KASPERSKY

Kaspersky Security for Windows Server

Manuel d'implantation pour la Protection des stockages réseau

Version du produit : 10.1.2.996

Chers utilisateurs !

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

Date de révision du document : 12.04.2019

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

Sommaire

A propos du guide

Le manuel d'implantation de Kaspersky Security for Windows Server 10.1 (ci-après "Kaspersky Security for Windows Server") pour la Protection des stockages réseau est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Security for Windows Server, ainsi qu'aux spécialistes qui offrent une assistance technique aux organisations qui ont choisi de travailler avec Kaspersky Security for Windows Server.

Ce manuel reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security for Windows Server 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 composants Protection RPC des stockages réseau connectés, Protection ICAP des stockages réseau connectés et Protection contre le chiffrement pour NetApp et d'une clé prenant en charge la Protection des stockages réseau (les informations relatives à l'installation et à la licence figurent dans le *Manuel de l'administrateur de Kaspersky Security for Windows Server*).

Contenu du chapitre

Dans ce document

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

Sources d'informations sur Kaspersky Security for Windows Server

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

Kaspersky Security for Windows Server

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Security for Windows Server.

Configurations logicielle et matérielle requises

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

Intégration de Kaspersky Security for Windows Server aux périphériques de stockage NAS

Cette section décrit les principes qui gouvernent l'interaction entre Kaspersky Security for Windows Server et les périphériques de stockage NAS.

Administration de la Console de Kaspersky Security for Windows Server

Cette section aborde la Console de Kaspersky Security for Windows Server et l'administration de Kaspersky Security for Windows Server via la console locale 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 périphériques de stockage NAS EMC™ du groupe Celerra™/VNX™

Cette section fournit des informations sur la protection des périphériques de stockage NAS EMC du groupe Celerra/VNX et sur l'intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS Celerra/VNX.

Protection RPC des stockages réseau connectés

Cette section fournit des informations sur la tâche Protection RPC des stockages réseau connectés, sur la configuration de la connexion entre un périphérique de stockage NAS et Kaspersky Security for Windows Server et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via RPC.

Protection ICAP des stockages réseau connectés

Cette section fournit des informations sur la tâche Protection ICAP des stockages réseau connectés, sur la configuration de la connexion entre un périphérique de stockage NAS et Kaspersky Security for Windows Server et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via ICAP.

Protection contre le chiffrement pour NetApp

Cette section contient des informations sur la tâche Protection contre le chiffrement pour NetApp et les instructions sur la configuration de cette tâche.

Contacter le Support Technique

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

Glossaire

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

Kaspersky Lab

Cette section contient des informations sur Kaspersky Lab.

Information sur le code tiers

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

Conventions

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

Tableau 1. Conventions

Exemple de texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui pourraient avoir des conséquences fâcheuses.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires et des conseils.
Exemple :	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments suivants sont en italique dans le texte : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison de touches **ALT+F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
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 for Windows Server

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

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

Contenu du chapitre

Sources de données pour des consultations indépendantes

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

- Page de Kaspersky Security for Windows Server sur le site Internet de Kaspersky Lab ;
- Page de Kaspersky Security for Windows Server sur le site du Support Technique (la Base de connaissances) ;
- Aide en ligne ;
- Manuels

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab.

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

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

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

La page de Kaspersky Security 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 des connaissances est une rubrique du site du Support Technique.

La page de Kaspersky Security for Windows Server (https://support.kaspersky.com/ksws10) dans la Base de connaissances 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 for Windows Server mais également d'autres applications de Kaspersky Lab. Ces articles peuvent également contenir des actualités du Support technique.

Documentation de Kaspersky Security for Windows Server

Le manuel de l'administrateur de Kaspersky Security for Windows Server décrit comment installer, désinstaller et activer l'application, comment configurer et utiliser Kaspersky Security for Windows Server et de la console d'application.

Le Manuel d'implantation pour la Protection des stockages réseau reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security for Windows Server 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 la soumettre aux experts de Kaspersky Lab et aux 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.

A propos de Kaspersky Security for Windows Server

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

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

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

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

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

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

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

Composants et fonctions de Kaspersky Security for Windows Server

L'application intègre les modules suivants :

- **Protection en temps réel**. Kaspersky Security for Windows Server analyse les objets à l'accès. Kaspersky Security for Windows Server analyse les objets suivants :
  - Les fichiers ;
  - Threads alternatives des systèmes de fichiers (flux NTFS) ;
  - L'enregistrement de démarrage principal et les secteurs d'amorçage des disques durs locaux ou amovibles.
- **Analyse à la demande**. Kaspersky Security for Windows Server recherche une fois des virus et autres menaces informatique dans la zone indiquée. L'application analyse les fichiers, la mémoire et les objets de démarrage sur un serveur protégé.
- **Protection RPC des stockages réseau connectés** et **Protection ICAP des stockages réseau connectés**. Kaspersky Security for Windows Server installé sur un serveur tournant sous un système d'exploitation Microsoft Windows protège les périphériques de stockage NAS contre les virus et autres

menaces informatiques qui s'introduisent sur les serveurs via l'échange de fichiers.

- **Contrôle du lancement des applications**. Ce composant surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus.
- **Contrôle des périphériques**. Ce composant contrôle l'enregistrement et l'utilisation des périphériques de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger l'ordinateur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou des périphériques externes d'un autre type connectés par USB.
- **Protection contre le chiffrement** et **Protection contre le chiffrement pour NetApp**. Les composants protègent les dossiers partagés sur les serveurs et les périphériques de stockage NAS contre le chiffrement malveillant en bloquant les hôtes qui affichent une activité malveillante.
- **Monitoring des scripts**. Ce composant analyse le code des scripts créés à l'aide des technologies Microsoft Windows Script Technologies.
- **Protection du trafic**. Ce module intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informations connues ou autres sur le serveur protégé.
- **Gestion du pare-feu**. Ce composant permet d'administrer le pare-feu Windows : il permet de configurer les paramètres et les règles du pare-feu du système d'exploitation et interdit toute possibilité de configuration du pare-feu externe.
- **Moniteur d'intégrité des fichiers**. Kaspersky Security for Windows Server détecte les modifications introduites dans les fichiers qui appartiennent aux zones de monitoring définies dans les paramètres de la tâche. Ces modifications peuvent signaler une violation de la sécurité sur le serveur protégé.
- **Inspection des journaux**. Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.

L'application peut remplir les fonctions suivantes :

- **Mise à jour des bases de l'application** et **Mise à jour des modules de l'application**. Kaspersky Security for Windows Server télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky Lab, depuis le Serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.
- **Quarantaine**. Kaspersky Security for Windows Server place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers la *quarantaine*. Pour des raisons de sécurité, une fois en quarantaine, les objets sont chiffrés.
- **Sauvegarde**. Kaspersky Security for Windows Server enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Probablement infecté* dans la *Sauvegarde* avant de procéder à la désinfection ou à la suppression de ces objets.
- **Notifications de l'administrateur et des utilisateurs**. Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Security for Windows Server et à l'état de la protection antivirus du serveur.
- **Importation et exportation des paramètres**. Vous pouvez exporter les paramètres de Kaspersky Security for Windows Server dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security for Windows Server depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.
- **Application des modèles**. Vous pouvez configurer manuellement les paramètres de sécurité du nœud dans l'arborescence des ressources fichier de l'ordinateur et enregistrer les valeurs définies comme un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Security for Windows Server.

- **Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server**. Vous pouvez configurer les autorisations d'administration de Kaspersky Security for Windows Server et des services Windows que l'application enregistre pour des utilisateurs ou des groupes d'utilisateurs.
- **Enregistrement des événements de l'application dans le journal**. Kaspersky Security for Windows Server enregistre les informations relatives aux paramètres de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution des tâches, aux événements associés avec Kaspersky Security for Windows Server et aux informations requises pour diagnostiquer les erreurs dans Kaspersky Security for Windows Server.
- **Stockage hiérarchique**. Kaspersky Security for Windows Server peut fonctionner en mode de gestion de stockage hiérarchique (système HSM). Le recours aux systèmes HSM permet de transférer des données entre des disques locaux rapides et des périphériques lents de stockage d'informations de longue durée.
- **Zone de confiance**. Vous pouvez composer la liste des exclusions de la zone de protection ou d'analyse que Kaspersky Security for Windows Server appliquera aux tâches d'analyse à la demande et de protection en temps réel.
- **Protection contre les exploits**. Vous pouvez protéger la mémoire des processus contre l'exploitation des vulnérabilités à l'aide de l'Agent de protection intégré dans ce processus.
- **Liste des ordinateurs bloqués**. Vous pouvez bloquer les hôtes distants qui essaient d'accéder aux dossiers partagés du serveur si une activité malveillante est détectée de leurs côté.

Configurations logicielle et matérielle requises

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

Contenu du chapitre

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

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

Vous pouvez installer Kaspersky Security for Windows Server sans supprimer la version de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition ou de Kaspersky Security 10 for Windows Server qui serait déjà installée.

Configuration matérielle requise pour le serveur

Recommandations d'ordre général :

- systèmes compatibles x86/64 avec un ou plusieurs processeurs ;
- Espace disque requis :
  - pour l'installation de tous les modules de l'application : 100 Mo ;
  - pour le téléchargement et le stockage des bases antivirus de l'application : 2 Go (recommandé) ;
  - pour l'enregistrement des objets en quarantaine et dans la sauvegarde : 400 Mo (recommandé) ;
  - pour l'enregistrement des journaux : 1 Go (recommandé).

Configuration minimale :

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

Configuration recommandée :

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

Configuration logicielle requise pour le serveur

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

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

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

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

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

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

- Windows Hyper-V Server 2012 R2 ;
- Windows Server 2016 Essentials / Standard / Datacenter ;
- Windows Server 2016 MultiPoint ;
- Windows Server 2016 Core Standard / Datacenter ;
- Microsoft Windows MultiPoint™ Server 2016 ;
- Windows Storage Server 2016 ;
- Windows Hyper-V Server 2016 ;
- Windows Server 2019 Essentials / Standard / Datacenter ;
- Windows Server 2019 Core ;
- Windows Storage Server 2019 ;
- Windows Hyper-V Server 2019.

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

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

- Microsoft Remote Desktop Services sur la base de Windows Server 2008 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2008 R2 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 R2 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2016 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2019 ;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15 ;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

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

- Kaspersky Security Center 10.4 ;
- Kaspersky Security Center 10.5 ;
- Kaspersky Security Center 11.

Configuration requise pour le périphérique de stockage NAS protégé

Kaspersky Security for Windows Server peut être utilisé pour la protection des périphériques de stockage NAS suivants :

- NetApp sous un des systèmes d'exploitation suivants :
  - Data ONTAP 7.x et Data ONTAP 8.x en mode 7-mode ;
  - Data ONTAP 8.2.1 ou suivant en mode cluster-mode.
- Dell™ EMC™ Celerra™ / VNX™ avec la configuration logicielle suivante :
  - Système d'exploitation EMC DART 6.0.36 ou suivant ;
  - Agent antivirus Celerra (CAVA) 4.5.2.3 ou plus.
- Dell EMC Isilon™ sous le système d'exploitation OneFS™ 7.0 ou suivant
- Hitachi NAS sur une des plateformes suivantes :
  - HNAS 4100 ;
  - HNAS 4080 ;
  - HNAS 4060 ;
  - HNAS 4040 ;
  - HNAS 3090 ;
  - HNAS 3080 ;
- IBM NAS série IBM System Storage N
- Oracle® NAS Systems de la série Oracle ZFS Storage Appliance
- Dell NAS sur la plateforme Dell Compellent™ FS8600

Configuration requise pour l'ordinateur sur lequel la console d'application est installée

Configuration matérielle requise pour l'ordinateur

Mémoire vive recommandée : 128 Mo minimum.

Espace disque disponible : 30 Mo.

Configuration logicielle requise pour l'ordinateur

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

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

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

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista® Editions ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8.1 ;
- Microsoft Windows 10 ;
- Windows 10 Redstone 1 ;
- Windows 10 Redstone 2 ;
- Windows 10 Redstone 3 ;
- Windows 10 Redstone 4 ;
- Windows 10 Redstone 5 ;
- Windows 10 Redstone 6 ;

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

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

- Microsoft Windows MultiPoint Server 2016 ;
- Windows Storage Server 2016 Essentials / Standard / Datacenter ;
- Windows Server 2019 Essentials / Standard / Datacenter ;
- Windows Storage Server 2019 ;
- Microsoft Windows XP Professional Edition SP2 ou suivant ;
- Microsoft Windows Vista ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8.1 ;
- Microsoft Windows 10 ;
- Windows 10 Redstone 1 ;
- Windows 10 Redstone 2 ;
- Windows 10 Redstone 3 ;
- Windows 10 Redstone 4 ;
- Windows 10 Redstone 5 ;
- Windows 10 Redstone 6.

Intégration de Kaspersky Security for Windows Server aux périphériques de stockage NAS

Cette section contient des informations sur les principes qui régissent l'interaction entre Kaspersky Security for Windows Server et les périphériques de stockage NAS.

Protection d'un périphérique de stockage NAS du groupe Celerra/VNX

Kaspersky Security for Windows Server interagit avec un périphérique de stockage NAS EMC du groupe Celerra/VNX via l'agent CAVA (Celerra Antivirus Agent) qui tourne sur l'ordinateur où est installé Kaspersky Security for Windows Server. Une fois lancé, Kaspersky Security for Windows Server vérifie si l'ordinateur est doté d'un agent CAVA qui doit répondre aux exigences de Kaspersky Security for Windows Server.

En cas de tentative de lecture ou de modification d'un fichier qui se trouve dans le périphérique de stockage NAS, 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 for Windows Server et sur la base des informations obtenues, il détermine le résultat de l'analyse et le transmet au périphérique de stockage NAS.

Protection RPC des stockages réseau connectés

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

Protection ICAP des stockages réseau connectés

Pour un stockage réseau connecté via le protocole ICAP (comme EMC Isilon, IBM NAS ou Hitachi NAS en mode ICAP), Kaspersky Security for Windows Server 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 périphérique de stockage NAS, le périphérique de stockage NAS crée une requête ICAP pour Kaspersky Security for Windows Server et transmet le fichier à l'intérieur de cette requête. Le module de l'application "Protection ICAP des stockages réseau connectés" analyse le fichier conformément aux paramètres définis pour la tâche "Protection ICAP des stockages réseau connectés". Si Kaspersky Security for Windows Server 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 périphérique de stockage NAS. Si l'action "Désinfecter" a été définie dans les paramètres et que le fichier a pu être désinfecté, Kaspersky Security for Windows Server renvoie le fichier désinfecté au périphérique de stockage NAS dans sa réponse à la requête.

Contenu du chapitre

Préparation au lancement de la tâche Protection des stockages réseau

Cette section contient des instructions pour préparer un serveur fonctionnant sous Microsoft Windows et doté de Kaspersky Security for Windows Server à l'intégration avec des stockages réseau de données et au lancement ultérieur de tâches de protection des stockages réseau.

Si vous avez l'intention d'utiliser la protection des stockages réseau sur le serveur tournant sous Microsoft Windows Server 2019, confirmez que la fonction de prise en charge du partage de fichiers SMB1.0/CIFS est installée. Pour en savoir plus, consultez la documentation de Microsoft Windows et les ressources en ligne correspondantes.

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**, saisissez la commande `gpedit.msc` dans la barre de recherche, puis appuyez sur la touche **ENTER**.
   - Si vous configurez les paramètres depuis un autre ordinateur, procédez comme suit :
     a. Cliquez sur le bouton **Démarrer**, saisissez la commande `mmc` dans la barre de recherche, 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 un composant logiciel enfichable**.

        La fenêtre **Ajout ou suppression de composants logiciels enfichables** s'ouvre.
     c. Dans la liste des composants logiciels enfichables disponibles, sélectionnez le composant logiciel enfichable **Editeur d'objets de stratégie de groupe** et cliquez sur le bouton **Ajouter**.

        L'**Assistant de stratégie de groupe** démarre.

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 for Windows Server d'une des méthodes suivantes :

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

2. Cliquez sur le bouton **OK**.

   Les modifications sont 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 doté de Kaspersky Security for Windows Server.

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**, saisissez la commande `wf.msc` dans la barre de recherche, puis appuyez sur la touche **ENTREE**.
   - Si vous configurez le pare-feu depuis un autre ordinateur, procédez comme suit :
     a. Cliquez sur le bouton **Démarrer**, saisissez la commande `mmc` dans la barre de recherche, 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 un composant logiciel enfichable**.

        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 d'ordinateur** s'ouvre.

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

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

2. Cliquez sur le bouton **OK**.

   Les modifications sont 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.

Si toutes les connexions sortantes sont refusées, ouvrez les ports suivants : TCP 443 (RPC(HTTP)), TCP 445 (SMB), TCP 88 (Kerberos), TCP 53 (DNS) et UDP 53 (DNS).

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.

Administration de la Console de Kaspersky Security for Windows Server

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

Contenu du chapitre

A propos de la console de Kaspersky Security for Windows Server

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

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

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

Si la console d'application et Kaspersky Security for Windows Server 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 l'application à la console d'application. Par exemple, après le démarrage d'une tâche quelconque de l'application, il se peut que l'état de cette tâche reste inchangé dans la console d'application.

Lors de l'installation de la console d'application, l'assistant d'installation crée le fichier kavfs.msc dans le répertoire d'installation et ajoute le composant logiciel enfichable Kaspersky Security for Windows Server à la liste des composants logiciels enfichables isolés de Microsoft Windows.

Vous pouvez démarrer la console d'application depuis le menu **Démarrer**. Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Security for Windows Server ou ajouter ce composant logiciel enfichable à la console Microsoft Management Console existante en tant que nouvel élément de son arborescence.

Sous la version 64 bits de Microsoft Windows, vous pouvez ajouter le composant logiciel enfichable de Kaspersky Security for Windows Server 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 for Windows Server afin de pouvoir administrer ainsi la protection de plusieurs serveurs sur lesquels Kaspersky Security for Windows Server est installé.

Lancement de la console de Kaspersky Security for Windows Server depuis le menu Démarrer

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

► *Pour démarrer la console d'application depuis le menu **Démarrer** :*

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

Pour ajouter d'autres composants logiciels enfichables à la console d'application, lancez-la en mode auteur.

► *Pour lancer la console d'application en mode auteur, procédez comme suit :*

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

La console d'application est lancée en mode auteur.

Si vous avez lancé la console d'application sur le serveur protégé, la fenêtre de la console d'application s'ouvre.

Si vous avez lancé la console d'application non pas sur le serveur protégé, mais sur un autre ordinateur, connectez-vous au serveur protégé.

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

1. Dans l'arborescence de la console d'application, ouvrez le menu contextuel du nœud **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 le bouton **OK**.

La console d'application est connectée au serveur protégé.

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

Interface de la console de Kaspersky Security for Windows Server

La Console de Kaspersky Security for Windows Server s'affiche dans l'arborescence de Microsoft Management Console en tant que nœud nommé Kaspersky Security.

Après la connexion à la copie de Kaspersky Security for Windows Server installée sur un autre serveur, le nom du nœud reprend le nom du serveur sur lequel l'application est installée ainsi que le nom du compte utilisateur sous les privilèges duquel la connexion a été réalisée : **Kaspersky Security <nom du serveur> sous <nom du compte>**. En cas de connexion à une instance de Kaspersky Security for Windows Server installée sur le même serveur que la console d'application, le nom du nœud devient **Kaspersky Security**.

Par défaut, la fenêtre de la console d'application contient les éléments suivants :

- Arborescence de la console d'application
- Panneau des résultats
- Barre d'outils.

Arborescence de la console d'application

L'arborescence de la console d'application affiche le nœud **Kaspersky Security** et ses nœuds enfants correspondant aux composants opérationnels de l'application.

Le nœud **Kaspersky Security** inclut les nœuds enfants suivants :

- **Protection en temps réel du serveur** : administration des tâches de protection en temps réel et des services KSN. Le nœud **Protection en temps réel du serveur** permet de configurer les tâches suivantes :
  - **Protection des fichiers en temps réel**
  - **Monitoring des scripts**
  - **Utilisation du KSN**
  - **Protection du trafic**
  - **Protection contre le chiffrement**
- **Contrôle du serveur** : contrôle les lancements des applications installées ainsi que les connexions des périphériques. Le nœud **Contrôle du serveur** permet de configurer les tâches suivantes :
  - **Contrôle du lancement des applications**
  - **Contrôle des périphériques**
  - **Gestion du pare-feu**
- **Génération automatique de règles** : configuration de la création automatique des règles de groupe et système pour les tâches Contrôle du lancement des applications et Contrôle des périphériques.
  - **Génération des règles du Contrôle du lancement des applications**
  - **Génération des règles du Contrôle des périphériques**
  - Tâches de groupe de génération de règles **<Noms des tâches>** (le cas échéant)

    Des tâches de groupe sont créées dans Kaspersky Security Center. Il est impossible d'administrer des tâches de groupe via la console d'application.

- **Diagnostic du système** : configuration des paramètres du contrôle des opérations réalisées sur les fichiers et de l'inspection des journaux des événements Windows.
  - **Moniteur d'intégrité des fichiers**
  - **Inspection des journaux**
- **Protection des stockages réseau** : configurez les tâches de protection des stockage réseau.
  - **Protection RPC des stockages réseau connectés**
  - **Protection ICAP des stockages réseau connectés**
  - **Protection contre le chiffrement pour NetApp**
- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Une entrée séparée existe pour chacune des tâches :
  - **Analyse au démarrage du système d'exploitation**
  - **Analyse des zones critiques**
  - **Analyse de la quarantaine**
  - **Vérification de l'intégrité de l'application**
  - Tâches définies par l'utilisateur **<Noms des tâches>** (le cas échéant)

  Le nœud affiche les tâches système créées lors de l'installation de l'application, les tâches définies par l'utilisateur et les tâches d'analyse à la demande de groupe créées et transmises à un ordinateur à l'aide de Kaspersky Security Center.
- **Mise à jour** : gère la mise à jour des bases de données et des modules de Kaspersky Security for Windows Server ainsi que la copie des mises à jour dans le dossier de la source locale de mises à jour. Le nœud contient des nœuds enfants permettant d'administrer chacune des tâches de mise à jour et la dernière annulation de la 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**

  L'entrée affiche toutes les tâches définies par l'utilisateur et les tâches de groupe de mise à jour créées et transmises à l'ordinateur via Kaspersky Security Center.
- **Stockages** : administration des paramètres de la quarantaine et de la sauvegarde :
  - **Quarantaine**
  - **Sauvegarde**
  - **Liste des ordinateurs bloqués**
- **Journaux et notifications** : gestion des journaux d'exécution des tâches locales, du journal de sécurité et du journal d'audit système de Kaspersky Security for Windows Server.
  - **Journaux de sécurité**
  - **Journal d'audit système**
  - **Journaux d'exécution de la tâche**
- **Licence** : ajout et suppression de clés et de codes d'activation pour Kaspersky Security for Windows Server, consultation des informations relatives aux licences.

Panneau des résultats

Le panneau de détails reprend les informations relatives au nœud sélectionné. Si vous avez choisi le nœud **Kaspersky Security**, le panneau de détails affiche des informations sur l'état actuel de la protection du serveur, sur Kaspersky Security for Windows Server, sur l'état de protection de ses composants fonctionnels et sur la date d'expiration de la licence.

Menu contextuel du nœud de Kaspersky Security

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

- **Se connecter à un autre ordinateur**. Se connecter à un autre ordinateur pour administrer la version de Kaspersky Security for Windows Server installée sur cet ordinateur. Pour effectuer cette opération, vous pouvez également cliquer sur le lien situé dans le coin inférieur droit du panneau de détails du nœud **Kaspersky Security**.
- **Démarrer le service** / **Arrêter le service**. Lancez ou arrêtez l'application 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 l'analyse des disques amovibles**. Configurez l'analyse des disques amovibles connectés via USB au serveur protégé.
- **Protection contre les exploits : paramètres généraux**. Configurez le mode Protection contre les exploits et configurez des actions de prévention.
- **Protection contre les exploits : paramètres de protection des processus**. Ajoutez des processus pour la protection et sélectionnez les techniques de protection contre les exploits.
- **Configurer les paramètres de la zone de confiance**. Consultez et configurez les paramètres de la zone de confiance.
- **Modifier les permissions utilisateur pour l'administration de l'application**. Consultez et configurez les privilèges d'accès aux fonctions de Kaspersky Security for Windows Server.
- **Modifier les droits d'utilisateurs pour l'administration du Service Kaspersky Security**. Consultez et configurez les privilèges d'accès à l'administration du Service Kaspersky Security.
- **Stockage hiérarchique**. Configurez la méthode d'accès au système HSM.
- **Exporter les paramètres**. Enregistrez 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**. Importez 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.
- **Données sur les mises à jour disponibles pour l'application et ses modules**. Affiche les informations relatives à Kaspersky Security for Windows Servers et aux mises à jour des modules de l'application disponibles.

- **Rafraîchir**. Actualisez le contenu de la fenêtre de la console d'application. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Propriétés**. Consultez et configurez les paramètres de fonctionnement de Kaspersky Security for Windows Server 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 de détails du nœud **Kaspersky Security** ou le bouton dans la barre d'outils.

- **Aide**. Consultez les informations reprises dans l'aide de Kaspersky Security for Windows Server. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Barre d'outils et menu contextuel des tâches de Kaspersky Security for Windows Server

Vous pouvez administrer les tâches de Kaspersky Security for Windows Server à l'aide des options du menu contextuel de chaque tâche dans l'arborescence de la console d'application.

A l'aide des options du menu contextuel de la tâche sélectionnée, vous pouvez exécuter les opérations suivantes :

- **Reprendre** / **Suspendre**. Reprenez ou suspendez 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 en temps réel et d'analyse à la demande.
- **Ajouter une tâche**. Créez une nouvelle tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.
- **Ouvrir le journal**. Consultez et administrez un journal d'exécution de la tâche. Cette opération est disponible pour toutes les tâches.
- **Enregistrer la tâche**. Enregistrez et appliquez les modifications apportées aux paramètres de la tâche. Cette action est disponible pour les tâches Protection des fichiers en temps réel et Analyse à la demande.
- **Supprimer la tâche**. Supprimez 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**. Administrez les modèles. Cette opération est disponible pour les tâches Protection des fichiers en temps réel et 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,*

Sélectionnez le nœud **Kaspersky Security** dans l'arborescence de la console d'application.

Par défaut, les informations du panneau de détails de la Console de Kaspersky Security for Windows Server 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 **Rafraîchir** dans le menu contextuel du nœud **Kaspersky Security**.

L'onglet **Protection des stockages réseau** dans le panneau de détails du nœud **Kaspersky Security** affiche les informations concernant l'état des périphériques de stockage NAS protégés.

La section **Protection en temps réel** affiche des informations sur la Protection ICAP des stockages réseau connectés et leur Protection RPC, ainsi que sur l'état d'intégration de Celerra/VNX (cf. tableau ci-dessous).

Tableau 2. Informations sur la Protection des stockages réseau.

Groupe Protection des stockages réseau	Informations

Indicateur de l'état 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 vert* apparaît dans le cas suivant : les tâches Protection RPC des stockages réseau connectés et Protection ICAP des stockages réseau connectés sont en cours d'exécution.
	• *Le jaune* apparaît dans les cas suivants :
	  • L'une des tâches suivantes est en cours d'exécution : Protection RPC des stockages réseau connectés ou Protection ICAP des stockages réseau connectés.
	  • Agent antivirus Celerra/VNX trouvé.
	• *Le rouge* apparaît dans le cas suivant : aucune tâche de protection n'est en cours et l'agent antivirus Celerra/VNX est trouvé.

Protection RPC des stockages réseau connectés	Le champ **Etat de la tâche** affiche l'état actuel de la tâche (par exemple, Exécution en cours ou Arrêtée). Le champ **Détecté** affiche le nombre d'objets malveillants détectés sur les dossiers partagés des stockages réseau RPC. Si le nombre de logiciels détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.

Groupe Protection des stockages réseau	Informations
Protection ICAP des stockages réseau connectés	Le champ **Etat de la tâche** affiche l'état actuel de la tâche (par exemple, Exécution en cours ou Arrêtée). Le champ **Détecté** spécifie le nombre d'objets malveillants détectés par les dossiers partagés des stockages réseau ICAP. Si le nombre de logiciels détectés dépasse 0, la valeur de la ligne est mise en évidence en rouge.
Connexion à EMC Celerra / VNX	Les valeurs suivantes sont possibles : • **Agent antivirus Celerra/VNX introuvable**. Kaspersky Security for Windows Server ne trouve aucun logiciel EMC ou une erreur s'est produite dans le code d'intégration. • **Protection désactivée**. Kaspersky Security for Windows Server a ouvert une connexion avec l'application EMC mais la tâche Protection des fichiers en temps réel n'est pas exécutée dans Kaspersky Security for Windows Server. • **Protection activée**. Kaspersky Security for Windows Server a ouvert une connexion avec l'application EMC et Kaspersky Security for Windows Server assure la Protection des fichiers en temps réel.

Le groupe **Protection contre le chiffrement** (cf. tableau ci-après) affiche des informations sur l'état actuel de la tâche Protection contre le chiffrement pour NetApp.

Tableau 3. Informations sur l'état de la protection contre le chiffrement

Groupe Contrôle	Informations
Indicateur d'état Protection contre le chiffrement	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Couleur verte du panneau : la tâche Protection contre le chiffrement pour NetApp est en cours d'exécution. • Couleur rouge du panneau : la tâche Protection contre le chiffrement pour NetApp n'est pas en cours d'exécution.
Protection contre le chiffrement pour NetApp	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Mode** : un des deux modes disponibles pour la tâche Protection contre le chiffrement pour NetApp. **Hôtes bloqués** : nombre d'hôtes compromis qui ont été bloqués lors d'une tentative d'accès aux dossiers partagés du réseau sur le serveur protégé.

Administration des tâches de protection des stockages réseau

Cette section contient des informations sur les tâches de Kaspersky Security for Windows Server, leur création, le

lancement et l'arrêt manuels ou automatiques des tâches et la configuration des paramètres d'exécution.

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 en cours d'exécution, les nouvelles valeurs des paramètres sont appliquées directement après l'enregistrement de la tâche.
- Si vous avez modifié les paramètres d'une tâche arrêtée (suspendue), les nouvelles valeurs sont 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 d'application 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 un autre nœud de la console :*

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

Lancement / suspension / rétablissement / arrêt manuel des tâches

► *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 for Windows Server.
2. Sélectionnez l'une des options : **Démarrer** ou **Arrêter**.

L'opération est effectuée et enregistrée dans le journal d'audit système.

Programmation des tâches

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

Configuration des paramètres de planification du lancement de la tâche

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

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

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

lancement.

2. Choisissez l'option **Propriétés**.
3. La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la programmation**.

   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.

5. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
   a. Choisissez une des options suivantes dans la liste **Fréquence** :
      - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
      - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
      - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence hebdomadaire que vous aurez définie dans le champ **Chaque : <nombre> semaine(s) le**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut la tâche est exécutée le lundi).
      - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security for Windows Server.
      - **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.
   b. Indiquez, dans le champ **Démarrer à**, l'heure 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 système planifiées est interdit par les paramètres d'une stratégie en vigueur de Kaspersky Security Center.

6. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.
   - Dans le groupe **Paramètres d'arrêt de la tâche** :
     a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la tâche.
     b. Cochez la case **Pause à partir de** jusqu'à 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 suspendue.
   - Dans le groupe **Paramètres avancés** :
     a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la

planification ne sera plus active.

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

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

7. Cliquez sur le bouton **Appliquer**.

Les paramètres de la planification de la tâche sélectionnées 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 de la tâche :*

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 **Exécuté selon la programmation** si vous souhaitez activer l'exécution planifiée d'une tâche.
   - Cochez la case **Exécuté selon la programmation** si vous souhaitez activer 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 du lancement planifié de la tâche seront enregistrés.

Protection des périphériques de stockage NAS EMC du groupe Celerra/VNX

Cette section fournit des informations sur la protection des stockages réseau EMC du groupe Celerra/VNX (ci-après Celerra/VNX) et sur l'intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS Celerra/VNX.

Contenu du chapitre

A propos de la protection des périphériques de stockage NAS EMC du groupe Celerra/VNX

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

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

Par défaut, Kaspersky Security for Windows Server réalise les opérations suivantes :

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

Pour pouvoir protéger le périphérique de stockage NAS, vous devez assurer l'intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS Celerra/VNX.

La protection des périphériques de stockage NAS 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 for Windows Server*.

Intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS EMC du groupe Celerra/VNX

Pour pouvoir protéger le périphérique de stockage NAS, vous devez assurer l'intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS Celerra/VNX.

L'intégration de Kaspersky Security for Windows Server au périphérique de stockage NAS Celerra/VNX a lieu si les conditions suivantes sont réunies :

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

   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 for Windows Server*.

L'état de l'intégration de Kaspersky Security for Windows Server (cf. section "Consultation d'informations concernant l'état de la Protection des stockages réseau" à la page 30) au périphérique de stockage NAS Celerra / VNX est indiqué dans le panneau des détails du nœud **Kaspersky Security**.

Protection RPC des stockages réseau connectés

Cette section fournit des informations sur la tâche Protection RPC des stockages réseau connectés, sur la configuration de la connexion entre un périphérique de stockage NAS et Kaspersky Security for Windows Server et explique également comment configurer les paramètres de la tâche Protection RPC des stockages réseau connectés ainsi que les paramètres de sécurité de la tâche.

Contenu du chapitre

A propos de la Protection RPC des stockages réseau connectés

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

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

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

Par défaut, Kaspersky Security for Windows Server réalise les opérations suivantes :

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

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

Pour profiter de la protection des périphériques de stockage NAS en temps réel, vous devez ajouter le périphérique de stockage NAS à Kaspersky Security for Windows Server dans la zone de protection et configurer une connexion entre ce périphérique de stockage NAS et le serveur doté de Kaspersky Security for Windows Server. Dans Kaspersky Security for Windows Server, une tâche de protection des stockages réseau connectés via le protocole RPC s'appelle Protection RPC des stockages réseau connectés.

La tâche Protection RPC des stockages réseau connectés est créée par défaut en tant que tâche système de Kaspersky Security for Windows Server. Vous ne pouvez pas supprimer ou renommer cette tâche. Vous ne pouvez pas créer de tâches définies par l'utilisateur de Protection RPC des stockages réseau connectés.

Vous pouvez configurer la tâche Protection RPC des stockages réseau connectés. Les paramètres configurés dans les propriétés de la tâche Protection RPC des stockages réseau connectés 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 for Windows Server ne protège pas les périphériques de stockage NAS.

Le composant Protection RPC des stockages réseau connectés est disponible dans le cadre de la solution Kaspersky Security for Windows Server pour périphériques de stockage NAS.

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

A propos 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 périphérique de stockage NAS.

L'analyse des liens symboliques dans les périphériques de stockage NAS possède les particularités suivantes. Kaspersky Security for Windows Server analyse le fichier vers lequel pointe le lien symbolique 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 for Windows Server ne l'analyse pas. Si le périphérique de stockage

NAS 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 périphérique de stockage NAS protégé est autorisé, il est conseillé de confirmer que la fonction d'analyse antivirus est activée pour tous les dossiers réseau partagés.

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

Kaspersky Security for Windows Server 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 for Windows Server et un périphérique de stockage NAS 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 for Windows Server ne protège pas les périphériques de stockage NAS.

Afin de pouvoir protéger des périphériques de stockage NAS connectés via le protocole RPC, vous devez configurer la connexion du périphérique de stockage NAS à Kaspersky Security for Windows Server.

► *Pour configurer la connexion entre le périphérique de stockage NAS et Kaspersky Security for Windows Server, procédez comme suit :*

1. Sur le serveur sur lequel est installé Kaspersky Security for Windows Server, configurez les paramètres suivants :
   - Ajout d'un périphérique de stockage NAS à Kaspersky Security for Windows Server (cf. section "Ajout d'un stockage réseau connecté via le protocole RPC à Kaspersky Security for Windows Server" à la page 42).
   - Dans la Console de Kaspersky Security for Windows Server, spécifiez le compte utilisateur sous lequel vous souhaitez exécuter la tâche Protection RPC des stockages réseau connectés (cf. section "Sélection du compte utilisateur pour le lancement de la tâche Protection RPC des stockages réseau connectés" à la page 40).

- Dans l'éditeur de stratégie de groupe local, 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 21).
- Dans la fenêtre des paramètres du pare-feu Windows, configurez les règles applicables aux connexions entrantes et sortantes dans le pare-feu Windows (cf. section "Configuration des règles applicables aux connexions entrantes et sortantes dans le pare-feu Windows" à la page 22).
- Si nécessaire, installez l'application de connexion pour le périphérique de stockage NAS connecté via le protocole RPC qui sera protégé par Kaspersky Security for Windows Server.

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

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

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

La connexion entre Kaspersky Security for Windows Server et un stockage réseau connecté via le protocole RPC est établie.

Sélection d'un compte utilisateur pour le lancement de la tâche Protection RPC des stockages réseau connectés

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

Si le périphérique de stockage NAS et le serveur doté de Kaspersky Security for Windows Server se trouvent dans le même domaine, vous pouvez utiliser le compte utilisateur du domaine. Si le périphérique de stockage NAS et le serveur doté de Kaspersky Security for Windows Server est installé se trouvent dans le même 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.

Si plusieurs comptes utilisateur existent sur Kaspersky Security for Windows Server, assurez-vous que l'utilisateur sous lequel vous configurez et démarrez la tâche Protection RPC des stockages réseau connectés est ajoutée à la liste des utilisateurs privilégiés NetApp. Si le compte utilisateur ne bénéficie pas des privilèges nécessaires sur le périphérique de stockage NAS, les dossiers partagés sont accessibles mais aucune analyse ne sera effectuée par les tâches de protection en cours.

► *Pour spécifier un compte utilisateur sous lequel la tâche Protection RPC des stockages réseau connectés va être lancée, procédez comme suit :*

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, 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 la section **Paramètres de connexion au périphérique de stockage NAS**, 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 le bouton **OK**.

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

Création de la zone de protection dans la tâche Protection RPC des stockages réseau connectés

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

Dans cette section

Ajout d'un périphérique de stockage NAS connecté via le protocole RPC à Kaspersky Security for Windows Server

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajouter une zone de protection**.
5. Dans la fenêtre **Ajouter une zone de protection**, saisissez le nom de domaine ou l'adresse IP du périphérique de stockage NAS.

   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 périphérique de stockage NAS à Kaspersky Security for Windows Server.

   Le périphérique de stockage NAS apparaît dans la liste des périphériques de stockage NAS protégés.
7. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la zone de protection définis seront enregistrés.

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

Si vous utilisez un périphérique de stockage NAS NetApp sous le système d'exploitation NetApp Clustered Data ONTAP, Kaspersky Security for Windows Server 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 for Windows Server protège le périphérique de stockage NAS ajouté.

Activation et désactivation de la protection d'un périphérique stockage NAS 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 d'application, développez le nœud **Protection des stockages réseau**.

2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des périphériques de stockage NAS protégés, décochez la case en regard du nom du périphérique de stockage NAS pour lequel vous souhaitez suspendre temporairement la protection en temps réel.
5. Cliquez sur le bouton **Enregistrer**.

Kaspersky Security for Windows Server interrompt la connexion avec le périphérique de stockage NAS sélectionné.

Si vous désactivez la fonction de protection pour tous les périphériques de stockage NAS ajoutés, Kaspersky Security for Windows Server arrête la tâche Protection RPC des stockages réseau connectés.

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des périphériques de stockage NAS protégés, cochez la case en regard du nom du périphérique de stockage NAS pour lequel vous souhaitez activer la protection.
5. Cliquez sur le bouton **Enregistrer**.

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

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des périphériques de stockage NAS protégés, sélectionnez celui que vous voulez supprimer de la zone de protection de la tâche.
5. Dans le menu contextuel du nom de la tâche ou sous l'adresse IP du périphérique de stockage NAS que vous souhaitez supprimer de la zone de protection de la tâche, sélectionnez l'entrée **Supprimer** de la liste.

Le périphérique de stockage NAS sélectionné sera supprimé de la liste des périphériques de stockage NAS protégés.

Configuration des paramètres de la tâche Protection RPC des stockages réseau connectés

Par défaut, la tâche Protection RPC des stockages réseau connectés 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 for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours. Kaspersky Security for Windows Server consigne la date et l'heure de la modification des paramètres de la tâche dans le journal d'audit système.

Tableau 4. Paramètres de la tâche Protection des périphériques de stockage NAS connectés via le protocole RPC

Paramètre	Valeur par défaut	Commentaires
Zone de protection	Absent.	Vous devez ajouter le périphérique de stockage NAS à Kaspersky Security for Windows Server.
Niveau de sécurité	Le niveau de sécurité **Recommandé** est appliqué.	Vous pouvez appliquer un des niveaux de sécurité prédéfinis à la protection du périphérique de stockage NAS ou vous pouvez définir les valeurs manuellement.
Analyse 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 des services KSN dans la tâche Protection RPC des stockages réseau connectés.
Paramètres de connexion au périphérique de stockage NAS	• **Nom d'utilisateur** et **Mot de passe** du compte utilisateur 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 ; • La case **Purger le cache des fichiers traités du périphérique de stockage NAS après la mise à jour des bases de l'application** est décochée.	Vous devez spécifier le compte utilisateur sous lequel la tâche Protection RPC des stockages réseau connectés va être lancée. Vous pouvez également modifier les autres paramètres de connexion aux périphériques de stockage NAS.

Paramètre	Valeur par défaut	Commentaires
Lancement d'une tâche planifiée	Pas appliqué. La case **Exécuté selon la programmation** est décochée. La tâche est lancée manuellement.	Vous pouvez configurer l'exécution planifiée d'une tâche, par exemple au démarrage de Kaspersky Security for Windows Server.

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, 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 :
   - Utilisation de l'analyse heuristique (à la page 46).
   - Lancement d'une tâche avec les autorisations du compte utilisateur (cf. section "Sélection du compte utilisateur pour le lancement de la tâche Protection RPC des stockages réseau connectés" à la page 40).
   - 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 48).
   - Intégration aux autres composants de Kaspersky Security for Windows Server (cf. section "Préparation au lancement de la tâche de protection des stockages réseau" à la page 21).
5. Sous les onglets **Planification** et **Avancé**, configurez les paramètres de planification du lancement de la tâche (cf. section "Configuration des paramètres de planification du lancement de la tâche" à la page 32).
6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

   Les modifications apportées aux paramètres seront enregistrées.
7. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, sélectionnez l'onglet **Configuration de la zone de protection**.
8. Exécutez les actions suivantes :
   - Ajouter un périphérique de stockage NAS connecté via le protocole RPC à la zone de protection de Kaspersky Security for Windows Server (cf. section "Ajout d'un stockage réseau connecté via le protocole RPC à Kaspersky Security for Windows Server" à la page 42).
   - Dans la liste des périphériques de stockage NAS connectés via le protocole RPC ajoutés, sélectionnez ceux dont vous souhaitez activer la protection.
   - Sélectionnez un des niveaux de sécurité prédéfinis (cf. section "Application d'un niveau de sécurité prédéfini dans la tâche Protection RPC des stockages réseau connectés" à la page 50) ou configurez les paramètres de sécurité des objets manuellement (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection RPC des stockages réseau connectés" à la page 51).
9. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server appliquera immédiatement les nouvelles valeurs des paramètres dans

la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

Utilisation de l'analyse heuristique

Dans la tâche Protection ICAP des stockages réseau connectés, vous pouvez utiliser l'analyse heuristique avec un niveau d'analyse configuré.

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, 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 **Analyse 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'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

       Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.
5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis sont appliqués

Intégration avec les autres composants de Kaspersky Security for Windows Server

Vous pouvez utiliser la tâche Protection RPC des stockages réseau connectés avec les composants opérationnels suivants de Kaspersky Security for Windows Server :

- Zone de confiance
- tâche Utilisation du KSN.

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

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

Kaspersky Security Network (KSN) est une infrastructure de services en ligne qui donne accès à la base de connaissances en ligne de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des applications.

Vous pouvez activer ou désactiver l'utilisation du KSN dans la tâche Protection RPC des stockages réseau connectés. Lorsque vous activez ou désactivez l'utilisation du KSN, la tâche commence ou arrête d'afficher des conclusion sur la réputation des fichiers analysés à partir des informations reçues du KSN.

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, 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 avec les autres composants de Kaspersky Security for Windows Server, 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 for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

     Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de

la zone de protection dans la tâche Protection des fichiers en temps réel.

Cette case est cochée par défaut.

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

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

  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 ICAP des stockages réseau connectés n'utilise pas le service KSN.

  Cette case est cochée par défaut.

5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres généraux de connexion à un périphérique de stockage NAS 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 d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, 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 périphérique de stockage NAS, réalisez les opérations suivantes :
   - Saisissez la valeur du délai d'attente entre les tentatives de restauration de la connexion au périphérique de stockage NAS.
   - Saisissez la valeur du nombre maximum de tentatives de restauration de la connexion au périphérique de stockage NAS.

     Il est recommandé de conserver les valeurs par défaut ou de les remplacer par des valeurs plus élevées.
   - Si vous souhaitez que Kaspersky Security for Windows Server purge le cache des fichiers analysés du périphérique de stockage NAS après chaque mise à jour des bases de l'application, cochez la case **Purger le cache des fichiers traités du périphérique de stockage NAS après la mise à jour des bases de l'application**.
   - Si vous souhaitez que Kaspersky Security for Windows Server conserve le cache des fichiers analysés du périphérique de stockage NAS après chaque mise à jour des bases de l'application, décochez la case **Purger le cache des fichiers traités du périphérique de stockage NAS après la mise à jour**

des bases de l'application.

5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

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

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 RPC des stockages réseau connectés.

A propos des niveaux de sécurité dans la tâche Protection RPC des stockages réseau connectés

Dans la tâche Protection RPC des stockages réseau connectés, vous pouvez appliquer à chaque périphérique de stockage NAS 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 prédéfinie (cf. tableau ci-dessous). Vous pouvez également configurer les valeurs des paramètres de sécurité manuellement. Dans ce cas, le niveau de sécurité du périphérique de stockage NAS 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 for Windows Server sur les serveurs et les postes de travail, comme des pare-feu ou le respect par les utilisateurs des stratégies de sécurité en vigueur.

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

Options	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 désinfecter. Supprimer si la désinfection est impossible	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible
Actions à exécuter sur les objets probablement infectés	Interdire l'accès et placer en quarantaine	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et placer en quarantaine
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 RPC des stockages réseau connectés

► *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 d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des périphériques de stockage NAS 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 périphérique de stockage NAS dans la liste des périphériques de stockage NAS 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 RPC des stockages réseau connectés" à la page 51).

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

► *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 d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection RPC des stockages réseau connectés**, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la liste des périphériques de stockage NAS 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 périphérique de stockage NAS sélectionné en fonction de vos exigences en matière de sécurité informatique. Pour ce faire, procédez comme suit :
   - Sous l'onglet **Général**, réalisez les actions suivantes :
     - Dans le groupe **Protection des objets**, désignez les objets qui seront analysés par Kaspersky Security for Windows Server :
       - **Tous les objets**.

         Kaspersky Security for Windows Server analyse tous les objets.
       - **Objets analysés en fonction du format**.

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

         Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

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

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

  Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

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

  Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

  Vous pouvez également configurer ce paramètre dans le périphérique de stockage NAS. Si le paramètre est configuré dans Kaspersky Security for Windows Server, le périphérique de stockage NAS envoie l'objet pour analyse et Kaspersky Security for Windows Server considère l'objet comme inoffensif sans réaliser la recherche de virus. Si le paramètre est configuré dans le périphérique de stockage NAS, 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 for Windows Server est installé, il est conseillé de définir la valeur du paramètre qui limite les objets à analyser dans le périphérique de stockage NAS.

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

- Sous l'onglet **Actions**, réalisez les actions suivantes :
  - Dans le groupe **Actions à exécuter sur les objets infectés et autres**, sélectionnez l'action réalisée par Kaspersky Security for Windows Server en cas de détection d'un objet infecté.
  - Dans le groupe **Actions à exécuter sur les objets probablement infectés**, sélectionnez l'action que Kaspersky Security for Windows Server exécutera suite à la détection d'un objet probablement infecté.
  - Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter.
  - Choisissez les actions à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case **Supprimer complètement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un élément infecté intégré**.

    La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

    Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

    Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.

    La case est cochée par défaut pour le niveau de sécurité **Protection maximale** et décochée pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- Sous l'onglet **Optimisation**, réalisez les actions suivantes :

- Dans le groupe **Exclusions**, désignez les objets que Kaspersky Security for Windows Server 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 détectables (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 détectables selon la classification de l'Encyclopédie des virus https://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.

  Si vous utilisez un périphérique de stockage NAS NetApp fonctionnant sous le système d'exploitation Clustered Data ONTAP, ce paramètre peut également être configuré dans le périphérique de stockage NAS. Si le paramètre est configuré dans Kaspersky Security for Windows Server, le périphérique de stockage NAS envoie l'objet pour analyse et Kaspersky Security for Windows Server considère l'objet comme inoffensif sans réaliser la recherche de virus. Si le paramètre est configuré dans le périphérique de stockage NAS, 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 for Windows Server est installé, il est conseillé de définir la valeur du paramètre qui limite les objets à analyser dans le périphérique de stockage NAS.

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 RPC des stockages réseau connectés

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

Création d'un modèle de paramètres de sécurité

► *Pour enregistrer manuellement les paramètres de sécurité du nœud et les enregistrer dans le modèle, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security for Windows Server sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le panneau de détails 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 de fichier réseau, sélectionnez le modèle que vous souhaitez consulter.
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 le bouton **OK**.

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

Vous pouvez également passer à la création d'un modèle de paramètres pour les tâches d'analyse à la demande depuis le panneau de détails du nœud principal **Analyse à la demande**.

Application du modèle de paramètres de sécurité

► *Pour appliquer les modèles de sécurité du modèle au nœud sélectionné, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security for Windows Server, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le panneau de détails 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 le nœud 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 de paramètres de sécurité sera appliqué au nœud sélectionné dans l'arborescence des ressources fichier du serveur. Sous l'onglet **Niveau de sécurité** du nœud sélectionné, la valeur **Personnalisé** apparaît.

Les paramètres de sécurité du modèle appliqués au nœud parent dans l'arborescence des ressources fichier du serveur sont appliqués à tous les nœuds enfants.

Si la zone de protection ou la zone d'analyse des nœuds enfants dans l'arborescence des ressources fichier du serveur a été configurée séparément, les paramètres de sécurité du modèle appliqués au nœud parent ne sont pas appliqués automatiquement aux nœuds enfants.

► *Pour appliquer les modèles de sécurité du modèle à toutes les entrées sélectionnées, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Security for Windows Server, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le panneau de détails 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 le nœud 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 de paramètres de sécurité est appliqué au nœud parent et à tous les nœuds enfants dans l'arborescence des ressources fichier du serveur. Sous l'onglet **Niveau de sécurité** du nœud sélectionné, la valeur **Personnalisé** apparaît.

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 d'application, 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 de détails du nœud principal **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 **Options** 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 :*

1. Dans l'arborescence de la console d'application, 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 de détails du nœud principal 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. Cliquez sur **Oui** dans la fenêtre qui s'ouvre.

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 RPC des stockages réseau connectés

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection RPC des stockages réseau connectés**.
3. Dans le panneau de détails, choisissez l'onglet **Consultation et administration**.

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

Tableau 6. Statistiques complètes de la tâche Protection des stockages réseau via le protocole RPC

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security for Windows Server. Par exemple, si Kaspersky Security for Windows Server a découvert un logiciel dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	Nombre d'objets que Kaspersky Security for Windows Server a détectés et classés comme infectés ou nombre de fichiers de logiciels légitimes trouvés qui n'ont pas été exclus de la zone d'action des tâches de la protection en temps réel et des tâches à la demande et que des intrus peuvent utiliser pour endommager votre ordinateur.
Objets probablement infectés détectés	Nombre d'objets découverts par Kaspersky Security for Windows Server et considérés comme probablement infectés.
Objets non désinfectés	Nombre d'objets que Kaspersky Security for Windows Server n'a pas pu désinfecter pour les raisons suivantes : • le type d'objet détecté ne peut être désinfecté ; • Une erreur s'est produite lors de la désinfection.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Security for Windows Server a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.

Champ	Description
Objets non supprimés	Nombre d'objets que Kaspersky Security for Windows Server 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 for Windows Server n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Security for Windows Server 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 désinfectés	Nombre d'objets désinfectés par Kaspersky Security for Windows Server.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Security for Windows Server.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security for Windows Server.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Security for Windows Server.
Objets protégés par mot de passe	Nombre d'objets (archives, par exemple) que Kaspersky Security for Windows Server a ignorés en raison d'une protection par mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Security for Windows Server a ignorés à cause de leur format endommagé.
Objets traités	Nombre d'objets traités par Kaspersky Security for Windows Server.

Protection ICAP des stockages réseau connectés

Cette section fournit des informations sur la tâche Protection ICAP des stockages réseau connectés, sur la configuration de la connexion entre un périphérique de stockage NAS et Kaspersky Security for Windows Server et explique également comment configurer les paramètres de la protection et de la sécurité des stockages réseau connectés via ICAP.

Contenu du chapitre

A propos de la Protection ICAP des stockages réseau connectés

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

Kaspersky Security for Windows Server 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 ICAP des stockages réseau connectés, Kaspersky Security for Windows Server ne peut pas supprimer ou bloquer des fichiers utilisés par des stockages de réseau connectés ICAP car au moment de la réception d'une conclusion douteuse 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 conclusion douteuse sont consignées dans le journal d'exécution de la tâche Utilisation du KSN.

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

La tâche Protection ICAP des stockages réseau connectés est créée par défaut en tant que tâche système de Kaspersky Security for Windows Server. Vous ne pouvez pas supprimer ou renommer cette tâche. Vous ne pouvez pas créer de tâches définies par l'utilisateur de Protection ICAP des stockages réseau connectés. Vous pouvez configurer la tâche Protection ICAP des stockages réseau connectés.

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 for Windows Server ne protège pas les périphériques de stockage NAS.

Le composant Protection ICAP des stockages réseau connectés est disponible dans le cadre de la solution Kaspersky Security for Windows Server for NAS.

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 for Windows Server*.

Configuration de la connexion entre Kaspersky Security for Windows Server et un périphérique de stockage NAS 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 for Windows Server ne protège pas les périphériques de stockage NAS.

Afin de pouvoir protéger des périphériques de stockage NAS connectés via le protocole ICAP, vous devez configurer la connexion du périphérique de stockage NAS à Kaspersky Security for Windows Server.

► *Pour configurer la connexion entre le périphérique de stockage NAS et Kaspersky Security for Windows Server, procédez comme suit :*

1. Sur le serveur sur lequel est installé Kaspersky Security for Windows Server, configurez les paramètres suivants :
   - Dans la Console de l'application, définissez les paramètres de connexion à un périphérique de stockage NAS connecté via le protocole ICAP que Kaspersky Security for Windows Server (cf. section "Configuration des paramètres de connexion à un stockage réseau connecté via le protocole ICAP" à la page 62) doit protéger.
   - Dans l'éditeur de stratégie de groupe local, 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 21).
   - Dans la fenêtre des paramètres du pare-feu Windows, configurez les règles applicables aux connexions entrantes et sortantes dans le pare-feu Windows (cf. section "Configuration des règles applicables aux connexions entrantes et sortantes dans le pare-feu Windows" à la page 22).
2. Configurez les paramètres suivants dans le périphérique de stockage NAS :
   - Activez la fonction de protection antivirus.
   - Indiquez l'adresse de connexion à Kaspersky Security for Windows Server dans les paramètres du périphérique de stockage NAS.

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

   La connexion entre Kaspersky Security for Windows Server et un stockage réseau connecté via le protocole ICAP est établie.

Configuration des paramètres de la tâche Protection ICAP des stockages réseau connectés

Par défaut, la tâche Protection ICAP des stockages réseau connectés 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 for Windows Server applique immédiatement les nouvelles valeurs des paramètres à la tâche en cours. Kaspersky Security for Windows Server consigne la date et l'heure de la modification des paramètres de la tâche dans le journal d'audit système.

Tableau 7. Paramètres de la tâche Protection des périphériques de stockage NAS 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 périphérique de stockage NAS ou vous pouvez définir les valeurs manuellement.
Analyse 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 des services KSN pour la Protection ICAP des stockages réseau connectés.
Paramètres de connexion au périphérique de stockage NAS	• **Numéro de port réseau** – 1344. • **Identification du service** – avscan.	Vous pouvez également modifier les autres paramètres de connexion aux périphériques de stockage NAS. Ces modifications doivent être prises en compte dans les périphériques de stockage NAS.
Lancement d'une tâche planifiée	Pas appliqué. La case **Exécuté selon la programmation** est décochée. La tâche est lancée manuellement.	Vous pouvez configurer l'exécution planifiée d'une tâche, par exemple au démarrage de Kaspersky Security for Windows Server.

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, 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 62).
   - Utilisation de l'analyse heuristique (à la page 63).
   - Utilisation du KSN pour la protection (cf. section "Utilisation du KSN pour la protection" à la page 64).

   Dans le groupe **Niveau de sécurité** :
   - Sélectionnez un des niveaux de sécurité prédéfinis (cf. section "A propos des niveaux de sécurité dans la tâche Protection ICAP des stockages réseau connectés" à la page 65) ou configurez les paramètres de sécurité des objets manuellement (cf. section "Configuration manuelle des paramètres du niveau de sécurité dans la tâche Protection RPC des stockages réseau connectés" à la page 67).
5. Sous les onglets **Planification** et **Avancé**, configurez les paramètres de planification du lancement de la tâche (cf. section "Programmation des tâches" à la page 32).
6. Cliquez sur le bouton **OK**.

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

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général**, saisissez les données suivantes dans les champs de la section **Paramètres de connexion** :
   - **Numéro de port réseau**

     Numéro du port réseau du serveur ICAP pour la connexion du périphérique de stockage NAS 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, ces paramètres serviront pour créer l'adresse RESPMOD URI suivante : `icap://192.168.10.10/avscan:1344`.
5. Cliquez sur le bouton **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 for Windows Server et la renseigner dans le périphérique de stockage NAS. 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 for Windows Server>/avscan:1344
```

Utilisation de l'analyse heuristique

Dans la tâche Protection ICAP des stockages réseau connectés, vous pouvez utiliser l'analyse heuristique avec un niveau d'analyse configuré.

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, 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 **Analyse 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'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

       Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.
5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis sont appliqués

Utilisation du KSN pour la protection

Kaspersky Security Network (KSN) est une infrastructure de services en ligne qui donne accès à la base de connaissances en ligne de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des applications.

Vous pouvez activer ou désactiver l'utilisation du KSN dans la tâche Protection RPC des stockages réseau connectés. Lorsque vous activez ou désactivez l'utilisation du KSN, la tâche commence ou arrête d'afficher des conclusion sur la réputation des fichiers analysés à partir des informations reçues du KSN.

Vous devez accepter la Déclaration de 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 for Windows Server.

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, 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 KSN pour la protection**.

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

   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 ICAP des stockages réseau connectés n'utilise pas le service KSN.

   Cette case est cochée par défaut.
5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

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

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 Protection ICAP des stockages réseau connectés.

A propos des niveaux de sécurité dans la tâche Protection ICAP des stockages réseau connectés

Dans la tâche Protection ICAP des stockages réseau connectés, vous pouvez appliquer à chaque périphérique de stockage NAS 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 prédéfinie (cf. tableau ci-dessous). Vous pouvez également configurer les valeurs des paramètres de sécurité manuellement. Dans ce cas, le niveau de sécurité du périphérique de stockage NAS 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 for Windows Server sur les serveurs et les postes de travail, comme des pare-feu ou le respect par les utilisateurs des stratégies de sécurité en vigueur.

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

Options	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

Options	Niveau de sécurité		
Actions à exécuter sur les objets infectés et autres	Désinfecter	Exécute l'action recommandée	Désinfecter
Actions à exécuter sur les objets probablement infectés	Quarantaine	Exécute l'action recommandée	Quarantaine
Exclure les fichiers	non	non	non
Ne pas détecter	non	non	non
Arrêter si l'analyse dure plus de (s.)	60	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 ICAP des stockages réseau connectés

► *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 d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, 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 le bouton **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 ICAP des stockages réseau connectés" à la page 67).

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

► *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 d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.
3. Dans le panneau de détails du nœud **Protection ICAP des stockages réseau connectés**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général** de la section **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 :
   - Sous l'onglet **Général**, réalisez les actions suivantes :
     - Dans le groupe **Protection des objets**, désignez les objets qui seront analysés par Kaspersky Security for Windows Server :
       - **Tous les objets**.

         Kaspersky Security for Windows Server analyse tous les objets.
       - **Objets analysés en fonction du format**.

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

         Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.
       - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**.

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

         Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.
       - **Objets analysés en fonction de la liste d'extensions indiquée**.

         Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

> Vous pouvez également configurer ce paramètre dans le périphérique de stockage NAS. Si le paramètre est configuré dans Kaspersky Security for Windows Server, le périphérique de stockage NAS envoie l'objet pour analyse et Kaspersky Security for Windows Server considère l'objet comme inoffensif sans réaliser la recherche de virus. Si le paramètre est configuré dans le périphérique de stockage NAS, 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 for Windows Server est installé, il est conseillé de définir la valeur du paramètre qui limite les objets à analyser dans le périphérique de stockage NAS.

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

- Sous l'onglet **Actions**, réalisez les actions suivantes :
  - Dans le groupe **Actions à exécuter sur les objets infectés et autres**, sélectionnez l'action réalisée par Kaspersky Security for Windows Server en cas de détection d'un objet infecté.
  - Dans le groupe **Actions à exécuter sur les objets probablement infectés**, sélectionnez l'action que Kaspersky Security for Windows Server exécutera suite à la détection d'un objet probablement infecté.
  - Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter.
- Sous l'onglet **Optimisation**, réalisez les actions suivantes :
  - Dans le groupe **Exclusions**, désignez les objets que Kaspersky Security for Windows Server 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 détectables (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 détectables selon la classification de l'Encyclopédie des virus https://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 le bouton **OK**.

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

Consultation des statistiques de la tâche Protection ICAP des stockages réseau connectés

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

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

1. Dans l'arborescence de la Console d'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection ICAP des stockages réseau connectés**.

Sous l'onglet **Consultation et administration** du panneau de détails, le groupe **Statistiques** reprend un tableau qui affiche les informations sur les objets que Kaspersky Security for Windows Server a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 9. Statistiques de la tâche Protection RPC des stockages réseau connectés

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Security for Windows Server. Par exemple, si Kaspersky Security for Windows Server a découvert une application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	Nombre d'objets que Kaspersky Security for Windows Server a détectés et classés comme infectés ou nombre de fichiers de logiciels légitimes trouvés qui n'ont pas été exclus de la zone d'action des tâches de la protection en temps réel et des tâches à la demande et que des intrus peuvent utiliser pour endommager votre ordinateur.
Objets probablement infectés détectés	Nombre d'objets découverts par Kaspersky Security for Windows Server et considérés comme probablement infectés.
Objets non désinfectés	Nombre d'objets que Kaspersky Security for Windows Server n'a pas pu désinfecter pour les raisons suivantes : • Le type d'objet détecté ne peut être désinfecté. • une erreur s'est produite lors de la désinfection.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Security for Windows Server 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 for Windows Server 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 for Windows Server n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Security for Windows Server 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 désinfectés	Nombre d'objets désinfectés par Kaspersky Security for Windows Server.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Security for Windows Server.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security for Windows Server.

Champ	Description
Objets supprimés	Nombre d'objets supprimés par Kaspersky Security for Windows Server.
Objets protégés par mot de passe	Nombre d'objets (archives, par exemple) que Kaspersky Security for Windows Server a ignorés en raison d'une protection par mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Security for Windows Server a ignorés à cause de leur format endommagé.
Objets traités	Nombre d'objets traités par Kaspersky Security for Windows Server.

Protection contre le chiffrement pour NetApp

Cette section contient des informations sur la tâche Protection contre le chiffrement pour NetApp et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la Protection contre le chiffrement pour NetApp

La Protection contre le chiffrement pour NetApp protège les dossiers des périphériques de stockage NAS contre le chiffrement malveillant. En cas de détection d'un chiffrement malveillant, Kaspersky Security for Windows Server interdit l'accès aux dossiers du périphérique de stockage NAS protégé.

Pour fonctionner sur le périphérique de stockage NAS, Kaspersky Security for Windows Server doit être connecté à un stockage protégé en tant que *moteur externe*. La connexion implique la réception de notifications relatives aux opérations sur les fichiers qui ont été réalisées par le moteur externe sur un périphérique de stockage NAS protégé, l'analyse des comportements des opérations sur les fichiers reçues et l'envoi des conclusions sur l'activité sur les fichiers (tentative de chiffrement malveillant potentiel ou non) et le blocage des hôtes compromis. Pour lancer la tâche Protection contre le chiffrement pour NetApp, le serveur (doté de Kaspersky Security for Windows Server) doit être désigné en tant que serveur FPolicy principal du côté du périphérique de stockage NAS. *FPolicy* est un cadre de notification d'accès aux fichiers qui permet de contrôler et de gérer les événements d'accès aux fichiers sur les machines virtuelles de stockage (SVM) avec volumes FlexVol. Le cadre génère des notifications qui sont envoyées aux serveurs FPolicy externes.

Le serveur Fpolicy n'est pas pris en charge pour les volumes FlexGroup. Par conséquent, le composant Protection contre le chiffrement pour NetApp peut être configuré pour protéger les périphériques de stockage NAS avec des volumes FlexGroup.

Les notifications d'un périphérique de stockage NAS à un serveur externe sont envoyées via le protocole FPolicy, uniquement en mode synchrone. Le serveur analyse chaque notification avant d'autoriser une opération sur les fichiers.

Le moteur externe (Kaspersky Security for Windows Server) et un périphérique de stockage NAS protégé sont connectés via le protocole FPolicy.

Pour configurer la protection, vous devez :

1. Créer et configurer FPolicy du côté du périphérique de stockage NAS protégé.
2. Désigner Kaspersky Security for Windows Server en tant que serveur FPolicy du côté du périphérique de stockage NAS protégé. Kaspersky Security for Windows Server est alors reconnu en tant que serveur externe.
3. Configurer la tâche Protection contre le chiffrement pour NetApp dans Kaspersky Security for Windows Server.

Pour finaliser la configuration requise, vous aurez besoin des données suivantes :

- nom de la machine SVM.
- Adresse IP du serveur externe et le nom qui lui a été affecté.
- Liste complète des nœuds de cluster d'un périphérique de stockage NAS protégé avec leurs noms.
- Adresse de l'interface de gestion du cluster.
- Le nom du FPolicy créé.
- Port pour établir une connexion sécurisée entre le périphérique de stockage NAS protégé et le moteur externe.
- Les identifiants (nom d'utilisateur et mot de passe) :
  - pour un utilisateur autorisé à accéder aux dossiers partagés du périphérique de stockage NAS ;
  - pour l'administrateur local du CDOT.

Tous ces paramètres doivent être définis lors de la création de FPolicy (cf. section "Création et configuration de FPolicy" à la page 73) et lors de la configuration de la tâche Protection contre le chiffrement pour NetApp sur Kaspersky Security for Windows Server (cf. section "Configuration de la tâche Protection contre le chiffrement pour NetApp" à la page 78).

Pour obtenir de plus amples informations sur la création de FPolicy, consultez l'article https://library.netapp.com/ecmdocs/ECMP12454941/html/GUID-DDFB957B-CE0F-4603-9629-669653B1E922.html.

Création et configuration de FPolicy

Si vous créez un FPolicy pour la première fois, les experts de Kaspersky Lab conseillent d'appliquer la configuration spécifiée dans le tableau suivant :

Tableau 10. Configuration de FPolicy

Paramètre	Chaîne	Valeur	Remarque
_EVENT CREATE Ce paramètre identifie les opérations sur les fichiers qui vont être interceptées et signalées à Kaspersky Security for Windows Server pour l'analyse et la détection de tentatives de chiffrement malveillant.	**Nom Vserver**	<nom_svm>	Doit correspondre à la valeur définie dans les paramètres de la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe (Kaspersky Security for Windows Server).
	Evénement	<source_événements>	Servira de source pour FPolicy.
	Protocole	cifs	
	Opérations sur les fichiers	create, open, rename, write, close, setattr, delete	
	Filtres	close-with-modification, first-write, write-with-size-change, open-with-delete-intent, open-with-write-intent	
	Opération sur volume requise	false	
_ENGINE CREATE Ce paramètre détermine les paramètres de connexion à un moteur externe (ou au serveur FPolicy).	**Nom Vserver**	<nom_svm>	Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.
	Moteur	<nom_du moteur>	Nom du moteur externe. Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.
	Serveurs FPolicy principaux	<ip_serveur_principal>	Un seul serveur est autorisé.

Paramètre	Chaîne	Valeur	Remarque
	Numéro de port du service FPolicy	<numéro_port>	1346 est conseillé. Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.
	Serveurs FPolicy secondaires	<ip_serveur_secondaire>	Si un serveur principal est sélectionné, le serveur secondaire n'est pas disponible.
	Type de moteur externe	Synchrone	Le mode asynchrone n'est pas pris en charge.
	Option SSL pour la communication externe	No-auth	
	FQDN ou CCN	-	
	Numéro de série du certificat	-	
	Autorité de certification	-	
_POLICY CREATE Ce paramètre détermine la configuration de FPolicy à venir.	**Nom Vserver**	<nom_svm>	Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.
	Fpolicy	<Nom_FPolicy>	Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.
	Evénements à surveiller	<source_événements>	
	Moteur FPolicy	<nom_du moteur>	Nom de chaîne du moteur externe. Doit correspondre à la valeur définie dans la tâche Protection contre le chiffrement pour NetApp du côté du moteur externe.

Paramètre	Chaîne	Valeur	Remarque
	Analyse obligatoire requise	true	
	Autoriser l'accès privilégié	oui	
	Nom d'utilisateur pour l'accès privilégié	<nom_utilisateur>	La même valeur doit être spécifiée dans les paramètres de la tâche Protection contre le chiffrement pour NetApp pour le champ Identifiants pour accéder aux dossiers partagés sur le périphérique de stockage NAS.
	Lecture en transfert direct activée	false	
_SCOPE CREATE Ce paramètre détermine la zone de protection couverte par le moteur externe.	**Nom Vserver**	<nom_svm>	Nous vous recommandons de définir la zone la plus large possible pour protéger le périphérique de stockage NAS. Nous vous recommandons d'ajouter des exclusions dans les paramètres de la tâche Protection contre le chiffrement pour NetApp.
	Stratégie	<Nom_FPolicy>	

Nous vous recommandons de spécifier les valeurs mises en évidence comme dans le tableau. Les autres valeurs peuvent varier en fonction de vos exigences.

Si les paramètres de FPolicy sont modifiés sur le périphérique de stockage NAS pendant l'exécution de la tâche Protection contre le chiffrement pour NetApp, vous devez redémarrer cette tâche pour appliquer les nouveaux paramètres.

Configuration de Kaspersky Security for Windows Server

Pour établir la connexion entre le composant Protection contre le chiffrement pour NetApp de Kaspersky Security for Windows Server et un périphérique de stockage NAS protégé, vous devez configurer les paramètres de la Protection contre le chiffrement pour NetApp (cf. tableau ci-dessous).

Tableau 11. Configuration de la Protection contre le chiffrement pour NetApp

Paramètre	Valeurs possibles	Par défaut
Mode	• Statistiques uniquement • Actif	Actif
Analyse heuristique	Superficielle - Moyenne - Minutieuse	Appliqué au niveau d'analyse heuristique "Moyenne".
Exclusions	Appliqué à tous les dossiers partagés protégés. Critères d'exclusion : • Masque (dossier, objet, extension) • Adresse IP de l'ordinateur client • Utilisateur de confiance	Non définie
Adressage	• Adresse IP du cluster • Liste complète des clusters • Les identifiants (nom d'utilisateur et mot de passe) pour l'administrateur local du CDOT. Le paramètre suivant dédouble la valeur qui a été configurée pour le paramètre _POLICY CREATE (nom d'utilisateur pour la chaîne d'accès privilégié) Les identifiants (nom d'utilisateur et mot de passe) pour l'utilisateur autorisé à accéder aux dossiers partagés du périphérique de stockage NAS. Les paramètres suivants dédoublent les valeurs qui ont été configurées pour le paramètre _ENGINE CREATE du côté du périphérique de stockage NAS. • Nom FPolicy • Nom SVM (Vserver) • Port (1346)	Non définie
Paramètres de planification	-	Non définie

Utilisation du Stockage des ordinateurs bloqués

Le Stockage des ordinateurs bloqués est rempli quand les conditions suivantes sont remplies :

- La tâche Protection contre le chiffrement pour NetApp a été lancée en mode **Actif**.
- La Protection contre le chiffrement pour NetApp détecte une tentative de chiffrement malveillant sur des dossiers partagés NetApp.

Après la détection de la tentative de chiffrement malveillant, le composant Protection contre le chiffrement pour NetApp envoie les informations relatives à l'hôte compromis au **Stockage de la liste des ordinateurs bloqués**. Ensuite, Kaspersky Security for Windows Server crée un événement critique pour le blocage d'hôte et interdit l'exécution d'opérations sur n'importe quel fichier depuis cet hôte.

Par défaut, Kaspersky Security for Windows Server bloque les hôtes 30 minutes après leur ajout à la liste. L'accès de l'ordinateur aux ressources de fichier réseau est rétabli automatiquement après sa suppression de la liste des ordinateurs douteux.

Vous pouvez modifier le contenu de la liste de la Liste des ordinateurs bloqués :

- Débloquer les hôtes manuellement.
- Configurer les conditions d'interdiction.

Lors de la configuration de la Protection contre le chiffrement pour NetApp, faites attention au type de moteur externe utilisé dans les paramètres de FPolicy (paramètre _ENGINE CREATE).

Kaspersky Security for Windows Server enregistre dans le journal l'événement avec la conclusion obtenue et réalise une action en fonction du mode de tâche.

Kaspersky Security for Windows Server prend en charge deux configurations possible :

#	**Mode périphérique de stockage NAS**	**Mode Protection contre le chiffrement pour NetApp**	**Description**
1	Synchrone	Statistiques uniquement	Cette configuration offre une protection contre le chiffrement malveillant en mode d'audit : l'application enregistre uniquement les événements de chiffrement malveillant dans le journal. Vous pouvez passer à la configuration 2 depuis Kaspersky Security for Windows Server.
2	Synchrone	Actif	Cette configuration offre une protection complète : tous les hôtes compromis sont stockés dans le Stockage des ordinateurs bloqués, n'importe quelle opération sur les fichiers exécutée par ces hôtes sont bloquées. Vous pouvez passer à la configuration 1 depuis un périphérique de stockage NAS protégé ou depuis un serveur externe.

Pour obtenir de plus amples informations sur la configuration du Stockage des ordinateurs bloqués, consultez le Manuel de l'administrateur ou le Manuel de l'utilisateur de Kaspersky Security for Windows Server.

Configuration de la tâche Protection contre le chiffrement pour NetApp

Définissez les paramètres du serveur externe et du périphérique de stockage NAS pour lancer et configurer la tâche Protection contre le chiffrement pour NetApp.

Configuration des paramètres de la tâche via la Console de Kaspersky Security for Windows Server

► *Pour configurez les paramètres de la tâche Protection contre le chiffrement pour NetApp :*

1. Dans l'arborescence de la console d'application développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection contre le chiffrement pour NetApp**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général**, configurez les paramètres suivants :
   - Sélectionnez le mode de tâche dans la section **Mode de tâche**.
   - Le groupe **Analyse heuristique** permet de configurer l'utilisation et le niveau d'analyse.
5. Sous l'onglet **Adressage**, configurez les paramètres de connexion et d'authentification (cf. section "Configuration de l'adressage" à la page 80).
6. Sous les onglets **Planification** et **Avancé**, configurez les paramètres de planification du lancement de la tâche.
7. Cliquez sur le bouton **OK**.

► *Pour créer la liste d'exclusions pour la tâche Protection contre le chiffrement pour NetApp :*

1. Dans l'arborescence de la console d'application développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection contre le chiffrement pour NetApp**.
3. Dans le panneau de détails, cliquez sur le lien **Liste d'exclusions**.

   La fenêtre **Liste d'exclusions** s'ouvre.
4. Configurez la liste d'exclusions (cf. section "Modification de la liste des exclusions" à la page 81).

Configuration des paramètres de la tâche via Kaspersky Security Center

► *Pour configurer la tâche Protection contre le chiffrement pour NetApp :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Pour configurer les paramètres de l'application pour un groupe de serveurs, ouvrez l'onglet **Stratégies**, puis les propriétés de la stratégie que vous souhaitez configurer.

3. Dans la section **Protection des stockages réseau**, cliquez sur le bouton **Configuration** du groupe **Protection contre le chiffrement pour NetApp**.
4. Sous l'onglet **Général**, configurez le mode de tâche et l'analyse heuristique.
5. Sous l'onglet **Adressage**, configurez les paramètres de connexion et d'authentification (cf. section "Configuration de l'adressage" à la page 80).
6. Sous l'onglet **Exclusions**, ajoutez des exclusions à la zone de protection (cf. section "Modification de la liste des exclusions" à la page 81).
7. Sous l'onglet **Administration des tâches**, lancez la tâche sur la base d'une planification.
8. Cliquez sur le bouton **OK**.

Configuration des paramètres de tâche généraux

► *Pour configurer la tâche Protection contre le chiffrement pour NetApp :*

1. Sous l'onglet **Général**, configurez les paramètres suivants :
   - Mode de tâche :
     - **Statistiques uniquement**

       Choisissez cette option pour recevoir des notifications sur les tentatives détectées de chiffrement malveillant de fichier. L'application crée des événements dans le journal d'exécution de la tâche.

     - **Actif**

       Sélectionnez cette option pour interdire les opérations sur les fichiers réalisées par les hôtes compromis d'un périphérique de stockage NAS protégé. L'application ajoute les hôtes au Stockage des ordinateurs bloqués en cas de détection d'une tentative de chiffrement malveillant de fichier. Toute opération sur un fichier en provenance de cet hôte sera bloquée pendant la durée définie dans les paramètres du stockage.
   - Analyse heuristique :
     - Cochez ou décochez la case **Utiliser l'analyse heuristique**.

       La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

       Si la case est cochée, l'analyse heuristique est activée.

       Si la case est décochée, l'analyse heuristique est désactivée.

       Cette case est cochée par défaut.
     - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

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

Il existe trois niveaux de détail pour l'analyse

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

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

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

2. Sous l'onglet **Adressage**, configurez les paramètres de connexion et d'authentification (cf. section "Configuration de l'adressage" à la page 80).
3. Sous l'onglet **Exclusions**, ajoutez des exclusions à la zone de protection (cf. section "Modification de la liste des exclusions" à la page 81).
4. Sous l'onglet **Administration des tâches**, lancez la tâche sur la base d'une planification.
5. Cliquez sur le bouton **OK**.

Configuration de l'adressage

► *Pour configurer une connexion avec des clusters protégés et accéder au périphérique de stockage NAS :*

1. Ouvrez l'onglet **Adressage** dans les paramètres de la tâche.
2. Dans la section **Connexion**, configurez les éléments suivants :
   - **Adresse IP de la grappe protégée**

     Indiquez l'adresse IP du cluster. Un cluster contient les types de Vserver suivants :

     - Vserver admin
     - Vserver du nœud
     - Vserver du cluster
   - **Nom Vserver**

     Indiquez un nom de serveur de stockage virtuel.
   - **Nom FPolicy**

     Saisissez le nom de FPolicy. Avant que FPolicy ne puisse surveiller les accès aux fichiers, il faut créer une configuration FPolicy et l'activer sur le Vserver qui a besoin des services FPolicy.
   - **Port**

3. Pour modifier la liste des nœuds de cluster protégés :
   a. Dans la section **Connexion**, cliquez sur la **liste des nœuds de cluster**.
   b. Saisissez le nom du nœud.
   c. Cliquez sur **Ajouter**.
   d. Cliquez sur le bouton **OK**.

   > Tous les nœuds existants d'un cluster protégé doivent être ajoutés à la liste.

4. Dans la section **Authentification**, saisissez :
   - Les identifiants d'un utilisateur avec accès privilégié aux dossiers du périphérique de stockage : nom d'utilisateur et mot de passe.

     > Ce compte doit correspondre au compte qui a été défini lors de l'opération _POLICY CREATE du côté du périphérique de stockage NAS.

   - Les identifiants d'un administrateur CDOT : nom d'utilisateur et mot de passe.
5. Cliquez sur le bouton **OK** dans la fenêtre **Protection contre le chiffrement pour NetApp**.

Les paramètres d'adressage définis sont enregistrés.

Modification de la liste des exclusions

Vous pouvez ajouter des exclusions sur la base de trois critères :

- Chemin d'accès
- Adresse IP
- ID utilisateur

Vous pouvez utiliser n'importe quelle combinaison de ces critères pour définir une exclusion. Plus le nombre de critères définis augmente, plus les paramètres d'exclusion sont stricts. Kaspersky Security for Windows Server n'analyse pas les opérations sur les fichiers pour les exclusions définies. Sachez que les exclusions ajoutées à cette liste sont utilisées pour tous les dossiers partagés sur un périphérique de stockage NAS.

> Si vous configurez simultanément la protection antivirus et FPolicy sur le même périphérique de stockage NAS, l'accès aux dossiers partagés de stockage est possible uniquement si les tâches Protection RPC des stockages réseau connectés et Protection contre le chiffrement pour NetApp sont en cours d'exécution.

Le moteur externe doit comporter une seule carte d'interface réseau avec une seule adresse IP.

► *Pour ajouter une entrée à la liste des exclusions ou pour modifier celle-ci :*

1. Ouvrez l'onglet **Liste d'exclusions** dans les paramètres de la tâche.
2. Cochez la case **Ne pas détecter le chiffrement malveillant pour les exclusions définies**.

   Si la case est cochée, toutes les opérations su les fichiers exécutées par l'utilisateur/l'adresse IP/le chemin d'accès dans la liste en-dessous sont autorisées.

   Si la case est décochée, Kaspersky Security for Windows Server détecte les activités de chiffrement malveillant pour tous les hôtes, utilisateurs et chemins d'accès.

   Cette case est décochée par défaut.

   La liste des exclusions devient active.
3. Cliquez sur **Ajouter**.

   La fenêtre **Paramètres d'exclusion** s'ouvre.
4. Pour ajouter une exclusion sur la base d'un masque :
   a. Sous l'onglet **Chemin**, cochez la case **Exclure selon un masque de chemin**.
   b. Saisissez le chemin.
   c. Cliquez sur **Ajouter**.
5. Pour ajouter une exclusion sur la base d'une adresse IP :
   a. Sous l'onglet **Adresses IP**, cochez la case **Exclure selon l'adresse IP de l'ordinateur client**.
   b. Saisissez l'adresse IP.
   c. Cliquez sur **Ajouter**.
6. Pour ajouter une exclusion définie par l'utilisateur :
   a. Sous l'onglet **Utilisateurs**, cochez la case **Exclure selon l'utilisateur**.
   b. Cliquez sur **Ajouter**.

      La fenêtre **Sélection des utilisateurs** s'ouvre.
   c. Sélectionnez l'utilisateur ou le groupe que vous souhaitez exclure.
   d. Cliquez sur le bouton **OK**.
7. Dans la fenêtre **Paramètres d'exclusion**, cliquez sur le bouton **OK**.

   La liste des exclusions est enrichie des exceptions définies.

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 <AN_NAME>.

Contenu du chapitre

A 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 for Windows Server.

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

Tâche de Protection des stockages réseau	Options
Protection RPC des stockages réseau connectés	Le bouton **Configuration** de la section **Protection RPC des stockages réseau connectés** permet de configurer les paramètres suivants de la tâche : • Précisez la zone de protection. • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de sécurité ; • Configurez l'utilisation de l'analyse heuristique. • Configurez l'application de la zone de confiance et du KSN. • Configurez les paramètres de connexion au périphérique de stockage NAS. • Configurez les paramètres de lancement de la tâche.
Protection ICAP des stockages réseau connectés	Le bouton **Configuration** de la section **Protection ICAP des stockages réseau connectés** permet de configurer les paramètres suivants de la tâche : • Configurez l'utilisation de l'analyse heuristique. • Configurez les paramètres de connexion au périphérique de stockage NAS. • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de sécurité ; • Configurez l'utilisation du KSN. • Configurez les paramètres de lancement de la tâche.
Protection contre le chiffrement pour NetApp	Le bouton **Configuration** de la section **Protection contre le chiffrement pour NetApp** permet de configurer les paramètres suivants : • Mode de tâche. • Configuration de l'analyse heuristique • Paramètres d'authentification au serveur proxy • Précisez les exclusions de la zone de protection ;

► *Pour 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 Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez la stratégie que vous souhaitez configurer, puis ouvrez la fenêtre **Propriétés <nom de la stratégie>** d'une des manières suivantes :
     a. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.
     b. Dans le panneau de droite des détails du nœud sélectionné, cliquez sur le lien **Configurer la stratégie**.
     c. Double-cliquez sur la stratégie sélectionnée.
   - Pour configurer l'application sur un seul serveur :
     a. Sous l'onglet **Périphériques**, ouvrez la fenêtre **Propriétés : <Nom de l'ordinateur>** à l'aide d'une des méthodes suivantes :
        - Double-clic sur le nom du serveur protégé.
        - Ouvrez le menu contextuel du nom du serveur protégé et sélectionnez l'option Propriétés.

        La fenêtre **Propriétés : <Nom de l'ordinateur>** s'ouvre.
     b. Dans la section **Tâches**, sélectionnez une tâche à configurer.
3. Lors de la configuration d'une stratégie, sélectionnez **Protection des stockages réseau** dans la liste de sections de la fenêtre **Propriétés : <Nom de la stratégie>**.
4. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Si vous souhaitez configurer les paramètres de la tâche Protection RPC des stockages réseau connectés, dans la section **Protection RPC des stockages réseau connectés**, cliquez sur le bouton **Configuration**.

     Dans la fenêtre **Options** qui s'ouvre, configurez les paramètres de la tâche en fonction de vos exigences. Cliquez sur le bouton **OK** pour enregistrer les modifications des paramètres dans la stratégie.
   - Si vous souhaitez configurer les paramètres de la tâche Protection ICAP des stockages réseau connectés, dans la section **Protection ICAP des stockages réseau connectés**, cliquez sur le bouton **Configuration**.

     Dans la fenêtre **Options** qui s'ouvre, configurez les paramètres de la tâche en fonction de vos exigences (cf. section "Configuration des paramètres de la tâche Protection ICAP des stockages réseau connectés" à la page 61). Cliquez sur le bouton **OK** pour enregistrer les modifications des paramètres dans la stratégie.
   - Si vous souhaitez configurer les paramètres de la tâche Protection contre le chiffrement pour NetApp, cliquez sur le bouton **Configuration** dans la section **Protection contre le chiffrement pour NetApp**.

     Dans la fenêtre **Options** qui s'ouvre, configurez les paramètres de la tâche en fonction de vos exigences (cf. section "Configuration des paramètres de la tâche Protection contre le chiffrement pour NetApp" à la page 78). Cliquez sur le bouton **OK** pour enregistrer les modifications des paramètres dans la stratégie.
5. 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 for Windows Server 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 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, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau de détails, sous l'onglet **Périphériques**, ouvrez le menu contextuel de la ligne reprenant les informations relatives au serveur protégé, puis sélectionnez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés : <Nom de l'ordinateur>** de la section **Tâches**, 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 :
   - Tâche Protection RPC des stockages réseau connectés (cf. section "Configuration des paramètres de la tâche Protection RPC des stockages réseau connectés" à la page 44).
   - Tâche Protection ICAP des stockages réseau connectés.
5. Cliquez sur le bouton **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 for Windows Server 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 for Windows Server*.

Contacter le Support Technique

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

Contenu du chapitre

Modes d'obtention de l'assistance technique

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

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

Avant de contacter le Support Technique, veuillez lire les règles d'octroi de l'assistance technique.

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

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

Assistance technique via Kaspersky CompanyAccount

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

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte utilisateur Kaspersky CompanyAccount. À l'aide d'un seul compte, vous pouvez centraliser l'administration des demandes électroniques envoyées par les employés à Kaspersky Lab et gérer les droits d'accès de ces employés à Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

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

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

Utilisation du fichier de trace et du script AVZ

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Security for Windows Server à envoyer au Support Technique de Kaspersky Lab. Les experts du Support Technique de Kaspersky Lab peuvent également vous demander de créer un fichier de trace. Le fichier de trace permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

L'analyse des données que vous envoyez permet aux experts du Support technique de Kaspersky Lab de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus actifs, de rechercher la présence éventuelle de menaces sur l'ordinateur, de désinfecter ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse de l'ordinateur.

Pour une assistance plus efficace en cas de questions sur l'utilisation de l'application, les experts du Support Technique peuvent vous demander (pour la réparation) de modifier les paramètres de l'application pendant les diagnostics. Pour ce faire, l'exécution des actions suivantes peut être requise :

- Activer la fonctionnalité de traitement et stockage des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules séparés de l'application, qui n'est pas disponibles via les outils standards de l'interface d'utilisateur.
- Modifier les paramètres de conservation et d'envoi des informations diagnostiques qui ont été traitées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Kaspersky Lab

Kaspersky Lab est connu dans le monde entier pour ses systèmes de protection contre diverses menaces numériques telles que les virus et autres applications malveillantes, les emails indésirables (spams), les attaques de réseaux et les piratages.

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

Kaspersky Lab a été fondée en Russie en 1997. La société est devenue un groupe international qui compte 38 bureaux dans 33 pays. L'entreprise emploie plus de 3 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des systèmes de contrôle industriel et la prévention des escroqueries financières. Ces solutions, associées à des outils d'administration centralisée, permettent de créer et d'exploiter une protection automatisée efficace de l'entreprise de n'importe quelle taille contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands laboratoires d'essai. Elles sont compatibles avec les logiciels de nombreux fournisseurs et sont optimisées pour une exécution sur de nombreuses plateformes.

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

Technologie. De nombreuses technologies, sans lesquelles les antivirus actuels ne seraient pas ce qu'ils sont, ont justement été mises au point par Kaspersky Lab. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu ou ZyXEL. Beaucoup des innovations technologiques de l'entreprise sont brevetées.

Résultats. Au cours de ses années de lutte contre les menaces informatiques, Kaspersky Lab a remporté de nombreux prix. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais pour Kaspersky Lab, la plus grande récompense de toutes, c'est la fidélité des utilisateurs à travers le monde. Les produits et les technologies de la société assurent la protection de plus de 400 millions de particuliers et plus de 270 000 entreprises.

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

Information sur le code tiers

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

Avis de marques déposées

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

Citrix, XenApp et XenDesktop sont des marques de Citrix Systems, Inc. et/ou d'une ou plusieurs de ses filiales et peuvent être enregistrées au bureau des marques et brevets (Patent and Trademark Office) aux Etats-Unis et dans d'autres pays.

Dell et Dell Compellent sont des marques de Dell, Inc.

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

Hitachi est une marque de Hitachi, Ltd.

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

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

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

Oracle est une marque déposée d'Oracle Corporation et/ou de ses filiales.

Glossaire

A

Analyse heuristique

Technologie de détection des menaces dont les informations ne figurent pas encore dans les bases de Kaspersky Lab. L'analyse heuristique permet de détecter des objets dont le comportement dans le système d'exploitation peut constituer une menace pour la sécurité. Les objets identifiés à l'aide de l'analyse heuristique sont considérés comme probablement infectés. Par exemple, un objet qui contient une succession de commandes propres à des objets malveillants (ouverture d'un fichier, écriture dans le fichier) pourrait être considéré comme probablement infecté.

Archive

Un ou plusieurs fichiers repris dans un fichier compressé. Une application dédiée, appelée archiveur, est requise pour le compactage et le décompactage des données.

B

Bases antivirus

Bases de données qui contiennent les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les bases antivirus sont composées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

E

Etat de la protection

Etat actuel de la protection, qui reflète le niveau de sécurité de l'ordinateur.

F

Fichier probablement infectable

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

K

Kaspersky Security Network (KSN)

Infrastructure de services cloud donnant accès à la base de données de Kaspersky Lab avec des informations constamment mises à jour sur la réputation des fichiers, les ressources Internet et le logiciel. Kaspersky Security Network assure une vitesse de réaction plus élevée que les applications de Kaspersky Lab face aux nouvelles menaces, augmente l'efficacité de certains composants de la protection et réduit la possibilité de faux positifs.

M

Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

N

Niveau de sécurité

Le niveau de sécurité est décrit comme un ensemble pré-configuré de paramètres de composants de l'application.

O

Objet OLE

Objet lié à un autre fichier ou imbriqué dans un autre fichier via la technologie Object Linking and Embedding (OLE). Exemple d'objet OLE : feuille de calcul Microsoft Office Excel® imbriquée dans un document Microsoft Office Word.

Objets de démarrage

Ensemble d'applications nécessaires au démarrage et au fonctionnement corrects du système d'exploitation et au logiciel installé sur l'ordinateur. Objets de démarrage : objets que le système d'exploitation charge au démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

Protection en temps réel

Mode de fonctionnement de l'application sous lequel celle-ci analyse les objets pour y détecter la présence d'un code malveillant en temps réel.

L'application intercepte toutes les tentatives d'ouverture d'objet (lecture, écriture ou exécution) et analyse les objets pour y détecter les menaces. Les objets non infectés sont transmis à l'utilisateur ; les objets contenant des menaces ou les objets probablement infectés sont traités en fonction des paramètres de la tâche (désinfecté, supprimé ou en quarantaine).

Q

Quarantaine

Dossier dans lequel l'application de Kaspersky Lab déplace les objets probablement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

S

Sauvegarde

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

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction de centralisation des informations relatives aux applications de Kaspersky Lab installées sur le réseau de la société et qui permet de les administrer. Il permet également de gérer ces applications.

Stratégie

Une stratégie détermine les paramètres d'une application gère l'accès à la configuration d'une application installée sur les ordinateurs d'un groupe d'administration. Une stratégie individuelle doit être créée pour chaque application. Vous pouvez créer un nombre illimité de stratégies pour les applications installées sur les ordinateurs dans chaque groupe d'administration mais une seule stratégie à la fois peut être appliquée à chaque application dans un groupe d'administration.

T

Témoin du niveau d'importance de l'événement

Propriété d'un événement rencontré pendant le fonctionnement d'une application Kaspersky Lab. Gravité de l'événement : niveau de gravité de l'événement.

- Evénement critique.
- Erreur.
- Avertissement.
- Info.

Les événements du même type peuvent avoir différents niveaux de gravité en fonction de la situation de survenue de l'événement.

U

Un objet infecté a été découvert

Objet dont une portion de code correspond parfaitement à une partie du code d'une application malveillante connue. Kaspersky Lab ne recommande pas d'accéder à ces objets.

Un objet suspect a été détecté

Fichier contenant soit le code modifié d'un virus connu, soit du code évoquant un virus, mais toujours inconnu de Kaspersky Lab. Les objets suspects sont détectés par analyse heuristique.

V

Vulnérabilité

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

Index

C

F

I