sur les médias, Médecine, Musique, Actualités, Rencontre entre jeunes non adultes, Nudisme, Boutiques en ligne, Boutiques en ligne (propre système de paiement), Animaux, Porno, Restaurants, café et alimentation, Sex shop, Réseaux sociaux, Sport, Torrents, Voyages, TV et radio, Jeux de guerre.
jeux	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif à différents types de jeux. Par exemple, des jeux de hasard et des paris, des loteries, des jeux en ligne ou occasionnels ainsi que des sites et des forums consacrés aux jeux.	Jeux occasionnels, Jeux vidéo, Sport, Jeux de guerre.
hasard	Cette catégorie désigne les pages Internet contenant : • Jeux de hasard payants. • Paris. • Loteries qui impliquent l'achat de billets/numéros de loterie.	Paris, Casinos, jeux de cartes, Jeux de hasard, Sport, Jeux de guerre.
santé & médecine	Pages Internet sur les modes de vie sains. Peuvent inclure des sites dédiés au fitness, à l'alimentation saine et à d'autres pratiques et méthodes de traitement ; pages Internet sur la médecine, la pharmacie, les sociétés pharmaceutiques et les médicaments et suppléments..	Avortement, Anorexie, Médicaments et drogues, Santé et beauté, Médecine, Pharmacie, Sport.
illicite	Ces catégories peuvent contenir des ressources Internet potentiellement illicites. Par exemple des sites de partage illégaux de fichiers musicaux/vidéo ou des pages Internet dont la visite est interdite par la législation de plusieurs pays.	Alcool, Audio, vidéo et logiciels, Drogues, Partage de fichiers, Drogues illicites, Loteries, Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Tabac.

Tag	Description	Liste des catégories
IT	Généralement, pages Internet qui permettent aux utilisateurs (avec ou sans la nécessité d'un compte) d'envoyer des messages personnels à d'autres utilisateurs (y compris des services email, des réseaux sociaux, des blogs, etc.)	Serveurs proxy anonymes, Services d'hébergement et de domaine, Logiciels illégaux, Technologies de l'information, Moteurs de recherche, Courrier Internet.
interdit par la loi	Ces catégories peuvent contenir des ressources Internet qui pourraient être soumises au contrôle de la législation fédérale ou qui pourraient être liées au gouvernement ou à la politique.	Législation et politique, Mentionné dans la Liste fédérale des extrémistes (Féd. de Russie), Limité par la Loi fédérale 436 (Féd. de Russie), Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie).
légal	Ces catégories peuvent contenir des ressources Internet potentiellement légales.	Alcool, Audio, vidéo et logiciels, Drogue, Partage de fichiers, Publicités licites, Loteries, Militaire, Pharmacie, Religion, Education sexuelle, Services de bandes annonces et d'annonces, Tabac, Jeux de guerre.
partage de médias	Ces catégories peuvent reprendre des ressources Internet qui peuvent permettre le partage de fichiers. Par exemple, des torrents, des sites de partage de fichiers, des sites d'hébergement audio et vidéo, licites ou non.	Audio, vidéo et logiciels, Livres et littérature, Partage de fichiers, Enfants, Services Internet, Hébergement et diffusion sur les médias, Musique, Moteurs de recherche, Torrents, TV et radio
argent et paiement	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux finances ou à des institutions financières. Par exemple, les sites officiels de banques, des banques en ligne, des magasins en lignes et des pages Internet pour la réalisation de transfert d'argent.	Banques, Livres et littérature, Jeux occasionnels, E-commerce, Boutiques en ligne (propre système de paiement), Paiement par carte de crédit, Systèmes de paiement, Restaurants, cafés et alimentation, Voyages.
collaboration en ligne	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux communications en ligne. Par exemple, des blogs spécialisés et des forums, des chats privés, des réseaux sociaux ou des sites de rencontre.	Rencontres entre adultes, Blogs, Chats et forums, Enfants, Santé et beauté, Sites de recherche d'emploi, Médecine, Rencontres entre jeunes non adultes, Réseaux sociaux, Voyages.
psychotrope & drogue	Ces catégories peuvent contenir des ressources Internet associées à tous types de drogues, médicaments psychotropes ou produits à base de tabac.	Médicaments et drogues, Santé et beauté, Drogues illicites, Médecine, Pharmacie, Tabac.

Tag	Description	Liste des catégories
sexe & contenu pour adultes	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu à caractère sexuel ou érotique. Par exemple, des hébergeurs de pornographie, des pages Internet sur l'éducation sexuelle et des sites Internet sur les minorités sexuelles.	Rencontres entre adultes, LGBT, Lingerie, Nudisme, Porno, Education sexuelle, Sex shops.
société et droit	Cette catégorie inclut de nombreux aspects de la société et de la vie humaine, y compris religion, associations religieuses, gouvernement, politique, lois, maison et famille, médias d'actualités, militaire et armes.	Culture et société, Droit et politique, Militaire, Religion, Armes.
shopping	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux achats en ligne.	Livres et littérature, Lingerie, Boutiques en ligne, Boutiques en ligne (propre système de paiement), Paiement par carte de crédit, Restaurants, cafés et alimentation, Sex shops, Voyages.
violence	Ces catégories peuvent contenir des ressources Internet qui pourraient présenter des expressions explicites d'agression, des descriptions d'actes de cruauté, de la propagande d'organisations extrémistes ou des descriptions de suicide.	Mécontentement, Discrimination, Extrémisme et racisme, Pêche et chasse, Haine et discrimination, Mentionné dans la Liste fédérale des extrémistes (Féd. de Russie), Militaire, Décision de police (JP), Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Suicide, Violence, Jeux de guerre, Armes.
service Internet	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer différents services Internet. Par exemple, des services d'anonymisation, d'hébergement de sites ou d'emails.	Serveurs proxy anonymes, Services d'hébergement et de domaine, Services Internet, Moteurs de recherche, Services de bandes annonces et d'annonces, Courrier Internet.

Monitoring des scripts

Cette section contient des informations sur la tâche Monitoring des scripts et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Monitoring des scripts

Au cours de l'exécution de la tâche Monitoring des scripts, Kaspersky Security 10.1.1 for Windows Server 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®. L'application peut également traiter des scripts PowerShell™ et les scripts s'exécutent dans les applications Microsoft Office sur les systèmes d'exploitation avec l'interface AMSI (Antimalware Scan Interface) installée. Vous pouvez autoriser ou bloquer l'exécution d'un script qui a été détecté comme dangereux ou probablement dangereux. Si Kaspersky Security 10.1.1 for Windows Server considère un script comme potentiellement dangereux, il exécute l'action que vous avez choisie : interdiction ou autorisation de l'exécution de ce script. Si l'action **Bloquer** est sélectionné, l'application autorise l'exécution du script uniquement si ce script a été détecté comme sûr.

A compter du système d'exploitation Microsoft Windows Server 2016, Kaspersky Security 10.1.1 for Windows Server prend en charge l'interface AMSI (Antimalware Scan Interface (AMSI). L'interface AMSI permet l'intégration des applications et des services avec n'importe quelle application antimalware installée pour que celle-ci intercepte et analyse les scripts.

Le module Monitoring des scripts n'est pas installé par défaut sur le serveur car l'exécution de cette tâche peut provoquer des erreurs de serveur. Lorsque le composant Monitoring des scripts est installé, l'application est enregistrée comme fournisseur AMSI et commence à surveiller les scripts exécutés.

Sur les ordinateurs fonctionnant sous des systèmes d'exploitation qui ne prennent pas en charge la fonction AMSI, l'utilisation de ce composant peut être incompatible avec certaines des applications tierces installées sur le serveur protégé. Dans ce cas, le monitoring des scripts tiers peut donner lieu à des erreurs de fonctionnement des scripts. Il est recommandé de ne pas utiliser de telles applications tierces ou de désactiver la tâche Monitoring des scripts. Si la tâche est désactivée, les risques associés à la sécurité d'exécution des scripts augmente.

Si vous souhaitez utiliser le module Monitoring des scripts, il faut le sélectionner manuellement dans la liste des modules à installer lors de l'installation de Kaspersky Security 10.1.1 for Windows Server. Si ce composant est installé, la tâche Monitoring des scripts est lancée automatiquement au démarrage de Kaspersky Security 10.1.1 for Windows Server par défaut.

Pour obtenir les détails relatifs à la sélection des modules de l'application lors de l'installation, consultez les *sections consacrées à l'installation dans le Manuel de l'administrateur de Kaspersky Security 10.1.1 for Windows Server*.

Vous trouverez plus d'informations sur la fonctionnalité AMSI sur le site de Microsoft Windows https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal.

Vous pouvez configurer la tâche Monitoring des scripts.

Configuration des paramètres de la tâche Monitoring des scripts

La tâche système Monitoring des scripts possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 39. Paramètres par défaut de la tâche Monitoring des scripts

Paramètre	Valeur par défaut	Description
Actions à exécuter sur les scripts probablement dangereux	**Interdire**	Vous pouvez indiquer les actions à effectuer en cas de détection de scripts potentiellement dangereux : interdire ou autoriser leur exécution.
Analyse 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 Monitoring des scripts, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

   La fenêtre **Propriétés : Monitoring des scripts** s'ouvre.

3. Dans la section **Actions à exécuter sur les scripts potentiellement dangereux**, réalisez l'une des opérations suivantes :

   - Si vous souhaitez autoriser l'exécution des scripts potentiellement dangereux, sélectionnez l'option **Autoriser**.

     Kaspersky Security 10.1.1 for Windows Server autorise l'exécution d'un script potentiellement dangereux.

   - Si vous souhaitez interdire l'exécution des scripts potentiellement dangereux, sélectionnez l'option **Interdire**.

     Kaspersky Security 10.1.1 for Windows Server interdit l'exécution d'un script potentiellement dangereux.

     Cette option est sélectionnée par défaut.

4. Dans le groupe **Analyse heuristique**, réalisez une des opérations suivantes :

   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.

     La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

     Si la case est cochée, l'analyse heuristique est activée.

     Si 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'analyse 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'analyse heuristique** est cochée.

5. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.

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

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server prend en compte les exclusions spécifiées par emplacement et/ou un objet détecté par nom ou masque de nom dans la liste d'exclusion.

   Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ignore les exclusions pour la tâche Monitoring des scripts.

   Cette case est cochée par défaut.

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

Les paramètres de la tâche définis sont appliqués

Contrôle de l'activité locale

Cette section fournit des informations sur la fonction de Kaspersky Security 10.1.1 for Windows Server qui contrôle les lancements des applications et les connexions de périphériques externes via USB.

Contenu du chapitre

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 du Contrôle du lancement des applications du côté de Kaspersky Security Center pour des groupes de serveurs.

Dans cette section

A propos de l'utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center

Les règles du 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 du 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. Cela permet d'optimiser la protection d'un serveur, puisque les règles spécifiées contrôlent uniquement les lancements des applications caractéristiques de ce type précis de serveur.

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 *Système d'aide 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 Kaspersky Security Center, développez le nœud **Appareils 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 de détails du groupe d'administration sélectionné, ouvrez l'onglet **Périphériques** et sélectionnez le serveur auquel vous souhaitez attribuer des tags. Dans la fenêtre **Propriétés : <Nom du serveur>** du serveur sélectionné, ouvrez la section **Tags** et composez la liste des tags. Cliquez sur le bouton **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 de détails 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 du Contrôle du lancement des applications pour le profil modifié.
     c. Cliquez sur le bouton **OK**.
4. Dans la fenêtre **Propriétés : <nom de la stratégie>**, cliquez sur le bouton **OK**.

Le profil configuré sera appliqué dans la stratégie pour la tâche Contrôle du lancement des applications.

Configuration des paramètres de la tâche Contrôle du lancement des applications

Vous pouvez modifier les paramètres de la tâche Contrôle du lancement des applications définis par défaut (cf. tableau ci-dessous).

Tableau 40. Paramètres par défaut de la tâche Contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Mode de tâche	**Statistiques uniquement**. La tâche consigne dans le journal d'exécution tous les événements de blocage et de lancement des applications conformément aux règles définies. Le lancement de l'application n'est pas interdit.	Vous pouvez sélectionner le mode **Actif** pour protéger le serveur après la composition de la liste définitive des règles.
Gestion des règles	**Remplacer les règles locales par les règles de la stratégie**	Vous pouvez choisir le mode d'application commune des règles spécifiées dans la stratégie et les règles sur l'ordinateur local.
Zone d'application des règles	La tâche 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.
Utilisation du KSN	Les données sur la réputation des applications dans KSN ne sont pas utilisées.	Vous pouvez utiliser les données sur la réputation des applications de KSN dans le fonctionnement de la tâche Contrôle du lancement des applications.
Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste	Pas appliqué.	Vous pouvez autoriser la diffusion de l'application à l'aide des paquets d'installation et des applications indiqués dans les paramètres. Par défaut, seule l'autorisation des applications à l'aide du service Windows Installer est autorisée.
Toujours autoriser la diffusion de logiciel via Windows Installer	Appliquée.	Vous pouvez autoriser l'installation ou la mise à jour de n'importe quel logiciel si les opérations sont exécutées via Windows Installer.
Interdire le lancement des interpréteurs de commande sans commande à exécuter	Pas appliqué.	Vous pouvez interdire le lancement des interpréteurs de commande sans commande à exécuter.
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 10.1.1 for Windows Server. 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 d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité locale**, cliquez sur le bouton **Configuration** dans la section **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.
4. Sous l'onglet **Général** du groupe **Mode**, sélectionnez les paramètres suivants :
   - Dans la liste déroulante **Mode de tâche**, définissez le mode de fonctionnement de la tâche.

     La liste déroulante vous permet de sélectionner un des modes d'exécution de la tâche Contrôle du lancement des applications :

     - **Actif**. Kaspersky Security 10.1.1 for Windows Server contrôle n'importe quelle application exécutée à l'aide des règles indiquées.
     - **Statistiques uniquement**. Kaspersky Security 10.1.1 for Windows Server ne contrôle pas le lancement des applications à l'aide des règles indiquées et consigne simplement dans le journal d'exécution de la tâche 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 du Contrôle du lancement des applications sur la base des informations consignées dans le journal d'exécution de la tâche.

     Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques uniquement**.
   - Décochez ou cochez la case **Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs**.

     La case active ou désactive le contrôle d'un nouveau lancement de l'application en fonction des informations d'incidents stockées dans le cache.

     Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server interdit ou autorise le relancement 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 du Contrôle du

lancement des applications, l'enregistrement relatif à cet événement est enregistré dans le cache et le relancement de cette application est lui aussi autorisé, sans vérification additionnelle.

Si la case est désactivée, Kaspersky Security 10.1.1 for Windows Server analyse l'application à chacune des tentatives de lancement.

Cette case est cochée par défaut.

- Décochez ou cochez la case **Interdire le lancement des interpréteurs de commande sans commande à exécuter**.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server refuse le lancer l'interpréteur de ligne de commande même si ce lancement est autorisé. La ligne de commande sans commande peut être lancée uniquement si les deux conditions suivantes sont remplies :

  - Le lancement de l'interpréteur de ligne de commande est autorisé.
  - La commande exécutée est autorisée.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server tient uniquement compte des règles d'autorisation pour lancer la ligne de commande. Le lancement est interdit si aucune règle d'autorisation n'est appliquée ou si le processus exécutable n'est pas considéré comme processus de confiance par KSN. Si la règle d'autorisation est appliquée ou si le processus est approuvé par KSN, il est possible de lancer la ligne de commande avec ou sans commande d'exécution.

  Kaspersky Security 10.1.1 for Windows Server reconnaît les interpréteurs de ligne de commande suivants :

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

5. Dans groupe **Règles**, configurez les paramètres d'application des règles :

   a. Cliquez sur le bouton **Liste des règles** pour ajouter des règles d'autorisation du contrôle du lancement des tâches.

   > Kaspersky Security 10.1.1 for Windows Server ne reconnaît pas les chemin qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

   b. Sélectionnez le mode d'application des règles :

   - **Remplacer les règles locales par les règles de la stratégie**.

     L'application applique la liste de règles indiquées dans la stratégie dans le cadre du contrôle centralisé du lancement des applications sur le groupe d'ordinateurs. La création, la modification ou l'application de règles locales ne sont pas disponibles.

   - **Ajouter les règles de la stratégie aux règles locales**.

     L'application applique la liste de règles définie dans la stratégie en même temps que les listes de règles locales. Vous pouvez modifier les listes de règles locales à l'aide de tâches de Génération des règles du Contrôle du lancement des applications.

Par défaut Kaspersky Security 10.1.1 for Windows Server applique deux règles prédéfinies qui autorisent l'exécution des scripts, des paquets MSI et des fichiers de lancement selon un certificat.

6. Définissez les 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 10.1.1 for Windows Server autorise ou interdit le lancement des fichiers exécutables des applications à l'aide des règles indiquées dont les paramètres incluent les fichiers exécutables dans la zone.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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.

- **Contrôle du chargement des modules DLL**.

  La case active/désactive le contrôle du chargement des modules DLL.

  Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server autorise ou interdit le chargement des modules DLL à l'aide des règles indiquées dont les paramètres incluent les fichiers exécutables dans la zone.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne contrôle pas le chargement des modules DLL à l'aide des règles indiquées. Le chargement des modules DLL est autorisé.

  La case est active 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 10.1.1 for Windows Server autorise ou interdit le lancement des scripts et paquets MSI à l'aide des règles indiquées dont les paramètres incluent les scripts et les paquets MSI dans la zone.

  Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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.

7. Dans la section **Utilisation du KSN**, configurez les paramètres suivants du lancement des applications :
   - **Interdire les applications douteuses selon 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 10.1.1 for Windows Server 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 contre les applications malveillantes.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server 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 les applications de confiance selon 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 10.1.1 for Windows Server interdit le lancement des applications considérées comme douteuses dans le KSN. De plus, les règles d'interdiction du Contrôle du lancement des applications qui s'appliquent aux applications de confiance dans KSN ont une priorité supérieure : si l'application est considérée comme une application de confiance par les services KSN, son lancement est interdit.

     Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne prend pas en compte la réputation des applications de confiance dans le KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

     Cette case est décochée par défaut.
   - Utilisateurs et/ou groupes d'utilisateurs pour lesquels le lancement d'applications considérées comme des applications de confiance dans le KSN est autorisé.
8. Sous l'onglet **Contrôle de la distribution des logiciels**, configurez les paramètres du contrôle de la distribution des logiciels (cf. section "Configuration du contrôle de la distribution des logiciels" à la page 250).
9. Sous l'onglet **Administration des tâches**, configurez les paramètres de planification du lancement de la tâche (cf. section "Configuration des paramètres de planification du lancement des tâches" à la page 143).
10. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

A propos du contrôle de la distribution des logiciels

La génération de règles de contrôle du lancement des applications peut être compliquée si vous devez également prendre en compte le contrôle de la distribution des logiciels sur un ordinateur géré. Par exemple, pour les ordinateurs où des mises à jour automatiques périodiques des logiciels installés se produisent. Dans ce cas, la liste de règles d'autorisation doit être mise à jour après chaque mise à jour de logiciel afin que les fichiers juste créés soient pris en compte dans les paramètres de la tâche Contrôle du lancement des applications. Pour simplifier le contrôle du lancement dans les scénarios de distribution des logiciels, vous pouvez utiliser le sous-système Contrôle du lancement des applications.

Un *paquet de distribution des logiciels* (également appelé “paquet”) représente une application logicielle à installer sur un serveur. Chaque paquet contient au moins une application et peut également contenir des fichiers séparés, des mises à jour, voire une commande séparée en plus des applications, notamment lorsque vous installée une application ou une mise à jour logicielle.

Le sous-système Contrôle de la distribution des logiciels est mis en œuvre en tant que liste supplémentaire d'exclusions. Lorsque vous ajoutez des paquets de distribution (également appelés “paquets de confiance”) à cette liste, l'application permet la décompression de ces paquets de confiance et le démarrage automatique du logiciel, créé ou modifié par un paquet de confiance. Les fichiers extraits peuvent hériter de l'attribut de confiance d'un paquet de distribution principal. Un *paquet de distribution principal* est un paquet qui a été ajouté à la liste d'exclusions de contrôle de la distribution des logiciels par l'utilisateur et qui est devenu un paquet de confiance.

Kaspersky Security 10.1.1 for Windows Server contrôle uniquement les cycles complet de distribution des logiciels. L'application ne peut pas traiter correctement le démarrage des fichiers qui sont modifiés par un paquet de confiance si, lors du premier démarrage du paquet, le contrôle de la distribution des logiciels est désactivé ou le composant Contrôle du lancement des applications n'est pas installé.

Le contrôle de la distribution des logiciels n'est pas disponible si la case **Utiliser les règles pour les fichiers exécutables** est décochée dans les paramètres de la tâche Contrôle du lancement des applications.

Cache de la distribution des logiciels

Kaspersky Security 10.1.1 for Windows Server établit la connexion entre les paquets de confiance et les fichiers créés pendant la procédure de distribution des logiciels à l'aide du *cache de distribution des logiciels* (aussi appelé « cache de distribution »). Au premier démarrage du paquet, Kaspersky Security 10.1.1 for Windows Server détecte tous les fichiers créés pendant le processus de distribution des logiciels de ce paquet et stocke les sommes de contrôle des fichiers et les chemins dans le cache de distribution. Ensuite, le démarrage de tous les fichiers stockés dans le cache de distribution est autorisé par défaut.

Vous ne pouvez pas réviser, effacer ou modifier manuellement le cache de distribution via l'interface utilisateur. Le cache est rempli et contrôlé par Kaspersky Security 10.1.1 for Windows Server.

Vous pouvez exporter le cache de distribution dans le fichier de configuration (au format XML) et aussi effacer le cache à l'aide des options de ligne de commande.

► *Pour exporter le cache de distribution dans un fichier de configuration, exécutez la commande suivante :*

```
kavshell appcontrol /config /savetofile:<chemin complet> /sdc
```

► *Pour effacer le cache de distribution, exécutez la commande :*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Security 10.1.1 for Windows Server le cache de distribution toutes les 24 heures. Si le chemin complet ou la somme de contrôle d'un fichier précédemment autorisé est modifié, l'application supprime l'enregistrement de fichier du cache de distribution. Si la tâche Contrôle du lancement des applications est lancée en mode actif, les lancements ultérieurs de ce fichier sont bloqués.

Configuration du traitement des données

L'attribut de confiance de tous les fichiers extraits du paquet de confiance est hérité dès le premier démarrage du paquet. Si vous décochez la case après le premier démarrage, l'héritage de tous les fichiers extraits de ce paquet est toujours maintenu. Pour réinitialiser l'héritage appliqué pour la première fois de tous les fichiers extraits, vous devez effacer le cache de distribution et décocher la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution** avant de redémarrer les paquets de distribution de confiance.

Les fichiers et paquets extraits, créés par un paquet de distribution principal de confiance, acquièrent l'attribut de confiance à mesure que leurs sommes de contrôle sont ajoutées au cache de distribution lorsque le paquet de distribution principal de la liste d'exclusions est ouvert pour la première fois. Par conséquent, les paquets de distribution proprement dits et tous les fichiers inclus sont également de confiance. Par défaut, le nombre de niveaux de l'héritage d'attributs de confiance est illimité.

L'attribut de confiance est maintenu par les fichiers extraits après le redémarrage du système d'exploitation.

Pour configurer le traitement des fichiers dans les paramètres du Contrôle de distribution de logiciels (cf. section "Configuration du Contrôle de distribution de logiciels" à la page 250), vous devez cocher ou décocher la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**.

Par exemple, vous ajoutez un paquet test.msi contenant un certain nombre d'autres paquets et applications à la liste d'exclusions et cochez la case. Dans ce cas, tous les paquets et applications contenu(e)s dans le paquet test.msi peuvent être exécuté(e)s ou extrait(e)s s'ils/si elles contiennent d'autres fichiers. Ce scénario est valable pour les fichiers extraits sur tous les niveaux imbriqués.

Si vous ajoutez un paquet test.msi à la liste d'exclusions et décochez la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**, l'application affecte l'attribut de confiance uniquement aux paquets et aux fichiers exécutables extraits d'un paquet de confiance principal (imbriqué au premier niveau). Ensuite, le démarrage de tous les fichiers stockés dans le cache de distribution est autorisé par défaut. Tous les fichiers imbriqués au second niveau et plus sont bloqués par le principe d'interdiction par défaut.

Interaction avec les règles de contrôle du lancement des applications en premier lieu

La liste des paquets de confiance du sous-système de contrôle de la distribution des logiciels est une liste d'exclusions, ce qui amplifie, mais ne remplace pas la liste générale de règles de contrôle du lancement des applications.

Les règles d'interdiction de contrôle du lancement des applications a la priorité la plus élevé : la décompression des paquets de confiance et le démarrage de fichiers nouveaux ou modifiés sont bloqués si ces paquets est fichiers sont affectés par les règles d'interdiction du contrôle du lancement des applications.

Les exclusions de contrôle de la distribution des logiciels sont appliquées à la fois pour les paquets de confiance et les fichiers créés ou modifiés par ces paquets si aucune règle d'interdiction dans la liste de contrôle du lancement

des applications n'est appliquée pour ces paquets et fichiers.

Utilisation des conclusions KSN

Les conclusions KSN douteuses ont une priorité plus élevée que les exclusions de contrôle de la distribution des logiciels : la décompression d'un paquet de confiance ou le démarrage des fichiers créés et modifiés par ce paquet est bloqué(e) si une conclusion douteuse de ces fichier est reçue de KSN.

Configuration du contrôle de la distribution des logiciels

► *Pour ajouter une distribution des paquets de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

   > Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité locale**, cliquez sur le bouton **Configuration** dans la section **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.
4. Sous l'onglet sélectionné, cochez la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste**.

   La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide des applications et des paquets d'installation repris dans la liste.

   Si la case est cochée, l'application autorise automatiquement le lancement des fichiers exécutés à l'aide des distributions des paquets de confiance. La liste des applications et des distributions qui peuvent être lancées est modifiable.

   Si la case est décochée, l'application ne tient pas compte des exclusions indiquées dans la liste.

   Cette case est décochée par défaut.

Vous pouvez cocher la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** si la case **Utiliser les règles pour les fichiers exécutables** est cochée dans les paramètres de la tâche **Contrôle du lancement des applications**.

5. Le cas échéant, décochez la case **Toujours autoriser la diffusion de logiciel via Windows Installer**.

   La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide du sous-système Windows Installer.

   Si la case est cochée, l'application autorise toujours le lancement des fichiers installés à l'aide de Windows Installer.

   Si la case est décochée, l'utilisation de Windows Installer pour le lancement de l'application n'est pas un critère d'autorisation pour cette application.

   Cette case est cochée par défaut.

   La case ne peut être modifiée si la case **Autoriser automatiquement la diffusion du logiciel pour les packages de la liste** n'est pas cochée.

Il est conseillé de décocher la case **Toujours autoriser la diffusion de logiciel via Windows Installer** uniquement dans les cas extrêmes. La désactivation de ce paramètre peut entraîner des problèmes lors de la mise à jour des fichiers du système d'exploitation ainsi que l'interdiction du lancement des fichiers enfants de la distribution des paquets de confiance.

6. Le cas échéant, cochez la case **Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)**.

   La case active ou désactive l'autorisation automatique de la diffusion du logiciel avec l'aide de la solution System Center Configuration Manager.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server autorise automatiquement le déploiement de Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de diffuser une application uniquement à l'aide du service de transfert intelligent en arrière-plan (Background Intelligent Transfer Service).

   L'application contrôle le lancement des objets qui portent les extensions suivantes :

   - .exe
   - .msi

   Cette case est décochée par défaut.

L'application contrôle le cycle de diffusion de l'application sur le serveur, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la diffusion avait été réalisée avant l'installation du système sur le serveur.

7. Pour modifier la liste des distributions des paquets de confiance, cliquez sur le bouton **Modifier la liste de paquets** et dans le menu qui s'ouvre, sélectionnez une des méthodes suivantes :

   - **Ajouter un paquet de distribution**.

     a. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de lancement de l'application ou le paquet d'installation.

Les données du fichier sélectionné sont ajoutées automatiquement au groupe **Critères de confiance**.

b. Cochez ou décochez la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**.

c. Choisissez une de deux options proposées pour les critères de confiance qui vont déterminer si un fichier ou un paquet d'installation peut être considéré comme étant de confiance :

- **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.

- **Utiliser le hash 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.

  Il est conseillé d'appliquer cette option lorsque les règles générées doivent répondre au niveau de sécurité le plus fiable : la somme de contrôle SHA256 peut être appliquée comme seul identifiant du fichier. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle réduit la zone d'application des règles à un fichier.

  Cette option est sélectionnée par défaut.

- **Ajouter plusieurs paquets selon le hash**.

  Vous pouvez choisir un nombre illimité de fichiers de lancement et de paquets d'installation et les ajouter simultanément à la liste. Kaspersky Security 10.1.1 for Windows Server tient compte du hash et autorise le lancement le système d'exploitation à lancer les fichiers indiqués.

- **Modifier le paquet sélectionné**.

  Cette option permet de sélectionner un autre fichier de lancement ou un autre paquet d'installation. Elle permet également la modification des critères de confiance.

- **Importer la liste des paquets de distribution depuis un fichier**.

  Vous pouvez importer la liste des distributions des paquets de confiance depuis le fichier de configuration enregistré. Pour être reconnu par Kaspersky Security 10.1.1 for Windows Server, le fichier doit répondre aux paramètres suivants :

  - posséder une extension de fichier texte ;
  - contenir des informations présentées sur la forme d'une liste de lignes contenant chacune des données pour un des fichiers de confiance ;
  - contenir une liste correspondant à un des deux formats suivants :
    - <nom du fichier>:<hash SHA256> ;
    - <hash SHA256>*<nom du fichier>.

Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des distributions des paquets de confiance.

8. Si vous voulez supprimer de la liste des éléments de confiance une application ou un paquet d'installation qui avait été ajouté antérieurement, cliquez sur le bouton **Supprimer les paquets d'installation**. Le lancement des fichiers intégrés sera autorisé.

   Pour interdire le lancement des fichiers enfants, désinstallez l'application du serveur protégé ou créez une règle d'interdiction dans les paramètres de la tâche Contrôle du lancement des applications.

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

Les paramètres de la tâche définis seront enregistrés.

Activation du mode d'autorisation par défaut

Le mode d'autorisation par défaut autorise le lancement de toutes les applications, si celles-ci ne sont pas interdites par des règles ou par une conclusion douteuse de KSN. Il est possible d'activer le mode d'autorisation par défaut en ajoutant des règles d'autorisation spécifiques. Vous pouvez activer l'autorisation par défaut uniquement pour les scripts ou pour tous les fichiers exécutables.

► *Pour ajouter une nouvelle règle d'autorisation par défaut :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Contrôle de l'activité locale**, cliquez sur le bouton **Configuration** dans le groupe **Contrôle du lancement des applications**.
4. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
5. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Ajouter une règle**.

   La fenêtre **Paramètres de règle** s'ouvre.
6. Dans le champ **Nom**, saisissez le nom de la règle.

7. Dans la liste déroulante **Type**, sélectionnez le type de règle **Autorisé**.
8. 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.
9. Dans la section **Critère de déclenchement de la règle**, sélectionnez une option **Chemin du fichier**.
10. Saisissez le masque suivant : **?:**
11. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server applique le mode d'autorisation par défaut.

A propos de la génération des règles du Contrôle du lancement des applications pour l'ensemble du réseau via Kaspersky Security Center

Vous pouvez créer des listes de règles du Contrôle du lancement des applications à l'aide de tâches et de stratégies 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.

Le composant Contrôle du lancement des applications est installé avec deux règles d'autorisation prédéfinies :

- Règle d'autorisation pour les scripts et MSI avec le certificat de confiance du système d'exploitation.
- Règle d'autorisation pour les fichiers exécutables avec le certificat de confiance du système d'exploitation.

Vous pouvez créer des listes de règles du Contrôle du lancement des applications dans Kaspersky Security Center de deux manières :

- Via une tâche de groupe de Génération des règles du Contrôle du lancement des applications.

  Dans ce scénario, la tâche de groupe crée pour chaque serveur du réseau sa propre liste de règles du 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. Vous pouvez configurer une stratégie Kaspersky Security Center pour l'ajout automatique des règles créées à la liste des règles Contrôle du lancement des applications à la fin de la tâche de groupe Génération des règles du Contrôle du lancement des applications.

  Il est conseillé d'utiliser ce scénario quand il faut créer rapidement des listes de règles du Contrôle du lancement des applications. Le lancement de la tâche Génération des règles du Contrôle du lancement des applications 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.

Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

- Sur la base du rapport relatif aux événements de la tâche, générés dans Kaspersky Security Center pour le fonctionnement du Contrôle du lancement des applications en mode **Statistiques uniquement**.

  Dans ce cas de figure, Kaspersky Security 10.1.1 for Windows Server n'interdit pas les lancements des applications mais consigne dans la section **Evénements** de Kaspersky Security Center 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 du Contrôle du lancement des applications en mode **Statistiques uniquement**. Kaspersky Security Center établit ensuite, sur la base du journal d'exécution de la tâche, une liste unique des événements d'interdiction de lancement 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 du 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 recommandé d'utiliser ce scénario quand le réseau de l'organisation compte un nombre élevé de serveurs de différents types (cf. section "A propos de l'utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center" à la page 241) (avec différentes applications installées).

- Sur la base des événements d'interdiction de lancement des applications reçus via Kaspersky Security Center, sans création et importation du fichier de configuration.

  Pour pouvoir exploiter cette possibilité, la tâche Contrôle du lancement des applications sur l'ordinateur local doit être placée sous une stratégie active de Kaspersky Security Center. Dans ce cas, tous les événements sur l'ordinateur local sont transmis au Serveur d'administration.

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 une liste actualisée de règles à l'aide de la tâche Génération des règles du Contrôle du lancement des applications ou la stratégie Contrôle du lancement des applications en mode **Statistiques uniquement**, exécutées sur les serveurs du groupe d'administration d'essai pour obtenir une liste actualisées de règles. 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.

Avant d'ajouter des règles d'autorisation, choisissez un des modes d'application des règles disponibles (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page 242). La liste des règles de la stratégie de Kaspersky Security Center affiche uniquement les règles définies dans cette stratégie, quel que soit le mode d'application des règles. La liste des règles de l'ordinateur local affiche toutes les règles appliquées, quelles soient locales ou ajoutées via une stratégie.

Dans cette section

Création de règles d'autorisation au départ d'événements de Kaspersky Security Center

► *Pour créer des règles d'autorisation via l'option 'Créer des règles d'autorisation des applications au départ des événements de Kaspersky Security Center' dans le module Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Développez le groupe d'administration dont vous souhaitez modifier les paramètres dans la stratégie et choisissez l'onglet **Stratégies** dans le panneau de détails.
3. Dans le menu contextuel de la stratégie dont vous souhaitez modifier les paramètres, choisissez l'option **Propriétés**.

   La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.
4. Dans la section **Contrôle de l'activité locale**, cliquez sur le bouton **Configuration** dans le groupe **Contrôle du lancement des applications**.
5. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
6. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Créer des règles d'autorisation des applications à partir des événements de Kaspersky Security Center**.
7. Sélectionnez le principe d'ajout des règles à la liste des règles du Contrôle du lancement des applications déjà créées :

   - **Ajouter 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 sont dédoublées.
   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
   - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   La fenêtre **Création de règles du Contrôle du lancement des applications** s'ouvre.

8. Définissez les paramètres de requête suivants :
   - **Adresse du Serveur d'administration**
   - **Port**
   - **Utilisateur**
   - **Mot de passe**
9. Sélectionnez le type d'événement sur lequel vous souhaitez baser la tâche de création :
   - **Statistiques uniquement : lancement de l'application interdit**.
   - **Lancement de l'application interdit**.
10. Sélectionnez la période dans la liste déroulante **Evénements de requête générés au cours de la période**.
11. Cliquez sur le bouton **Créer des règles**.
12. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du contrôle du lancement des applications**.

    La liste des règles dans la stratégie Contrôle du lancement des applications est enrichie de nouvelles règles formées sur la base des données du système du serveur sur lequel la Console d'administration Kaspersky Security Center est installée.

    Si la liste des règles du Contrôle du lancement des applications est déjà définie dans la stratégie, Kaspersky Security 10.1.1 for Windows Server ajoute les règles choisies parmi les événements du verrouillage aux règles déjà définies. Les règles possédant le même hash ne sont pas ajoutées car toutes les règles d'une liste doivent être uniques.

Importation des règles du Contrôle du lancement des applications depuis un fichier XML

Vous pouvez importer les rapports créés sur la base des résultats de l'exécution de la tâche de groupe Génération des règles du Contrôle du lancement des applications 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 des règles du Contrôle du lancement des applications, l'application exporte les règles d'autorisation créées dans un fichier au format XML enregistré dans le dossier réseau partagé indiqué. 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 Génération des règles du Contrôle du lancement des applications.

La procédure de configuration des paramètres des composants fonctionnels de Kaspersky Security 10.1.1 for Windows Server dans Kaspersky Security Center est semblable à la configuration locale des paramètres de ces composants dans la console d'application. Les instructions détaillées relatives à la configuration des paramètres des tâches et des fonctions figurent dans les chapitres correspondants du *Manuel de l'utilisateur de Kaspersky Security 10.1.1 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 des règles du Contrôle du lancement des applications ou choisissez une tâche existante.
2. Dans les propriétés de la tâche de groupe de Génération des règles du Contrôle du lancement des applications créée ou dans l'Assistant de création de tâche, configurez les paramètres suivants :
   - Dans la section **Notification**, configurez les paramètres d'enregistrement du rapport sur l'exécution de la tâche.

     Les détails sur la configuration des paramètres de cette section sont repris dans le *Système d'aide de Kaspersky Security Center*.

   - Dans la section **Configuration**, indiquez les types d'applications 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 **Options**, 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 de planification du lancement de la tâche.
   - Dans la section **Compte**, désignez le compte utilisateur sous les privilèges duquel la tâche sera exécutée.
   - Dans la section **Exclusions de la zone de la tâche**, définissez les groupes de serveurs qu'il faut exclure de la zone d'action de la tâche.

     Kaspersky Security 10.1.1 for Windows Server ne crée pas de règles d'autorisation pour les applications lancées sur les serveurs exclus.

3. Sous l'onglet **Tâches** du panneau d'administration du groupe de serveurs configurés, sélectionnez la Génération des règles du Contrôle du lancement des applications créée 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.

   Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

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 du Contrôle du lancement des applications déjà créées :

      - **Ajouter 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 sont dédoublées.
      - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
      - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   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 des règles du Contrôle du lancement des applications.

   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 application, sélectionnez le mode d'exécution **Actif** 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 serveurs du réseau soumis à la stratégie configurée. Pour ces serveurs, l'application autorise 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 uniquement** 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 utiliser 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 uniquement**.
2. Dans la section **Evénements** des propriétés de la stratégie, assurez-vous que :
   - L'onglet **Evénements critiques** de l'événement Lancement des applications refusé indique une durée de conservation de l'événement supérieure à la durée de fonctionnement prévue de la tâche en mode **Statistiques uniquement** (valeur par défaut : 30 jours).
   - La durée de conservation de l'événement est supérieure à la durée prévue de fonctionnement de la tâche en mode **Statistiques uniquement** (valeur par défaut : 30 jours) sous l'onglet **Avertissement** pour l'événement *Statistiques uniquement : 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 uniquement**, 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 :
   a. Pour ce faire, développez le nœud **Journaux et notifications** dans les propriétés de la tâche Contrôle du lancement des applications.
   b. Dans le nœud enfant **Evénements**, créez une sélection d'événements sur la base de la caractéristique *Bloqués* afin de voir les applications dont le lancement sera bloqué par la tâche de Contrôle du lancement des applications.
   c. Dans le panneau de détails de la sélection créée, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites 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 du Contrôle du lancement des applications existantes :

- **Ajouter 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 sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

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 du Contrôle du lancement des applications.

Administration de la connexion des périphériques depuis Kaspersky Security Center

Vous pouvez autoriser ou limiter la connexion des disques flash et d'autres périphériques de stockage de masse à tous les serveurs du réseau en composant des listes uniques de règles du contrôle des serveurs du côté de Kaspersky Security Center pour les groupes de serveurs.

Dans cette section

A propos de la tâche Contrôle des périphériques

Kaspersky Security 10.1.1 for Windows Server contrôle l'enregistrement et l'utilisation des périphériques de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger le serveur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou d'autres types de périphérique externe connecté par USB. Un périphérique de stockage de masse est un périphérique externe qui peut être connecté à un serveur pour copier ou stocker des fichiers.

Kaspersky Security 10.1.1 for Windows Server contrôle les connexions USB des périphériques externes suivants :

- Disques flash USB ;
- Lecteurs de CD ;
- Lecteurs de disquettes USB ;
- Périphériques mobiles MTP.

Kaspersky Security 10.1.1 for Windows Server vous informe des périphériques connectés via USB avec l'événement correspondant dans les journaux d'exécution des tâches et des événements. Les détails des événements incluent le type de périphérique et le chemin de connexion. Lors la tâche Contrôle des périphériques est lancée, Kaspersky Security 10.1.1 for Windows Server analyse et énumère tous les périphériques connectés via USB. Vous pouvez configurer les notifications dans la section Configuration des notifications de Kaspersky Security Center.

La tâche Contrôle des périphériques surveille les tentatives de connexions USB de périphériques externes au serveur protégé et interdit leur utilisation en tant que stockages de masse s'il n'existe pas de règles d'autorisation pour ces périphériques. En raison du blocage, il est impossible de consulter le contenu du périphérique ou d'exécuter des opérations sur les fichiers de ce périphérique (par exemple, lecture ou écriture des fichiers).

L'application attribue à chaque périphérique de stockage de masse connecté un de deux états :

- *De confiance*. Périphérique avec lequel l'échange de fichiers est autorisé. Le chemin d'accès à ce périphérique tombe sous le coup au moins d'une règle d'autorisation.
- *Douteuse*. Périphérique avec lequel l'échange de données est interdit. Le chemin d'accès à l'instance d'un tel périphérique ne tombe pas sous le coup de la définition des règles d'autorisation.

Vous pouvez créer les règles d'autorisation pour les périphériques externes avec lesquels vous souhaitez autoriser l'échange de données à l'aide de la tâche Génération des règles du Contrôle des périphériques. Vous pouvez aussi élargir la zone d'application des règles d'autorisation déjà créées. Vous pouvez également créer des règles d'autorisation manuellement.

Kaspersky Security 10.1.1 for Windows Server identifie le stockage de masse enregistré dans le système sur la base de la valeur du *chemin d'accès à l'instance du périphérique*. Le chemin d'accès à l'instance du périphérique est un élément unique pour chaque périphérique externe. La valeur du chemin d'accès à l'instance du périphérique est définie pour chaque périphérique externe dans ses propriétés Windows et est définie automatiquement par Kaspersky Security 10.1.1 for Windows Server au moment de la création des règles.

La tâche Contrôle des périphériques peut être exécutée selon un des deux modes suivants :

- **Actif**. Kaspersky Security 10.1.1 for Windows Server contrôle, à l'aide de règles, la connexion de disques flash et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe de l'interdiction par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.

  Si un périphérique externe que vous considérez douteux a été connecté à un serveur protégé avant le lancement de la tâche Contrôle des périphériques en mode Actif, ce périphérique n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement le périphérique douteux ou de redémarrer le serveur. Dans le cas contraire, le principe d'interdiction par défaut ne sera pas appliqué à l'appareil.

- **Statistiques uniquement**. Kaspersky Security 10.1.1 for Windows Server ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le serveur protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

  Vous pouvez utiliser ce mode pour générer des règles sur la base des informations consignées pendant l'exécution de la tâche.

A propos de la génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center

Vous pouvez créer des listes de règles de contrôle des périphériques à l'aide de tâches de Kaspersky Security Center directement pour tous les serveurs et groupes de serveurs du réseau de l'organisation.

Vous pouvez créer des listes de règles de contrôle des périphériques dans Kaspersky Security Center de deux manières :

- Avec l'aide de la tâche de groupe Génération des règles du Contrôle des périphériques.

  D'après ce scénario, la tâche de groupe compose les listes des règles sur la base des données du système de chaque ordinateur relatives à tous les périphérique de stockage de masse jamais connectés aux serveurs protégés. La tâche tient également compte de tous les périphériques de stockage de masse connectés au moment de l'exécution de la tâche de groupe. À la fin de l'exécution de la tâche de groupe, Kaspersky Security 10.1.1 for Windows Server compose les listes des règles d'autorisation pour tous les périphériques de stockage de masse du réseau enregistrés et enregistre ces listes dans un fichier XML dans le dossier indiqué. Vous pouvez ensuite importer manuellement les listes de règles composées dans les propriétés de la stratégie Contrôle des périphériques. A la différence d'une tâche sur l'ordinateur local, la stratégie n'accepte pas la configuration de l'ajout automatique des règles créées dans la liste des règles de contrôle des périphériques à la fin de la tâche de groupe de Génération des règles du Contrôle du lancement des applications.

Il est recommandé d'utiliser ce scénario pour composer une liste de règles d'autorisation avant le premier lancement de la stratégie Contrôle des périphériques en mode d'application active des règles.

> Avant d'appliquer la stratégie de Contrôle des périphériques, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

- Sur la base du rapport généré dans Kaspersky Security Center et relatif aux événements survenus pendant le fonctionnement de la tâche Contrôle des périphériques en mode **Statistiques uniquement**.

  Selon ce scénario, Kaspersky Security 10.1.1 for Windows Server ne bloque pas la connexion des périphériques de stockage de masse, mais consigne dans la section **Evénements** de Kaspersky Security Center toutes les tentatives de connexion et d'enregistrement de périphériques de stockage de masse sur tous les ordinateurs du réseau pendant la période de fonctionnement de la tâche de contrôle des périphériques en mode **Statistiques uniquement**. Kaspersky Security Center établit ensuite, sur la base du journal d'exécution de la tâche, une liste unique des événements de blocage et de connexion des périphériques de stockage de masse.

  Vous devez configurer la période de l'exécution de la tâche de telle sorte que toutes les connexions de périphériques de stockage de masse puissent avoir lieu au cours de la période indiquée. Par la suite, lors de l'ajout de règles à la tâche de contrôle des périphériques, vous pouvez importer les données relatives aux connexions de périphériques 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 de ces périphériques. Les règles d'autorisations sont créées à l'importation du journal créé sur la base des événements de n'importe quel type.

  Il est conseillé d'utiliser ce scénario s'il faut ajouter des règles d'autorisation pour un nombre important de nouveaux périphériques de stockage de masse et pour créer des règles d'autorisation pour les périphériques mobiles de confiance connectés via le protocole MTP.

- Sur la base des données système relatives aux périphériques de stockage de masse connectés (à l'aide de l'option Créer les règles sur la base des données du système dans les paramètres de la stratégie Contrôle des périphériques).

  Dans le cadre ce scénario, Kaspersky Security 10.1.1 for Windows Server compose les règles d'autorisation pour les périphériques de stockage de masse connectés auparavant ou connectés actuellement à l'ordinateur doté de Kaspersky Security Center.

  Il est conseillé d'utiliser ce scénario quand il faut composer des règles pour un nombre réduit de nouveaux périphériques de stockage de masse dont vous souhaitez autoriser l'utilisation sur tous les ordinateurs du réseau.

- Sur la base des données relatives aux périphériques connectés actuellement (à l'aide de l'option **Créer des règles sur la base des périphériques connectés**).

  Dans le cadre de ce scénario, Kaspersky Security 10.1.1 for Windows Server crée des règles d'autorisation uniquement pour les périphériques connectés actuellement. Vous pouvez sélectionner un ou plusieurs périphériques pour lesquels vous souhaitez confirmer des règles d'autorisation.

  Kaspersky Security 10.1.1 for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles de confiance connectés via MTP à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

Création de règles sur la base des données du système relatives aux périphériques externes connectés aux ordinateurs du réseau

Vous pouvez créer des règles (cf. section "A propos de la génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center" à la page 263) sur la base des données Windows relatives aux stockages de masse connectés par le passé ou actuellement selon trois scénarios :

- Avec l'aide de la tâche de groupe Génération des règles du Contrôle des périphériques. Utilisez ce mode si voulez que, lors de la composition des règles d'autorisation, les données relatives à tous les périphériques de stockage de masse connectés à un moment donné soient enregistrées dans les systèmes sur tous les ordinateurs du réseau.
- Grâce à l'option **Créer les règles sur la base des données du système** dans les paramètres de la stratégie Contrôle des périphériques. Utilisez ce mode si voulez que, lors de la composition des règles d'autorisation, les données relatives à tous les périphériques de stockage de masse connectés à un moment donné soient enregistrées dans le système de l'ordinateur doté de la Console d'administration de Kaspersky Security Center.
- A l'aide de l'option **Créer des règles sur la base des périphériques connectés** dans les paramètres de la stratégie Contrôle des périphériques et de la tâche Génération des règles du Contrôle des périphériques. Utilisez cette méthode si vous souhaitez que seules les données relatives aux périphériques connectés actuellement au serveur protégé soient prises en compte lors de la création des règles d'autorisation.

Kaspersky Security 10.1.1 for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles de confiance connectés via MTP à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

Dans cette section

Création de règles à l'aide de la tâche Génération des règles du Contrôle des périphériques

► *Pour définir les règles d'autorisation du contrôle des périphériques pour un groupe de serveurs à l'aide de la tâche Génération des règles du Contrôle des périphériques, exécutez les actions suivantes.*

1. Sous l'onglet **Tâches** dans le panneau d'administration du groupe d'ordinateurs configuré, créez une tâche de groupe Génération des règles du Contrôle des périphériques ou choisissez une tâche existante.
2. Dans les propriétés de la tâche de groupe de Génération des règles du Contrôle du lancement des applications 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.
   - Dans la section **Configuration**, indiquez les actions de la tâche à son issue. Indiquez le nom du fichier dans lequel les règles créées seront exportées.
   - Dans la section **Planification**, configurez les paramètres de planification du lancement de la tâche.
3. Sous l'onglet **Tâches** du panneau d'administration du groupe de serveurs configurés, sélectionnez la tâche de Génération des règles du Contrôle des périphériques 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.

   > Avant d'appliquer la stratégie de Contrôle des périphériques, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

4. Ajoutez les listes de règles d'autorisation créées à la tâche de contrôle des périphériques. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie configurée, dans les paramètres de la tâche Contrôle des périphériques :
   a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

      La fenêtre **Règles du Contrôle des périphériques** 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 des périphériques déjà créées :

- **Ajouter 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 sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

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 des règles du Contrôle des périphériques.

e. Cliquez sur le bouton **OK** dans la fenêtre Règles du Contrôle des périphériques et dans la fenêtre **Paramètres de la tâche**.

5. Si vous voulez appliquer les règles créées pour le contrôle des périphériques, sélectionnez le mode de tâche **Actif** dans les paramètres de la stratégie **Contrôle des périphériques**.

Les règles d'autorisation générées automatiquement sur la base des données du système sur chaque serveur distinct sont appliquées à tous les serveurs du réseau soumis à la stratégie configurée. Pour ces serveurs, l'application autorise la connexion des périphériques pour lesquels des règles d'autorisation ont été créées.

Création de règles d'autorisation sur la base des données du système dans la stratégie de Kaspersky Security Center

► *Pour définir les règles d'autorisation à l'aide de l'option **Créer les règles sur la base des données du système**, dans les paramètres de la stratégie Contrôle des périphériques, procédez comme suit :*

1. Le cas échéant, connectez à l'ordinateur doté de la console d'administration de Kaspersky Security Center un nouveau périphérique de stockage de masse dont vous souhaitez autoriser l'utilisation.
2. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**.
3. Développez le groupe d'administration dont vous souhaitez modifier les paramètres dans la stratégie et choisissez l'onglet **Stratégies** dans le panneau de détails.
4. Dans le menu contextuel de la stratégie dont vous souhaitez modifier les paramètres, choisissez l'option **Propriétés**.
5. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.

6. Dans les propriétés de la stratégie, ouvrez la fenêtre de configuration des paramètres de la tâche Contrôle des périphériques et procédez comme suit :
   a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

      La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

   b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.

   c. Sélectionnez le principe d'ajout des règles d'autorisation à la liste des règles de contrôle des périphériques déjà créées :

      - **Ajouter 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 sont dédoublées.
      - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
      - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.
7. Cliquez sur le bouton **OK** dans la fenêtre **Règles du Contrôle des périphériques** et dans la fenêtre **Paramètres de la tâche**.

La liste des règles dans la stratégie Contrôle des périphériques sera enrichie de nouvelles règles formées sur la base des données du système de l'ordinateur sur lequel la Console d'administration de Kaspersky Security Center est installée.

Création de règles pour les périphériques connectés

► *Pour définir les règles d'autorisation à l'aide de l'option **Créer les règles sur la base des données du système**, dans les paramètres de la stratégie Contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Développez le groupe d'administration dont vous souhaitez modifier les paramètres dans la stratégie et choisissez l'onglet **Stratégies** dans le panneau de détails.
3. Dans le menu contextuel de la stratégie dont vous souhaitez modifier les paramètres, choisissez l'option **Propriétés**.
4. La fenêtre **Propriétés : <Nom de la stratégie>** s'ouvre.
5. Dans la section **Contrôle de l'activité locale**, cliquez sur le bouton **Configuration** dans le groupe **Contrôle des périphériques**.
6. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
7. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer des règles sur la base des périphériques connectés**.

   La fenêtre **Créer les règles sur la base des données du système** s'ouvre.

8. Dans la liste des périphériques détectés qui sont connectés au serveur protégé, choisissez les périphériques pour lesquels vous voulez créer des règles d'autorisation.
9. Cliquez sur le bouton **Ajouter** des règles pour les périphériques sélectionnés.
10. Cliquez sur le bouton **Enregistrer** dans la fenêtre Règles du **Contrôle des périphériques**.

La liste des règles dans la stratégie Contrôle des périphériques sera enrichie de nouvelles règles formées sur la base des données du système de l'ordinateur sur lequel la Console d'administration de Kaspersky Security Center est installée.

Importation des règles depuis un fichier du rapport de Kaspersky Security Center sur les périphériques bloqués

Vous pouvez importer les données relatives aux connexions des périphériques bloqués depuis le rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche Contrôle des périphériques en mode **Statistiques uniquement** 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 des périphériques, vous pouvez surveiller la connexion des périphériques qu'il faudra bloquer.

Lors de l'importation depuis le rapport des données sur les périphériques bloques dans les paramètres de la stratégie, confirmez que la liste à appliquer contient uniquement les périphériques dont vous souhaitez autoriser la connexion.

► *Pour créer des règles d'autorisation de connexion des périphériques pour un groupe de serveurs sur la base d'un rapport de Kaspersky Security Center relatif aux tentatives de connexion bloquées, procédez comme suit :*

1. Dans les propriétés de la stratégie, accédez aux paramètres de la tâche Contrôle des périphériques et sélectionnez le mode **Statistiques uniquement**.
2. Dans la section **Evénements** des propriétés de la stratégie, assurez-vous que :
   - L'onglet **Evénements critiques** de l'événement *Stockage de masse restreint* indique une durée de conservation de l'événement supérieure à la durée de fonctionnement prévue de la tâche en mode **Statistiques uniquement** (valeur par défaut : 30 jours).
   - La durée de conservation de l'événement est supérieure à la durée prévue de fonctionnement de la tâche en mode **Statistiques uniquement** (valeur par défaut : 30 jours) sous l'onglet **Avertissement** pour l'événement *Statistiques uniquement : périphérique de stockage de masse inconnu détecté*.

     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 des périphériques en mode **Statistiques uniquement**, 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 le nœud **Journaux et notifications** et, dans le nœud enfant **Evénements**, créez une sélection d'événements sur la base du critère *Interdit* afin de voir les périphériques dont les connexions seront bloquées par la tâche Contrôle des périphériques. Dans le panneau de détails de la sélection créée, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites 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 périphériques dont vous souhaitez autoriser la connexion.

4. Importez les données sur les tentatives bloquées de connexion des périphériques dans la stratégie du contrôle des périphériques. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie, dans les paramètres de la tâche Contrôle des périphériques :

   a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

      La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

   b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel, sélectionnez l'option **Importer les données relatives aux périphériques bloqués 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 du Contrôle des périphériques existantes :

      - **Ajouter 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 sont dédoublées.
      - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.
      - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   d. Dans la fenêtre Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les périphériques bloqués ont été exportés.

   e. Cliquez sur le bouton **OK** dans la fenêtre **Règles du Contrôle des périphériques** et dans la fenêtre **Paramètres de la tâche**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les périphériques bloqués seront ajoutées à la liste des règles de la stratégie de contrôle des périphériques.

Contrôle de l'activité réseau

Cette section contient des informations sur les tâches Gestion du pare-feu et Protection contre le chiffrement.

Contenu du chapitre

Gestion du pare-feu

Cette section contient des informations sur la tâche Gestion du pare-feu et sa configuration.

Dans cette section

A propos de la tâche Gestion du pare-feu

Kaspersky Security 10.1.1 for Windows Server offre une solution fiable et ergonomique pour la protection des connexions réseau grâce à la tâche Gestion du pare-feu.

La tâche Gestion du pare-feu ne réalise pas un filtrage indépendant du trafic réseau, mais il permet d'administrer le pare-feu Windows via l'interface graphique de Kaspersky Security 10.1.1 for Windows Server. Au cours de l'exécution de la tâche Gestion du pare-feu, Kaspersky Security 10.1.1 for Windows Server assume complètement l'administration des paramètres et des règles du pare-feu du système d'exploitation et interdit tout tentative de configuration de pare-feu externe.

Au cours de l'installation de l'application, le composant Gestion du pare-feu lit et copie l'état du pare-feu Windows, ainsi que toutes les règles définies. Par la suite, la modification de l'ensemble des règles ou de leurs paramètres, ainsi que l'arrêt ou le lancement du pare-feu seront possibles uniquement via Kaspersky Security 10.1.1 for Windows Server.

Si le pare-feu Windows est désactivé lors de l'installation de Kaspersky Security 10.1.1 for Windows Server, la tâche Gestion du pare-feu n'est pas lancée à la fin de l'installation. Si le pare-feu Windows est activé lors de l'installation de l'application, la tâche Gestion du pare-feu est exécutée à la fin de l'installation et bloque toutes les connexions de réseau sur la base des règles définies autorisées.

Le composant Gestion du pare-feu n'est pas repris dans la sélection de composants de l'installation Recommandée et n'est pas installé par défaut.

La tâche Gestion du pare-feu force l'interdiction de tous les connexions entrantes et sortantes si elles ne sont pas autorisées par les règles définies de la tâche.

La tâche interroge régulièrement le pare-feu Windows et contrôle son état. L'intervalle de sondage par défaut est de 1 minute et il n'est pas modifiable. Si à l'issue de l'interrogation Kaspersky Security 10.1.1 for Windows Server détecte un écart entre les paramètres du pare-feu Windows et ceux de la tâche Gestion du pare-feu, l'application impose les paramètres de la tâche au pare-feu du système d'exploitation.

Lors de l'interrogation du pare-feu Windows qui a lieu toutes les minutes, Kaspersky Security 10.1.1 for Windows Server contrôle les éléments suivants :

- état de fonctionnement du pare-feu Windows ;
- l'état de règles ajoutées après l'installation de Kaspersky Security 10.1.1 for Windows Server par d'autres applications ou outils (par exemple, ajout d'une nouvelle règle de l'application pour un port/une application à l'aide de wf.msc).

Lors de l'application de nouvelles règles au pare-feu Windows, Kaspersky Security 10.1.1 for Windows Server crée un ensemble de règles Kaspersky Security Group dans le composant logiciel enfichable **Pare-feu Windows**. Cet ensemble réunit toutes les règles créées par Kaspersky Security 10.1.1 for Windows Server via la tâche Gestion du pare-feu. Les règles qui figurent dans le groupe Kaspersky Security Group ne sont pas contrôlées par l'application lors du sondage toutes les minutes et elles ne sont pas synchronisées automatiquement avec la liste des règles définies dans les paramètres de la tâche Gestion du pare-feu. Le cas échéant, vous pouvez actualiser manuellement les règles de Kaspersky Security.

► *Pour mettre à jour manuellement la liste des règles Kaspersky Security Group,*

redémarrez la tâche Gestion du pare-feu de Kaspersky Security 10.1.1 for Windows Server.

Vous pouvez également modifier les règles de Kaspersky Security Group manuellement dans le composant logiciel enfichable **Pare-feu Windows**.

Le lancement de la tâche Gestion du pare-feu est impossible si le pare-feu Windows est administré par une stratégie de groupe Kaspersky Security Center.

A propos des règles du pare-feu

La tâche Gestion du pare-feu contrôle le filtrage du trafic entrant et sortant à l'aide de règles d'autorisation qui sont imposées au pare-feu Windows lors de l'exécution de la tâche.

Au premier lancement de la tâche, Kaspersky Security 10.1.1 for Windows Server lit toutes les règles pour le trafic entrant définies dans les paramètres du pare-feu Windows et les copies dans la tâche Gestion du pare-feu. Par la suite, l'application fonctionne conformément aux algorithmes suivants :

- si une règle est créée, manuellement ou automatiquement suite à l'installation d'une nouvelle application, dans les paramètres du pare-feu Windows, Kaspersky Security 10.1.1 for Windows Server supprime cette règle ;
- si une règle existante est supprimée dans les paramètres du pare-feu Windows, Kaspersky Security 10.1.1 for Windows Server restaure cette règle ;
- si les paramètres d'une règle existante sont modifiés dans les paramètres du pare-feu Windows, Kaspersky Security 10.1.1 for Windows Server annule les modifications ;
- si une règle est créée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Security 10.1.1 for Windows Server impose cette règle au pare-feu Windows ;
- si un règle existante est supprimée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Security 10.1.1 for Windows Server impose la suppression de cette règle dans les paramètres du pare-feu Windows.

Kaspersky Security 10.1.1 for Windows Server ne fonctionne pas avec les règles d'interdiction, ni avec les règles de contrôle du trafic sortant. Au lancement de la tâche Gestion du pare-feu, Kaspersky Security 10.1.1 for Windows Server supprime toutes les règles de ce genre dans les paramètres du pare-feu Windows.

Vous pouvez créer, supprimer et modifier les règles de filtrage du trafic entrant.

Vous ne pouvez pas définir une nouvelle règle pour le contrôle du trafic sortant via les paramètres de la tâche Gestion du pare-feu. Toutes les règles du pare-feu définies via Kaspersky Security 10.1.1 for Windows Server contrôlent uniquement le trafic réseau entrant.

Vous pouvez utiliser les règles de pare-feu des types suivants :

- Règles pour les applications.
- Règles pour les ports.

Règles pour les applications

Les règles de ce type autorisent au cas par cas les connexions pour les apps indiquées. Le critère de déclenchement de ces règles est le chemin d'accès au fichier exécutable.

Vous pouvez administrer les règles pour les apps :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le chemin d'accès au fichier exécutable et la zone d'application de la règle.

Règles pour les ports

Les règles de ce type autorisent les connexions réseau pour les ports et les protocoles indiqués (TCP / UDP). Les critères de déclenchement de ces règles sont le numéro du port et le type de protocole.

Vous pouvez administrer les règles pour les ports :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le numéro de port, le type de protocole et la zone d'application de la règle.

Les règles pour les ports ont une plus grande zone d'action que les règles pour les apps. En autorisant les connexions sur la base de règles pour les ports, vous abaissez le niveau de sécurité du serveur protégé.

Activation et désactivation des règles du pare-feu

► *Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le bloc **Gestion du pare-feu.**
4. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

   La fenêtre **Liste des règles** s'ouvre.
5. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
6. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :
   - Si vous voulez qu'une règle inactive soit appliquée, cochez la case à gauche du nom de la règle.

     La règle choisie sera activée.
   - Si vous voulez qu'une règle active ne soit plus appliquée, décochez la case à gauche du nom de la règle.

     La règle choisie sera désactivée.
7. Dans la fenêtre Règles du pare-feu, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Ajout manuel de règles du pare-feu

Vous pouvez ajouter et modifier uniquement les règles pour les apps et les ports. Vous ne pouvez pas ajouter de règles pour les groupes, ni modifier les règles existantes.

► *Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le bloc **Gestion du pare-feu**.
4. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

   La fenêtre **Liste des règles** s'ouvre.
5. En fonction du type de règle que vous souhaitez ajouter, choisissez l'onglet **Applications** ou **Ports** et exécutez une des actions suivantes :
   - Pour modifier une règle existante, sélectionnez dans la liste des règles celle dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Modifier**.
   - Pour créer une règle, cliquez sur le bouton **Ajouter**.

     En fonction du type de la règle à configurer, la fenêtre **Règle pour un port** ou **Règle pour l'application** s'ouvre.
6. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Si vous travaillez avec la règle pour une app, procédez comme suit :
     a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
     b. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.

        Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.
     c. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

        Les adresses IP doivent obligatoirement être saisies au format IPv4.

   - Si vous travaillez avec une règle pour un port, procédez comme suit :
     a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
     b. Saisissez dans le champ **Numéro de port** le numéro du port pour lequel l'application autorisera les connexions.
     c. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.
     d. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

        Les adresses IP doivent obligatoirement être saisies au format IPv4.

7. Dans la fenêtre **Règle pour l'application** ou **Règle pour un port**, cliquez sur le bouton OK.
8. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

► *Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le bloc **Gestion du pare-feu.**
4. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

   La fenêtre **Liste des règles** s'ouvre.
5. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
6. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
7. Cliquez sur le bouton **Supprimer**.

   La règle sélectionnée sera supprimée.
8. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche Gestion du pare-feu sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Protection contre le chiffrement

Cette section contient des informations sur la tâche Protection contre le chiffrement et sur sa configuration.

Dans cette section

A propos de la tâche Protection contre le chiffrement

La tâche Protection contre le chiffrement permet de détecter le chiffrement malveillant des ressources de fichier réseau sur un serveur protégé qui provient d'ordinateurs distants dans le réseau de l'entreprise.

Lors de l'exécution de la tâche Protection contre le chiffrement, Kaspersky Security 10.1.1 for Windows Server analyse les requêtes des ordinateurs distants adressées aux fichiers qui se trouvent dans les dossiers réseau partagés du serveur protégé. Si l'application considère les actions d'un ordinateur distant sur les ressources de fichier réseau comme des actions de chiffrement malveillant, cet ordinateur est ajouté à la liste des ordinateurs douteux et n'a plus accès au dossier réseau partagé.

Kaspersky Security 10.1.1 for Windows Server ne considère pas qu'il s'agit d'une tentative de chiffrement malveillant si l'activité de chiffrement détectée a lieu dans des répertoires exclus de la zone d'action de la tâche Protection contre le chiffrement.

Par défaut, l'application empêche l'accès des hôtes douteux aux ressources de fichier réseau pendant 30 minutes.

La tâche Protection contre le chiffrement ne bloque pas l'accès aux ressources de fichier réseau tant que l'activité de l'hôte n'est pas considérée comme malveillante. Cela peut durer un certain temps pendant lequel le malware de chiffrement peut réaliser son activité malveillante.

Si la tâche de protection contre le chiffrement est lancée en mode Informer uniquement, Kaspersky Security 10.1.1 for Windows Server consigne uniquement les tentatives de chiffrement malveillant émanant des ordinateurs distants dans le journal d'exécution de la tâche.

Configuration des paramètres de la Protection contre le chiffrement

La tâche Protection contre le chiffrement possède les paramètres par défaut suivants :

- **Mode de tâche**. La tâche Protection contre le chiffrement peut être lancée en mode **Actif** ou **Statistiques uniquement**. Le mode **Actif** est le mode par défaut.
- **Zone de protection**. Kaspersky Security 10.1.1 for Windows Server applique la tâche Protection contre le chiffrement à tous les dossiers réseau partagés du serveur par défaut. Vous pouvez modifier la zone de protection en indiquant les dossiers partagés auxquels doit s'appliquer la tâche.

- **Exclusions**. Spécifiez les zones que vous souhaitez inclure dans la zone de protection de la tâche.
- **Analyse heuristique**. Kaspersky Security 10.1.1 for Windows Server applique le niveau d'analyse **Moyenne**. Vous pouvez activer ou désactiver l'analyse heuristique et régler le niveau de détail de l'analyse.
- **Paramètres de planification**. Par défaut, le premier lancement n'est pas défini. La tâche Protection contre le chiffrement n'est pas lancée automatiquement au démarrage de Kaspersky Security 10.1.1 for Windows Server. 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 d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le groupe **Protection contre le chiffrement**.

   La fenêtre **Protection contre le chiffrement** s'ouvre.
4. Configurez les paramètres suivants dans la fenêtre qui s'ouvre :
   - Utilisation du mode Tâche et de l'analyseur heuristique (cf. section "Paramètres généraux de la tâche" à la page 280) sous l'onglet **Général**.
   - Zone de protection (cf. section "Constitution de la zone de protection" à la page 282) sous l'onglet **Zone de protection**.
   - Exclusions (cf. Section "Ajout d'exclusions" à la page 283) sous l'onglet **Exclusion**.
   - Paramètres de lancement de la tâche planifiée (cf. section "Programmation des tâches" à la page 143) sous l'onglet **Administration des tâches**.
5. Cliquez sur le bouton **OK**.

Kaspersky Security 10.1.1 for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

Paramètres des tâches de groupe

► *Pour configurer les paramètres d'une tâche locale :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le groupe **Protection contre le chiffrement**.

   La fenêtre **Protection contre le chiffrement** s'ouvre.
4. Dans le groupe **Mode de tâche**, indiquez le mode de fonctionnement de la tâche :
   - **Informer uniquement**.

     Si ce mode est sélectionné, toutes les tentatives de chiffrement malveillant sont consignées dans le journal des événements de la tâche Protection contre le chiffrement et aucune action n'est exécutée. Ce mode est sélectionné par défaut.
   - **Actif**.

     En cas de détection d'un chiffrement malveillant, Kaspersky Security 10.1.1 for Windows Server interdit l'accès aux dossiers partagés des ordinateurs compromis.
5. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

   La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

   Si la case est cochée, l'analyse heuristique est activée.

   Si la case est décochée, l'analyse heuristique est désactivée.

   Cette case est cochée par défaut.

6. 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'analyse 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'analyse heuristique** est cochée.

7. Cliquez sur le bouton **OK** pour appliquer la nouvelle configuration.

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 si 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 malveillant. Cette valeur est appliquée quand le paramètre **Uniquement les dossiers partagés indiqués** est sélectionné.

Vous pouvez utiliser le chemin d'accès local pour configurer la zone de protection de la tâche Protection contre le chiffrement.

► *Pour configurer une zone de protection pour la tâche Protection contre le chiffrement, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le groupe **Protection contre le chiffrement**.

   La fenêtre **Protection contre le chiffrement** s'ouvre.

4. Dans la section **Zone de protection**, sélectionnez les dossiers que Kaspersky Security 10.1.1 for Windows Server va analyser dans le cadre 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 10.1.1 for Windows Server 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 10.1.1 for Windows Server analyse uniquement les dossiers réseau partagés que vous avez désignés manuellement lors de l'exécution de la tâche Protection contre le chiffrement.
5. Pour spécifier les dossiers partagés du serveur que vous souhaitez inclure dans la zone de protection contre le chiffrement malveillant :
   a. Cliquez sur **Ajouter**.

      La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.
   b. Cliquez sur le bouton **Parcourir** pour sélectionner un dossier ou entrez manuellement le répertoire.
   c. Cliquez sur le bouton **OK**.
6. Dans la fenêtre **Protection contre le chiffrement**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Ajout de règles d'exclusion

► *Pour ajouter des exclusions de la zone de protection contre le chiffrement malveillant, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans le groupe **Protection contre le chiffrement**.

   La fenêtre **Protection contre le chiffrement** s'ouvre.

4. Sous l'onglet **Exclusions**, cochez la case **Appliquer la liste d'exclusions**.

   Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les zones de monitoring reprises dans la liste des exclusions lors de l'exécution de la tâche Protection contre le chiffrement.

   Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server détecte les activités de chiffrement malveillant pour tous les dossiers réseau partagés.

   La case est décochée par défaut, la liste des exclusions est vide.

5. Cliquez sur **Ajouter**.

   La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.

6. Entrez le nom du dossier ou cliquez sur **Parcourir** pour sélectionner un dossier.

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

La zone exclue est ajoutée à la liste.

Diagnostic du système

Cette section contient des informations sur la tâche de Moniteur d'intégrité des fichiers et les possibilités d'inspection du journal système du système d'exploitation.

Contenu du chapitre

Moniteur d'intégrité des fichiers

Cette section contient des informations sur le lancement et la configuration de la tâche Moniteur d'intégrité des fichiers.

Dans cette section

A propos de la tâche Moniteur d'intégrité des fichiers

La tâche Moniteur d'intégrité des fichiers permet de surveiller les actions exécutées sur les fichiers et les dossiers indiqués au sein des zones de monitoring définies dans les paramètres de la tâche. Vous pouvez utiliser la tâche pour détecter les modifications des fichiers afin d'identifier une violation de la sécurité sur le serveur protégé. Il est également possible de configurer le suivi des modifications des fichiers pendant la durée d'interruption du monitoring.

L'*interruption du monitoring* désigne une période au cours de laquelle la zone de monitoring est exclue temporairement de la zone d'action de la tâche, par exemple suite à l'arrêt de la tâche ou en l'absence physique d'un périphérique protégé sur le serveur protégé. Kaspersky Security 10.1.1 for Windows Server signale la détection d'opérations sur les fichiers dans la zone de monitoring dès que le périphérique de stockage de masse est à nouveau connecté.

Une suspension de l'exécution de la tâche dans la zone de monitoring définie suite à la réinstallation du composant Moniteur d'intégrité des fichiers ne constitue pas une interruption du monitoring. Dans ce cas, la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

Exigences applicables à l'environnement

Pour permettre le lancement de la tâche Moniteur d'intégrité des fichiers, les conditions suivantes doivent être remplies :

- un périphérique de stockage de masse, compatible avec les systèmes de fichiers ReFS et NTFS, doit être installé sur le serveur protégé ;
- Le journal USN Windows doit être activé. Le composant interroge ce journal afin d'obtenir des informations sur les opérations sur les fichiers.

  Si vous avez activé le journal USN après que vous avez créé une règle pour un volume et lancé la tâche Moniteur d'intégrité des fichiers, il faut relancer la tâche. Dans le cas contraire, cette règle n'est pas prise en compte par le monitoring.

Exclusions pour la zone de monitoring

Vous pouvez créer des exclusions de la zone de monitoring (cf. section "Configuration des règles de monitoring" à la page 290). Les exclusions sont définies pour chaque règle distincte et fonctionnent uniquement pour la zone de monitoring indiquée. Vous pouvez définir un nombre illimité d'exclusions pour chaque règle.

Les exclusions possèdent une priorité plus grande dans la zone de monitoring et elles ne sont pas contrôlées par la tâche, même si un dossier ou fichier indiqué se trouve dans la zone de monitoring. Si les paramètres d'une des règles définissent une zone de monitoring à un niveau inférieur à celui du dossier défini dans les exclusions, la zone de monitoring n'est pas prise en compte quand la tâche est exécutée.

Pour définir les exclusions, il convient d'utiliser les mêmes masques que ceux utilisés pour déterminer la zone de monitoring.

A propos des règles de monitoring des opérations sur les fichiers

La tâche Moniteur d'intégrité des fichiers est exécutée sur la base de règles de monitoring des opérations sur les fichiers. Les critères de déclenchement de la règle permettent de configurer les conditions de déclenchement d'une tâche et de régler le niveau d'importance des événements pour les opérations réalisées sur les fichiers qui ont été détectées et consignées dans le journal d'exécution de la tâche.

La règle de monitoring des opérations sur les fichiers est définie pour chaque zone de monitoring.

Vous pouvez configurer les critères de déclenchement de la règle suivants :

- Utilisateurs de confiance
- Marqueurs d'opérations sur les fichiers.

Utilisateurs de confiance

L'application considère par défaut les actions de tous les utilisateurs comme des violations potentielles de la sécurité. La liste des utilisateurs de confiance est vide. Vous pouvez configurer le niveau d'importance de l'événement en dressant une liste d'utilisateurs de confiance dans les paramètres de la règle de monitoring des opérations sur les fichiers.

Un *utilisateur douteux* désigne n'importe quel utilisateur qui ne figure pas dans la liste des utilisateurs de confiance définie dans les paramètres de la zone de monitoring. Si Kaspersky Security 10.1.1 for Windows Server détecte une opération sur un fichier réalisée par un utilisateur douteux, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance Evénement critique dans le journal d'exécution de la tâche.

L'*utilisateur de confiance* est un utilisateur ou un groupe d'utilisateurs autorisé à exécuter des opérations sur les fichiers dans la zone de monitoring indiquée. Si Kaspersky Security 10.1.1 for Windows Server détecte une opération sur un fichier réalisée par un utilisateur de confiance, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance Evénement d'information dans le journal d'exécution de la tâche.

Kaspersky Security 10.1.1 for Windows Server ne peut pas identifier l'utilisateur à l'origine des opérations quand celles-ci ont lieu dans la durée d'interruption du monitoring. Dans ce cas, l'état de l'utilisateur est défini comme inconnu.

L'*utilisateur inconnu* est un état attribué à un utilisateur quand Kaspersky Security 10.1.1 for Windows Server ne peut pas recevoir les données relatives à l'utilisateur suite à une interruption de la tâche ou à un échec du pilote de synchronisation des données et du journal USN. Si Kaspersky Security 10.1.1 for Windows Server détecte une opération sur un fichier réalisée par un utilisateur inconnu, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance *Avertissement* dans le journal d'exécution de la tâche.

Marqueurs d'opérations sur les fichiers

Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Security 10.1.1 for Windows Server utilise les marqueurs d'opérations sur les fichiers pour confirmer si une action a été réalisée sur le fichier.

Le marqueur d'opération sur les fichiers est un indice unique qui permet de définir une opération réalisée sur un fichier.

Chaque opération réalisée sur un fichier peut être composée d'une seule action ou d'une série d'actions exécutées sur les fichiers. Chaque action de ce genre reçoit un marqueur d'opérations sur les fichiers. Quand un marqueur que vous avez désigné comme critère de déclenchement de la règle de monitoring est détecté dans la chaîne d'opérations réalisées sur un fichier, l'application consigne l'événement lié à la réalisation d'une telle action.

Le niveau d'importance des événements consignés ne dépend pas des marqueurs d'opérations sur les fichiers choisis, ni de leur quantité.

Par défaut, Kaspersky Security 10.1.1 for Windows Server tient compte de tous les marqueurs d'opérations sur les fichiers disponibles. Vous pouvez sélectionner les marqueurs d'opérations sur les fichiers manuellement dans les paramètres des règles de la tâche (cf. tableau ci-dessous).

Tableau 41. Marqueurs d'opérations sur les fichiers

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
BASIC_INFO_CHANGE	attributs ou horodatage d'un fichier ou d'un dossier modifiés	NTFS, ReFS
COMPRESSION_CHANGE	compression d'un fichier ou d'un dossier modifiée	NTFS, ReFS
DATA_EXTEND	taille du fichier ou du dossier augmentée	NTFS, ReFS

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
DATA_OVERWRITE	Données dans le fichier ou me dossier écrasées	NTFS, ReFS
DATA_TRUNCATION	fichier ou dossier tronqués	NTFS, ReFS
EA_CHANGE	attributs étendus du fichier ou du dossier modifiés	NTFS uniquement
ENCRYPTION_CHANGE	état de chiffrement malveillant du fichier ou du dossier modifié	NTFS, ReFS
FILE_CREATE	fichier ou dossier créés pour la première fois	NTFS, ReFS
FILE_DELETE	Fichier ou dossier supprimé définitivement par une combinaison MAJ+SUPPR	NTFS, ReFS
HARD_LINK_CHANGE	lien physique pour le fichier ou le dossier créé ou supprimé	NTFS uniquement
INDEXABLE_CHANGE	état d'indexation du fichier ou du dossier modifié	NTFS, ReFS
INTEGRITY_CHANGE	attribut d'intégrité pour le flux de fichiers nommé modifié	ReFS uniquement
NAMED_DATA_EXTEND	taille du flux de fichiers nommé augmentée	NTFS, ReFS
NAMED_DATA_OVERWRITE	flux de fichiers nommé écrasé	NTFS, ReFS
NAMED_DATA_TRUNCATION	flux de fichiers nommé tronqué	NTFS, ReFS
OBJECT_ID_CHANGE	identifiant de fichier ou de dossier modifié	NTFS, ReFS
RENAME_NEW_NAME	nouveau nom attribué au fichier ou au dossier	NTFS, ReFS
REPARSE_POINT_CHANGE	point d'analyse répétée pour le fichier ou le dossier créé ou point d'analyse répétée existant modifié	NTFS, ReFS
SECURITY_CHANGE	autorisations d'accès au fichier ou au dossier modifiées	NTFS, ReFS
STREAM_CHANGE	flux de fichier nommé créé ou flux existant modifié	NTFS, ReFS
TRANSACTED_CHANGE	flux de fichier nommé modifié par la transaction TxF	ReFS uniquement

Configuration de la tâche Moniteur d'intégrité des fichiers

Vous pouvez modifier les paramètres de la tâche Moniteur d'intégrité des fichiers précisés par défaut (cf. tableau ci-dessous).

Tableau 42. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
Zones de monitoring	Non configuré	Vous pouvez définir les dossiers et les fichiers pour lesquels les opérations doivent être surveillées. Des événements de monitoring sont créés pour les dossiers et les fichiers de la zone de monitoring définie.
Liste des utilisateurs de confiance	Non configuré	Vous pouvez désigner des utilisateurs ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.
Contrôler les opérations sur les fichiers pendant la pause de la tâche	Appliquée	Vous pouvez activer ou désactiver la comptabilisation des opérations réalisées sur les fichiers dans les zones de monitoring indiquées pendant la durée d'interruption de la tâche.
Tenir compte de la zone de monitoring exclue	Pas appliqué	Vous pouvez contrôler l'application des exclusions pour les dossiers où il n'est pas nécessaire de surveiller les opérations réalisées sur les fichiers. Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Security 10.1.1 for Windows Server ignore les zones de monitoring définies en tant qu'exclusion.
Calcul de la somme de contrôle	Pas appliqué	Vous pouvez configurer le calcul de la somme de contrôle d'un fichier après que des modifications ont été introduites dans celui-ci.
Tenir compte des marqueurs d'opérations sur les fichiers	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Vous pouvez définir un ensemble de marqueurs pour caractériser les opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de monitoring se caractérise par au moins un des marqueurs indiqués, Kaspersky Security 10.1.1 for Windows Server génère un événement d'audit.
Planification du lancement de la tâche	Le premier lancement n'est pas défini	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Pour configurer les paramètres généraux de la tâche Moniteur d'intégrité des fichiers, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Cliquez sur le bouton **Configuration** dans le groupe **Moniteur d'intégrité des fichiers** de la section **Diagnostic du système**.

   La fenêtre **Moniteur d'intégrité des fichiers** s'ouvre.
4. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Paramètres de monitoring des opérations sur les fichiers**, puis configurez les paramètres de la zone de monitoring :
   a. Cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du monitoring**.

      La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

      Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server consigne les événements survenus dans toutes les zones de monitoring quand la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

      Si la case est décochée, les opérations sur les fichiers réalisées dans les zones de monitoring pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

      Cette case est cochée par défaut.

   b. Ajoutez les zones de monitoring que la tâche. (cf. section "Configuration des règles de monitoring" à la page 290) doit surveiller.
5. Sous l'onglet **Administration des tâches**, lancez la tâche sur la base d'une planification (cf. section "Programmation des tâches" à la page 143).
6. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Configuration des règles de monitoring

Par défaut, la zone de monitoring n'est pas définie ; la tâche ne contrôle l'exécution des opérations sur les fichiers dans aucun répertoire.

► *Pour ajouter une zone de monitoring, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
   - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

     Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Cliquez sur le bouton **Configuration** dans le groupe **Moniteur d'intégrité des fichiers** de la section **Diagnostic du système**.

   La fenêtre **Propriétés : Moniteur d'intégrité des fichiers** s'ouvre.
4. Dans le groupe **Zone de monitoring**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Zone de monitoring** s'ouvre.
5. Ajoutez une zone de monitoring à l'aide d'une des méthodes suivantes :
   - Si vous voulez choisir les dossiers via la boîte de dialogue Microsoft Windows standard :
     a. Cliquez sur le bouton **Parcourir**.

        La fenêtre standard de Microsoft Windows Parcourir le dossier s'ouvre.
     b. Dans la fenêtre qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations, puis cliquez sur le bouton **OK**.
   - Si vous voulez définir la zone de monitoring manuellement, ajoutez le chemin d'accès à l'aide d'un des masques pris en charge :
     - <*.ext> : tous les fichiers avec l'extension <ext>, quel que soit leur emplacement ;
     - <*\name.ext> : tous les fichiers portant le nom name et l'extension <ext>, quel que soit leur emplacement ;

- <\dir*> : tous les fichiers du répertoire <\dir> ;
- <\dir*\name.ext> : tous les fichiers portant le nom name et l'extension <ext> dans le dossier <\dir> et l'ensemble de ses sous-dossiers.

Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque>. En l'absence de l'indication du volume, Kaspersky Security 10.1.1 for Windows Server n'ajoute pas la zone de monitoring indiquée.

6. Cliquez sur le bouton **Ajouter** sous l'onglet **Utilisateurs de confiance**.

   La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

7. Choisissez les utilisateurs ou les groupes d'utilisateurs qui pourront réaliser des opérations sur les fichiers dans la zone de monitoring choisie, puis cliquez sur le bouton **OK**.

   Kaspersky Security 10.1.1 for Windows Server considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page 286) et génère pour ceux-ci des événements de niveau Critique.

8. Choisissez l'onglet **Marqueurs d'opérations sur les fichiers**.
9. Le cas échéant, sélectionnez plusieurs marqueurs d'opération sur les fichiers en réalisant les opérations suivantes :
   a. Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.
   b. Dans la liste des opérations sur les fichiers disponibles qui s'ouvre (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page 286), cochez les cases en regard des opérations que vous souhaitez contrôler.

   Kaspersky Security 10.1.1 for Windows Server détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

10. Si vous souhaitez que Kaspersky Security 10.1.1 for Windows Server calcule la somme de contrôle des fichiers après l'opération, procédez comme suit :
    a. Dans le groupe **Calcul de la somme de contrôle**, cochez la case **Calculer, si possible, la somme de contrôle du fichier modifié**.

       Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server calcule la somme de contrôle du fichier modifié dans lequel une opération correspondant à au moins un marqueur sélectionné a été détectée.

       Si l'opération sur le fichier est détectée à l'aide de plusieurs marqueurs, seule la somme de contrôle finale est calculée après la totalité des modifications.

Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server ne calcule pas la somme de contrôle pour les fichiers modifiés.

Aucune somme de contrôle n'est calculée dans les cas suivants :

- si le fichier est devenu inaccessible (par exemple, modification des autorisations d'accès au fichier) ;
- si l'opération réalisée sur le fichier concerne un fichier qui a été supprimé par la suite.

Cette case est décochée par défaut.

b. Sélectionnez une des options de la liste déroulante **Calculer la somme de contrôle selon l'algorithme** :

- **Hash MD5**
- **Hash SHA256**

11. Si vous ne souhaitez contrôler que certaines opérations sur les fichiers, ouvrez la liste des opérations disponibles (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page 286), puis cochez les cases en regard des opérations que vous souhaitez contrôler.
12. Le cas échéant, ajoutez des exclusions pour la zone de monitoring de la manière suivante :
    a. Sélectionnez l'onglet **Exclusions**.
    b. Cochez la case **Tenir compte des zones de monitoring exclues**.

    La case désactive l'application des exclusions pour les dossiers dans lesquels il n'est pas nécessaire de contrôler les opérations sur les fichiers.

    Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server ignore les zones de monitoring reprises dans la liste des exclusions lors de l'exécution de la tâche Moniteur d'intégrité des fichiers.

    Si la case est décochée, Kaspersky Security 10.1.1 for Windows Server enregistre les événements pour toutes les zones de monitoring définies.

    La case est décochée par défaut, la liste des exclusions est vide.

    c. Cliquez sur **Ajouter**.

    La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.

    d. Dans la fenêtre qui s'ouvre, sélectionnez le dossier que vous souhaitez exclure de la zone de monitoring.
    e. Cliquez sur le bouton **OK**.

    Le dossier indiqué est ajouté à la liste des zones exclues.
13. Cliquez sur le bouton **OK** dans la fenêtre **Zone de monitoring**.

Les paramètres des règles indiqués sont appliqués à la zone de monitoring choisie pour la tâche Moniteur d'intégrité des fichiers.

Inspection des journaux

Cette section contient des informations sur la tâche Inspection des journaux et la configuration de ses paramètres.

Dans cette section

A propos de la tâche Inspection des journaux

Au cours de l'exécution de la tâche Inspection des journaux, Kaspersky Security 10.1.1 for Windows Server contrôle l'intégrité de l'environnement protégé d'après les résultats de l'inspection des journaux des événements Windows. L'application informe l'administrateur en cas de détection de signes de comportement atypique dans le système pouvant indiquer des tentatives d'attaques informatiques.

Kaspersky Security 10.1.1 for Windows Server tient compte des données des journaux des événements Windows et définit les violations conformément aux règles précisées par l'utilisateur ou par les paramètres de l'analyse heuristique, appliqués par la tâche d'inspection des journaux.

Règles prédéfinie et analyse heuristique

Vous pouvez utiliser la tâche Inspection des journaux pour contrôler l'état du système protégé en appliquant les règles prédéfinies sur la base des heuristiques prédéterminées. L'analyseur heuristique définit la présence d'une activité anormale sur le serveur protégé, ce qui peut être le signe d'une tentative attaque. Les modèles de définition d'une activité anormale sont repris dans les règles disponibles dans les paramètres de règles prédéfinies.

La liste des règles de la tâche Inspection des journaux répertorie sept règles. Vous pouvez activer et désactiver l'application de n'importe quelle règle. Vous ne pouvez pas supprimer de règles existantes ou en créer de nouvelles.

Vous pouvez configurer les critères de déclenchement des règles qui contrôlent les événements pour les opérations suivantes :

- Détection des attaques brute-force
- Traitement de la connexion au réseau

Dans les paramètres de la tâche, vous pouvez configurer également les exclusions. L'analyseur heuristique ne fonctionne pas si l'accès au système est exécuté par un utilisateur de confiance ou via une adresse IP de confiance.

Kaspersky Security 10.1.1 for Windows Server n'applique pas l'heuristique à l'inspection des journaux Windows si l'analyseur heuristique n'est pas utilisé par la tâche. Par défaut, l'analyseur heuristique est activé.

Lors de l'application des règles, l'application consigne un événement avec le niveau d'importance *Critique* dans le journal d'exécution de la tâche Inspection des journaux.

Règles personnalisées de la tâche Inspection des journaux

A l'aide des paramètres des règles de la tâche, vous pouvez préciser et modifier les critères de déclenchement de la règle en cas de détection des événements choisis dans le journal Windows indiqué. Par défaut, la liste des règles de la tâche Inspection des journaux contient quatre règles. Vous pouvez activer et désactiver l'application de ces règles, supprimer les règles et en modifier les paramètres.

Vous pouvez configurer les critères suivants de déclenchement de chaque règle :

- Liste des identificateurs des enregistrements dans le journal des événements Windows.

  La règle se déclenche à l'apparition d'un nouvel enregistrement dans le journal des événements Windows, si dans les paramètres de l'événement, l'identificateur de l'événement indiqué dans la règle est détecté. Vous pouvez ajouter et supprimer aussi des identificateurs pour chaque règle précisée.

- Source des événements.

  Pour chaque règle, vous pouvez préciser un sous-journal du journal des événements Windows. L'application exécutera la recherche des enregistrements avec les identificateurs d'événements indiqués seulement dans ce sous-journal. Vous pouvez sélectionner un des journaux secondaires standard (Application, Sécurité ou Système) ou définir un journal secondaire personnalisé en saisissant le nom dans le champ de sélection de la source.

  L'application ne contrôle pas la présence réelle du sous-journal indiqué dans le journal des événements Windows.

Quand la règle est déclenchée, Kaspersky Security 10.1.1 for Windows Server enregistre un événement Critique dans le journal d'exécution de la tâche d'inspection des journaux.

Par défaut, la tâche Inspection des journaux ne prend pas en charge les règles utilisateur.

Avant de démarrer la tâche Inspection des journaux, assurez-vous que la stratégie d'audit système est correctement configurée. Consultez l'article de Microsoft https://technet.microsoft.com/en-us/library/cc952128.aspx pour plus de détails.

Configuration des règles prédéfinies d'une tâche

► *Pour configurer les règles prédéfinies de la tâche Inspection des journaux, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).

- Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

  Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.

3. Dans la section **Diagnostic du système** du groupe **Inspection des journaux**, cliquez sur le bouton **Configuration**.

   La fenêtre **Paramètres d'inspection des journaux** s'ouvre.

4. Sélectionnez l'onglet **Règles prédéfinies**.
5. Cochez ou décochez la case **Inspecter les journaux selon les règles prédéfinies**.

   Si cette case est cochée, Kaspersky Security 10.1.1 for Windows Server applique l'analyse heuristique pour détecter toute activité anormale sur le serveur protégé.

   Si cette case n'est pas cochée, l'analyse heuristique est désactivée, Kaspersky Security 10.1.1 for Windows Server utilise les règles prédéfinies ou définies par l'utilisateur pour détecter les activités anormales.

   Cette case est cochée par défaut.

   Pour que la tâche fonctionne, il faut sélectionner au moins une règle d'inspection des journaux.

6. Sélectionnez les éléments heuristiques que vous souhaitez appliquer à l'inspection des journaux dans la liste des éléments disponibles :
   - Tentative d'attaque brute-force dans le système.
   - Des signes d'abus potentiel du journal des événements Windows ont été détectés.
   - Des actions suspectes émanant d'un nouveau service installé ont été détectées.
   - Une authentification suspecte avec des identifiants explicites a été détectée.
   - Le système affiche les signes d'une éventuelle attaque Kerberos forged PAC (MS14-068).
   - Des actions suspectes contre un groupe Administrateurs privilégié intégré ont été détectées.
   - Une activité suspecte a été détectée lors d'une session de connexion au réseau.
7. Pour configurer les règles sélectionnées, cliquez sur le bouton **Paramètres avancés**.

   La fenêtre **Inspection des journaux** s'ouvre.

8. Dans le groupe **Détection des attaques brute-force**, définissez le nombre de tentatives et l'intervalle d'exécution de celles-ci qui vont servir de critères de déclenchement de l'analyse heuristique.
9. Dans le groupe **Détection de la connexion au réseau**, définissez le début et la fin de l'intervalle de temps pendant lequel Kaspersky Security 10.1.1 for Windows Server considère les tentatives de connexion comme une activité anormale.
10. Sélectionnez l'onglet **Exclusions**.

11. Pour ajouter des utilisateurs considérés comme des utilisateurs de confiance, procédez comme suit :
    a. Cliquez sur le bouton **Parcourir**.
    b. Choisissez l'utilisateur.
    c. Cliquez sur le bouton **OK**.

    L'utilisateur indiqué est ajouté à la liste des utilisateurs de confiance.
12. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :
    a. Saisissez l'adresse IP.
    b. Cliquez sur **Ajouter**.
13. L'adresse IP indiquée est ajoutée à la liste des adresses de confiance.
14. Sélectionnez l'onglet **Administration des tâches**pour configurer la planification du lancement de la tâche (cf. section "Configuration des paramètres de planification du lancement des tâches" à la page 143).
15. Cliquez sur le bouton **OK**.

Les paramètres de la tâche Inspection des journaux sont enregistrés.

Configuration des règles d'inspection des journaux

► *Pour ajouter et configurer une nouvelle règle d'inspection des journaux définies par l'utilisateur, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
    - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies**, puis ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page 109).
    - Si vous souhaitez configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).

    > Si l'appareil est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés dans la fenêtre **Paramètres de l'application**.
3. Dans la section **Diagnostic du système** du groupe **Inspection des journaux**, cliquez sur le bouton **Configuration**.

    La fenêtre **Inspection des journaux** s'ouvre.

4. Sous l'onglet **Règles d'inspection des journaux**, décochez ou cochez la case **Inspecter les journaux selon les règles personnalisées**.

   Si cette case est cochée, Kaspersky Security 10.1.1 for Windows Server applique les règles définies par l'utilisateur pour l'inspection des journaux conformément aux paramètres de chaque règle. Vous pouvez ajouter, supprimer ou configurer des règles d'inspection des journaux.

   Si la case est décochée, vous ne pouvez pas ajouter de règles personnalisées ni en modifier. Kaspersky Security 10.1.1 for Windows Server applique les paramètres de règles par défaut.

   Cette case est cochée par défaut. Seule la règle de détection de pop-up d'application est active.

   Vous pouvez contrôler l'application des règles prédéfinies à l'inspection des journaux. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

5. Pour créer une nouvelle règle définie par l'utilisateur, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règles d'inspection des journaux** s'ouvre.

6. Dans le groupe **Général**, saisissez les données suivantes pour la nouvelle règle :

   - **Nom**
   - **Source**

     Sélectionnez le journal dont les événements sont utilisés pour l'inspection. Vous avez le choix parmi les types de journaux d'événements Windows suivants :

     - Application
     - Sécurité
     - System

     Vous pouvez ajouter un nouveau journal personnalisé en saisissant le nom du journal dans le champ **Source**.

7. Dans le groupe **ID des événements déclenchés**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

   a. Saisissez la valeur numérique de l'identifiant.

   b. Cliquez sur **Ajouter**.

      L'identifiant de la règle indiqué est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

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

   La règle d'inspection des journaux est ajoutée à la liste générale des règles.

Génération de rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils sont basés sur les informations stockées sur le serveur d'administration.

A partir de Kaspersky Security Center 11, les types de rapports suivants sont disponibles pour Kaspersky Security 10.1.1 for Windows Server :

- Rapport sur l'état des composants de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Consultez l'*aide de Kaspersky Security Center* pour en savoir plus sur les rapports de Kaspersky Security Center et leur configuration.

Rapport sur l'état des composants de l'application

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée du composant défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque composant : *Exécution en cours, En pause, Arrêté, Dysfonctionnement, Non installé, Démarrage en cours*.

L'état *Non installé* désigne le composant, et non l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de composants et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de composants et leur état

Cf. *Aide de Kaspersky Security Center* pour plus de détails sur la création et l'utilisation de sélections.

► *Pour consulter les états des composants dans les paramètres de l'application :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Sélectionnez l'onglet **Périphériques**, puis ouvrez 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 123).
3. Sélectionnez la section **Composants**.
4. Consultez le tableau d'état.

► *Pour consulter un rapport standard Kaspersky Security Center :*

1. Sélectionnez le nœud **Serveur d'administration <nom du serveur>** dans l'arborescence de la Console d'administration.
2. Ouvrez l'onglet **Rapports**.
3. Double-cliquez sur l'élément de liste **Rapport sur l'état des composants de l'application**.

   Un rapport est généré.
4. Définissez les paramètres de requête suivants :
   - Diagramme graphique.
   - Tableau récapitulatif des composants et nombres totaux d'appareils de réseau où chacun des composants est installé et groupes auxquels ils appartiennent.
   - Tableau détaillé spécifiant l'état des composants, la version, l' et le groupe.

Rapports sur les applications bloquées dans les modes actifs et statistiques

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications (cf. section "Administration du lancement de l'application via Kaspersky Security Center" à la page 241), deux types de rapports peuvent être générés : rapport sur les applications interdites (si la tâche est démarrée en mode **Actif**), rapport sur les applications interdites en mode test (si la tâche est démarrée en mode **Statistiques seulement**). Ces rapports affichent des informations sur les applications interdites sur les serveurs protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky Lab installées sur les appareils protégés.

► *Pour consulter un rapport sur les applications interdites en mode test :*

1. Démarrez la tâche Contrôle des applications en mode Statistiques seulement (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page 242).
2. Sélectionnez le nœud **Serveur d'administration <nom du serveur>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur l'élément de liste **Rapport sur les applications interdites en mode test**.

   Un rapport est généré.
5. Définissez les paramètres de requête suivants :
   - Diagramme graphique qui affiche les dix application avec la plus grande quantité de démarrages bloqués.
   - Tableau récapitulatif des interdictions d'applications survenues spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
   - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

► *Pour afficher un rapport sur les applications interdites en mode Actif :*

1. Lancez la tâche Contrôle des applications en mode Actif (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page 242),
2. Sélectionnez le nœud **Serveur d'administration <nom du serveur>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur un élément de liste **Rapport sur les applications interdites**.

   Un rapport est généré.

Ce rapport comprend les mêmes blocs de données que le rapport sur les applications interdites en mode test.

Utilisation de Kaspersky Security 10.1.1 for Windows Server depuis la ligne de commande

Cette section décrit l'utilisation de Kaspersky Security 10.1.1 for Windows Server via la ligne de commande.

Contenu du chapitre

Commandes de la ligne de commande

Vous pouvez exécuter les instructions d'administration de base Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server.

La ligne de commande permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Security 10.1.1 for Windows Server.

Certaines commandes de Kaspersky Security 10.1.1 for Windows Server sont exécutées 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**.

Respectez les règles suivantes lors de la saisie des instructions de Kaspersky Security 10.1.1 for Windows Server :

- 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, 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 10.1.1 for Windows Server (cf. tableau ci-dessous).

Tableau 43. Commandes de Kaspersky Security 10.1.1 for Windows Server

Instruction	Description
KAVSHELL APPCONTROL (cf. section "Enrichissement de la liste des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL" à la page 316)	Enrichit la liste des règles du Contrôle du lancement des applications créées conformément au principe d'ajout sélectionné.
KAVSHELL APPCONTROL /CONFIG (cf. section "Administration de la tâche Contrôle du lancement des applications KAVSHELL APPCONTROL /CONFIG" à la page 312)	Gère les modes de fonctionnement de la tâche Contrôle du lancement des applications.
KAVSHELL APPCONTROL /GENERATE (cf. section "Génération des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL /GENERATE" à la page 313)	Lance la tâche de génération des règles du Contrôle du lancement des applications.
KAVSHELL VACUUM (cf. section "Défragmentation des fichiers journaux de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL VACUUM" à la page 325)	Défragmente les fichiers journaux de Kaspersky Security 10.1.1 for Windows Server.
KAVSHELL PASSWORD	Administre les paramètres de la protection par mot de passe.
KAVSHELL HELP (cf. section "Affichage de l'aide sur les commandes de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL HELP" à la page 304)	Affiche l'aide sur les commandes de Kaspersky Security 10.1.1 for Windows Server.
KAVSHELL START (cf. section "Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP" à la page 305)	Lance le Service Kaspersky Security 10.1.1 for Windows Server.
KAVSHELL STOP (cf. section "Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP" à la page 305)	Arrête le Service Kaspersky Security 10.1.1 for Windows Server
KAVSHELL SCAN (cf. section "Analyse de la zone sélectionnée. KAVSHELL SCAN" à la page 305)	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. section "Lancement de la tâche Analyse des zones critiques. KAVSHELL SCANCRITICAL" à la page 309)	Lance la tâche système Analyse des zones critiques.
KAVSHELL TASK (cf. section "Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK" à la page 310)	Lance/suspend/relance/arrête la tâche indiquée en mode asynchrone/rend l'état actuelle de la tâche/les statistiques de la tâche.
KAVSHELL RTP (cf. section "Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP" à la page 312)	Lance ou arrête toutes les tâches de protection en temps réel.

Instruction	Description
KAVSHELL UPDATE (cf. section "Lancement de la tâche de mise à jour des bases de l'application de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL UPDATE" à la page 318)	Lance la tâche de mise à jour des bases de Kaspersky Security 10.1.1 for Windows Server selon les paramètres définis à l'aide des arguments de l'instruction.
KAVSHELL ROLLBACK (cf. section "Annulation des mises à jour des bases de l'application Kaspersky Security 10.1.1 for Windows Server. KAVSHELL ROLLBACK" à la page 321)	Remet les bases à l'état antérieur à la mise à jour.
KAVSHELL LICENSE (cf. section "Activation de l'application KAVSHELL LICENSE" à la page 322)	Gère les clés et les codes d'activation.
KAVSHELL TRACE (cf. section "Activation, configuration et désactivation de la constitution d'un journal de traçage. KAVSHELL TRACE" à la page 323)	Active ou désactive la création du journal de trace, gère les paramètres du journal de trace.
KAVSHELL DUMP (cf. section "Activation et désactivation de la création de fichiers dump. KAVSHELL DUMP" à la page 326)	Active ou désactive la création de fichiers dump de mémoire des processus de Kaspersky Security 10.1.1 for Windows Server en cas d'arrêt suite à une erreur.
KAVSHELL IMPORT (cf. section "Importation des paramètres. KAVSHELL IMPORT" à la page 328)	Importe les paramètres généraux de Kaspersky Security 10.1.1 for Windows Server, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration créé au préalable.
KAVSHELL EXPORT (cf. section "Exportation des paramètres. KAVSHELL EXPORT" à la page 328)	Exporte tous les paramètres de Kaspersky Security 10.1.1 for Windows Server et des tâches existantes dans un fichier de configuration.
KAVSHELL DEVCONTROL (cf. section "Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier. KAVSHELL DEVCONTROL" à la page 317)	Enrichit la liste des règles du Contrôle des périphériques créées conformément au principe d'ajout sélectionné.

Affichage de l'aide sur les commandes de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL HELP

Pour obtenir la liste de toutes les instructions de Kaspersky Security 10.1.1 for Windows Server, exécutez une des commandes suivantes :

```
KAVSHELL
```

```
KAVSHELL HELP

KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une commande, exécutez 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 l'instruction suivante :

```
KAVSHELL HELP SCAN
```

Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP

Pour lancer le Service Kaspersky Security, exécutez la commande

```
KAVSHELL START
```

Le lancement du Service Kaspersky Security s'accompagne par défaut du lancement des tâches Protection des fichiers en temps réel et Analyse au démarrage du système d'exploitation ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Pour arrêter le Service Kaspersky Security, exécutez la commande

```
KAVSHELL STOP
```

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Analyse de la zone indiquée. 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 du nœud sélectionné.

La tâche d'analyse à la demande lancée à l'aide de l'instruction `KAVSHELL SCAN` est temporaire. Elle apparaît dans la console d'application uniquement pendant son exécution (la console d'application ne vous permet pas de consulter les paramètres de la tâche). Le journal des performances de la tâche est créé à ce moment. Il apparaît

dans le nœud **Journaux d'exécution de la tâche** de la console d'application.

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 d'analyse à la demande existante via la ligne de commande, utilisez la commande KAVSHELL TASK (cf. section " Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK" à la page 310).

Syntaxe de la commande 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
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:c:\log.log
```

Tableau 44. Arguments de l'instruction `KAVSHELL SCAN`

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 dossier 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 10.1.1 for Windows Server analyse 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.

Clé	Description
/SHARED	Analyse les dossiers partagés sur le serveur.
/STARTUP	Analyse les objets de démarrage.
/REMDRIVES	Analyse les disques amovibles.
/FIXDRIVES	Analyse les disques durs.
/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 (Types de fichier). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security 10.1.1 for Windows Server analyse les objets en fonction du format.	
/FA	Analyse tous les objets
/FC	Analyse les objets en fonction du format (par défaut). Kaspersky Security 10.1.1 for Windows Server analyse uniquement les objets dont le format figure dans la liste des formats des objets infectables.
/FE	Analyse les objets en fonction de l'extension. Kaspersky Security 10.1.1 for Windows Server analyse uniquement les objets dont l'extension figure dans la liste des extensions des objets infectables.
/NEWONLY	Analyser uniquement les nouveaux fichiers et les fichiers modifiés. Si vous n'utilisez pas cet argument, Kaspersky Security 10.1.1 for Windows Server analyse tous les objets.
Actions à exécuter sur les objets infectés et autres. Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security 10.1.1 for Windows Server applique l'action **Ignorer**.	
DISINFECT	Désinfecter, ignorer si la désinfection est impossible
DISINFDEL	Désinfecter, supprimer si la désinfection est impossible
DELETE	Supprimer Les paramètres DISINFECT et DELETE ont été préservés dans la version actuelle de Kaspersky Security 10.1.1 for Windows Server pour garantir la compatibilité avec les versions antérieures. Ces paramètres peuvent être utilisés à la place des commandes clés /AI et /AS. Dans ce cas, Kaspersky Security 10.1.1 for Windows Server ne traite pas les objets probablement infectés.
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée

Clé	Description
/AS : **Actions à exécuter sur les objets probablement infectés**/ Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security 10.1.1 for Windows Server applique l'action **Ignorer**.	
QUARANTAINE	Quarantaine
DELETE	Supprimer
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée
Exclusions	
/E:ABMSPO	L'argument exclut les objets composés des types suivants : A : archives SFX ; B : bases de données d'emails ; 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".
/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>. Kaspersky Security 10.1.1 for Windows Server analyse par défaut toutes les tailles d'objet.
/TZOFF	Annule les exclusions de la zone de confiance.
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. Les niveaux d'analyse heuristique suivants sont disponibles : 1 – superficielle ; 2 – moyenne ; 3 – minutieuse. Si vous n'utilisez pas cet argument, Kaspersky Security 10.1.1 for Windows Server n'utilise pas l'analyse heuristique.

Clé	Description
/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 10.1.1 for Windows Server. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple update_1234. Dans la console d'application, la tâche reçoit le nom Analyser les objets (<date et heure>), par exemple, Analyser les objets 16/8/2007 5:13:14 PM.
Paramètres des journaux d'exécution des tâches (Report settings)	
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security 10.1.1 for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier 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 10.1.1 for Windows Server dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud Journaux d'exécution de la tâche de la console d'application. Si Kaspersky Security 10.1.1 for Windows Server ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche un message d'erreur.
/ANSI	La clé permet d'enregistrer les événements dans le journal d'exécution de la tâche 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, le journal d'exécution de la tâche s'effectue dans l'encodage UNICODE.

Lancement de la tâche Analyse des zones critiques. KAVSHELL SCANCRITICAL

Utilisez la commande `KAVSHELL SCANCRITICAL` pour lancer la tâche prédéfinie d'analyse à la demande Analyse des zones critiques selon les paramètres définis dans la console d'application.

Syntaxe de la commande KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<nom du fichier journal d'exécution de la tâche>]
```

Exemple de l'instruction KAVSHELL SCANCRITICAL

Pour exécuter la tâche d'analyse à la demande Analyse des zones critiques et 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 45. Syntaxe de l'argument /W de la commande KAVSHELL SCANCRITICAL

Clé	Description
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security 10.1.1 for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier 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 journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution de la tâche** de la console d'application. Si Kaspersky Security 10.1.1 for Windows Server ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche un message d'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.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Instruction de la commande KAVSHELL TASK

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemples de la commande 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 46. Arguments de l'instruction KAVSHELL TASK

Clé	Description
Sans argument	Renvoie la liste de toutes les tâches de Kaspersky Security 10.1.1 for Windows Server. La liste contient les champs : nom alternatif de la tâche, catégorie de tâche (tâche système 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 10.1.1 for Windows Server. Pour consulter les noms alternatifs des tâches dans Kaspersky Security 10.1.1 for Windows Server, 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
/STATE	Récupère l'état actuel de la tâche (par exemple, **Exécution en cours**, **Terminée**, **En pause**, **Arrêtée**, **Echec**, **Lancement en cours**, **Restauration en cours**)

Clé	Description
/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. section "Codes de retour de l'instruction KAVSHELL TASK" à la page 332).

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.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Exemples de la commande 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).

Tableau 47. Arguments de l'instruction KAVSHELL RTP

Clé	Description
/START	Lance toute les tâches de protection en temps réel : Protection des fichiers en temps réel, Monitoring des scripts et Utilisation du KSN.
/STOP	Arrête toutes les tâches de protection en temps réel.

Administration de la tâche Contrôle du lancement des applications KAVSHELL APPCONTROL /CONFIG

A l'aide de la commande `KAVSHELL APPCONTROL/CONFIG`, vous pouvez configurer le mode de fonctionnement de la tâche Contrôle du lancement des applications et contrôle du chargement des modules DLL.

Syntaxe de la commande KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
```

/savetofile:<chemin d'accès complet au fichier XML>

Exemples de la commande KAVSHELL APPCONTROL /CONFIG

► *Pour exécuter la tâche Contrôle du lancement des applications sous le mode **Actif** sans chargement du module DLL et enregistrer les paramètres de la tâche à la fin, exécutez la commande :*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Vous pouvez configurer les paramètres de la tâche le Contrôle du lancement des applications à l'aide de clés (cf. tableau ci-dessous).

Tableau 48. Arguments de la commande KAVSHELL APPCONTROL /CONFIG

Clé	Description
/mode:<applyrules|statistics>	Mode de fonctionnement de la tâche Contrôle du lancement des applications. Vous avez le choix entre les modes suivants de fonctionnement de la tâche : • actif : appliquer les règles du Contrôle du lancement des applications ; • statistics : statistiques uniquement.
/dll:<no|yes>	Désactiver ou activer le contrôle du chargement des modules DLL.
/savetofile: <chemin d'accès complet au fichier XML>	Exporter les règles précisées dans le fichier indiqué au format XML.
/savetofile: <nom complet du fichier XML>	Enregistrez la liste des règles dans un fichier.
/savetofile: <nom complet du fichier XML> /sdc	Enregistrez la liste des règles du contrôle de la distribution des logiciels.
/clearsdc	Supprimez de la liste toutes les règles du contrôle de la distribution des logiciels.

Génération des règles du contrôle du lancement des applications KAVSHELL APPCONTROL /GENERATE

La commande KAVSHELL APPCONTROL /GENERATE permet de composer la liste des règles du Contrôle du lancement des applications.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /GENERATE <chemin d'accès au dossier> | /source:<chemin d'accès au fichier contenant la liste des dossiers> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<utilisateur ou groupe d'utilisateurs>] [/export:<chemin d'accès complet au fichier XML>] [/import:<a|r|m>] [/prefix:<préfixe pour les noms de règles>] [/unique]
```

Exemples de commande KAVSHELL APPCONTROL /GENERATE

► *Pour créer des règles pour les fichiers des dossiers sélectionnés, exécutez la commande :*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

► *Pour créer les règles pour les fichiers exécutables de toutes les extensions accessibles dans le dossier indiqué et enregistrer à la fin de la tâche les règles créées dans le fichier indiqué au format XML, exécutez la commande :*

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c\rules\appctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez configurer les paramètres de création automatique des règles du Contrôle du lancement des applications (cf. tableau ci-après).

Tableau 49. Arguments de la commande `KAVSHELL APPCONTROL /GENERATE`

Clé	Description
Zone d'application des règles d'autorisation	
<chemin d'accès au dossier>	Indiquer le chemin d'accès au dossier qui contient les fichiers exécutables pour lesquels il faut créer automatiquement des règles d'autorisation.
/source: <chemin d'accès à la liste des dossiers>	Indiquer le chemin d'accès au fichier TXT qui contient la liste des dossiers avec les fichiers exécutables pour lesquels il faut créer automatiquement les règles d'autorisation.

Clé	Description
/masks: <edms>	Indiquer les extensions des fichiers exécutables pour lesquels il faut créer des règles d'autorisation du Contrôle du lancement des applications. Vous pouvez inclure dans la zone d'application des règles créées les fichiers portant les extensions suivantes : • e - fichiers portant l'extension exe ; • d - fichiers portant l'extension dll ; • m - fichiers portant l'extension msi ; • s - scripts.
/runapp	Tenir compte lors de la création des règles d'autorisation des applications lancées sur le serveur protégé au moment de l'exécution de la tâche.
Actions lors de la génération automatique de règles d'autorisation	
/rules: <ch|cp|h>	Indiquer les actions que la tâche réalise pendant la création des règles d'autorisation du Contrôle du lancement des applications : • ch – utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser le hash SHA256. • cp – utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser la valeur du chemin d'accès au fichier exécutable. • h – utiliser le hash SHA256.
/strong	Utiliser l'objet et l'empreinte du certificat numérique lors de la création automatique des règles d'autorisation du Contrôle du lancement des applications. La commande est exécutée si la clé /rules: <ch|cp> est spécifiée.
/user: <utilisateur ou groupe d'utilisateurs>	Indiquer le nom d'utilisateur ou du groupe d'utilisateurs auxquels la règle sera appliquée. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini.
Actions à réaliser à la fin de la génération des règles du Contrôle du lancement des applications	
/export: <chemin d'accès complet au fichier XML>	Enregistrer les règles créées dans un fichier au format XML.
/unique	Ajouter des informations relatives au serveur dotés des applications qui servent à créer les règles d'autorisation du Contrôle du lancement des applications.

Clé	Description
/prefix: <préfixe des noms des règles>	Définir le préfixe pour les noms des règles d'autorisation du Contrôle du lancement des applications.
/import: <a|r|m>	Importe les règles créées dans la liste des règles définies du Contrôle du lancement des applications conformément au principe défini d'ajout de nouvelles règles : • a - **Ajouter aux règles existantes** (les règles identiques apparaissent en double) ; • r - **Remplacer les règles existantes** (les nouvelles règles remplacent les règles définies) ; • m - **Fusionner avec les règles existantes** (les nouvelles règles dont les paramètres ne correspondent pas aux paramètres des règles déjà créées sont ajoutées).

Enrichissement de la liste des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL

La commande `KAVSHELL APPCONTROL` permet d'ajouter des règles du fichier XML à la liste des règles de la tâche Contrôle du lancement des applications conformément au principe choisi et de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Instruction de la commande KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

Exemples de la commande KAVSHELL APPCONTROL

► *Pour ajouter des règles depuis un fichier au format XML aux règles définies du contrôle du lancement des applications selon le principe Ajouter aux règles existantes, procédez comme suit :*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez sélectionner le principe d'ajout de nouvelles règles au départ d'un fichier désigné au format XML à la liste des règles définies de la tâche Contrôle du lancement des applications (cf. ill. ci-dessous).

Tableau 50. Arguments de l'instruction KAVSHELL APPCONTROL

Clé	Description
/append <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - **Ajouter aux règles existantes** (les règles identiques apparaissent en double).
/replace <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - **Remplacer les règles existantes** (les nouvelles règles remplacent les règles définies).
/merge <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - **Fusionner avec les règles existantes** (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
/clear	Purger la liste des règles du Contrôle du lancement des applications.

Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier. KAVSHELL DEVCONTROL

La commande `KAVSHELL DEVCONTROL` permet d'ajouter des règles à la liste des règles de la tâche Contrôle des périphériques au départ d'un fichier du format XML conformément au principe choisi ainsi que de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Instruction de la commande KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

Exemples de la commande KAVSHELL DEVCONTROL

► *Pour ajouter des règles depuis un fichier au format XML aux règles définies du contrôle des périphériques selon le principe **Ajouter aux règles existantes**, procédez comme suit :*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez sélectionner le principe d'ajout de nouvelles règles à la liste des règles définies de la tâche Contrôle des périphériques au départ d'un fichier désigné au format XML (cf. ill. ci-dessous).

Tableau 51. Arguments de l'instruction KAVSHELL DEVCONTROL

Clé	Description
/append <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - **Ajouter aux règles existantes** (les règles identiques apparaissent en double).
/replace <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - **Remplacer les règles existantes** (les nouvelles règles remplacent les règles définies).
/merge <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - **Fusionner avec les règles existantes** (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
/clear	Purger la liste des règles du Contrôle des périphériques.

Lancement de la tâche de mise à jour des bases de l'application de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL UPDATE

La commande KAVSHELL UPDATE vous permet de lancer la tâche de mise à jour des bases de Kaspersky Security 10.1.1 for Windows Server en mode synchrone.

La tâche de mise à jour des bases de données de Kaspersky Security 10.1.1 for Windows Server, lancée à l'aide de la commande KAVSHELL UPDATE, est une tâche temporaire. Elle est affichée dans la console d'application uniquement pendant son exécution. Le journal d'exécution de la tâche est créé à ce moment. Il apparaît dans le nœud **Journaux d'exécution de la tâche** de la console d'application. Les stratégies de Kaspersky Security Center peuvent s'appliquer aux tâches de mise à jour créées et lancées via la commande KAVSHELL UPDATE, ainsi qu'aux tâches de mises à jour créées dans la console d'application. Pour en savoir plus sur l'administration de Kaspersky Security 10.1.1 for Windows Server sur les ordinateurs à l'aide de Kaspersky Security Center, lisez la section "Administration de Kaspersky Security 10.1.1 for Windows Server 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 la commande 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 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 la commande KAVSHELL UPDATE

► *Pour lancer une tâche de mise à jour des bases de données définie par l'utilisateur, exécutez l'instruction suivante :*

```
KAVSHELL UPDATE
```

► *Pour lancer une tâche de mise à jour des bases de données 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 l'application Kaspersky Security 10.1.1 for Windows Server 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 52. Arguments de l'instruction KAVSHELL UPDATE

Clé	Description
Source des mises à jour (clé obligatoire). Indiquez une ou plusieurs sources. Kaspersky Security 10.1.1 for Windows Server 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 dossier de mise à jour réseau au format UNC.
<URL>	Source de mises à jour définies par l'utilisateur. adresse du serveur FTP ou HTTP sur lequel se trouve le dossier contenant les mises à jour.
<Dossier local>	Source de mises à jour définies 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 mise 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).

Clé	Description
Paramètres du serveur proxy	
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas cette clé, Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server contactera le serveur proxy sous le compte **Système local** (**SYSTÈME**) ; **1** : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Security 10.1.1 for Windows Server contactera le serveur proxy sous le compte dont le nom d'utilisateur et le mot de passe sont définis par les clés /PROXYUSER et /PROXYPWD. **2** : authentification selon le nom et le mot de passe de l'utilisateur définis par les clés /PROXYUSER et /PROXYPWD (Basic authentication). Si l'accès au serveur proxy ne requiert pas l'authentification, il n'est pas nécessaire d'indiquer cet argument.
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, les arguments /PROXYUSER:<nom d'utilisateur> è /PROXYPWD:<mot de passe> sont ignorés.
/PROXYPWD:<mot de passe>	Nom d'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, 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 le serveur proxy pour les adresses locales** est appliquée.
Paramètres généraux du serveur FTP ou HTTP	
/NOFTPPASSIVE	Si vous utilisez cet argument, Kaspersky Security 10.1.1 for Windows Server utilisera le mode actif de l'ordinateur FTP pour se connecter au serveur protégé. Si vous ne définissez pas cette clé, Kaspersky Security 10.1.1 for Windows Server utilisera le mode passif de l'ordinateur 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 cette clé, Kaspersky Security 10.1.1 for Windows Server utilisera la valeur par défaut : 10 s. Vous ne pouvez entrer que des nombres entiers.

Clé	Description
/REG:<code iso3166>	Paramètres régionaux. Cet argument intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab. Kaspersky Security 10.1.1 for Windows Server 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 ignorez cette clé ou si vous indiquez un code de pays incorrect, Kaspersky Security 10.1.1 for Windows Server identifiera l'emplacement du serveur protégé à l'aide des paramètres régionaux de l'ordinateur doté de la console d'application.
/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 10.1.1 for Windows Server. Si vous ne définissez pas cette clé, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple, update_1234. Dans la console d'application, la tâche reçoit automatiquement le nom Update-databases (<date heure>), par exemple, Update-databases 16/8/2007 05:41:02 PM.
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Security 10.1.1 for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier 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 10.1.1 for Windows Server dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution de la tâche** de la console d'application. Si Kaspersky Security 10.1.1 for Windows Server 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 l'instruction KAVSHELL UPDATE (à la page 333).

Annulation des mises à jour des bases de l'application Kaspersky Security 10.1.1 for Windows Server. KAVSHELL ROLLBACK

L'instruction `KAVSHELL ROLLBACK` vous permet d'exécuter la tâche système d'annulation de la mise à jour des bases de l'application de Kaspersky Security 10.1.1 for Windows Server (rétablissement de Kaspersky Security 10.1.1 for Windows Server à la version installée antérieurement). La commande est exécutée en mode synchrone.

Syntaxe de la commande

```
KAVSHELL ROLLBACK
```

Codes de retour de l'instruction KAVSHELL ROLLBACK (à la page 333).

Gestion de l'inspection des journaux. KAVSHELL TASK LOG-INSPECTOR

La commande `KAVSHELL TASK LOG-INSPECTOR` permet de surveiller l'intégrité de l'environnement sur la base de l'analyse du journal des événements Windows.

Syntaxe de la commande

```
KAVSHELL TASK LOG-INSPECTOR
```

Exemples de commandes

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tableau 53. Syntaxe de la commande KAVSHELL TASK LOG-INSPECTOR

Clé	Description
/START	Lance la tâche indiquée en mode asynchrone
/STOP	Arrête la tâche indiquée
/STATE	Récupère l'état actuel de la tâche (par exemple, *Exécution en cours, Complétée, En pause, Arrêtée, 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 LOG-INSPECTOR (cf. section "Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR" à la page 331).

Activation de l'application KAVSHELL LICENSE

La commande `KAVSHELL LICENSE` permet de gérer les clés et les codes d'activation de Kaspersky Security 10.1.1 for Windows Server.

> L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<fichier clé | code d'activation> [/R] | /DEL:<clé | numéro du code d'activation>]
```

Exemples de la commande KAVSHELL LICENSE

► *Pour activer l'application, exécutez la commande :*

```
KAVSHELL.EXE LICENSE / ADD: <code d'activation ou clé>
```

► *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 54. Arguments de l'instruction KAVSHELL LICENSE

Clé	Description
Sans argument	L'instruction affiche les informations suivantes sur les clés ajoutées : • Clé. • Type de licence (commerciale). • 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 clé additionnelle.
/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:<clé ou numéro 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. section "Codes de retour de l'instruction KAVSHELL LICENSE" à la page 334).

Activation, configuration et désactivation 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 pour tous les sous-systèmes de Kaspersky Security 10.1.1 for Windows Server ainsi que de définir le niveau de détail des informations reprises dans le journal.

Kaspersky Security 10.1.1 for Windows Server consigne les informations dans les fichiers de trace et le fichier dump en clair.

Syntaxe de la commande KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<dossier contenant les fichiers journaux de traçage>
[/S:<taille maximale du fichier de trace 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 55. Arguments de l'instruction KAVSHELL TRACE

Clé	Description
/ON	Active la constitution du journal de traçage.
/F:<dossier contenant les fichiers journaux de traçage>	Cet argument indique le chemin d'accès complet au dossier dans lequel les fichiers journaux 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 journaux 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 journal de traçage. Dès que la taille du fichier journal atteint la valeur maximale, Kaspersky Security 10.1.1 for Windows Server consigne les informations dans un nouveau fichier ; le fichier journal antérieur est enregistré. Si vous ne définissez pas cet argument, la taille maximale d'un fichier journal sera limitée à 50 Mo.
/LVL:debug|info|warning|error|critical	Cette clé définit le niveau de détail du journal depuis le niveau le plus détaillé (**Toutes les informations de débogage**) où tous les événements sont enregistrés dans le journal jusqu'au niveau minimum (**Evénements critiques**) où seuls les événements critiques sont enregistrés. Si vous ne définissez pas cette clé, le journal de trace contiendra les événements correspondant au niveau de détail **Toutes les informations de débogage**.
/OFF	Cet argument désactive la constitution du journal de traçage.

Exemples de la commande KAVSHELL TRACE :

- *Pour activer le journal de trace avec le niveau de détail **Toutes les informations de débogage** et la taille maximale du fichier journal de 200 Mo et enregistrer le fichier journal dans le répertoire C:\Trace Folder, exécutez la commande suivante :*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

- *Pour activer le journal de trace avec le niveau de détail **Evénements importants** et enregistrer le fichier journal dans le dossier C:\Trace Folder, exécutez la commande :*

```
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. section "Codes de retour de l'instruction KAVSHELL TRACE" à la page 334).

Défragmentation des fichiers journaux de Kaspersky Security 10.1.1 for Windows Server. KAVSHELL VACUUM

La commande `KAVSHELL VACUUM` permet de défragmenter les fichiers journaux des événements de l'application. Cela permet d'éviter les erreurs dans le fonctionnement du système ou de Kaspersky Security 10.1.1 for Windows Server liées au stockage des journaux.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Il est conseillé d'appliquer la commande `KAVSHELL VACUUM` pour optimiser la taille des fichiers journaux en cas d'exécution fréquente des tâches d'analyse à la demande et des tâches de mise à jour. Lors de l'exécution de la commande, Kaspersky Security 10.1.1 for Windows Server met à jour la structure logique des fichiers journaux de l'application enregistrés sur un serveur protégé au chemin d'accès indiqué.

Par défaut, les fichiers journaux de l'application sont conservés à l'emplacement C:\ProgramData\Kaspersky Lab\Kaspersky Security 10.1.1 for Windows Server\10.1.1\Reports. Si vous avez désigné un autre chemin d'accès manuellement pour la sauvegarde des fichiers journaux, la commande `KAVSHELL VACUUM` exécute une défragmentation des fichiers dans le dossier que vous aurez désigné dans les paramètres des journaux de Kaspersky Security 10.1.1 for Windows Server.

Des fichiers journaux des événements de grande taille à défragmenter augmente la durée d'exécution de la commande `KAVSHELL VACUUM`.

Pendant l'exécution de la commande `KAVSHELL VACUUM`, l'exécution des tâches de protection en temps réel et de contrôle du serveur est impossible. La procédure de défragmentation bloque l'accès au journal e Kaspersky Security 10.1.1 for Windows Server et interdit l'enregistrement des événements dans le journal. Afin d'éviter de réduire le niveau de sécurité de l'ordinateur, il est conseillé de planifier l'exécution de la commande `KAVSHELL VACUUM` en dehors des heures de bureau.

► *Pour défragmenter les fichiers journaux créés suite aux événements survenus pendant l'utilisation de Kaspersky Security 10.1.1 for Windows Server, exécutez la commande :*

```
KAVSHELL VACUUM
```

L'exécution de la commande est accessible en cas de lancement sous les autorisations du compte utilisateur de l'administrateur local.

Purge de la base iSwift. KAVSHELL FBRESET

Kaspersky Security 10.1.1 for Windows Server 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**).

Kaspersky Security 10.1.1 for Windows Server crée dans le répertoire système %SYSTEMDRIVE%\System Volume Information les fichiers klamfb.dat et klamfb2.dat qui contiennent des informations relatives aux objets sains déjà analysés. Plus le nombre de fichiers différents analysés par Kaspersky Security 10.1.1 for Windows Server est élevé, plus la taille du fichier klamfb.dat (klamfb2.dat) augmente. Ce fichier contient uniquement les informations actuelles sur les fichiers existant dans le système : si un fichier quelconque est supprimé, Kaspersky Security 10.1.1 for Windows Server supprime les informations qui le concerne dans le fichier klamfb.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 klamfb.dat à l'aide de l'instruction KAVSHELL FBRESET, Kaspersky Security 10.1.1 for Windows Server ne suspend pas la protection (à la différence de la suppression manuelle du fichier).
- Après la purge du fichier klamfb.dat, Kaspersky Security 10.1.1 for Windows Server peut augmenter la charge sur le serveur. Dans ce cas, l'Antivirus analyse tous les fichiers sollicités pour la première fois après la purge du fichier klamfb.dat. Après l'analyse, Kaspersky Security 10.1.1 for Windows Server introduit à nouveau dans le fichier klamfb.dat les informations relatives à chaque 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.

L'exécution de la commande `KAVSHELL FBRESET` requiert le lancement de la ligne de code sous le compte SYSTEM.

Activation et désactivation de la création de fichiers dump. KAVSHELL DUMP

L'instruction `KAVSHELL DUMP` permet d'activer ou de désactiver la création de modèles de mémoire (fichier dump) des processus de Kaspersky Security 10.1.1 for Windows Server en cas d'arrêt provoqué par une erreur (cf. tableau ci-dessous). De plus, vous pouvez prendre à n'importe quel moment un instantané de la mémoire des processus de Kaspersky Security 10.1.1 for Windows Server en cours d'exécution.

Pour obtenir le fichier dump, la commande `KAVSHELL DUMP` doit être lancée sous le compte système local (SYSTEM).

Syntaxe de la commande 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 56. 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>	Cet argument est obligatoire. Il 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

Clé	Description
/SNAPSHOT	Crée un instantané du modèle de mémoire du processus de Kaspersky Security 10.1.1 for Windows Server 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. section "Codes de retour de l'instruction KAVSHELL DUMP" à la page 335).

Importation des paramètres. KAVSHELL IMPORT

L'instruction `KAVSHELL IMPORT` permet d'importer les paramètres de Kaspersky Security 10.1.1 for Windows Server, de ses fonctions et de ses tâches depuis un fichier de configuration dans Kaspersky Security 10.1.1 for Windows Server sur le serveur protégé. Vous pouvez créer le fichier de configuration à l'aide de l'instruction `KAVSHELL EXPORT`.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL IMPORT

```
KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de la commande KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tableau 57. 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. section "Codes de retour de l'instruction KAVSHELL IMPORT" à la page 335).

Exportation des paramètres. KAVSHELL EXPORT

L'instruction `KAVSHELL EXPORT` permet d'exporter tous les paramètres de Kaspersky Security 10.1.1 for Windows Server et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Security 10.1.1 for Windows Server sur d'autres serveurs.

Syntaxe de la commande KAVSHELL EXPORT

```
KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de la commande KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tableau 58. 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. section "Codes de retour de l'instruction KAVSHELL EXPORT" à la page 336).

Intégration avec Microsoft Operation Management Suite. KAVSHELL OMSINFO

A l'aide de la commande KAVSHELL OMSINFO, vous pouvez réviser l'état de l'application et les informations sur les menaces détectées par les bases antivirus et le service KSN. Les données sur les menaces proviennent des journaux des événements disponibles.

Instruction de la commande KAVSHELL DEVCONTROL

```
KAVSHELL OMSINFO <chemin et nom du fichier généré>
```

Exemples de la commande KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tableau 59. Arguments de l'instruction KAVSHELL UPDATE

Clé	Description
<chemin et nom du fichier généré>	Nom du fichier généré qui contient des informations sur l'état de l'application et les menaces détectées.

Codes de retour de la ligne de commande

Dans cette section

Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Tableau 60. Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Code de retour	Description
0	L'opération a réussi
-3	Erreur de privilèges d'accès
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (par exemple, le service de Kaspersky Security 10.1.1 for Windows Server est déjà exécuté ou est déjà arrêté)
-7	Le service n'est pas enregistré
-8	Le lancement automatique du service est désactivé
-9	La tentative de démarrage de l'ordinateur sous un autre compte utilisateur a échoué (par défaut, le service de Kaspersky Security 10.1.1 for Windows Server fonctionne sous le compte utilisateur Système local).
-99	Erreur inconnue

Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL

Tableau 61. 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
-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 la commande incorrecte ou zone d'analyse non définie.
-80	Objets infectés et autres détectés
-81	Objets probablement infectés détectés
-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 journal d'exécution de la tâche
-99	Erreur inconnue
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR

Tableau 62. Code de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR

Code de retour	Description
0	L'opération a réussi
-6	Opération invalide (par exemple, le service de Kaspersky Security 10.1.1 for Windows Server est déjà exécuté ou est déjà arrêté)
402	La tâche est déjà lancée (pour l'argument /STATE)

Codes de retour de l'instruction KAVSHELL TASK

Tableau 63. 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)
-5	Syntaxe de la commande 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 64. 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 la commande incorrecte
-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 65. 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 la commande incorrecte
-99	Erreur inconnue
-206	Les fichiers d'extension 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 10.1.1 for Windows Server n'a pas subi d'authentification lors de la connexion à la source des mises à jour
-236	Les bases de Kaspersky Embedded Systems Security sont endommagées
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL ROLLBACK

Tableau 66. 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 67. Codes de retour de l'instruction KAVSHELL LICENSE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Privilèges insuffisants pour l'administration des clés
-4	Clé portant le numéro indiqué introuvable
-5	Syntaxe de la commande 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 68. 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 journaux de traçage est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (tentative d'exécution de la commande 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 69. 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 70. 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 le fichier dump est introuvable ; le processus avec le PID indiqué est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (tentative d'exécution de la commande 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 71. 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

Code de retour	Description
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 10.1.1 for Windows Server n'a pas importé les 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 10.1.1 for Windows Server postérieure ou incompatible)

Codes de retour de l'instruction KAVSHELL EXPORT

Tableau 72. 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 10.1.1 for Windows Server n'a pas exporté les paramètres d'un composant fonctionnel quelconque

Interruptions SNMP

Les paramètres des interruptions SNMP de Kaspersky Security 10.1.1 for Windows Server sont décrits dans le tableau ci-dessous.

Tableau 73. Interruptions SNMP de Kaspersky Security 10.1.1 for Windows Server

Piège	Description	Options
eventThreatDetected	Un objet a été détecté.	eventDateAndTime eventSeverity computerName UserName objectName threatName detectType detectCertainty
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 10.1.1 for Windows Server poursuit la mise en sauvegarde des objets infectés.	eventDateAndTime eventSeverity eventSource

Piège	Description	Options
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 (Mo)**, est inférieure ou égale à la valeur indiquée. Kaspersky Security 10.1.1 for Windows Server poursuit la mise en sauvegarde des objets infectés.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Dépassement de la taille maximale de la quarantaine. Le volume total de données de la quarantaine a dépassé la valeur du paramètre **Taille maximale de la quarantaine (Mo)**. Kaspersky Security 10.1.1 for Windows Server poursuit la mise en quarantaine des objets probablement infectés.	eventDateAndTime eventSeverity eventSource

Piège	Description	Options
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 disponible (Mo)**, est inférieure à la valeur indiquée. Kaspersky Security 10.1.1 for Windows Server poursuit la mise en quarantaine des objets probablement infectés.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Erreur de quarantaine.	eventSeverity eventDateAndTime eventSource UserName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Erreur d'enregistrement d'une copie de l'objet dans la Sauvegarde.	eventSeverity eventDateAndTime eventSource objectName UserName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Erreur de quarantaine.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Erreur de sauvegarde.	eventSeverity eventDateAndTime eventSource eventReason

Piège	Description	Options
eventAVBasesOutdated	La base antivirus n'est plus à jour. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de données (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	La base antivirus est périmée. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de données (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Security 10.1.1 for Windows Server est en cours d'exécution.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security 10.1.1 for Windows Server est arrêté.	eventSeverity eventDateAndTime eventSource

Piège	Description	Options
eventCriticalAreasScanWasntPerformForALongTime	Analyse des zones critiques non réalisée depuis longtemps. Le nombre de jours écoulés depuis la dernière tâche dont le statut est *Tâche d'analyse des zones critiques* est compté.	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Licence expirée.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Si la durée de validité de la 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 74. 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 du serveur (par exemple, nom du serveur 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 de la tâche ; • 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 10.1.1 for Windows Server dans son ensemble ; • systemAudit (8) – Journal d'audit système.

Paramètre	Description et valeurs possibles
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 10.1.1 for Windows Server utilise le dossier de sauvegarde ou de quarantaine indiqué par défaut.
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. Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Security 10.1.1 for Windows Server 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 "Configuration des paramètres du journal" à la page 170).
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 applications malveillantes ; • adware – applications publicitaires ; • pornware – logiciels pornographiques ; • riskware – applications légitimes pouvant être utilisées à des fins malveillantes pour endommager l'ordinateur ou les données de l'utilisateur.
detectCertainty	Coefficient de certitude de la découverte d'une menace. Le paramètre peut prendre les valeurs suivantes : • Suspicion (probablement infecté) : Kaspersky Security 10.1.1 for Windows Server a détecté une correspondance partielle entre un morceau de code de l'objet et un morceau de code malveillant connu. • Sure (infecté) : Kaspersky Security 10.1.1 for Windows Server 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.

Paramètre	Description et valeurs possibles
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) – cause indéterminée ; • 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 ; • 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 de données. Essayez à nouveau de réaliser la mise à jour dans quelques minutes.

Paramètre	Description et valeurs possibles
storageObjectNotAddedEventReason	Cause du non placement de l'objet en sauvegarde ou en quarantaine. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown(0) – cause indéterminée ; • reasonStorageInternalError : erreur de base de données ; restaurez Kaspersky Security 10.1.1 for Windows Server. • reasonStorageReadOnly – la base de données est uniquement accessible en lecture seule ; restaurez Kaspersky Security 10.1.1 for Windows Server. • reasonStorageIOError : erreur entrée/sortie : a) Kaspersky Security 10.1.1 for Windows Server est endommagé, restaurez Kaspersky Security 10.1.1 for Windows Server ; b) le disque contenant les fichiers de Kaspersky Security 10.1.1 for Windows Server est endommagé. • reasonStorageCorrupted : stockage endommagé ; restaurez Kaspersky Security 10.1.1 for Windows Server. • 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 10.1.1 for Windows Server. • reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigences de Kaspersky Security 10.1.1 for Windows Server. • reasonObjectNotFound – l'objet placé dans la Quarantaine 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.

Intégration aux systèmes tiers

Cette section décrit l'intégration de Kaspersky Security 10.1.1 for Windows Server aux fonctionnalités et technologies tierces.

Contenu du chapitre

Contrôle des performances. Compteurs de Kaspersky Security 10.1.1 for Windows Server

Cette section contient des informations sur les compteurs de Kaspersky Security 10.1.1 for Windows Server : compteurs de performance pour l'application Moniteur système et compteurs et interruptions SNMP.

Contenu du chapitre

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 10.1.1 for Windows Server pendant l'installation.

Dans cette section

A propos des compteurs SNMP de Kaspersky Security 10.1.1 for Windows Server

Les composants à installer de Kaspersky Security 10.1.1 for Windows Server reprennent par défaut le composant **Compteurs de performance**. Pendant l'installation, Kaspersky Security 10.1.1 for Windows Server enregistre ses compteurs de performance pour l'application Moniteur système de Microsoft Windows.

Grâce aux compteurs de Kaspersky Security 10.1.1 for Windows Server, 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 10.1.1 for Windows Server et les échecs de fonctionnement.

Pour consulter les compteurs de performance de Kaspersky Security 10.1.1 for Windows Server, 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 seuils et les recommandations pour la configuration de Kaspersky Security 10.1.1 for Windows Server lorsque les compteurs dépassent ces valeurs.

Total de requêtes rejetées

Tableau 75. Total de requêtes rejetées

Nom	Total de requêtes rejetées (Total number of requests denied)
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de l'application, le calcul est réalisé depuis la dernière exécution de Kaspersky Security 10.1.1 for Windows Server. L'application ignore les objets dont les requêtes de traitement sont rejetées par les processus de Kaspersky Security 10.1.1 for Windows Server.
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 10.1.1 for Windows Server. • L'interruption de la Protection en temps réel en raison d'un refus du gestionnaire d'intercepteurs de fichiers.
Valeur normale / seuil	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 plusieurs requêtes rejetées durant une longue période : tous les processus de Kaspersky Security 10.1.1 for Windows Server étaient totalement occupés, si bien que Kaspersky Security 10.1.1 for Windows Server n'a pas pu analyser les objets. Pour éviter que des objets soient ignorés, augmentez le nombre de processus de l'application pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security 10.1.1 for Windows Server **Quantité maximale de processus actifs** et **Nombre de processus de 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 10.1.1 for Windows Server n'analyse pas les objets à l'accès. Relancez Kaspersky Security 10.1.1 for Windows Server.

Total de requêtes ignorées

Tableau 76. Total de requêtes ignorées

Nom	Total de requêtes ignorées (Total number of requests skipped).
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par Kaspersky Security 10.1.1 for Windows Server mais qui n'ont pas donné d'événement sur la fin du traitement, ce nombre est calculé 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 reçu la requête de traitement (ils étaient occupés) ou n'a pas envoyé d'événement sur la fin du traitement, Kaspersky Security 10.1.1 for Windows Server 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 / seuil	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 10.1.1 for Windows Server afin de rétablir les flux gelés.

Nombre de requêtes non traitées en raison d'un manque de ressources système

Tableau 77. 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)
Définition	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources système (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Security 10.1.1 for Windows Server. Kaspersky Security 10.1.1 for Windows Server 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 / seuil	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 10.1.1 for Windows Server 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 78. Nombre de requêtes envoyées pour traitement

Nom	Nombre de requêtes envoyées pour traitement.
Définition	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 10.1.1 for Windows Server et le niveau général de l'activité de fichiers sur le serveur.
Valeur normale / seuil	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 79. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers.
Définition	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 10.1.1 for Windows Server et d'y remédier.
Valeur normale / seuil	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 10.1.1 for Windows Server ignorera l'objet. Augmentez le nombre de processus de Kaspersky Security 10.1.1 for Windows Server pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security 10.1.1 for Windows Server **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 80. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers
Définition	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 / seuil	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 compteur **Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers**, Kaspersky Security 10.1.1 for Windows Server répartit de manière inégale la charge sur les processus exécutés. Relancez Kaspersky Security 10.1.1 for Windows Server.

Nombre d'éléments dans la file d'attente des objets infectés

Tableau 81. Nombre d'éléments dans la file d'attente des objets infectés

Nom	Nombre d'éléments dans la file d'attente des objets infectés (Number of items in the infected object queue).
Définition	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment.
Fonction	Ce compteur permet d'identifier : • L'interruption de la Protection en temps réel en raison d'un éventuel refus du gestionnaire d'intercepteurs de fichiers. • La surcharge des processus suite à une répartition inégale du temps de processeur entre Kaspersky Security 10.1.1 for Windows Server et les autres applications exécutées. • Les épidémies de virus.
Valeur normale / seuil	La valeur du compteur peut être différente de zéro tant que Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Relancez Kaspersky Security 10.1.1 for Windows Server. • Manque de temps de processus pour le traitement des objets ; Accordez à Kaspersky Security 10.1.1 for Windows Server plus de temps de processeur, par exemple en réduisant la charge des autres applications sur l'ordinateur. • 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. Les informations relatives au nombre d'objets détectés figure dans les statistiques de la tâche ou dans le journal d'exécution de la tâche.

Nombre d'objets traités par seconde

Tableau 82. Nombre d'objets traités par seconde

Nom	Nombre d'objets traités par seconde.
Définition	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 10.1.1 for Windows Server ou d'un échec de Kaspersky Security 10.1.1 for Windows Server et d'y remédier.
Valeur normale / seuil	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 10.1.1 for Windows Server 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 10.1.1 for Windows Server ne disposent pas des ressources de processeur suffisantes pour traiter les objets. Accordez à Kaspersky Security 10.1.1 for Windows Server plus de temps de processeur, par exemple en réduisant la charge des autres applications sur le serveur. • Un échec s'est produit dans le fonctionnement de Kaspersky Security 10.1.1 for Windows Server (plusieurs flux sont gelés). Relancez Kaspersky Security 10.1.1 for Windows Server.

Compteurs et interruptions SNMP de Kaspersky Security 10.1.1 for Windows Server

Cette section contient des informations sur les compteurs et les interruptions SNMP de Kaspersky Security 10.1.1 for Windows Server.

Dans cette section

A propos des compteurs et interruptions SNMP de Kaspersky Security 10.1.1 for Windows Server

Si vous avez inclus le composant **Compteurs et pièges SNMP** dans les composants antivirus à installer, vous pouvez consulter les compteurs et les interruptions de Kaspersky Security 10.1.1 for Windows Server à l'aide du protocole Simple Network Management Protocol (SNMP).

Pour consulter les compteurs et les interruptions de Kaspersky Security 10.1.1 for Windows Server depuis le poste de travail de l'administrateur, lancez sur le serveur protégé le service SNMP (SNMP Service) et le service d'interruptions SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

Compteurs SNMP de Kaspersky Security 10.1.1 for Windows Server

Cette section propose un tableau contenant la description des paramètres des compteurs SNMP de Kaspersky Security 10.1.1 for Windows Server.

Dans cette section

Compteurs de performance

Tableau 83. Compteurs de performance

Compteur	Définition
currentRequestsAmount	Nombre de requêtes envoyées pour traitement (à la page 349)
currentInfectedQueueLength	Nombre d'éléments dans la file d'attente d'objets infectés (cf. section "Nombre d'éléments dans la file d'attente des objets infectés" à la page 351)
currentObjectProcessingRate	Nombre d'objets traités par seconde (à la page 351)
currentWorkProcessesNumber	Nombre actuel de processus actifs utilisés par Kaspersky Security 10.1.1 for Windows Server

Compteurs de quarantaine

Tableau 84. Compteurs de quarantaine

Compteur	Définition
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 85. Compteurs de sauvegarde

Compteur	Définition
currentBackupStorageSize	Volume de données en sauvegarde (Mo)

Compteurs généraux

Tableau 86. Compteurs généraux

Compteur	Définition
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 d'expiration 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 additionnelle ou au code d'activation.
currentApplicationUptime	Durée de fonctionnement de Kaspersky Security 10.1.1 for Windows Server depuis sa dernière exécution (en centièmes de secondes).
currentFileMonitorTaskStatus	Etat de la tâche Protection des fichiers en temps réel : **on** – exécution en cours ; **off** – stoppée ou en pause.

Compteur de mise à jour

Tableau 87. Compteur de mises à jour

Compteur	Définition
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 88. Compteurs de Protection en temps réel

Compteur	Définition
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalInfectedObjectsFound	Nombre d'objets infectés et autres 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, probablement infectés ou autres que Kaspersky Security 10.1.1 for Windows Server 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 10.1.1 for Windows Server 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 qui ont été désinfectés par Kaspersky Security 10.1.1 for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDisinfected	Nombre total d'objets infectés ou autres que Kaspersky Security 10.1.1 for Windows Server a tenté de désinfecter 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, probablement infectés ou autres désinfectés par Kaspersky Security 10.1.1 for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDeleted	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Security 10.1.1 for Windows Server a tenté de désinfecter en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

Compteur	Définition
totalObjectsBackedUp	Nombre total d'objets infectés ou autres placés dans la Sauvegarde par Kaspersky Security 10.1.1 for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotBackedUp	Nombre total d'objets infectés ou autres que Kaspersky Security 10.1.1 for Windows Server 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

Intégration à WMI

Kaspersky Security 10.1.1 for Windows Server prend en charge l'intégration à Windows Management Instrumentation (WMI) : vous pouvez utiliser des systèmes clients qui utilisent WMI pour recevoir des données via le standard WBEM (Web-Based Enterprise Management) afin de collecter des informations sur l'état de Kaspersky Security 10.1.1 for Windows Server et de ses composants.

Lorsque Kaspersky Security 10.1.1 for Windows Server est installé, il enregistre le module propriétaire sur le système, ce qui facilite la création d'un espace-nom racine WMI de Kaspersky Security 10.1.1 for Windows Server sur l'ordinateur local. Un espace-nom de Kaspersky Security 10.1.1 for Windows Server vous permet de travailler avec les classes et instances de Kaspersky Security 10.1.1 for Windows Server et leurs propriétés.

Les valeurs de certaines propriétés d'instances dépend des types de tâche.

Une *tâche non-périodique* est une tâche d'application qui n'est pas limitée dans le temps et qui peut être soit constamment exécutée, soit arrêtée. Il n'existe pas de progression de l'exécution pour ces tâches. Les résultats de l'exécution de la tâche sont enregistrés sans interruption pendant que la tache est exécutée en tant qu'événement unique (par exemple : détection d'un objet infecté par n'importe laquelle des tâches de Protection en temps-réel des serveurs). Ce type de tâches est administré via les stratégies de Kaspersky Security Center.

Une *tâche périodique* est une tâche d'application qui est limitée dans le temps et dont la progression d'exécution est affichée sous forme de pourcentage. Les résultats de la tâche sont générés une fois la tâche terminée et sont représentés en tant qu'élément unique ou état d'application modifié (par exemple : mise à jour des bases de données de l'application terminée, fichiers de configuration générés pour les tâches de génération d'une règle). Un certain nombre de tâches périodiques du même type peut être exécuté simultanément sur un même ordinateur (trois tâches d'analyse à la demande avec différentes portées d'analyse). Les tâches périodiques peuvent être administrées via Kaspersky Security Center en tant que tâches de groupe.

Si vous utilisez des outils pour générer des requêtes d'espaces-noms WMI et recevoir des données dynamiques à partir d'espaces-noms WMI sur votre réseau d'entreprise, vous pouvez recevoir les informations sur l'état actuel de l'application (cf. tableau ci-dessous).

Tableau 89. Informations sur l'état de l'application

Propriété d'instance	Description	Valeurs
ProductName	Nom de l'application installée.	Nom complet de l'application sans numéro de version.
ProductVersion	Version complète de l'application installée.	Numéro de version complète de l'application, y compris numéro de version.
InstalledPatches	Ensemble des noms d'affichage des correctifs déployés pour l'application.	Liste des correctifs critiques installés pour l'application.
IsLicenseInstalled	Etat d'activation de l'application.	État de la clé utilisée pour activer l'application. Valeurs possibles : • False : Pas de clé ou de code d'activation défini dans l'application. • True : Une clé ou un code d'activation a été ajouté à l'application.
LicenseDaysLeft	Indique le nombre de jours restants avant l'expiration de la licence en cours.	Nombre de jours restants avant l'expiration de la licence en cours. Valeurs non positives possibles : • 0 : La licence a expiré • -1 : Impossible d'obtenir des informations sur la clé en cours ou la clé indiquée ne peut pas être utilisée pour activer l'application (par exemple, elle est bloquée sur la base d'une liste noire de clés).
AVBasesDatetime	Horodatage d'une version en cours des bases antivirus.	Date et heure de la création des bases antivirus actuellement utilisées. Si l'application installée n'utilise pas de base antivirus, le champ possède la valeur «Not installed».
IsExploitPreventionEnabled	Etat du composant Protection contre les exploits.	Statut du composant Protection contre les exploits. Valeurs possibles : • True : Le composant Protection contre les exploits est activé et fournit une protection. • False : Le composant Protection contre les exploits est activé et fournit une protection. Par exemple : désactivé, non installé, le contrat de licence a été violé.

Propriété d'instance	Description	Valeurs
ProtectionTasksRunning	Ensemble des tâches de protection en cours d'exécution.	Liste des tâches de protection, de contrôle et de monitoring en cours d'exécution. Ce champ doit tenir compte de toutes les tâches non périodiques en cours d'exécution. Si aucune tâche non périodique n'est en cours d'exécution, le champ a la valeur « Non ».
IsAppControlRunning	Etat de la tâche Contrôle du lancement des applications.	Statut de tâche Contrôle du lancement des applications. • True : La tâche Contrôle du lancement des applications n'est pas en cours d'exécution. • False : Le Contrôle du lancement des applications n'est pas en cours d'exécution ou le composant Contrôle du lancement des applications n'est pas installé.
AppControlMode	Mode de la tâche du Contrôle du lancement des applications.	Description de l'état actuel du composant Contrôle du lancement des applications et du mode sélectionné pour la tâche correspondante. Valeurs possibles : • Active : le mode **Actif** est sélectionné dans les paramètres de la tâche. • Statistics Only : le mode **Statistiques seulement** est sélectionné dans les paramètres de la tâche. • Not installed : Le composant Contrôle du lancement des applications n'est pas installé
AppControlRulesNumber	Nombre total de règles de contrôle du lancement des applications.	Nombre de règles actuellement indiquées dans les paramètres de la tâche Contrôle du lancement des applications.
AppControlLastBlocking	Horodatage du dernier blocage de lancement d'une application par la tâche de Contrôle du lancement des applications dans n'importe quel mode.	Date et heure auxquelles le composant Contrôle du lancement des applications a bloqué pour la dernière fois le lancement d'une application. Ce champ inclut toutes les applications bloquées, quel que soit le mode de la tâche. Si aucune instance de lancement d'applications bloquées n'est enregistrée au moment du traitement de la requête WMI, la valeur « Non » est attribuée au champ.

Propriété d'instance	Description	Valeurs
PeriodicTasksRunning	Ensemble des tâches périodiques en cours d'exécution.	Liste des tâches d'analyse à la demande, de mise à jour et de prise d'inventaire en cours d'exécution. Ce champ doit inclure toutes les tâches périodiques en cours d'exécution. Si aucune tâche périodique n'est en cours d'exécution, le champ a la valeur « Non ».
ConnectionState	Etat de connexion entre le composant WMI Provider et le Service Kaspersky Security (KAVFS).	Informations sur l'état de connexion entre le module WMI Provider et le Service Kaspersky Security. Valeurs possibles : • Success : La connexion a été établie avec succès : le client WMI peut recevoir des informations sur l'état de l'application. • Failed. Code d'erreur : <code> - La connexion n'a pas pu être établie en raison d'une erreur avec le code indiqué.

Ces données représentent les propriétés d'instance KasperskySecurity_ProductInfo.ProductName=Kaspersky Security for Windows Server, où :

- KasperskySecurity_ProductInfo est le nom de la classe de Kaspersky Security 10.1.1 for Windows Server
- .ProductName=Kaspersky Security for Windows Server est le paramètre clé de Kaspersky Security 10.1.1 for Windows Server

L'instance est créée dans l'espace-nom ROOT\Kaspersky\Security.

Contacter le Support Technique

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

Contenu du chapitre

Modes d'obtention de l'assistance 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.

Voici comment contacter les experts du Support Technique de Kaspersky Lab :

- appeler le Support Technique par téléphone ;
- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Assistance 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 utilisateur 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/faq/companyaccount_help.

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 10.1.1 for Windows Server 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 trace. 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 actifs, de rechercher la présence éventuelle de menaces sur l'ordinateur, de désinfecter 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 traitement et stockage 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 qui ont été traitées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Kaspersky Lab

Kaspersky Lab est connu dans le monde entier pour ses systèmes de protection contre diverses menaces numériques telles que les virus et autres applications malveillantes, les emails indésirables (spams), les attaques de réseaux et les piratages.

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. La société est devenue un groupe international qui compte 38 bureaux dans 33 pays. L'entreprise emploie plus de 3 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection 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 systèmes de contrôle industriel et la prévention des escroqueries financières. Ces solutions, associées à des outils d'administration centralisée, permettent de créer et d'exploiter une protection automatisée efficace de l'entreprise de n'importe quelle taille contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands laboratoires d'essai. 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 désinfection de ces menaces et les ajoutent 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.

Résultats. 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 à travers le monde. Les produits et les technologies de la société assurent la protection de plus de 400 millions de particuliers et plus de 270 000 entreprises.

Site de Kaspersky Lab :	https://www.kaspersky.com/fr
Encyclopédie des virus :	https://securelist.fr/
Laboratoire de virus :	https://virusdesk.kaspersky.fr (pour l'analyse de fichiers ou de sites Internet suspects)
Forum Internet de Kaspersky Lab :	https://forum.kaspersky.fr

Information 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.

Avis de marques déposées

Les marques déposées et les marques de service appartiennent à leur propriétaire.

Citrix, XenApp et XenDesktop sont des marques de Citrix Systems, Inc. et/ou d'une ou plusieurs de ses filiales et peuvent être enregistrées au bureau des marques et brevets (Patent and Trademark Office) aux Etats-Unis et dans d'autres pays.

Dell et Dell Compellent sont des marques de Dell, Inc.

EMC, Celerra, 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 Hitachi, Ltd.

IBM et System Storage sont des marques d'International Business Machines Corporation déposées dans de nombreuses juridictions à travers le monde.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server et Windows Vista sont des marques déposées de Microsoft Corporation aux Etats-Unis et dans d'autres pays.

Linux est la marque déposée de Linus Torvalds aux Etats-Unis et dans d'autres pays.

NetApp and Data ONTAP 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 déposée d'Oracle Corporation et/ou de ses filiales.

Glossaire

A

Analyse heuristique

Technologie de détection des menaces dont les informations ne figurent pas encore dans les bases de Kaspersky Lab. L'analyse heuristique permet de détecter des objets dont le comportement dans le système d'exploitation peut constituer une menace pour la sécurité. Les objets identifiés à l'aide de l'analyse heuristique sont considérés comme probablement infectés. Par exemple, un objet qui contient une succession de commandes propres à des objets malveillants (ouverture d'un fichier, écriture dans le fichier) pourrait être considéré comme probablement infecté.

Archive

Un ou plusieurs fichiers repris dans un fichier compressé. Une application dédiée, appelée archiveur, est requise pour le compactage et le décompactage des données.

B

Bases antivirus

Bases de données qui contiennent les informations relatives aux menaces informatiques connues de Kaspersky Lab 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 composées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

C

Clé active

Clé actuellement utilisée par l'application.

D

Données relatives à la licence

Période de temps pendant laquelle vous avez accès aux fonctions de l'application et aux droits d'utiliser des services supplémentaires. Les services utilisables dépendent du type de licence.

Désinfection

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être désinfectés.

E

Etat de la protection

Etat actuel de la protection, qui reflète le niveau de sécurité de l'ordinateur.

F

Faux positifs

Situation où un objet non infecté est considéré comme infecté par une application de Kaspersky Lab car son code évoque celui d'un virus.

Fichier probablement 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 de code malveillant est assez élevé pour ces fichiers.

K

Kaspersky Security Network (KSN)

Infrastructure de services cloud donnant accès à la base de données de Kaspersky Lab avec des informations constamment mises à jour sur la réputation des fichiers, les ressources Internet et le logiciel. Kaspersky Security Network assure une vitesse de réaction plus élevée que les applications de Kaspersky Lab face aux nouvelles menaces, augmente l'efficacité de certains composants de la protection et réduit la possibilité de faux positifs.

M

Masque de fichier

Représentation d'un nom de fichier à l'aide de caractères génériques. Les caractères génériques standard utilisés dans les masques de fichier sont * et ?, où * représente n'importe quel nombre de n'importe quels caractères et ? représente n'importe quel caractère unique.

Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

N

Niveau de sécurité

Le niveau de sécurité est décrit comme un ensemble pré-configuré de paramètres de composants de l'application.

O

Objets de démarrage

Ensemble d'applications nécessaires au démarrage et au fonctionnement corrects du système d'exploitation et au logiciel installé sur l'ordinateur. Objets de démarrage : objets que le système d'exploitation charge au démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

Objet OLE

Objet lié à un autre fichier ou imbriqué dans un autre fichier via la technologie Object Linking and Embedding (OLE). Exemple d'objet OLE : feuille de calcul Microsoft Office Excel® imbriquée dans un document Microsoft Office Word.

P

Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

Protection en temps réel

Mode de fonctionnement de l'application sous lequel celle-ci analyse les objets pour y détecter la présence d'un code malveillant en temps réel.

L'application intercepte toutes les tentatives d'ouverture d'objet (lecture, écriture ou exécution) et analyse les objets pour y détecter les menaces. Les objets non infectés sont transmis à l'utilisateur ; les objets contenant des menaces ou les objets probablement infectés sont traités en fonction des paramètres de la tâche (désinfecté, supprimé ou en quarantaine).

Q

Quarantaine

Dossier dans lequel l'application de Kaspersky Lab déplace les objets probablement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

S

Sauvegarde

Stockage spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur désinfection 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. Il permet également de gérer ces applications.

SIEM

Technologie qui analyse les événements de sécurité provenant de plusieurs périphériques réseau et applications.

Stratégie

Une stratégie détermine les paramètres d'une application gère l'accès à la configuration d'une application installée sur les ordinateurs d'un groupe d'administration. Une stratégie individuelle doit être créée pour chaque application. Vous pouvez créer un nombre illimité de stratégies pour les applications installées sur les ordinateurs dans chaque groupe d'administration mais une seule stratégie à la fois peut être appliquée à chaque application dans un groupe d'administration.

T

Tâche

Fonctions exécutées par l'application de Kaspersky Lab sous forme de tâches, par exemple : Protection des fichiers en temps réel, Analyse complète de l'ordinateur et Mise à jour des bases de l'application.

Tâche locale

Tâche définie et exécutée sur un ordinateur client unique.

Témoin du niveau d'importance de l'événement

Propriété d'un événement rencontré pendant le fonctionnement d'une application Kaspersky Lab. Gravité de l'événement : niveau de gravité de l'événement.

- Evénement critique.
- Erreur.
- Avertissement
- Info.

Les événements du même type peuvent avoir différents niveaux de gravité en fonction de la situation de survenue de l'événement.

U

Un objet infecté a été découvert

Objet dont une portion de code correspond parfaitement à une partie du code d'une application malveillante connue. Kaspersky Lab ne recommande pas d'accéder à ces objets.

Un objet suspect a été détecté

Fichier contenant soit le code modifié d'un virus connu, soit du code évoquant un virus, mais toujours inconnu de Kaspersky Lab. Les objets suspects sont détectés par analyse heuristique.

V

Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs d'applications malveillantes 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.

Index

I

P