KASPERSKY lab

Kaspersky Security 10 for Windows Server

Manuel d'implantation pour la protection des stockages réseau

Version de l'application : 10

Chers utilisateurs !

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

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

Date d'édition : 12/02/2016

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

Table des matières

Présentation du guide

Le manuel d'implantation de Kaspersky Security 10 for Windows Server® (ci-après "Kaspersky Security") est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Security, ainsi qu'aux spécialistes qui offrent un support technique aux organisations qui ont choisi de travailler avec Kaspersky Security.

Ce manuel reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security dans le cadre de la protection des stockages réseau.

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

Nous supposons qu'au moment de lire le présent manuel, vous disposez déjà d'une copie de l'application avec les modules Protection des stockages réseau connectés via le protocole RPC et Protection des stockages réseau connectés via le protocole ICAP (cf. *Manuel d'installation de Kaspersky Security 10 for Windows Server*) et d'une clé prenant en charge la protection des stockages réseau (les informations relatives à la licence figurent dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*).

Dans cette section

Dans ce document

Le Manuel d'implantation pour la protection des stockages réseau contient les sections suivantes :

Sources d'informations sur Kaspersky Security

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

Kaspersky Security

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Security.

Configurations logicielle et matérielle requises

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

Intégration de Kaspersky Security aux stockages réseau

Cette section décrit les principes qui gouvernent l'interaction entre Kaspersky Security et les stockages réseau.

Utilisation de la console de Kaspersky Security

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

Consultation de l'état de la protection des stockages réseau

Cette section explique comment consulter les informations relatives à l'état actuel de la protection des stockages réseau.

Protection des stockages réseau EMC™ du groupe Celerra™/VNX™

Cette section fournit des informations sur la protection des stockages réseau EMC Celerra et sur l'intégration de Kaspersky Security au stockage réseau Celerra / VNX.

Protection des stockages réseau connectés via le protocole RPC

Cette section fournit des informations sur la tâche de protection des stockages réseau connectés via le protocole RPC, sur la configuration de la connexion entre le stockage réseau et Kaspersky Security et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via RPC.

Protection des stockages réseau connectés via le protocole ICAP

Cette section fournit des informations sur la tâche de protection des stockages réseau connectés via le protocole ICAP, sur la configuration de la connexion entre le stockage réseau et Kaspersky Security et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via ICAP.

Contacter le Support Technique

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

Glossaire

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

AO KASPERSKY LAB

Cette section contient des informations sur AO Kaspersky Lab.

Informations sur le code tiers

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

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".

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

Sources d'informations sur Kaspersky Security

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

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

Dans cette section

Sources de données pour des consultations indépendantes

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

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

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab (cf. section « Contacter le Support Technique » à la page 99).

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

Page de Kaspersky Security sur le site Web de Kaspersky Lab

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

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

Page de Kaspersky Security dans la base de connaissances

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

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

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

Sauvegardes de Kaspersky Security

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

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

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

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

Discussion sur les logiciels de Kaspersky Lab sur le forum

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

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

Kaspersky Security

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

Vous pouvez installer Kaspersky Security les serveurs suivants :

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

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

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

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

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

Modules et fonctions de Kaspersky Security

L'application intègre les modules suivants :

- Protection en temps réel.

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

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

- Contrôle du serveur.

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

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

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

- Analyse à la demande.

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

L'application peut remplir les fonctions suivantes :

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

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

- Quarantaine.

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

- Sauvegarde.

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

- Notifications de l'administrateur et des utilisateurs.

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

- Importation et exportation des paramètres.

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

- Application des modèles.

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

- Consignation des événements.

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

- Stockage hiérarchique.

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

- Zone de confiance.

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

- Administration des autorisations.

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

Configurations logicielle et matérielle requises

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

Dans cette section

Configuration requise pour le serveur sur lequel Kaspersky Security est installé

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

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

Configuration matérielle requise pour le serveur

Recommandations d'ordre général :

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

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

Configuration minimale :

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

Configuration recommandée :

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

Configuration logicielle requise pour le serveur

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

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

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

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

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

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

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

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

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

Configuration requise pour le stockage réseau protégé

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

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

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

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

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

Configuration matérielle requise pour l'ordinateur

Mémoire vive recommandée : 128 Mo minimum.

Espace disque disponible : 30 Mo.

Configuration logicielle requise pour l'ordinateur

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

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

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

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

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

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

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

Intégration de Kaspersky Security aux stockages réseau

Cette section contient des informations sur les principes qui régissent l'interaction entre Kaspersky Security et les stockages réseau.

Protection d'un stockage réseau EMC du groupe Celerra/VNX

Kaspersky Security interagit avec un stockage réseau EMC du groupe Celerra/VNX via l'agent CAVA (Celerra Antivirus Agent) qui tourne sur l'ordinateur où est installé Kaspersky Security. Une fois lancé, Kaspersky Security vérifie si l'ordinateur est doté d'un agent CAVA qui répond aux exigences de Kaspersky Security (cf. section "Configuration requise pour le stockage réseau protégé" la page 20).

En cas de tentative de lecture ou de modification d'un fichier qui se trouve dans le stockage réseau, le stockage lance une requête réseau et transmet le fichier à l'agent CAVA. L'agent CAVA enregistre le fichier reçu sur le disque local de l'ordinateur dans un dossier spécial. Le module "Protection des fichiers en temps réel" intercepte l'opération fichier et analyse le fichier selon les paramètres définis pour la tâche "Protection des fichiers en temps réel", par exemple réparer ou supprimer le fichier. L'agent CAVA analyse les actions de Kaspersky Security et sur la base des informations obtenues, il détermine le résultat de l'analyse et le transmet au stockage réseau.

Protection d'un stockage réseau connecté via le protocole RPC

L'interaction entre Kaspersky Security et un stockage réseau connecté via le protocole RPC (comme NetApp ou Hitachi NAS en mode RPC) s'opère via le protocole RPC (Remote Procedure Call).

Kaspersky Security maintient la connexion avec le stockage réseau en lui envoyant des requêtes RPC à intervalle régulier. En cas de tentative de lecteur ou de création/modification d'un fichier qui se trouve dans le stockage réseau, le stockage réseau octroie à Kaspersky Security un accès direct à ce fichier via le protocole CIFS. Le module de l'application "Protection des stockages réseau connectés via le protocole RPC" analyse le fichier conformément aux paramètres définis pour la tâche "Protection des stockages réseau connectés via le protocole RPC". Si Kaspersky Security découvre une menace, il exécute sur les fichiers les actions définies dans les paramètres de la tâche (dont la réparation ou la suppression du fichier) et transmet les résultats de l'analyse au stockage réseau.

Protection d'un stockage réseau connecté via le protocole ICAP

Pour un stockage réseau connecté via le protocole ICAP (comme EMC Isilon, IBM NAS ou Hitachi NAS en mode ICAP), Kaspersky Security se présente comme un service fonctionnant sur le protocole ICAP (Internet Content Adaptation Protocol).

En cas de tentative de lecture ou de création/modification d'un fichier qui se trouve dans le stockage réseau, le stockage réseau crée une requête ICAP pour Kaspersky Security et transmet le fichier à l'intérieur de cette requête. Le module de l'application "Protection des stockages réseau connectés via le protocole ICAP" analyse le fichier conformément aux paramètres définis pour la tâche "Protection des stockages réseau connectés via le protocole ICAP". Si Kaspersky Security découvre une menace, il exécute sur le fichier les actions définies dans les paramètres de la tâche et transmet les résultats de l'analyse au stockage réseau. Si l'action "Réparer" a été définie dans les paramètres et que le fichier a pu être réparé, Kaspersky Security renvoie le fichier réparé au stockage réseau dans sa réponse à la requête.

Dans cette section

Préparation au lancement de la tâche de protection des stockages réseau

Cette section contient des instructions pour préparer un serveur fonctionnant sous Microsoft Windows, et sur lequel est installé Kaspersky Security, à l'intégration avec des stockages réseau de données, et au lancement ultérieur de tâches de protection des stockages réseau.

Dans cette section

Configuration des paramètres de sécurité des stratégies locales dans l'éditeur d'une stratégie de groupe locale

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

► *Pour configurer les paramètres de sécurité des stratégies locales dans l'éditeur de stratégie de groupe locale, procédez comme suit :*

1. Ouvrez l'**éditeur de stratégie de groupe local** d'une des manières suivantes :

   - Si vous configurez les paramètres localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `gpedit.msc`, puis appuyez sur la touche **ENTER**.

   - Si vous configurez les paramètres depuis un autre ordinateur, procédez comme suit :

     a. Si vous configurez les paramètres localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `mmc`, puis appuyez sur la touche **ENTER**.

     La fenêtre **Console de gestion** s'ouvre

     b. Dans la fenêtre qui s'ouvre, choisissez **Fichier** → **Ajouter ou supprimer des composants logiciels enfichables**.

     La fenêtre **Ajout et suppression de composants logiciels enfichables** s'ouvre.

     c. Dans la liste des composants logiciels enfichables disponibles, sélectionnez **Editeur d'objets de stratégie de groupe** et cliquez sur le bouton **Ajouter**.

     L'Assistant de stratégie de groupe s'ouvre.

     d. Dans la fenêtre de l'Assistant, cliquez sur le bouton **Parcourir**.

     La fenêtre **Recherche d'objet de stratégie de groupe**.

e. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Ordinateurs**, choisissez l'option **Autre ordinateur** et désignez le serveur doté de Kaspersky Security d'une des méthodes suivantes :

- Dans le champ de saisie, indiquez le nom de domaine du serveur doté de Kaspersky Security ;
- Cliquez sur le bouton **Parcourir** et dans la fenêtre de sélection de l'ordinateur qui s'ouvre, sélectionnez le serveur doté de Kaspersky Security à l'aide de la recherche par domaine ou groupe de travail.

2. Cliquez sur **OK**.

   a. Les modifications seront enregistrées.

3. Choisissez **Configuration de l'ordinateur** > **Configuration Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Paramètres de sécurité**.

4. Attribuez les valeurs suivantes aux paramètres de l'accès réseau :

   - **Accès réseau : les autorisations Tout le monde s'appliquent aux utilisateurs anonymes** - **Activé**
   - **Accès réseau : Interdire l'énumération anonyme des comptes SAM** - **Désactivé**
   - **Accès réseau : Restreindre l'accès anonyme aux canaux nommés et aux partages** - **Désactivé**.

5. Redémarrez le serveur sur lequel est installé Kaspersky Security.

Les modifications apportées sont alors appliquées.

Configuration des connexions entrantes et sortantes dans le pare-feu Windows

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

► *Pour configurer les connexions entrantes et sortantes du pare-feu Windows, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du pare-feu Windows d'une des méthodes suivantes :

   - Si vous configurez le pare-feu Windows localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `wf.msc`, puis appuyez sur la touche **ENTREE**.

   - Si vous configurez le pare-feu depuis un autre ordinateur, procédez comme suit :

     a. Si vous configurez les paramètres localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `mmc`, puis appuyez sur la touche **ENTER**.

     La fenêtre **Console de gestion** s'ouvre

     b. Dans la fenêtre qui s'ouvre, choisissez **Fichier** → **Ajouter ou supprimer des composants logiciels enfichables**.

     La fenêtre **Ajout et suppression de composants logiciels enfichables** s'ouvre.

     c. Dans la liste des composants logiciels enfichables disponibles, sélectionnez **Pare-feu Windows** et cliquez sur le bouton **Ajouter**.

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

d. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Autre ordinateur** et désignez le serveur doté de Kaspersky Security d'une des méthodes suivantes :

- Dans le champ de saisie, indiquez le nom de domaine du serveur doté de Kaspersky Security ;
- Cliquez sur le bouton **Parcourir** et dans la fenêtre de sélection du sujet de sécurité intégré qui s'ouvre, sélectionnez le serveur doté de Kaspersky Security à l'aide de la recherche par domaine ou groupe de travail.

2. Cliquez sur **OK**.

    a. Les modifications seront enregistrées.

3. Créez les règles pour les connexions entrantes et sortantes à l'aide des paramètres suivants :

- Autorisez les connexions entrantes depuis tous les ports distants sur les ports locaux TCP 137 à 139 et TCP 445.
- Autorisez les connexions sortantes depuis tous les ports locaux sur les ports distants TCP 137 à 139 et TCP 445.

  Par défaut, le pare-feu Windows autorise toutes les connexions sortantes qui ne sont pas soumises à des règles d'interdiction. Si vous conservez les paramètres par défaut, il n'est pas nécessaire de créer une règle pour les connexions sortantes.

Les paramètres du pare-feu Windows peuvent également être définis à l'aide d'une stratégie de groupe ou de domaine.

Utilisation de la console de Kaspersky Security

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

Dans cette section

Présentation de la console de Kaspersky Security

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

Il est possible d'administrer Kaspersky Security via la console de Kaspersky Security installée sur le serveur protégé ou sur tout autre ordinateur du réseau de l'organisation.

Le *Manuel d'installation de Kaspersky Security 10 for Windows Server* présente en détails l'installation et la configuration de la console de Kaspersky Security.

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

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

Vous pouvez ouvrir la console de Kaspersky Security depuis le menu **Démarrer.** Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Security ou ajouter ce composant logiciel enfichable à la console Microsoft Management Console existante en tant que nouvel élément de son arborescence (cf. section "Interface de la fenêtre de la Console de Kaspersky Security" à la page 32).

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

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

Lancement de la console de Kaspersky Security depuis le menu Démarrer

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

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

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

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

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

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

1. Dans le menu **Démarrer,** sélectionnez **Programmes → Kaspersky Security 10 for Windows Server → Outils d'administration**.

2. Dans le menu contextuel de l'application **Console de Kaspersky Security**, choisissez la commande **Auteur**.

La Console de Kaspersky Security sera lancée en mode auteur.

Si vous avez lancé la console de Kaspersky Security sur le serveur à protéger, la fenêtre de la console s'ouvre (cf. section "Interface de la fenêtre de la console de Kaspersky Security" à la page 32).

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

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

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

2. Sélectionnez la commande **Se connecter à un autre ordinateur**.

   La fenêtre **Sélection d'ordinateur** s'ouvre.

3. Dans la fenêtre qui s'ouvre, sélectionnez **Autre ordinateur**.

4. Dans le champ de saisie de droite, indiquez le nom réseau du serveur à protéger.

5. Cliquez sur **OK**.

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

Si le compte utilisateur employé pour accéder à Microsoft Windows ne dispose pas des privilèges d'accès au service d'administration de Kaspersky Security sur le serveur, cochez la case **Se connecter sous le compte utilisateur** et indiquez un autre compte qui dispose de tels privilèges.

Interface de la fenêtre de la console de Kaspersky Security

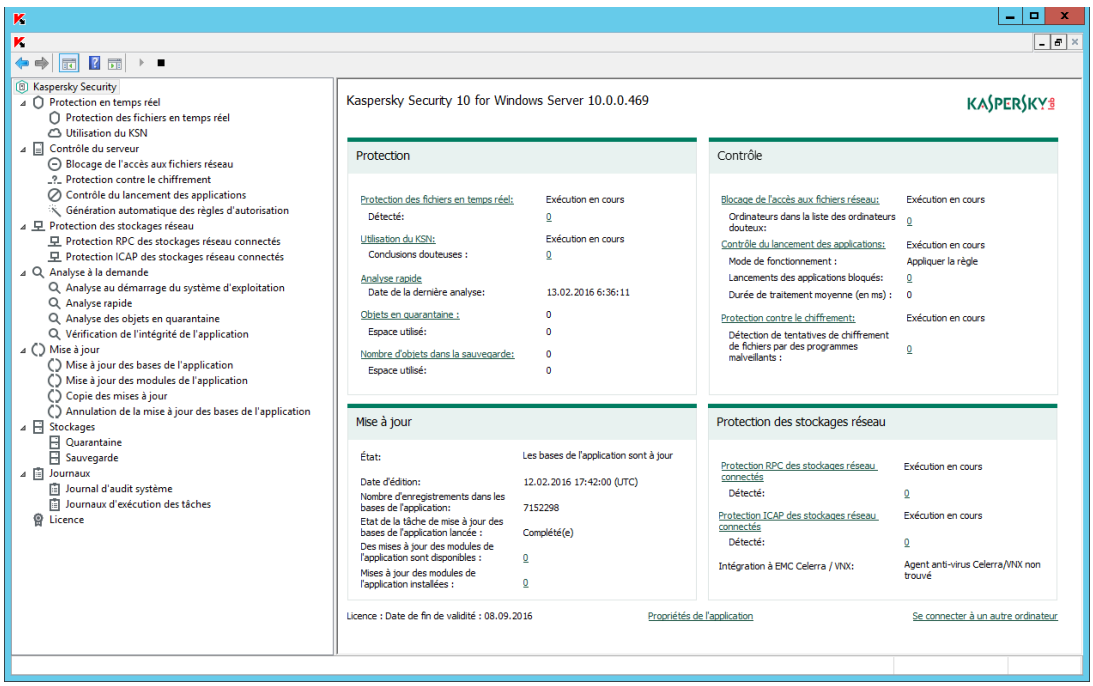
La console de Kaspersky Security s'affiche dans l'arborescence de Microsoft Management Console sous l'entrée **Kaspersky Security**.

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

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

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

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



Arborescence de la Console

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

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

- **Protection en temps réel** : administration de la protection des fichiers en temps réel et de l'analyse des scripts, ainsi que des paramètres d'utilisation des services du KSN. Chaque zone fonctionnelle dispose de son propre élément d'administration :
  - **Protection des fichiers en temps réel**.
  - **Analyse des scripts**.
  - **Utilisation du KSN**.
- **Contrôle du serveur** : contrôle de l'accès aux fichiers réseau appliqué aux ordinateurs distants et contrôle du lancement des applications. Chaque zone fonctionnelle dispose de son propre élément d'administration :
  - **Blocage de l'accès aux fichiers réseau**.
  - **Protection contre le chiffrement**.
  - **Contrôle du lancement des applications**.
  - **Génération automatique des règles d'autorisation**.
  - Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).
- **Protection des stockages réseau** : gestion de la protection des stockages réseau.
  - **Protection des stockages réseau connectés via le protocole RPC**.
  - **Protection des stockages réseau connectés via le protocole ICAP**.
- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Une entrée séparée existe pour chacune des tâches prédéfinie :
  - **Analyse au démarrage du système d'exploitation**.
  - **Analyse rapide**.
  - **Analyse des objets en quarantaine**.
  - **Vérification de l'intégrité de l'application**.
  - Tâches définies par l'utilisateur **<Nom des tâches>** (le cas échéant).

Une entrée séparée existe pour chaque tâche définie par l'utilisateur et pour chaque tâche de groupe créée pour l'analyse à la demande et transmise au serveur par la console d'administration de Kaspersky Security Center.

- **Mise à jour** : gère la mise à jour des bases et des modules de Kaspersky Security ainsi que la copie des mises à jour dans le dossier de la source locale de mises à jour. Le nœud contient des nœuds secondaires permettant d'administrer chacune des tâches prédéfinies de mise à jour ou d'annulation de la dernière mise à jour des bases de l'application :
  - **Mise à jour des bases de l'application**.
  - **Mise à jour des modules de l'application**.
  - **Copie des mises à jour**.
  - **Annulation de la mise à jour des bases de l'application**.

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

Panneau de résultats

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

Menu contextuel de l'entrée Kaspersky Security

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

- **Se connecter à un autre ordinateur**. Se connecter à un autre serveur pour administrer la copie de Kaspersky Security installée sur ce serveur. Pour effectuer cette opération, vous pouvez également utiliser le lien situé dans le coin inférieur droit du panneau des résultats de l'entrée **Kaspersky Security**.

- **Lancer Kaspersky Security** / **Arrêter Kaspersky Security** (**Démarrer** / **Arrêter**). Lancer ou arrêter Kaspersky Security ou une tâche sélectionnée. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. L'exécution de ces opérations est également disponible dans les menus contextuels des tâches de l'application.

- **Configurer les paramètres de la zone de confiance**. Consulter et configurer les paramètres de la zone de confiance.

- **Modifier les permissions utilisateur pour l'administration de l'application**. Consulter et configurer les privilèges d'accès aux fonctions de Kaspersky Security.

- **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service**. Consulter et configurer les privilèges d'accès à l'administration du Service Kaspersky Security.

- **Configurer les paramètres des notifications**. Consulter et configurer les paramètres de notification de l'administrateur et des utilisateurs de Kaspersky Security.

- **Stockage hiérarchique**. Consulter et configurer les paramètres de fonctionnement du stockage hiérarchique de Kaspersky Security.

- **Exporter les paramètres**. Enregistrer les paramètres de l'application dans un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

- **Importer les paramètres**. Importer les paramètres de l'application depuis un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

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

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

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

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

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

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

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

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

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

- **Reprendre / Suspendre**. Reprendre ou suspendre l'exécution de la tâche. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches de protection des fichiers en temps réel et d'analyse à la demande.

- **Ajouter tâche**. Créer une nouvelle tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.

- **Ouvrir le journal d'exécution**. Accéder à la consultation et à l'utilisation du journal d'exécution de la tâche. L'opération est disponible pour toutes les tâches.

- **Enregistrer la tâche**. Enregistrer et appliquer les modifications apportées aux paramètres de la tâche (cf. section « Enregistrement de la tâche après modification de ses paramètres » à la page 39). Cette action est disponible pour les tâches de protection des fichiers en temps réel, de protection des stockages réseau connectés via le protocole RPC et d'analyse à la demande.

- **Supprimer la tâche**. Supprimer une tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.

- **Statistiques**. Accéder à la consultation des statistiques de la tâche. L'opération est disponible pour la tâche de vérification de l'intégrité de l'application.

- **Modèles des paramètres**. Accéder à l'utilisation des modèles. Cette action est disponible pour les tâches de protection des fichiers en temps réel, de protection des stockages réseau connectés via le protocole RPC et d'analyse à la demande.

Consultation d'informations concernant l'état de la protection des stockages réseau

► *Pour consulter les informations relatives à l'état de la protection des stockages réseau,*

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

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

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

► *Pour actualiser manuellement les informations du nœud Kaspersky Security,*

choisissez l'option **Mettre à jour** dans le menu contextuel du nœud Kaspersky Security.

Le bloc **Protection des stockages réseau** dans le panneau des résultats du nœud **Kaspersky Security** affiche les informations concernant l'état des stockages réseau protégés (cf. tableau ci-dessous).

Tableau 2. Informations sur la protection des stockages réseau.

Groupe Protection des stockages réseau	Conseil

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

Protection des stockages réseau connectés via le protocole RPC	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Détecté** : nombre d'objets détectés par Kaspersky Security depuis le lancement de la tâche. Si le nombre de programmes malveillants détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.
Protection des stockages réseau connectés via le protocole ICAP	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppé*). **Détecté** : nombre d'objets détectés par Kaspersky Security depuis le lancement de la tâche. Si le nombre de programmes malveillants détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.
Intégration à EMC Celerra / VNX	Le paramètre peut prendre les valeurs suivantes : • **Agent anti-virus Celerra / VNX non trouvé** : Kaspersky Security n'a pas trouvé le logiciel de la société EMC ou une erreur s'est produite dans le code d'intégration. • **Protection désactivée** : Kaspersky Security a ouvert une connexion avec l'application de la société EMC, mais Kaspersky Security n'assure pas la protection des fichiers en temps réel. • **Protection activée** : Kaspersky Security a ouvert une connexion avec l'application de la société EMC, et Kaspersky Security assure la protection des fichiers en temps réel.

Administration des tâches de protection des stockages réseau

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

Dans cette section

Enregistrement d'une tâche après modification de ses paramètres

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

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

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

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

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

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

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

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

► *Pour lancer ou arrêter une tâche de protection des stockages réseau, procédez comme suit :*

1. Ouvrez le menu contextuel du nom de la tâche dans la console de Kaspersky Security.

2. Sélectionnez l'une des options : **Démarrer** ou **Arrêter**.

L'opération sera effectuée et consignée dans le journal d'audit système.

Programmation des tâches

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

Dans cette section

Configuration des paramètres de planification du lancement des tâches

La console de Kaspersky Security permet de planifier le lancement des tâches locales prédéfinies 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 d'une tâche,* procédez comme suit *:*

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez configurer la planification du lancement.

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

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

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

> Les champs contenant les paramètres de planification de la tâche d'analyse à la demande et de la tâche de mise à jour ne sont pas accessibles si le lancement planifié de la tâche est interdit par une stratégie de l'application Kaspersky Security Center.

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

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

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

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

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

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

La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches prédéfinies planifiées est interdit par les paramètres d'une stratégie en vigueur de Kaspersky Security Center.

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

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

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

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

   - Dans le groupe **Paramètres avancés** :

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

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

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

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

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

Activation et désactivation du lancement programmé

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

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

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez configurer la planification du lancement.

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

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

3. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes sous l'onglet **Planification** :

   - Cochez la case **Exécuter de manière planifiée** si vous souhaitez activer l'exécution planifiée d'une tâche ;

   - Décochez la case **Exécuter de manière planifiée** si vous souhaitez désactiver l'exécution planifiée d'une tâche ;

   > Les paramètres de la planification du lancement de la tâche ne seront pas supprimés. Ils seront toujours valides à la prochaine activation de l'exécution planifiée de la tâche.

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

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

Protection des stockages réseau EMC du groupe Celerra/VNX

Cette section fournit des informations sur la protection des stockages réseau EMC du groupe Celerra/VNX (plus loin Celerra/VNX) et sur l'intégration de Kaspersky Security au stockage réseau Celerra/VNX.

Dans cette section

À propos de la protection des stockages réseau EMC du groupe Celerra/VNX

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

Kaspersky Security analyse les fichiers placés dans les dossiers partagés du stockage réseau EMC du groupe Celerra/VNX en cas de tentative de lecture ou de modification de ces fichiers depuis des postes de travail. Le stockage réseau autorisera la lecture ou la modification du fichier uniquement si Kaspersky Security l'a considéré comme un fichier sain. Si Kaspersky Security considère que le fichier est infecté ou probablement infecté, le stockage réseau interdit la lecture ou la modification du fichier.

Kaspersky Security permet de configurer les actions que l'application doit exécuter sur les fichiers infectés ou probablement infectés.

Par défaut, Kaspersky Security effectue les actions suivantes :

- il répare les fichiers infectés ;
- il supprime les fichiers infectés si la réparation est impossible ;

- il place les fichiers probablement infectés en quarantaine ;
- il place une copie des fichiers infectés dans la sauvegarde avant leur réparation ou leur suppression.

Pour pouvoir protéger le stockage réseau, vous devez assurer l'intégration de Kaspersky Security au stockage réseau Celerra/VNX

La protection des stockages réseau Celerra / VNX est effectuée par la tâche de Protection des fichiers en temps réel.

Vous trouverez plus d'informations sur la tâche de Protection des fichiers en temps réel dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Intégration de Kaspersky Security au stockage réseau EMC du groupe Celerra/VNX

Pour pouvoir protéger le stockage réseau, vous devez assurer l'intégration de Kaspersky Security au stockage réseau Celerra/VNX

L'intégration de Kaspersky Security au stockage réseau Celerra/VNX a lieu si les conditions suivantes sont réunies :

1. Sur l'ordinateur protégé par Kaspersky Security, l'agent logiciel CAVA (Celerra Antivirus Agent), intégré à la distribution d'EMC Celerra/VNX, est installé. Kaspersky Security interagit avec le stockage réseau Celerra/VNX à l'aide de cet agent logiciel.
2. La tâche Protection des fichiers en temps réel est effectuée.

   > Vous trouverez plus d'informations sur la tâche de Protection des fichiers en temps réel et des instructions concernant la configuration de ses paramètres dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

L'état de l'intégration de Kaspersky Security au stockage réseau Celerra/VNX s'affiche dans le panneau des résultats du nœud **Kaspersky Security** (cf. section "**Consultation d'informations concernant l'état de la protection des stockages réseau**" à la page 37).

Protection des stockages réseau connectés via le protocole RPC

Cette section fournit des informations sur la tâche de protection des stockages réseau connectés via le protocole RPC, sur la configuration de la connexion entre le stockage réseau et Kaspersky Security et explique également comment configurer les paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC ainsi que les paramètres de sécurité de la tâche.

Dans cette section

A propos de la protection des stockages réseau connectés via le protocole RPC

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

Kaspersky Security analyse les fichiers situés dans les dossiers réseau partagés (network share) du stockage réseau connecté via le protocole RPC (ci-après le *stockage réseau*) lors des tentatives de lecture ou de modification de ces fichiers depuis des postes de travail. Le stockage réseau autorisera la lecture ou la modification du fichier uniquement si Kaspersky Security l'a considéré comme un fichier sain. Si Kaspersky Security considère que le fichier est infecté ou probablement infecté, le stockage réseau effectue les actions nécessaires conformément aux paramètres (par exemple, il interdit la lecture ou la modification du fichier).

Kaspersky Security permet de configurer les actions que l'application doit exécuter sur les fichiers infectés ou probablement infectés.

Par défaut, Kaspersky Security effectue les actions suivantes :

- il répare les fichiers infectés ;
- il supprime les fichiers infectés si la réparation est impossible ;
- il place les fichiers probablement infectés en quarantaine ;
- il place une copie des fichiers infectés dans la sauvegarde avant leur réparation ou leur suppression.

Vous pouvez protéger un stockage réseau ou plusieurs à l'aide d'un serveur doté de Kaspersky Security. Pour améliorer la rapidité du stockage réseau et du serveur doté de Kaspersky Security, vous pouvez utiliser plusieurs serveurs dotés de Kaspersky Security pour la protection d'un seul stockage réseau. Dans ce cas, le stockage réseau répartit la charge entre les serveurs connectés et dotés de Kaspersky Security.

Pour profiter de la protection des stockages réseau en temps réel, vous devez ajouter le stockage réseau à Kaspersky Security en tant que zone de protection et configurer la connexion entre ce stockage et le serveur doté de Kaspersky Security. Dans Kaspersky Security, la tâche de protection des stockages réseau connectés via le protocole RPC s'appelle Protection des stockages réseau connectés via le protocole RPC.

La tâche Protection des stockages réseau connectés via le protocole RPC est créée par défaut et est une tâche prédéfinie de Kaspersky Security. Vous ne pouvez pas supprimer ou renommer cette tâche. Vous ne pouvez pas créer des tâches de protection des stockages réseau connectés via le protocole RPC.

Vous pouvez configurer la tâche de Protection des stockages réseau connectés via le protocole RPC. Les paramètres configurés dans les propriétés de la tâche Protection des stockages réseau connectés via le protocole RPC sont appliqués à toutes les zones de protection ajoutées. Il est également possible de configurer les paramètres de protection de chaque zone de protection.

Vous pouvez lancer la tâche de protection des stockages réseau si la clé active prend en charge la protection des stockages réseau. Si vous lancez une tâche de protection des stockages réseau, mais que la clé active ne prend pas en charge la protection des stockages réseau, la tâche se solde sur une erreur. Dans ce cas, Kaspersky Security ne protège pas les stockages réseau.

Le composant Protection des stockages réseau connectés via le protocole RPC est disponible dans le cadre de la solution Kaspersky Security for Data Storage.

Vous trouverez plus d'informations sur les solutions de protection de l'entreprise, notamment sur Kaspersky Security for Windows Server dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Présentation de l'analyse des liens symboliques

Un *lien symbolique* est un type de fichier spécial qui contient un index vers un autre objet présenté sous la forme d'un chemin d'accès absolu ou relatif. Le lien symbolique peut pointer, par exemple, vers un objet qui se trouve dans le dossier réseau partagé d'un autre stockage réseau.

L'analyse des liens symboliques dans les stockages réseau possède les particularités suivantes. Kaspersky Security analyse le fichier vers lequel pointe le lien uniquement si ce fichier appartient à la zone de protection. Si le fichier vers lequel pointe le lien symbolique se trouve en dehors de la zone de protection, Kaspersky Security ne l'analyse pas. Si le stockage réseau autorise le suivi d'un lien symbolique en dehors des limites du dossier dans lequel se trouve le lien symbolique, il convient de confirmer que le dossier cible se trouve dans la zone de protection. Par exemple, si le suivi d'un lien symbolique entre des dossiers réseau partagés au sein du stockage réseau protégé est autorisé, il est conseillé de confirmer que la fonction d'analyse antivirus est activée pour tous les dossiers réseau partagés.

Présentation de l'analyse des instantanés et autres volumes et dossiers accessibles en lecture seule

Kaspersky Security analyse les fichiers qui se trouvent dans les instantanés et autres volumes et dossiers, accessibles uniquement en lecture, mais il n'exécute aucune action sur les fichiers dans ces volumes et dossiers. Par exemple, il ne bloque pas l'accès aux fichiers infectés. Pour éviter la menace d'infection des postes de travail, il est conseillé de faire des instantanés et autres volumes ou dossiers accessibles uniquement en lecture et dissimulés des utilisateurs et octroyer l'accès aux instantanés et autres volumes et dossier accessibles en écriture via l'administrateur.

Configuration de la connexion entre Kaspersky Security et un stockage réseau connecté via le protocole RPC

Vous pouvez lancer la tâche de protection des stockages réseau si la clé active prend en charge la protection des stockages réseau. Si vous lancez une tâche de protection des stockages réseau, mais que la clé active ne prend pas en charge la protection des stockages réseau, la tâche se solde sur une erreur. Dans ce cas, Kaspersky Security ne protège pas les stockages réseau.

Afin de pouvoir protéger des stockages réseau connectés via le protocole RPC, vous devez configurer la connexion du stockage réseau à Kaspersky Security.

► *Pour configurer la connexion entre le stockage réseau et Kaspersky Security, procédez comme suit :*

1. Sur le serveur sur lequel est installé Kaspersky Security, configurez les paramètres suivants :
   - Ajoutez le stockage réseau dans Kaspersky Security (cf. section "Ajout d'un stockage réseau connecté via le protocole RPC à Kaspersky Security" à la page 52).
   - Dans la console de Kaspersky Security, indiquez le compte avec les privilèges duquel vous souhaitez lancer la tâche Protection des stockages réseau connectés via le protocole RPC (cf. section "Sélection du compte pour le lancement de la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 51).

- Dans l'éditeur de stratégies de groupe locales, configurez les paramètres de sécurité des stratégies locales (cf. section "Configuration des paramètres de sécurité des stratégies locales dans l'éditeur d'une stratégie de groupe locale" à la page 25).
- Dans la fenêtre de configuration du pare-feu Windows, configurez les règles pour les connexions entrantes et sortantes dans le pare-feu Windows (cf. section Configuration des connexions entrantes et sortantes dans le pare-feu Windows" à la page 27).
- Si nécessaire, installez l'application de connexion pour stockage réseau connecté via le protocole RPC qui sera protégé par Kaspersky Security.

> Vous trouverez des informations sur l'installation de l'application de connexion pour le stockage réseau protégé dans la documentation de ce stockage réseau.

2. Configurez les paramètres suivants dans le stockage réseau :
   - Activer la fonction de protection antivirus (vscan).
   - Ajouter le compte utilisateur avec les privilèges duquel la tâche Protection des stockages réseau connectés via le protocole RPC est lancée dans le groupe Backup Operators.

> Les informations relatives à la configuration du stockage réseau que vous utilisez figurent dans la documentation de ce stockage.

La connexion entre Kaspersky Anti-Virus et un stockage réseau connecté via le protocole RPC sera effectuée.

Sélection du compte pour le lancement de la tâche Protection des stockages réseau connectés via le protocole RPC

Le compte utilisateur sous lequel la tâche Protection des stockages réseau connectés via le protocole RPC va être lancée doit posséder les privilèges d'administrateur sur le serveur où est installé Kaspersky Security et appartenir au groupe Backup Operators du stockage réseau.

Si le stockage réseau et le serveur où Kaspersky Security est installé se trouvent dans le même domaine, vous pouvez utiliser le compte utilisateur du domaine. Si le stockage réseau et le serveur où Kaspersky Security est installé se trouvent dans un groupe de travail, vous pouvez utiliser des comptes utilisateur locaux possédant un nom d'utilisateur et un mot de passe identiques.

Pour les stockages réseau fonctionnant sous Data ONTAP 8.2.1 ou une version supérieure en mode cluster-mode, seuls les domaines du compte peuvent être utilisés.

► *Pour sélectionner le compte utilisateur avec les privilèges duquel la tâche Protection des stockages réseau connectés via le protocole RPC va être lancée, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et dans le groupe **Paramètres de connexion au stockage réseau**, saisissez le nom du compte utilisateur sous les privilèges duquel la tâche sera lancée, ainsi que le mot de passe de ce compte et la confirmation du mot de passe.
5. Cliquez sur **OK**.

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

Création des zones de protection dans la tâche Protection des stockages réseau connectés via le protocole RPC

Cette section contient des informations sur la constitution et l'utilisation de la zone de protection dans la tâche Protection des stockages réseau connectés via le protocole RPC.

Dans cette section

Ajout d'un stockage réseau connecté via le protocole RPC à Kaspersky Security

► *Pour ajouter un stockage réseau connecté via le protocole RPC à la zone de protection de Kaspersky Security, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout d'une zone de protection**.

5. Dans la fenêtre **Ajout d'une zone de protection**, saisissez le nom de domaine ou l'adresse IP du stockage réseau.

   Si vous utilisez un stockage réseau NetApp sous le système d'exploitation NetApp Clustered Data ONTAP, indiquez dans ce champ l'adresse IP de l'ordinateur sur lequel l'application de connexion est installée, à savoir 127.0.0.1.

6. Cliquez sur le bouton **OK** pour ajouter le stockage réseau à Kaspersky Security.

   Le stockage réseau apparaît dans la liste des stockages réseau protégés.

7. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la zone de protection définis seront enregistrés.

Kaspersky Security se connecte au stockage réseau lorsque la tâche Protection des stockages réseau connectés via le protocole RPC se lance. Si le nom de domaine ou l'adresse IP du stockage réseau est incorrecte, la tâche se solde sur une erreur. Kaspersky Security consigne les informations relatives à cet événement dans le journal d'audit système et dans le journal d'exécution des tâches.

Si vous utilisez un stockage réseau NetApp sous le système d'exploitation NetApp Clustered Data ONTAP, Kaspersky Security se connecte à l'application de connexion installée sur le serveur protégé. Il est conseillé de confirmer que la connexion entre l'application de connexion et le stockage réseau NetApp a bien été configurée et que Kaspersky Security protège le système de stockage NetApp ajouté.

Activation et désactivation des fonctions de protection d'un stockage réseau connecté via le protocole RPC ajouté

► *Pour désactiver la fonction de protection d'un stockage réseau connecté via le protocole RPC qui a été ajouté, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.

4. Dans la liste des stockages réseau protégés, décochez la case en regard du nom du stockage réseau pour lequel vous souhaitez suspendre temporairement la protection en temps réel.

5. Cliquez sur le bouton **Enregistrer**.

Kaspersky Security interrompt la connexion avec le stockage réseau sélectionné.

Si vous désactivez la fonction de protection pour tous les stockages réseau ajoutés, Kaspersky Security arrête la tâche Protection des stockages réseau connectés via le protocole RPC.

► *Pour activer la fonction de protection d'un stockage réseau connecté via le protocole RPC qui a été ajouté, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.

4. Dans la liste des stockages réseau protégés, cochez la case en regard du nom du stockage réseau pour lequel vous souhaitez activer la protection.

5. Cliquez sur le bouton **Enregistrer**.

Si la tâche Protection des stockages réseau connectés via le protocole RPC est en cours d'exécution, Kaspersky Security établit une connexion avec le stockage réseau. Si la tâche Protection des stockages réseau connectés via le protocole RPC est suspendue, il faut la lancer afin d'établir une connexion entre Kaspersky Security et le stockage réseau.

Suppression d'un stockage réseau connecté via le protocole RPC de la zone de protection

► *Pour supprimer un stockage réseau connecté via le protocole RPC de la tâche Protection des stockages réseau connectés via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des stockages réseau protégés, sélectionnez celui que vous voulez supprimer de la zone de protection de la tâche.
5. Dans le menu contextuel au nom de la tâche ou sous l'adresse IP du stockage réseau que vous souhaitez supprimer de la zone de protection de la tâche, sélectionnez l'entrée **Supprimer de la liste**.

Le stockage réseau sélectionné sera supprimé de la liste des stockages réseau protégés.

Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC

Par défaut, la tâche prédéfinie Protection des stockages réseau connectés via le protocole RPC possède les paramètres décrits dans le tableau ci-après. Vous pouvez modifier les valeurs de ces paramètres.

Quand vous modifiez les paramètres de la tâche (par exemple, désignation d'une nouvelle zone de protection), Kaspersky Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours. Kaspersky Security consigne la date et l'heure de la modification des paramètres de la tâche dans le journal d'audit système.

Tableau 3. Paramètres par défaut de la tâche Protection des stockages réseau connectés via le protocole RPC

Paramètre	Valeur par défaut	Commentaires
Zone de protection	Absent.	Vous devez ajouter un stockage réseau à Kaspersky Security.
Niveau de sécurité	Le niveau de sécurité **Recommandé** est appliqué.	Vous pouvez appliquer un des niveaux de sécurité prédéfinis à la protection du stockage réseau ou vous pouvez définir les valeurs manuellement.
Analyseur heuristique	Le niveau d'analyse **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.	Vous pouvez activer ou désactiver l'application de la zone de confiance et configurer ses paramètres.
Utilisation du KSN	Appliquée.	Vous pouvez activer et désactiver l'utilisation du service KSN dans la tâche Protection des stockages réseau connectés via le protocole RPC.
Paramètres de connexion au stockage réseau	• **Nom d'utilisateur** et **Mot de passe** du compte sous les privilèges duquel la tâche est lancée : non disponible • **Délai d'attente entre les tentatives de reconnexion (s.)** : 5 ; • **Nombre maximal de tentatives de reconnexion** : 3 • **Purger la mémoire cache des fichiers traités du stockage réseau après la mise à jour des bases de l'application** : la case est décochée.	Vous devez désigner le compte utilisateur avec les privilèges duquel la tâche Protection des stockages réseau connectés via le protocole RPC va être lancée. Vous pouvez également modifier les autres paramètres de connexion aux stockages réseau.
Lancement d'une tâche planifiée	Pas appliqué. La case **Exécuter de manière planifiée** est décochée. La tâche est lancée manuellement.	Vous pouvez configurer l'exécution planifiée d'une tâche, par exemple au démarrage de Kaspersky Security.

► *Pour configurer les paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Propriétés**.

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

4. Dans l'onglet **Général** de la fenêtre qui s'ouvre, configurez les paramètres suivants de la tâche :

   - Application de l'analyseur heuristique (à la page 58).
   - Lancement de la tâche avec les privilèges du compte (cf. section "Sélection du compte pour le lancement de la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 51).
   - Connexion à un stockage réseau connecté via le protocole RPC (cf. section "Configuration des paramètres généraux de connexion à un stockage réseau connecté via le protocole RPC" à la page 62).
   - Intégration aux autres composants de Kaspersky Security (à la page 60).

5. Les onglets **Planification** et **Avancé** permettent de configurer les paramètres de lancement planifié de la tâche (cf. section "Configuration des paramètres de planification du lancement des tâches" à la page 40).

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

   Les modifications apportées aux paramètres seront enregistrées.

7. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, sélectionnez l'onglet **Configuration de la zone de la protection**.

8. Exécutez les actions suivantes :

   i. Ajoutez les stockages réseau connectés via le protocole RPC à la zone de protection

de Kaspersky Security (cf. section "Ajout d'un stockage réseau connecté via le protocole RPC à Kaspersky Security" à la page 52).

ii. Dans la liste des stockages réseau connectés via le protocole RPC ajoutés, sélectionnez ceux dont vous souhaitez activer la protection.

iii. Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section "Application d'un niveau de sécurité prédéfini dans la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 66) ou configurez manuellement les paramètres de protection des objets (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 67).

9. Dans le menu contextuel portant le nom de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, sélectionnez **Enregistrer la tâche**.

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

Application de l'analyseur heuristique

Dans la tâche Protection des stockages réseau connectés via le protocole RPC, vous pouvez utiliser l'analyseur heuristique et configurer le niveau de l'analyse.

► *Pour configurer les paramètres d'utilisation de l'analyse heuristique dans la tâche Protection des stockages réseau connectés via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Propriétés**.

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

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et dans le groupe **Analyseur heuristique**, réalisez une des opérations suivantes.

   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.
   - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

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

     Il existe trois niveaux de détail pour l'analyse

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

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

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

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Intégration aux autres composants de Kaspersky Security

Vous pouvez utiliser la tâche Protection des stockages réseau connectés via le protocole RPC avec les modules opérationnels suivants de Kaspersky Security :

- zone de confiance ;
- tâche Utilisation du KSN.

La *Zone de confiance* est une liste préétablie d'exclusions de la zone de protection ou de l'analyse.

Vous pouvez activer ou désactiver l'application de la zone de confiance dans la tâche Protection des stockages réseau connectés via le protocole RPC. Dès que la zone de confiance est activée/désactivée, les exclusions seront appliquées ou levées immédiatement.

Le *Kaspersky Security Network (KSN)* est une infrastructure de services et d'outils 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.

Vous pouvez activer ou désactiver l'application du KSN dans la tâche Protection des stockages réseau connectés via le protocole RPC. Lorsque vous activez ou désactivez l'application du KSN, la tâche commence à établir la réputation des fichiers analysés à partir des informations reçues du KSN, ou arrête de le faire.

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN. Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security.

Vous trouverez plus d'informations sur la zone de confiance et la tâche Utilisation du KSN dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour activer ou désactiver l'utilisation d'autres modules de l'application dans la tâche Protection des stockages réseau connectés via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Propriétés**.

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

4. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Général** et dans le groupe **Intégration aux autres composants de Kaspersky Security**, procédez comme suit :

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

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

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

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

     Cette case est cochée par défaut.

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

     Cette case permet d'activer ou de désactiver l'utilisation du service KSN dans la tâche Protection des stockages réseau connectés via le protocole RPC.

     Si la case est cochée, l'application utilise les données du Kaspersky Security Network 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 Protection des stockages réseau connectés via le protocole RPC n'utilise pas le service KSN.

     Cette case est cochée par défaut.

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres généraux de connexion à un stockage réseau connecté via le protocole RPC

► *Pour configurer les paramètres généraux de connexion à un stockage réseau connecté via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, ouvrez l'onglet **Général** et dans le groupe **Paramètres de connexion au stockage réseau**, réalisez les opérations suivantes :
   - Saisissez dans le champ la valeur du délai d'attente entre les tentatives de restauration de la connexion au stockage réseau.
   - Saisissez dans le champ du nombre maximum de tentatives de restauration de la connexion au stockage réseau.

     Il est conseillé de conserver les valeurs par défaut ou de les remplacer par des valeurs plus élevées.
   - Si vous souhaitez que Kaspersky Security purge le cache des fichiers analysés du stockage réseau après chaque mise à jour des bases de l'application, cochez la case **Purger la mémoire cache des fichiers traités du stockage réseau après la mise à jour des bases de l'application**.
   - Si vous souhaitez que Kaspersky Security conserve le cache des fichiers analysés du stockage réseau après chaque mise à jour des bases de données de l'application, décochez la case **Purger la mémoire cache des fichiers traités du stockage réseau après la mise à jour des bases de l'application**.
5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC

Cette section décrit les paramètres de sécurité et les instructions à suivre pour appliquer les niveaux de sécurité prédéfinis et configurer manuellement les paramètres de la sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC.

Dans cette section

À propos des niveaux de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC

Dans la tâche Protection des stockages réseau connectés via le protocole RPC, vous pouvez appliquer à chaque stockage réseau protégé un des niveaux de sécurité prédéfinis : **Performance maximale**, **Recommandé** ou **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous). Vous pouvez également configurer les valeurs des paramètres de sécurité manuellement. Dans ce cas, le niveau de sécurité du stockage réseau protégé devient **Personnalisé**.

Performance maximale

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 4. Paramètres des niveaux de sécurité prédéfinis dans la tâche Protection des stockages réseau connectés via le protocole RPC

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Protection des objets	Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus	Objets analysés en fonction du format	Objets analysés en fonction du format
Protection des objets composés	Objets compactés	• Archives SFX • Objets compactés • Objets OLE	• Archives SFX • Objets compactés • Objets OLE

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Actions à exécuter sur les objets infectés	Interdire l'accès et réparer. Supprimer si la réparation est impossible	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et réparer. Supprimer si la réparation est impossible
Actions à exécuter sur les objets potentiellement infectés	Interdire l'accès et placer en quarantaine	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et placer en quarantaine
Actions en fonction du type d'objet détecté	Non	Non	Non
Exclure les fichiers	Non	Non	Non
Ne pas détecter	Non	Non	Non
Arrêter si l'analyse dure plus de (s.)	60	60	60
Ne pas analyser les objets composés de plus de (Mo)	8	8	Non

Application d'un niveau de sécurité prédéfini dans la tâche Protection des stockages réseau connectés via le protocole RPC

► *Pour appliquer un des niveaux de sécurité prédéfinis au stockage réseau connecté via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des stockages réseau protégés, sélectionnez celui auquel vous souhaitez attribuer un niveau de sécurité prédéfini.
5. Sous l'onglet **Niveau de sécurité**, sélectionnez un des niveaux de sécurité prédéfinis suivants :
   - **Protection maximale ;**
   - **Recommandé ;**
   - **Performance maximale**.

   L'onglet **Niveau de sécurité** affiche les principales valeurs des paramètres du niveau de sécurité sélectionné. Le niveau de sécurité appliqué apparaît en regard du nom du stockage réseau dans la liste des stockages réseau protégés.
6. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés du niveau de sécurité seront enregistrés et appliqués à la tâche en cours.

Vous pouvez également configurer manuellement les paramètres de sécurité du stockage réseau protégé (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP" à la page 67).

Voir également

Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC

► *Pour configurer manuellement les paramètres de sécurité applicables au stockage réseau connecté via le protocole RPC, réalisez les opérations suivantes :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole RPC**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des stockages réseau à protéger, sélectionnez celui dont vous souhaitez configurer le niveau de sécurité.

   Vous pouvez appliquer un modèle prédéfini de paramètres de sécurité.

5. Configurez les paramètres de sécurité requis pour le stockage réseau sélectionné en fonction de vos exigences en matière de sécurité informatique. Pour ce faire, procédez comme suit :

   - Sur l'onglet **Général**, réalisez les actions suivantes, le cas échéant :

     - Dans le groupe **Protection des objets**, désignez les objets qui seront analysés par Kaspersky Security :

       - **Tous les objets**.

       Kaspersky Security analyse tous les objets.

       - **Objets analysés en fonction du format**.

       Kaspersky Security analyse uniquement les fichiers infectables sur la base du format du fichier.

       La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

       - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**.

       Kaspersky Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

       La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

       - **Objets analysés en fonction de la liste d'extensions indiquée.**

       Kaspersky Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

       Vous pouvez également configurer ce paramètre dans le stockage réseau. Si le paramètre est configuré dans Kaspersky Security, le stockage réseau envoie l'objet pour analyse et Kaspersky Security considère l'objet comme inoffensif sans réaliser d'analyse antivirus. Si le paramètre est configuré dans le stockage réseau, celui-ci n'envoie pas le fichier pour analyse. Afin d'économiser le trafic réseau et de réduire la charge sur le serveur où Kaspersky Security est installé, il est conseillé de définir la valeur du paramètre qui limite les objets à analyser dans le stockage réseau.

- Dans le groupe **Protection des objets composés**, désignez les objets composés qui seront analysés par Kaspersky Security.

- Sur l'onglet **Actions**, réalisez les actions suivantes, le cas échéant :
  - Dans le groupe **Actions à exécuter sur les objets infectés**, sélectionnez l'action réalisée par Kaspersky Security en cas de détection d'un objet infecté.
  - Dans le groupe **Actions à exécuter sur les objets potentiellement infectés**, sélectionnez l'action que Kaspersky Security exécutera suite à la détection d'un objet probablement infecté.
  - Dans le groupe **Actions en fonction du type d'objet détecté**, désignez les actions que Kaspersky Security exécutera sur les objets en fonction du type d'objet à détecter.

- Sous l'onglet **Optimisation**, réalisez les actions suivantes, le cas échéant :
  - Dans le groupe **Exclusions**, désignez les objets que Kaspersky Security exclut de l'analyse d'une des méthodes suivantes :
    - Si vous souhaitez exclure des fichiers de l'analyse, cochez la case **Exclure les fichiers** et indiquez les noms ou les masques de nom de fichiers à exclure.
    - Si vous souhaitez exclure des objets détectés (par exemple, des utilitaires d'administration à distance), cochez la case **Ne pas détecter** et indiquez les noms ou les masques de noms des objets détectés selon la classification de l'Encyclopédie des virus (http://www.securelist.fr/).

    Vous pouvez également configurer ces paramètres pour la tâche dans son ensemble dans les paramètres d'exclusion de la zone de confiance.

  - Dans le groupe **Paramètres avancés**, indiquez la durée maximale de l'analyse d'un objet et la taille maximale d'un fichier composé.

    Si vous utilisez un stockage réseau NetApp fonctionnant sous le système d'exploitation Clustered Data ONTAP, ce paramètre peut également être configuré dans le stockage réseau. Si le paramètre est configuré dans Kaspersky Security, le stockage réseau envoie l'objet pour analyse et Kaspersky Security considère l'objet comme inoffensif sans réaliser d'analyse antivirus. Si le paramètre est configuré dans le stockage réseau, celui-ci n'envoie pas le fichier pour analyse. Afin d'économiser le trafic réseau et de réduire la charge sur le serveur où Kaspersky Security est installé, il est conseillé de définir la valeur du paramètre qui limite les objets à analyser dans le stockage réseau.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés du niveau de sécurité de l'utilisateur seront enregistrés et appliqués à la tâche en cours.

Utilisation des modèles de paramètres de niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC

Cette section fournit des instructions sur l'utilisation des modèles de paramètres de niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole RPC.

Dans cette section

Création d'un modèle de paramètres de sécurité

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

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

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

3. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.

4. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Enregistrer comme modèle**.

   La fenêtre **Propriétés du modèle** s'ouvre.

5. Dans le champ **Nom du modèle**, saisissez le nom du modèle.

6. Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.

7. Cliquez sur **OK**.

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

Application du modèle de paramètres de sécurité

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

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

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

3. Dans l'arborescence ou dans la liste des ressources fichier du serveur, sélectionnez l'entrée pour laquelle vous souhaitez appliquer un modèle.

4. Sélectionnez **Appliquer un modèle** → **<Nom du modèle>**.

5. Dans l'arborescence de la console, ouvrez le menu contextuel du nom de la tâche à configurer.

6. Sélectionnez l'option **Enregistrer la tâche**.

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

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

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

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

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

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

Consultation des paramètres de sécurité du modèle

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

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche dont vous souhaitez consulter le modèle de sécurité.
2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

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

   La fenêtre **Modèles** s'ouvre.

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

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

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

Suppression du modèle de paramètres de sécurité

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

1. Dans l'arborescence de la console de Kaspersky Security, sélectionnez la tâche pour la configuration de laquelle vous ne souhaitez plus utiliser un modèle de paramètres de sécurité.

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

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

   La fenêtre **Modèles** s'ouvre.

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

4. Cliquez sur le bouton **Supprimer**.

   La fenêtre de confirmation de la suppression s'ouvre.

5. Dans la fenêtre de confirmation, cliquez sur **Oui**.

Le modèle sélectionné sera supprimé.

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

Consultation des statistiques de la tâche Protection des stockages réseau connectés via le protocole RPC

Quand la tâche Protection des stockages réseau connectés via le protocole RPC est en cours d'exécution, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis son lancement jusqu'à maintenant, autrement dit, les statistiques de la tâche.

► *Pour consulter les statistiques de la tâche Protection des stockages réseau connectés via le protocole RPC, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole RPC**.

3. Dans le panneau des résultats, choisissez l'onglet **Consultation et administration**.

Dans le groupe **Statistiques**, un tableau affiche les informations sur les objets que Kaspersky Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 5. Statistiques complètes de la tâche Protection des stockages réseau connectés via le protocole RPC

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security. Par exemple, si Kaspersky Security a découvert un programme malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres objets détectés	Nombre d'objets que Kaspersky Security détecte et classifie comme infectés ou nombre de fichiers de logiciels légitimes détectés, qui n'ont pas été exclus de l'analyse en temps réel et de la zone d'analyse des tâches à la demande, et qui ont été classés en tant que riskware.
Objets potentiellement infectés détectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Security.

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

Protection des stockages réseau connectés via le protocole ICAP

Cette section fournit des informations sur la tâche de protection des stockages réseau connectés via le protocole ICAP, sur la configuration de la connexion entre le stockage réseau et Kaspersky Security et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via ICAP.

Dans cette section

A propos de la protection des stockages réseau connectés via le protocole ICAP

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

Kaspersky Security ne dispose pas d'un accès direct aux fichiers situés sur un stockage réseau connecté via le protocole ICAP (plus loin *stockage réseau*). En cas de tentative de lecture, de création ou de modification d'un fichier, le stockage réseau crée une requête ICAP pour Kaspersky Security et transmet le fichier à l'intérieur de cette requête. L'application analyse le fichier conformément aux paramètres indiqués dans la tâche Protection des stockages réseau connectés via le protocole ICAP. Si Kaspersky Security découvre une menace, il exécute sur le fichier les actions définies dans les paramètres de la tâche et transmet les résultats de l'analyse au stockage réseau. Si l'action "Réparer" a été définie dans les paramètres de la tâche et que le fichier a pu être réparé, Kaspersky Security renvoie le fichier réparé au stockage réseau dans sa réponse à la requête.

Kaspersky Security permet de configurer les actions que l'application doit exécuter sur les fichiers infectés ou probablement infectés.

Lors de l'utilisation du KSN dans la tâche Protection des stockages réseau connectés via le protocole ICAP, Kaspersky Security ne peut supprimer ou bloquer des fichiers utilisés par des stockages de réseau connectés via le protocole ICAP car au moment de la réception d'une réponse négative des services KSN, l'application ne dispose pas d'un accès direct aux catalogues réseau du stockage. Les informations relatives à la réception d'une réponse négative sont consignées dans le journal d'exécution de la tâche Utilisation du KSN.

Vous pouvez protéger un stockage réseau à l'aide d'un serveur doté de Kaspersky Security. Pour améliorer la rapidité du stockage réseau et du serveur doté de Kaspersky Security, vous pouvez utiliser plusieurs serveurs dotés de Kaspersky Security pour la protection d'un seul stockage réseau. Dans ce cas, le stockage réseau répartit la charge entre les serveurs connectés et dotés de Kaspersky Security.

La tâche Protection des stockages réseau connectés via le protocole ICAP est créée par défaut et est une tâche prédéfinie de Kaspersky Security. Vous ne pouvez pas supprimer ou renommer cette tâche. Vous ne pouvez pas créer des tâches de protection des stockages réseau connectés via le protocole ICAP. Vous pouvez configurer la tâche de Protection des stockages réseau connectés via le protocole ICAP.

Vous pouvez lancer la tâche de protection des stockages réseau si la clé active prend en charge la protection des stockages réseau. Si vous lancez une tâche de protection des stockages réseau, mais que la clé active ne prend pas en charge la protection des stockages réseau, la tâche se solde sur une erreur. Dans ce cas, Kaspersky Security ne protège pas les stockages réseau.

Le composant Protection des stockages réseau connectés via le protocole ICAP est disponible dans le cadre de la solution Kaspersky Security for Data Storage.

Vous trouverez plus d'informations sur les solutions de protection de l'entreprise, notamment sur Kaspersky Security for Windows Server dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Configuration de la connexion entre Kaspersky Anti-Virus et un stockage réseau connecté via le protocole ICAP

Vous pouvez lancer la tâche de protection des stockages réseau si la clé active prend en charge la protection des stockages réseau. Si vous lancez une tâche de protection des stockages réseau, mais que la clé active ne prend pas en charge la protection des stockages réseau, la tâche se solde sur une erreur. Dans ce cas, Kaspersky Security ne protège pas les stockages réseau.

Afin de pouvoir protéger des stockages réseau connectés via le protocole ICAP, vous devez configurer la connexion du stockage réseau à Kaspersky Security.

► *Pour configurer la connexion entre le stockage réseau et Kaspersky Security, procédez comme suit :*

1. Sur le serveur sur lequel est installé Kaspersky Security, configurez les paramètres suivants :
   - Dans la console de Kaspersky Security, définissez les paramètres de connexion au stockage réseau connecté via le protocole ICAP qui sera protégé par Kaspersky Security (cf. section "Configuration des paramètres de connexion à un stockage réseau connecté via le protocole ICAP" à la page 82).
   - Dans l'éditeur de stratégies de groupe locales, configurez les paramètres de sécurité des stratégies locales (cf. section "Configuration des paramètres de sécurité des stratégies locales dans l'éditeur d'une stratégie de groupe locale" à la page 25).
   - Dans la fenêtre de configuration du pare-feu Windows, configurez les règles pour les connexions entrantes et sortantes dans le pare-feu Windows (cf. section Configuration des connexions entrantes et sortantes dans le pare-feu Windows" à la page 27).

2. Configurez les paramètres suivants dans le stockage réseau :

   - Activez la fonction de protection antivirus.
   - Indiquez l'adresse de connexion à Kaspersky Security dans les paramètres du stockage réseau.

   > Les informations relatives à la configuration du stockage réseau que vous utilisez figurent dans la documentation de ce stockage.

La connexion entre Kaspersky Anti-Virus et un stockage réseau connecté via le protocole ICAP sera effectuée.

Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole ICAP

Par défaut, la tâche prédéfinie Protection des stockages réseau connectés via le protocole ICAP possède les paramètres décrits dans le tableau ci-après. Vous pouvez modifier les valeurs de ces paramètres.

Quand vous modifiez les paramètres de la tâche, par exemple en modifiant le niveau de sécurité, Kaspersky Security applique immédiatement les nouvelles valeurs des paramètres à la tâche en cours. Kaspersky Security consigne la date et l'heure de la modification des paramètres de la tâche dans le journal d'audit système.

Tableau 6. Paramètres par défaut de la tâche Protection des stockages réseau connectés via le protocole ICAP

Paramètre	Valeur par défaut	Commentaires
Niveau de sécurité.	Le niveau de sécurité **Recommandé** est appliqué.	Vous pouvez appliquer un des niveaux de sécurité prédéfinis à la protection du stockage réseau ou vous pouvez définir les valeurs manuellement.

Paramètre	Valeur par défaut	Commentaires
Analyseur heuristique.	Le niveau d'analyse **Moyenne** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Utilisation du KSN pour la protection	Appliquée.	Vous pouvez activer et désactiver l'utilisation du service KSN pour la Protection des stockages réseau connectés via le protocole ICAP.
Paramètres de connexion au stockage réseau.	• **Numéro de port réseau du serveur ICAP** : 1344 ; • **Identification du service** – avscan.	Vous pouvez modifier les autres paramètres de connexion aux stockages réseau. Ces modifications doivent être prises en compte dans les stockages réseau.
Lancement d'une tâche planifiée.	Pas appliqué. La case **Exécuter de manière planifiée** est décochée. La tâche est lancée manuellement.	Vous pouvez configurer l'exécution planifiée d'une tâche, par exemple au démarrage de Kaspersky Security.

► *Pour configurer les paramètres de la tâche Protection des stockages réseau connectés via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

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

4. Dans l'onglet **Général** de la fenêtre qui s'ouvre, configurez les paramètres suivants de la tâche :

   - Connexion à un stockage réseau connecté via le protocole ICAP (cf. section "Configuration des paramètres de connexion à un stockage réseau connecté via le protocole ICAP" à la page 82).
   - Application de l'analyseur heuristique (à la page 83).
   - Utilisation du KSN pour la protection (à la page 84).

   Dans le groupe **Niveau de sécurité** :

   - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section "Application d'un niveau de sécurité prédéfini dans la tâche Protection des stockages réseau connectés via le protocole ICAP" à la page 88) ou configurez manuellement les paramètres de protection des objets (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP" à la page 89).

5. Les onglets **Planification** et **Avancé** permettent de configurer les paramètres de lancement planifié de la tâche (cf. section "Configuration des paramètres de planification du lancement des tâches" à la page 40).

6. Cliquez sur **OK**.

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

Dans cette section

Configuration des paramètres de connexion à un stockage réseau connecté via le protocole ICAP

► *Pour configurer les paramètres de connexion à un stockage réseau connecté via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

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

4. Dans l'onglet **Général** dans les champs du groupe **Paramètres de connexion**, saisissez les données suivantes :

   - Numéro de port réseau du serveur ICAP ;

     Numéro du port réseau du serveur ICAP pour la connexion du stockage réseau à l'application.

   - 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 1344 et que l'identification du service ICAP est avscan, alors ces paramètres serviront pour créer l'adresse RESPMOD URI suivante : `icap://192.168.10.10/avscan:1344`.

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Après avoir configuré les paramètres de la connexion, il faut créer l'adresse de connexion à Kaspersky Security et la renseigner dans le stockage réseau. Les paramètres de connexion sont inclus dans cette adresse. Par exemple, si les paramètres conservent leurs valeurs par défaut, l'adresse de connexion prend l'aspect suivant :

```
icap://<adresse IP de l'ordinateur doté de Kaspersky
Security>/avscan:1344
```

Application de l'analyseur heuristique

Dans la tâche Protection des stockages réseau connectés via le protocole ICAP, vous pouvez utiliser l'analyseur heuristique et configurer le niveau de l'analyse.

► *Pour configurer les paramètres d'utilisation de l'analyse heuristique dans la tâche Protection des stockages réseau connectés via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.
3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et dans le groupe **Analyseur heuristique**, réalisez une des opérations suivantes.
   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.
   - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

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

Il existe trois niveaux de détail pour l'analyse

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

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

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

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Utilisation du KSN pour la protection

Le *Kaspersky Security Network (KSN)* est une infrastructure de services et d'outils 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.

Vous pouvez activer ou désactiver l'application du KSN dans la tâche Protection des stockages réseau connectés via le protocole RPC. Lorsque vous activez ou désactivez l'application du KSN, la tâche commence à établir la réputation des fichiers analysés à partir des informations reçues du KSN, ou arrête de le faire.

Il est indispensable d'accepter le Règlement du KSN afin de lancer la tâche Utilisation du KSN. Par défaut, la tâche Utilisation du KSN n'est pas lancée automatiquement au démarrage de Kaspersky Security.

Vous trouverez plus d'informations sur la tâche Utilisation du KSN dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

► *Pour activer ou désactiver l'utilisation du KSN dans la tâche Protection des stockages réseau connectés via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

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

4. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Général** et dans le groupe **Utilisation du KSN**, cochez ou décochez la case **Utiliser le KSN pour la protection**.

   La case active ou désactive l'utilisation des services des services du Kaspersky Security Network (KSN) par la tâche Protection des stockages réseau connectés via le protocole ICAP.

   Si la case est cochée, l'application utilise les données du Kaspersky Security Network 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 Protection des stockages réseau connectés via le protocole ICAP n'utilise pas le service KSN.

   Cette case est cochée par défaut.

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP

Cette section décrit les paramètres de la sécurité et les instructions à suivre pour appliquer les niveaux de sécurité prédéfinis et configurer manuellement les paramètres de la sécurité dans la tâche Protocole ICAP. Protection des stockages réseau.

Dans cette section

À propos des niveaux de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP

Dans la tâche Protection des stockages réseau connectés via le protocole ICAP, vous pouvez appliquer à chaque stockage réseau protégé un des niveaux de sécurité prédéfinis : **Performance maximale**, **Recommandé** ou **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous). Vous pouvez également configurer les valeurs des paramètres de sécurité manuellement. Dans ce cas, le niveau de sécurité du stockage réseau protégé devient **Personnalisé**.

Performance maximale

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 7. Paramètres des niveaux de sécurité prédéfinis dans la tâche Protection des stockages réseau connectés via le protocole ICAP

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Protection des objets	Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus	Objets analysés en fonction du format	Objets analysés en fonction du format
Protection des objets composés	Objets compactés	• Archives SFX • Objets compactés • Objets OLE	• Archives SFX • Objets compactés • Objets OLE
Actions à exécuter sur les objets infectés	Interdire l'accès et réparer.	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et réparer.
Actions à exécuter sur les objets potentiellement infectés	Interdire l'accès et placer en quarantaine	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et placer en quarantaine

Paramètres	Niveau de sécurité		
Exclure les fichiers	Non	Non	Non
Ne pas détecter	Non	Non	Non
Arrêter si l'analyse dure plus de (s.)	60	60	60
Ne pas analyser les objets composés de plus de (Mo)	8	8	Non

Application d'un niveau de sécurité prédéfini dans la tâche Protection des stockages réseau connectés via le protocole ICAP

► *Pour appliquer un des niveaux de sécurité prédéfinis au stockage réseau connecté via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

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

4. Sous l'onglet **Général** du groupe **Niveau de sécurité**, sélectionnez un des niveaux de sécurité prédéfinis suivants :

   - **Protection maximale**
   - **Recommandé**
   - **Performance maximale**.

   Les principales valeurs des paramètres du niveau de sécurité s'affichent sous la liste.

5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Vous pouvez également configurer manuellement les paramètres de sécurité du stockage réseau protégé (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP" à la page 89).

Voir également

Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection des stockages réseau connectés via le protocole ICAP

► *Pour configurer manuellement les paramètres de sécurité applicables au stockage réseau connecté via le protocole ICAP, réalisez les opérations suivantes :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.

3. Dans le panneau des résultats de l'entrée **Protection des stockages réseau connectés via le protocole ICAP**, cliquez sur le lien **Propriétés**.

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

4. Sous l'onglet **Général** du groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Paramètres de sécurité** s'ouvre.

5. Configurez les paramètres en fonction de vos exigences en matière de sécurité informatique. Pour ce faire, procédez comme suit :

   - Sur l'onglet **Général**, réalisez les actions suivantes, le cas échéant :

     - Dans le groupe **Protection des objets**, désignez les objets qui seront analysés par Kaspersky Security :

       - **Tous les objets** ;

       Kaspersky Security analyse tous les objets.

       - **Objets analysés en fonction du format** ;

       Kaspersky Security analyse uniquement les fichiers infectables sur la base du format du fichier.

       La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

       - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus** ;

       Kaspersky Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

       La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

       - **Objets analysés en fonction de la liste d'extensions indiquée**.

       Kaspersky Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

     - Dans le groupe **Protection des objets composés**, désignez les objets composés qui seront analysés par Kaspersky Security.

- Sur l'onglet **Actions**, réalisez les actions suivantes, le cas échéant :
  - Dans le groupe **Actions à exécuter sur les objets infectés**, sélectionnez l'action réalisée par Kaspersky Security en cas de détection d'un objet infecté.
  - Dans le groupe **Actions à exécuter sur les objets potentiellement infectés**, sélectionnez l'action que Kaspersky Security exécutera suite à la détection d'un objet probablement infecté.
- Sous l'onglet **Optimisation**, réalisez les actions suivantes, le cas échéant :
  - Dans le groupe **Exclusions**, désignez les objets que Kaspersky Security exclut de l'analyse d'une des méthodes suivantes :
    - Si vous souhaitez exclure des fichiers de l'analyse, cochez la case **Exclure les fichiers** et indiquez les noms ou les masques de nom de fichiers à exclure.
    - Si vous souhaitez exclure des objets détectés (par exemple, des utilitaires d'administration à distance), cochez la case **Ne pas détecter** et indiquez les noms ou les masques de noms des objets détectés selon la classification de l'Encyclopédie des virus (http://www.securelist.fr).
  - Dans le groupe **Paramètres avancés**, indiquez la durée maximale de l'analyse d'un objet et la taille maximale d'un fichier composé.

6. Dans la fenêtre **Paramètres de sécurité**, cliquez sur le bouton **OK**.

   La fenêtre **Paramètres de sécurité** se ferme.

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

Les paramètres définis du niveau de sécurité de l'utilisateur seront enregistrés.

Consultation des statistiques de la tâche Protection des stockages réseau connectés via le protocole ICAP

Quand la tâche Protection des stockages réseau connectés via le protocole ICAP est en cours d'exécution, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security depuis son lancement jusqu'à maintenant, autrement dit, les statistiques de la tâche.

► *Pour consulter les statistiques de la tâche Protection des stockages réseau connectés via le protocole ICAP, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez la sous-entrée **Protection des stockages réseau connectés via le protocole ICAP**.

Dans l'onglet **Consultation et administration** du panneau des résultats, dans le groupe **Statistiques**, un tableau affiche les informations sur les objets que Kaspersky Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 8. Statistiques de la tâche Protection des stockages réseau connectés via le protocole RPC

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security. Par exemple, si Kaspersky Security a découvert un programme malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres objets détectés	Nombre d'objets que Kaspersky Security détecte et classifie comme infectés ou nombre de fichiers de logiciels légitimes détectés, qui n'ont pas été exclus de l'analyse en temps réel et de la zone d'analyse des tâches à la demande, et qui ont été classés en tant que riskware.
Objets potentiellement infectés détectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Security.

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

Administration des tâches de protection des stockages réseau dans Kaspersky Security Center

Cette section contient des informations sur l'administration des tâches de protection des stockages réseau via le Serveur d'administration Kaspersky Security Center ainsi que des instructions concernant la configuration des paramètres des tâches pour le groupe de serveurs et pour un serveur à partir de Kaspersky Security Center.

Dans cette section

À propos de la protection des stockages réseau dans Kaspersky Security Center

Vous pouvez utiliser l'une des méthodes suivantes pour administrer les tâches de protection des stockages réseau dans Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center**. Vous pouvez configurer les paramètres uniques de protection des stockages réseau et les appliquer aux tâches du groupe de serveurs sélectionné.
- **Dans la fenêtre Paramètres de l'application**. Vous pouvez configurer les paramètres de protection des stockages réseau individuellement pour chacun des serveurs sur lequel est installé Kaspersky Security.

Configuration des paramètres de protection des stockages réseau à l'aide de stratégies

Par défaut, les tâches de protection des stockages réseau dans la stratégie de Kaspersky Security Center possèdent les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 9. Paramètres des tâches de protection des stockages réseau dans une stratégie Kaspersky Security Center

Tâche de protection des stockages réseau	Paramètres
Protection des stockages réseau connectés via le protocole RPC	Le bouton **Configuration** de la tâche Protection des stockages réseau connectés via le protocole RPC permet de configurer les paramètres suivants d'exécution de la tâche : • composition de la zone de protection ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de la sécurité ; • utilisation de l'analyse heuristique ; • application de la zone de confiance et utilisation du KSN ; • paramètres de connexion au stockage réseau ; • paramètres de lancement de la tâche.
Protection des stockages réseau connectés via le protocole ICAP	Le bouton **Configuration** de la tâche Protection des stockages réseau connectés via le protocole ICAP permet de configurer les paramètres suivants d'exécution de la tâche : • utilisation de l'analyse heuristique ; • paramètres de connexion au stockage réseau ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de la sécurité ; • utilisation du KSN ; • paramètres de lancement de la tâche.

► *Pour configurer les paramètres de la tâche de protection des stockages réseau dans la stratégie de Kaspersky Security Center, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie et sélectionnez enfin l'onglet **Stratégies** dans le panneau des résultats.

2. Dans le menu contextuel de la stratégie dont vous souhaitez modifier les paramètres, choisissez l'option **Propriétés**, et dans la liste des sections de la fenêtre qui s'ouvre, sélectionnez **Protection des stockages réseau**.

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

   - Si vous souhaitez configurer les paramètres de la tâche **Protection des stockages réseau connectés via le protocole RPC**, appuyez sur le bouton **Configuration**.

     Dans la fenêtre **Paramètres** qui s'ouvre, configurez les paramètres de la tâche selon vos exigences (cf. section "Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 55). Cliquez sur **OK** pour enregistrer les modifications des paramètres dans la stratégie.

   - Si vous souhaitez configurer les paramètres de la tâche **Protection des stockages réseau connectés via le protocole ICAP**, appuyez sur le bouton **Configuration**.

     Dans la fenêtre **Paramètres** qui s'ouvre, configurez les paramètres de la tâche selon vos exigences (cf. section "Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 55). Cliquez sur **OK** pour enregistrer les modifications des paramètres dans la stratégie.

4. Dans la fenêtre **Propriétés : <nom de la stratégie>**, cliquez sur le bouton **OK**.

Les paramètres configurés de la tâche de protection des stockages réseau seront enregistrés et appliqués à la stratégie active.

Vous trouverez plus d'informations sur l'utilisation de Kaspersky Security avec les stratégies de Kaspersky Security Center, ainsi que des informations sur les stratégies de Kaspersky Security Center dans le *Manuel de l'administrateur de Kaspersky Security Center* et dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Configuration des paramètres de protection des stockages réseau pour un serveur dans Kaspersky Security Center

► *Pour configurer les paramètres de protection des stockages réseau pour un seul serveur dans Kaspersky Security Center, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

2. Dans le panneau des résultats, sous l'onglet **Ordinateurs**, ouvrez le menu contextuel de la ligne reprenant les informations relatives au serveur protégé, puis sélectionnez l'option **Propriétés**.

3. Dans la section **Tâches** de la fenêtre **Propriétés : <Nom de l'ordinateur>**, ouvrez le menu contextuel de la tâche de protection des stockages réseau que vous souhaitez configurer et choisissez l'option **Propriétés**.

4. Dans la fenêtre qui s'ouvre, configurez les paramètres de la tâche de protection des stockages réseau selon vos exigences :

   - Protection des stockages réseau connectés via le protocole RPC (cf. section "Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole RPC" à la page 55).

   - Protection des stockages réseau connectés via le protocole ICAP (cf. section "Configuration des paramètres de la tâche Protection des stockages réseau connectés via le protocole ICAP" à la page 79).

5. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués à la tâche en cours pour un seul serveur.

Si l'application est soumise à une stratégie de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de la tâche, ces paramètres ne pourront pas être modifiés via la fenêtre **Propriétés : <Nom de l'ordinateur>**.

Vous trouverez plus d'informations sur l'utilisation de Kaspersky Security avec les stratégies de Kaspersky Security Center, ainsi que des informations sur les stratégies de Kaspersky Security Center dans le *Manuel de l'administrateur de Kaspersky Security Center* et dans le *Manuel de l'administrateur de Kaspersky Security 10*.

Contacter le Support Technique

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

Dans cette section

Modes d'obtention du Support Technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des sources d'informations relatives à l'application, contactez le Support Technique. Les employés du Support Technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Le Support Technique n'est pas proposé aux utilisateurs d'une version d'essai.

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

Voici comment contacter les experts du Support Technique de Kaspersky Lab :

- appeler le Support Technique par téléphone (http://support.kaspersky.com/fr/b2b)
- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Support Technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un portail à disposition des entreprises qui utilisent les applications de Kaspersky Lab. Le portail Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le portail Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky Lab des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte Kaspersky CompanyAccount. Un compte permet de gérer de manière centralisée les requêtes électroniques des employés inscrits chez Kaspersky Lab ainsi que de gérer les autorisations de ces employés au sein du Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Vous pouvez également obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

Support Technique par téléphone

Vous pouvez téléphoner aux experts du Support Technique dans la plupart des régions du monde. Vous pourrez trouver des informations sur les modes d'obtention de l'assistance technique dans votre région et les coordonnées du Support Technique sur le site Internet du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/b2b).

Avant de contacter le Support Technique, prenez connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Utilisation du fichier de trace et du script AVZ

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Security à envoyer au Support Technique. Les experts du Support Technique 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 créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus exécutés, de rechercher la présence éventuelle de menaces sur l'ordinateur, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse de l'ordinateur.

Glossaire

A

Analyse heuristique

Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky Lab. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.

Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état *probablement infecté*.

Analyse sur la base de signatures

Technologie d'identification des menaces qui utilise les bases de Kaspersky Security contenant les descriptions des menaces connues et les méthodes pour les éliminer. La protection selon cette méthode offre le niveau minimum de sécurité. Conformément aux recommandations des spécialistes de Kaspersky Lab, cette méthode est toujours activée.

Analyseur heuristique

Module de Kaspersky Security qui exécute l'analyse heuristique.

Archive

Fichier qui contient un ou plusieurs autres fichiers qui peuvent être des archives.

B

Bases antivirus

Bases de données contenant 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. Ces bases antivirus sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

F

Faux positif

Situation où un objet sain est considéré comme infecté par une application de Kaspersky Lab car son code évoque celui d'un virus.

Fichier infecté

Fichier contenant un code malveillant (pendant l'analyse du fichier, le code d'un programme connu présentant une menace a été détecté). Les experts de Kaspersky Lab vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

Fichier potentiellement infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'insertion et d'activation de code malveillant est nettement élevé pour ces fichiers.

Fichier probablement infecté

Fichier contenant le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets probablement infectés sont identifiés à l'aide de l'analyse heuristique.

M

Masque de fichier

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- ***** : remplace zéro ou plus de caractère de n'importe quel type.
- **?** : remplace n'importe quel caractère.

Il faut prendre en considération que le nom est toujours séparé de l'extension du fichier par un point.

O

Objets exécutés au démarrage du système

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur l'ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

Objet OLE

Fichier associé ou intégré à un autre fichier. Les programmes de Kaspersky Lab permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Microsoft Office Excel® dans un document Microsoft Office Word, ce tableau sera analysé en tant qu'objet OLE.

P

Paramètres de l'application

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

Q

Quarantaine

Dossier spécial prévu pour conserver les copies de sauvegarde des objets créés avant leur réparation ou leur suppression. C'est également dans la quarantaine que l'application de Kaspersky Lab place les fichiers potentiellement infectés détectés. Les objets en quarantaine sont chiffrés afin de les empêcher d'agir sur l'ordinateur.

R

Réparation des objets

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être réparés.

S

Sauvegarde

Dossier spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur réparation ou leur suppression.

T

Tâche

Fonctions exécutées par l'application de Kaspersky Lab sous la forme de tâches, par exemple : Protection des fichiers en temps réel, Analyse complète de l'ordinateur, Mise à jour des bases.

V

Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs de programme malveillant pour pénétrer dans un système ou une application et nuire son intégrité. Un grand nombre de vulnérabilités dans un système rend son fonctionnement peu fiable car les virus, installés dans le système, peuvent entraîner des erreurs du système d'exploitation ou des applications installées.

AO KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre diverses menaces dont les virus et autres programmes malveillants, le courrier indésirable (spam), les attaques de réseau et les attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie ("IDC Endpoint Tracker 2014").

Kaspersky Lab a été fondée en Russie en 1997. Kaspersky Lab est devenu un groupe international qui compte 34 bureaux dans 31 pays. L'entreprise emploie plus de 3000 experts qualifiés.

PRODUITS. Les 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 de l'information sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des équipements gérés par l'automatisation industrielle et la prévention des escroqueries financières. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace et automatisée de toute organisation, quelle que soit sa taille, contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands organismes d'évaluation. Elles sont compatibles avec les logiciels de nombreux fournisseurs et sont optimisées pour une exécution sur de nombreuses plateformes.

Les experts antivirus de Kaspersky Lab travaillent 24 heures sur 24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et ajoutent les signatures de ces menaces aux bases utilisées par les applications de Kaspersky Lab.

TECHNOLOGIE. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu ou ZyXEL. Beaucoup des innovations technologiques de l'entreprise sont brevetées.

RESULTATS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a remporté des centaines de récompenses. 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 la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 400 millions de personnes. Kaspersky Lab compte plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.fr/
Laboratoire de virus :	http://newvirus.kaspersky.com/fr (pour l'analyse de fichiers ou de sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

Informations sur le code tiers

Les informations sur le code tiers se trouvent dans le fichier legal_notices.txt, situé dans le dossier d'installation de l'application.

Avis de marques déposées

Les marques déposées et les marques de service appartiennent à leur propriétaire.

Citrix, Citrix Presentation Server, XenApp et XenDesktop sont de marques de commerce de Citrix Systems, Inc. et/ou de ses filiales déposées aux Etats-Unis et dans d'autres pays.

Dell, Dell Compellent - sont de marques de commerce de Dell, Inc.

Celerra, EMC, Isilon, OneFS et VNX sont des marques de commerce ou des marques déposées d'EMC Corporation aux Etats-Unis et/ou dans d'autres pays.

Hitachi - est une marque de commerce de Hitachi, Ltd.

Domino et System Storage sont des marques de commerce d'International Business Machines Corporation déposées dans de nombreuses juridictions à travers le monde.

Excel, Hyper-V, Microsoft, Windows, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Data ONTAP et NetApp sont des marques de commerce ou des marques déposées de NetApp, Inc. aux Etats-Unis et/ou dans d'autres pays.

Oracle – est une marque de commerce de Oracle Corporation et / ou ses filiales.

Index