



Kaspersky Security 10 for Windows Server

Manuel d'installation

Version de l'application : 10

Chers utilisateurs !

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

Attention ! Ce document demeure la propriété de Kaspersky Lab AO (puis dans le texte Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, en tout ou en partie, est passible de poursuites civile, administrative ou judiciaire conformément à la législation applicable.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et informatives.

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

Kaspersky Lab ne pourra être tenue responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Date d'édition : 16/02/2016

© 2016 AO Kaspersky Lab. Tous droits réservés.

<http://www.kaspersky.com/fr>

<http://support.kaspersky.fr>

Table des matières

A propos de ce document	6
Dans ce document	6
Conventions	9
Sources d'informations sur Kaspersky Security	11
Sources de données pour des consultations indépendantes	11
Discussion sur les logiciels de Kaspersky Lab sur le forum	13
Configurations logicielle et matérielle requises	14
Configuration requise pour le serveur sur lequel Kaspersky Security est installé.....	14
Configuration requise pour le stockage réseau protégé	17
Configuration requise pour l'ordinateur sur lequel la console de Kaspersky Security est installée	18
Kaspersky Security	20
Modules logiciels de Kaspersky Security et code pour le service Windows Installer	24
Composants logiciels de Kaspersky Security	24
Composants logiciels de la sélection « Outils d'administration »	29
Journal d'installation et de suppression de Kaspersky Security	30
Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer	30
Modifications dans le système après l'installation de Kaspersky Security	41
Processus de Kaspersky Security	46
Planification de l'installation	47
Sélection des outils d'administration	47
Sélection du mode d'installation	49
Installation et suppression de l'application à l'aide de l'Assistant	51
Installation à l'aide de l'assistant d'installation	51
Installation de Kaspersky Security sur le serveur protégé	52
Installation de la console de Kaspersky Security	56
Configuration avancée après l'installation de la console de Kaspersky Security sur un autre ordinateur	58

À propos des autorisations d'accès au service Kaspersky Security Management	59
Autorisation des connexions réseau pour le service Kaspersky Security Management Service	60
Autorisation des connexions de réseau pour la Console de Kaspersky Security dans Microsoft Windows	61
Actions après l'installation de Kaspersky Security	64
Configuration et lancement de la tâche de mise à jour des bases de données de Kaspersky Security	65
Analyse rapide.....	67
Modification de la liste des composants et restauration de Kaspersky Security	68
Suppression à l'aide de l'Assistant d'installation.....	70
Suppression de Kaspersky Security sur le serveur protégé	70
Suppression de la console de Kaspersky Security	71
Installation et suppression de l'application via la ligne de commande	73
Présentation de l'installation et de la suppression de Kaspersky Security via la ligne de commande	74
Exemples d'instructions pour l'installation de Kaspersky Security.....	74
Actions après l'installation de Kaspersky Security	76
Ajout et suppression de composants Exemples d'instructions	78
Suppression de Kaspersky Security. Exemples d'instructions	78
Codes de retour	79
Installation et suppression de Kaspersky Anti-Virus via Kaspersky Security Center	80
Présentation générale de l'installation via Kaspersky Security Center	80
Privilèges pour l'installation ou la suppression de Kaspersky Security	81
Procédure d'installation de Kaspersky Security via Kaspersky Security Center	82
Actions après l'installation de Kaspersky Security	84
Création et lancement de la tâche de groupe de mise à jour des bases de données de l'application.....	86
Création et lancement de la tâche de groupe d'analyse des serveurs et attribution de l'état de tâche d'analyse des zones critiques	87
Installation de la console de Kaspersky Security via Kaspersky Security Center	88
Suppression de Kaspersky Security via Kaspersky Security Center	89
Installation et suppression de Kaspersky Anti-Virus via les stratégies de groupe Active Directory	90
Installation de Kaspersky Security via les stratégies de groupe Active Directory	90

Actions après l'installation de Kaspersky Security	91
Suppression de Kaspersky Security via les stratégies de groupe Active Directory ...	92
Migration depuis une version antérieure de l'application	93
Migration des paramètres de Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ..	94
Migration des paramètres de Kaspersky Anti-Virus 8.0 for Servers Enterprise Edition Service Pack 1	95
Vérification des fonctions de Kaspersky Security. Utilisation du virus d'essai EICAR ...	96
Présentation du virus d'essai EICAR	96
Vérification des fonctions « Protection en temps réel » et « Analyse à la demande » de Kaspersky Security	98
Schémas de déploiement de Kaspersky Security	101
Protection des stockages à connexion directe (DAS)	102
Protection des clusters	103
Protection des serveurs de terminaux	105
Protection des stockages réseau	106
Contacter le Support Technique	108
Modes d'obtention de l'assistance technique	108
Assistance technique via Kaspersky CompanyAccount	109
Assistance technique par téléphone	110
Utilisation du fichier de trace et du script AVZ	110
Glossaire	111
AO KASPERSKY LAB	117
Informations sur le code tiers	119
Avis de marques déposées	120
Index	121

A propos de ce document

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

Vous pouvez utiliser les informations de ce guide pour exécuter les tâches suivantes :

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

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

Dans cette section

Dans ce document	6
Conventions	9

Dans ce document

Le Manuel d'installation de Kaspersky Security contient les sections suivantes.

Sources d'informations sur Kaspersky Security

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

Configurations logicielle et matérielle requises

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

Kaspersky Security

Cette section décrit les fonctions et les modules de Kaspersky Security.

Planification de l'installation

Cette section décrit les outils d'administration de Kaspersky Security et les particularités de l'installation de Kaspersky Security à l'aide de l'Assistant d'installation, via la ligne de commande et via Kaspersky Security Center, ainsi que les stratégies de groupe d'Active Directory®.

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

Cette section explique la procédure d'installation et de suppression de Kaspersky Security et de la console de Kaspersky Security sur le serveur protégé à l'aide de l'Assistant d'installation. Elle fournit également des informations sur la configuration complémentaire de Kaspersky Security et sur les actions à réaliser après l'installation de Kaspersky Security.

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

Cette section décrit les particularités de l'installation et de la suppression de Kaspersky Security via la ligne de commande. Elle fournit également des exemples de commande pour l'installation et la suppression de Kaspersky Security et des exemples de commande pour l'ajout et la suppression de modules de Kaspersky Security.

Installation et suppression de Kaspersky Anti-Virus via Kaspersky Security Center

Cette section fournit des informations d'ordre général sur l'installation de Kaspersky Security via Kaspersky Security Center, décrit les procédures d'installation et de désinstallation de Kaspersky Security via Kaspersky Security Center et présente également les opérations à réaliser après l'installation de l'application.

Installation et suppression de Kaspersky Anti-Virus via les stratégies de groupe Active Directory

Cette section décrit l'installation et la suppression de Kaspersky Security via des stratégies de groupe Active Directory et présente les actions à réaliser après l'installation de l'application via les stratégies de groupe d'Active Directory.

Migration depuis une version antérieure de l'application

Cette section présente les paramètres des versions installées qui sont conservés par Kaspersky Security 10 for Windows Server, leur nom et les valeurs qu'ils reçoivent après la migration.

Vérification de la configuration de Kaspersky Security. Utilisation du virus d'essai EICAR

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

Schémas de déploiement de Kaspersky Security

Cette section décrit les schémas de déploiement dans le cadre de l'utilisation de Kaspersky Security pour protéger des stockages DAS, des clusters, des serveurs de terminaux et des stockages réseau.

Contacter le Support Technique

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

Glossaire

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

AO KASPERSKY LAB

Cette section contient des informations sur AO Kaspersky Lab.

Informations sur le code tiers

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

Avis de marques déposées

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

Index

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

Conventions

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

Tableau 1. Conventions

Exemple de texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui pourraient avoir des conséquences fâcheuses.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires et des conseils.
Exemple :	Les exemples sont présentés sur un fond jaune sous le titre « Exemple ».
La <i>mise à jour</i> , c'est ... L'événement <i>Bases dépassées</i> survient.	Les éléments suivants sont en italique dans le texte : <ul style="list-style-type: none">• nouveaux termes ;• noms des états et des événements de l'application.
Appuyez sur la touche ENTER . Appuyez sur la combinaison des touches ALT+F4 .	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère « + » représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton Activer .	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.

Exemple de texte	Description de la convention
<p>► <i>Pour programmer une tâche, procédez comme suit :</i></p>	<p>Les phrases d'introduction des instructions sont en italique et possèdent l'icône « flèche ».</p>
<p>Dans la ligne de commande, saisissez le texte <code>help</code></p> <p>Les informations suivantes s'affichent :</p> <p>Indiquez la date au format <code>JJ:MM:AA.</code></p>	<p>Les types de texte suivants apparaissent dans un style spécial :</p> <ul style="list-style-type: none"> • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir via le clavier.
<p><Nom d'utilisateur></p>	<p>Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les chevrons sont omis.</p>

Sources d'informations sur Kaspersky Security

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

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

Dans cette section

Sources de données pour des consultations indépendantes	11
Discussion sur les logiciels de Kaspersky Lab sur le forum	13

Sources de données pour des consultations indépendantes

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

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

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab (cf. section « Contacter le Support Technique » à la page [108](#)).

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

Page de Kaspersky Security sur le site Web de Kaspersky Lab

La page de Kaspersky Security 10 for Windows Server

(<http://www.kaspersky.fr/business-security/windows-server-security>) fournit des informations générales sur l'application, sur ses fonctionnalités et ses particularités.

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

Page de Kaspersky Security dans la base de connaissances

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

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

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

Sauvegardes de Kaspersky Security

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

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

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

Le manuel d'implantation pour la protection des référentiels réseau reprend les informations relatives à la configuration et à l'utilisation de Kaspersky Security 10 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 en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs sur notre forum (<http://forum.kaspersky.fr>).

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

Configurations logicielle et matérielle requises

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

Dans cette section

Configuration requise pour le serveur sur lequel Kaspersky Security est installé	14
Configuration requise pour le stockage réseau protégé	17
Configuration requise pour l'ordinateur sur lequel la console de Kaspersky Security est installée	18

Configuration requise pour le serveur sur lequel Kaspersky Security est installé

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

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

Configuration matérielle requise pour le serveur

Recommandations d'ordre général :

- systèmes compatibles x86-64 avec un ou plusieurs processeurs ;
- Espace disque requis :
 - pour l'installation de tous les modules de l'application : 70 Mo ;
 - pour le téléchargement et le stockage des bases antivirus de l'application : 2 Go (recommandé) ;
 - pour l'enregistrement des fichiers en quarantaine et dans la sauvegarde : 400 Mo (recommandé) ;
 - pour l'enregistrement des journaux : 1 Go (recommandé).

Configuration minimale :

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

Configuration recommandée :

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

Configuration logicielle requise pour le serveur

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

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

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

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

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

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

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

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

Configuration requise pour le stockage réseau protégé

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

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

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

Configuration matérielle requise pour l'ordinateur

Mémoire vive recommandée : 128 Mo minimum.

Espace disque disponible : 30 Mo.

Configuration logicielle requise pour l'ordinateur

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

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

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

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional ;
- Microsoft Windows 10 Enterprise / Professional.

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

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

Kaspersky Security

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

Vous pouvez installer Kaspersky Security les serveurs suivants :

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

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

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

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

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

Modules et fonctions de Kaspersky Security

L'application intègre les modules suivants :

- Protection en temps réel.

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

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

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

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

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

- Analyse à la demande.

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

L'application peut remplir les fonctions suivantes :

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

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

- Quarantaine.

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

- Sauvegarde.

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

- Notifications de l'administrateur et des utilisateurs.

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

- Importation et exportation des paramètres.

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

- Application des modèles.

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

- Enregistrement des événements.

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

- Stockage hiérarchique.

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

- Zone de confiance.

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

- Administration des autorisations.

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

Dans cette section

Modules logiciels de Kaspersky Security et code pour le service Windows Installer	24
Journal d'installation et de suppression de Kaspersky Security	30
Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer.....	30
Modifications dans le système après l'installation de Kaspersky Security.....	41
Processus de Kaspersky Security.....	46

Modules logiciels de Kaspersky Security et code pour le service Windows Installer

Par défaut, les fichiers \server\ks4ws_x86(x64).msi installent tous les composants logiciels de Kaspersky Security à l'exception du composant Analyse des scripts (Script Checker). Vous pouvez activer l'installation du composant lors de l'installation personnalisée de l'application.

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

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

Dans cette section

Composants logiciels de Kaspersky Security.....	24
Composants logiciels de la sélection « Outils d'administration ».....	29

Composants logiciels de Kaspersky Security

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

Tableau 2. Description des composants logiciels de Kaspersky Security

Composant	Code	Fonction exécutée
Fonction principale	Core	Ce composant contient une sélection de fonctions de base de l'application et garantit leur fonctionnement.

Composant	Code	Fonction exécutée
Contrôle du lancement des applications	APPCtrl	<p>Ce composant surveille les tentatives de lancement des applications par les utilisateurs et autorise ou interdit le lancement des applications conformément aux règles définies.</p> <p>Le composant exécute la tâche Contrôle du lancement des applications.</p>
Protection antivirus	AVProtection	<p>Ce composant garantit la protection antivirus et reprend les composants suivants :</p> <ul style="list-style-type: none"> • Analyse à la demande ; • Blocage de l'accès aux fichiers réseau ; • Protection contre le chiffrement ; • Protection des stockages réseau connectés via le protocole ICAP ; • Protection des stockages réseau connectés via le protocole RPC ; • Protection des fichiers en temps réel ; • Analyse des scripts ;
Analyse à la demande	Ods	<p>Ce composant installe les fichiers système de Kaspersky Security et les fichiers qui exécutent les tâches d'analyse à la demande (analyse des objets du serveur protégé exécutée à la demande).</p> <p>Si lors de l'installation de Kaspersky Security via la ligne de commande vous désignez d'autres composants de Kaspersky Security sans le composant Core, celui-ci sera installé automatiquement.</p>

Composant	Code	Fonction exécutée
Blocage de l'accès aux fichiers réseau	HostBlocker	<p>Ce composant bloque l'accès aux fichiers réseau pour les ordinateurs d'où provient une activité malveillante.</p> <p>Le composant exécute la tâche Blocage de l'accès aux fichiers réseau.</p> <p>Il contient le composant Protection contre le chiffrement.</p>
Protection contre le chiffrement	Anticryptor	<p>Ce composant ajoute à la liste des ordinateurs douteux tous les périphériques distants à l'origine d'une activité de chiffrement.</p> <p>Le composant exécute la tâche Protection contre le chiffrement.</p>
Protection des fichiers en temps réel	Oas	<p>Ce composant réalise l'analyse antivirus des fichiers sur le serveur protégé lorsque ces fichiers sont sollicités.</p> <p>Le composant exécute la tâche Protection des fichiers en temps réel.</p>
Protection des stockages réseau connectés via le protocole ICAP	ICAPStorageProtection	<p>Ce composant exécute la tâche Protection des stockages réseau connectés via le protocole ICAP (analyse des fichiers placés dans les dossiers partagés du stockage réseau connectés via le protocole ICAP en cas de tentative de lecture ou de modification de ceux-ci depuis des postes clients).</p>

Composant	Code	Fonction exécutée
Protection des stockages réseau connectés via le protocole RPC	NetApp	Ce composant exécute la tâche Protection des stockages réseau connectés via le protocole RPC (analyse des fichiers placés dans les dossiers partagés du stockage réseau connectés via le protocole RPC en cas de tentative de lecture ou de modification de ceux-ci depuis des postes clients).
Analyse des scripts	ScriptChecker	<p>Ce composant analyse le code des scripts créés à l'aide des technologies Microsoft Windows Script Technologies. L'analyse a lieu lors de la tentative d'exécution de scripts.</p> <p>Le composant exécute la tâche Analyse des scripts.</p>
Utilisation de Kaspersky Security Network	KSN	<p>Ce module offre une protection sur la base des technologies cloud de Kaspersky Lab.</p> <p>Le composant exécute la tâche Utilisation du KSN (envoi de requêtes au service Kaspersky Security Network et réception des résultats).</p>
Module d'intégration à l'agent d'administration Kaspersky Security Center	AKIntegration	<p>Garantit la connexion entre Kaspersky Anti-Virus et l'agent d'administration Kaspersky Security Center.</p> <p>Vous pouvez installer ce composant sur le serveur protégé si vous avez l'intention d'administrer l'application via Kaspersky Security Center.</p>

Composant	Code	Fonction exécutée
Sélection de compteurs de performance de l'application « System Monitor ».	PerfMonCounters	Le composant installe la sélection de compteurs de performance de l'application « System Monitor ». Ces compteurs permettent de mesurer les performances de Kaspersky Security et de localiser les éventuels goulots d'étranglement lors de l'utilisation de Kaspersky Security avec d'autres applications.
Prise en charge du protocole SNMP	SnmpSupport	Le composant publie les compteurs et les pièges de Kaspersky Security via le service Simple Network Management Protocol (SNMP) de Microsoft Windows. Vous pouvez installer ce composant sur le serveur protégé uniquement si le service Microsoft SNMP est installé sur le serveur.
Icône de Kaspersky Security	TrayApp	Le composant affiche l'icône de Kaspersky Security dans la zone de notification de la barre des tâches du serveur protégé. L'icône de Kaspersky Security affiche l'état de la protection du serveur, permet d'ouvrir la console de Kaspersky Security (si elle est installée) et la fenêtre A propos du logiciel .
Utilitaire de la ligne de commande	Shell	Permet d'administrer Kaspersky Security via la ligne de commande du serveur protégé.

Composants logiciels de la sélection

« Outils d'administration »

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

Tableau 3. Description des composants logiciels de la sélection « Outils d'administration »

Composant	Code	Fonctions du composant
Composant logiciel enfichable Kaspersky Security	MmcSnapin	<p>Le composant installe le composant logiciel enfichable Microsoft Management Console pour l'administration via la console de Kaspersky Security.</p> <p>Si lors de l'installation de la sélection « Outils d'administration » via la ligne de commande vous désignez d'autres composants de la sélection sans le composant MmcSnapin, celui-ci sera installé automatiquement.</p>
Aide	Help	<p>Fichier Chm de l'aide ; conservé dans le dossier avec les fichiers de Kaspersky Security. Vous pouvez ouvrir le fichier de l'aide au départ du menu Démarrer.</p>
Documentation	Docs	<p>Les documents « Manuel de l'administrateur », « Manuel d'installation » et « Manuel d'implantation pour la protection des stockages réseau » au format PDF sont conservés dans le dossier de Kaspersky Security ; vous pouvez ouvrir le « Manuel de l'administrateur » depuis le menu Démarrer.</p>

Journal d'installation et de suppression de Kaspersky Security

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

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

► *Pour installer Kaspersky Security en créant un fichier journal ks4ws.log sur le disque C:\, exécutez l'instruction suivante :*

- `msiexec /i ks4ws_x86.msi /l*v C:\ks4ws.log /qn EULA=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\ks4ws.log /qn EULA=1`

Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer

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

Tableau 4. Paramètres d'installation et arguments dans Windows Installer

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
Acceptation des termes du contrat de licence Utilisateur final	Rejet des termes du contrat de licence	EULA=<valeur> 0 : vous n'acceptez pas les termes du contrat de licence Utilisateur final 1 : vous acceptez les termes du contrat de licence Utilisateur final	Vous devez accepter les termes du contrat de licence Utilisateur final pour pouvoir installer Kaspersky Security.
Analyse des processus actifs et des secteurs d'amorçage des disques locaux avant l'installation (Rechercher la présence éventuelle de virus sur l'ordinateur)	Ne pas réaliser l'analyse	PRESCAN=<valeur> 0 : ne pas exécuter l'analyse avant l'installation ; 1 : exécuter l'analyse avant l'installation.	Il est conseillé de lancer l'analyse des processus actifs et des secteurs d'amorçage des disques locaux avant l'installation car la présence d'un code malveillant dans ces secteurs de l'ordinateur peut nuire à la bonne installation de Kaspersky Security. L'analyse peut durer plusieurs minutes. Si des processus dangereux ou suspects sont découverts pendant l'analyse, ils sont supprimés de la mémoire de l'ordinateur (les fichiers exécutables des processus ne sont pas supprimés). Dans

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			ce cas, les informations relatives aux applications en cours d'exécution peuvent être perdues. Par conséquent, il est recommandé de quitter toute les applications en cours d'exécution avant de lancer l'analyse.
Dossier cible	<p>Kaspersky Security : %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10 for Windows Server Outils d'administration : %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10 for Windows Server Admins Tools</p> <p>Dans la version 64 bits de Microsoft Windows : %ProgramFiles (x86)%.</p>	INSTALLDIR=<chemin d'accès complet au répertoire>	<p>Dossier qui abritera les fichiers de Kaspersky Security lors de son installation.</p> <p>Vous pouvez indiquer un autre dossier.</p>

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
Lancement de la protection des fichiers en temps réel et de l'analyse des scripts au démarrage de Kaspersky Security (Activer la protection en temps réel après l'installation de l'application)	Démarrer	RUNRTP=<valeur> 1 : démarrer ; 0 : ne pas démarrer.	Activez ce paramètre pour lancer la protection des fichiers en temps réel et l'analyse des scripts au lancement de Kaspersky Security (recommandé).
Exclusions de l'analyse, recommandées par Microsoft Corporation (Ajouter les exclusions recommandées par Microsoft)	Exclure.	ADDMSEXCLUSION=<valeur> 1 : exclure ; 0 : ne pas exclure.	Dans la tâche Protection des fichiers en temps réel sont exclus de la zone de protection les objets du serveur que Microsoft Corporation recommande d'exclure. Certains programmes sur le serveur peuvent devenir instables lorsque les logiciels antivirus interceptent ou modifient les fichiers auxquels ces applications font appel. Ainsi, Microsoft Corporation inclus

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			certaines logiciels chargés du contrôle des domaines dans cette catégorie.
Exclusions de l'analyse recommandées par Kaspersky Lab (Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions)	Exclure.	ADDKLEXCLUSION=<valeur> 1 : exclure ; 0 : ne pas exclure.	Dans la tâche Protection des fichiers en temps réel sont exclus de la zone de protection les objets du serveur que Kaspersky Lab recommande d'exclure.
Exclusion des programmes d'administration à distance du traitement (Ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions)	Ne pas ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions	RADMINEXCLUSION=<valeur> 1 : ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions. 0 : ne pas ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions.	Quand vous lancez l'utilitaire Radmin, Kaspersky Security y découvre un programme malveillant potentiel et supprime son module exécutable du disque du serveur. Kaspersky Security attribue à ces objets le nom not-a-virus:RemoteAdmin*. Si vous avez l'intention d'utiliser un utilitaire d'administration à distance après

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			<p>l'installation de Kaspersky Security, vous pouvez exclure cet objet du traitement par l'application à l'aide du paramètre d'installation Ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions</p> <p>Vous pouvez exclure l'utilitaire d'administration à distance du traitement dans la tâche Protection des fichiers en temps réel et dans les tâches d'Analyse à la demande après l'installation de Kaspersky Security (cf. document « <i>Kaspersky Security 10 for Windows Server. Manuel de l'administrateur</i> »).</p>

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
Chemin d'accès au fichier clé (Clé)	Dossier de la distribution \server	LICENSEKEYPATH=<nom_fichier_clé>	<p>Par défaut, le programme d'installation tente de trouver le fichier clé avec l'extension .key dans le dossier \server de la distribution.</p> <p>Si le répertoire \server contient plusieurs fichiers de licence, le programme d'installation choisit le fichier dont la clé possède la date de fin de validité la plus lointaine.</p> <p>Vous pouvez enregistrer au préalable le fichier clé dans le répertoire \server ou indiquer un autre chemin d'accès au fichier clé à l'aide du paramètre Ajout d'une clé.</p> <p>Vous pouvez ajouter un argument après l'installation de Kaspersky Security à l'aide de l'outil d'administration que</p>

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			<p>vous aurez choisi, par exemple via la console de Kaspersky Security. Si vous n'ajoutez pas la clé de l'application lors de son installation, Kaspersky Security ne fonctionnera pas.</p> <p>Vous trouverez plus d'informations sur la licence de l'application dans le <i>Manuel de l'administrateur de Kaspersky Security 10 for Windows Server</i>.</p>
Chemin d'accès au fichier de configuration	Désactivé	CONFIGPATH=<nom_fichier_configuration>	<p>Kaspersky Security importe les paramètres depuis le fichier de configuration indiqué et créé dans l'application.</p> <p>Kaspersky Security n'importe pas les mots de passe contenus dans le fichier de configuration tels que les mots de passe des comptes utilisateur d'exécution de tâches ou les mots de passe de connexion au</p>

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			<p>serveur proxy. Après l'importation des paramètres, vous devrez saisir tous les mots de passe manuellement.</p> <p>Si vous ne désignez pas le fichier de configuration, Kaspersky Security fonctionnera après l'installation selon les paramètres par défaut.</p>
Autorisation des connexions de réseau pour la Console de Kaspersky Security	Désactivée	<p>ADDWFEXCLUSION=<valeur></p> <p>1 : autoriser ;</p> <p>0 : ne pas autoriser.</p>	<p>Utilisez ce paramètre si vous installez Kaspersky Security non pas sur le serveur protégé mais sur un autre ordinateur. Cette console permet d'administrer à distance la protection du serveur.</p> <p>Le port TCP 135 sera ouvert dans le pare-feu de Microsoft Windows, les connexions réseau seront autorisées pour le fichier exécutable du processus d'administration à distance de Kaspersky</p>

Paramètre	Valeur par défaut	Argument Windows Installer et valeurs	Description
			<p>Security kavfsrcn.exe et l'accès aux applications DCOM sera ouvert.</p> <p>Après l'installation, ajoutez les utilisateurs chargés de l'administration à distance de Kaspersky Security au groupe KAVWSEE Administrators sur le serveur et si le serveur fonctionne sous Microsoft Windows Server 2008, autorisez sur celui-ci les connexions réseau pour le service d'administration de Kaspersky Security (fichier kavfsgt.exe).</p> <p>Vous pouvez consulter les informations sur la procédure de configuration complémentaire lors de l'installation de la console de Kaspersky Security sur un autre ordinateur (cf. page 58).</p>

Tableau 5. Paramètres de suppression et arguments dans Windows Installer

Paramètre	Valeur par défaut	Description, arguments de Windows Installer et valeurs
Restauration du contenu de la quarantaine	Supprimer	<p>RESTOREQTN =<valeur></p> <p>0 : supprimer le contenu de la quarantaine ;</p> <p>1 : restaurer le contenu de la quarantaine dans le dossier défini par le paramètre RESTOREPATH.</p>
Restauration du contenu de la sauvegarde	Supprimer	<p>RESTOREBCK =<valeur></p> <p>0 : supprimer le contenu de la sauvegarde ;</p> <p>1 : restaurer le contenu de la sauvegarde dans le dossier défini par le paramètre RESTOREPATH.</p>
Dossier pour la restauration des objets	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored	<p>RESTOREPATH=<chemin d'accès complet au dossier></p> <p>Les objets restaurés seront enregistrés dans le dossier défini par ce paramètre :</p> <p>Les objets de la quarantaine seront conservés dans le sous-dossier \Quarantine.</p> <p>Les objets de la sauvegarde seront conservés dans le sous-dossier \Backup.</p>

Modifications dans le système après l'installation de Kaspersky Security

Lors de l'installation de Kaspersky Security et de sa console (sélection « Outils d'administration »), le service Windows Installer procède aux modifications suivantes sur l'ordinateur :

- Les dossiers de Kaspersky Security sont créés sur le serveur protégé ainsi que sur l'ordinateur où la console de Kaspersky Security est installée ;
- Les services de Kaspersky Security sont enregistrés ;
- Le groupe d'utilisateurs de Kaspersky Security est créé ;
- Les clés de Kaspersky Security sont enregistrées dans la base de registres système.

Ces modifications sont décrites dans le tableau ci-dessous.

Dossiers de Kaspersky Security

Tableau 6. Dossiers de Kaspersky Security sur le serveur à protéger

Dossier	Fichiers de Kaspersky Security
Dossier %Kaspersky Security%; par défaut : Dans la version 32 bits de Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\; • Dans la version 64 bits de Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Security for Windows Server\.	Fichiers exécutables de Kaspersky Security (dossier d'installation désigné lors de l'installation)
Dossier %Kaspersky Security%\mibs	Les fichiers Management Information Base (MIB) ; contiennent une description des compteurs et des pièges publiés par Kaspersky Security selon le protocole SNMP

Dossier	Fichiers de Kaspersky Security
Dossier %Kaspersky Security%\x64	Version 64 bits des fichiers exécutables de Kaspersky Security (le dossier est créé uniquement en cas d'installation de Kaspersky Security sur une version 64 bits de Microsoft Windows)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Data \	Fichiers de service de Kaspersky Security
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Settings \	
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Dskm \	
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Update \	Fichiers contenant les paramètres des sources des mises à jour
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Update\Distribution \	Mises à jour des bases de données et des modules logiciels récupérés à l'aide de la tâche Copie des mises à jour (le dossier est créé à la première réception des mises à jour à l'aide de la tâche Copie des mises à jour).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Reports \	Journaux d'exécution des tâches et journal d'audit système
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\ Bases\Current \	Sélection des bases utilisées à l'heure actuelle

Dossier	Fichiers de Kaspersky Security
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Bases\Backup\	Copie de sauvegarde des bases ; écrasée à chaque mise à jour des bases de données
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Bases\Temp\	Fichiers temporaires créés lors de l'exécution des tâches de mise à jour
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Quarantine\	Objets en quarantaine (dossier par défaut)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Backup\	Objets dans la sauvegarde (dossier par défaut)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\	Objets restaurés de la sauvegarde ou de la quarantaine (dossier par défaut pour les objets restaurés)

Tableau 7. Dossier créés lors de l'installation de la console de Kaspersky Security

Dossier	Fichiers de Kaspersky Security
%Dossier Kaspersky Security%; par défaut : <ul style="list-style-type: none"> Dans la version 32 bits de Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\; Dans la version 64 bits de Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\ 	Fichiers de la sélection « Outils d'administration » (répertoire cible indiqué lors de l'installation de la console de Kaspersky Security) ;

Services de Kaspersky Security

Les services de Kaspersky Security sont lancés sous le compte utilisateur **Système local** (SYSTEM).

Tableau 8. Services de Kaspersky Security

Service	Fonction
Service Kaspersky Security Service (KAVFS)	Service principal de Kaspersky Security ; administre les tâches et les processus de travail de Kaspersky Security.
Service Kaspersky Security Management Service (KAVFSGT)	Ce service est prévu pour l'administration via la console de Kaspersky Security.
Service Kaspersky Security Script Checker (kavfsscs)	Service de traitement des requêtes d'analyse des scripts.

Groupes de Kaspersky Security

Tableau 9. Groupes de Kaspersky Security

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

Clés de la base de registres système

Tableau 10. Clés de la base de registres système

Clé	Fonction
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Paramètres du service Kaspersky Security
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Anti-Virus]	Paramètres du journal des événements de Kaspersky Security (Kaspersky Event Log)

Clé	Fonction
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsscs]	Paramètres du service du gestionnaire d'interception des scripts
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Paramètres du service d'administration de Kaspersky Security
<p>Dans la version 32 bits de Microsoft Windows :</p> <p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]</p> <p>Dans la version 64 bits de Microsoft Windows :</p> <p>[[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].</p>	Paramètres des compteurs de performance
<p>Dans la version 32 bits de Microsoft Windows :</p> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\SnmpAgent]</p> <p>Dans la version 64 bits de Microsoft Windows :</p> <p>[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\WSEE\SnmpAgent]</p>	Paramètres du composant « prise en charge du protocole SNMP »
<p>Dans la version 32 bits de Microsoft Windows :</p> <p>HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\10.0\Trace\</p> <p>Dans la version 64 bits de Microsoft Windows :</p> <p>HKEY_LOCAL_MACHINE\SoftwareWow6432Node\KasperskyLab\WSEE\10.0\Trace\</p>	Paramètres du journal de traçage

Clé	Fonction
<p>Dans la version 32 bits de Microsoft Windows :</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.0\CrashDump\</p> <p>Dans la version 64 bits de Microsoft Windows :</p> <p>HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.0\CrashDump\</p>	Paramètres de vidage sur incident

Processus de Kaspersky Security

Kaspersky Security lance les processus décrits dans le tableau suivant :

Tableau 11. Processus de Kaspersky Security

Nom du fichier	Fonction
kavfs.exe	Processus du service Kaspersky Security
kavswp.exe	Processus de travail Kaspersky Security
kavfscs.exe	Processus du service Kaspersky Security Script Checker
kavtray.exe	Processus du module Icône de Kaspersky Security
Kavsgt.exe	Processus du service d'administration Kaspersky Security Management
kavshell.exe	Processus de l'utilitaire de la ligne de commande
kavsrcn.exe	Processus d'administration à distance de Kaspersky Security

Planification de l'installation

Cette section décrit les outils d'administration de Kaspersky Security et les particularités de l'installation de Kaspersky Security à l'aide de l'Assistant d'installation, via la ligne de commande et via Kaspersky Security Center, ainsi que les stratégies de groupe d'Active Directory.

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

► *Pour planifier l'installation, procédez comme suit :*

1. Définissez les outils d'administration que vous utiliserez pour l'administration Kaspersky Security et de ses paramètres.
2. Définissez les composants logiciels qu'il faut installer (cf. page [24](#)).
3. Sélectionnez le mode d'installation.

Dans cette section

Sélection des outils d'administration	47
Sélection du mode d'installation	

Sélection des outils d'administration

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

Console de Kaspersky Security

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

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

La console de Kaspersky Security fait partie des composants « Outils d'administration ».

Utilitaire de la ligne de commande

Vous pouvez administrer Kaspersky Security via la ligne de commande du serveur protégé.

L'utilitaire de la ligne de commande fait partie des composants logiciels de Kaspersky Security.

Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center afin de centraliser l'administration de la protection antivirus des ordinateurs de votre entreprise, alors vous pourrez administrer Kaspersky Security via le serveur d'administration de Kaspersky Security Center.

Il faudra installer les composants suivants :

- **Module d'intégration de l'Agent et de Kaspersky Security Center.** Ce composant fait partie des composants logiciels de Kaspersky Security. Il établit la liaison entre Kaspersky Security et l'agent d'administration. Installez le module d'intégration à l'agent d'administration de Kaspersky Security Center sur le serveur protégé.
- **Agent d'administration Kaspersky Security Center** Installez-le sur chaque serveur protégé. Ce composant garantira l'interaction entre la copie de Kaspersky Security sur le serveur et le serveur d'administration Kaspersky Security Center. Le fichier d'installation de l'agent d'administration fait partie de la distribution de Kaspersky Security Center.
- **Plug-in d'administration de Kaspersky Security.** De plus, sur l'ordinateur où est installée la console d'administration Kaspersky Security Center, installez le plug-in d'administration de Kaspersky Security via le serveur d'administration. Il assure l'interface d'administration de l'application via Kaspersky Security Center. Le fichier d'installation du plug-in, `\server\klcfginst.exe`, fait partie de la distribution de Kaspersky Security.

Sélection du mode d'installation

Après avoir déterminé les composants logiciels pour l'installation de Kaspersky Security (cf. section « Modules logiciels de Kaspersky Security et code pour le service Windows Installer » à la page [24](#)), il faut sélectionner le mode d'installation de l'application.

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

- Devrez-vous définir des paramètres d'installation spéciaux pour Kaspersky Security ou comptez-vous utiliser les paramètres d'installation par défaut (cf. page [30](#)) ;
- Les paramètres d'installation seront-ils identiques pour tous les serveurs ou propres à chaque serveur ;

Vous pouvez installer Kaspersky Security à l'aide d'un Assistant d'installation ou en mode silencieux en désignant les paramètres d'installation dans la ligne de commande. Vous pouvez réaliser une installation centralisée à distance de Kaspersky Security via les stratégies de groupe Active Directory ou à l'aide d'une tâche d'installation à distance de Kaspersky Security Center.

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

Lancement de l'Assistant d'installation

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

- Les composants logiciels de Kaspersky Security sur le serveur protégé (cf. page [52](#)) depuis le fichier `\server\setup.exe` de la distribution ;
- La console de Kaspersky Security depuis le fichier `\client\setup.exe` de la distribution sur le serveur protégé ou un autre ordinateur du réseau.

Lancement via la ligne de commande du fichier du paquet d'installation avec les paramètres d'installation

Si vous exécutez le fichier du paquet d'installation sans clé, Kaspersky Security sera installé selon les paramètres par défaut. Grâce aux arguments de Kaspersky Security, vous pouvez modifier les paramètres d'installation.

Vous pouvez installer la console de Kaspersky Security sur un serveur protégé et/ou sur le poste de travail de l'administrateur.

Des exemples d'instructions pour l'installation de Kaspersky Security et de la console de Kaspersky Security sont fournis dans la rubrique « Installation et suppression de Kaspersky Security via la ligne de commande » (cf. page [73](#)).

Installation centralisée du logiciel via Kaspersky Security Center

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

Les serveurs sur lesquels vous souhaitez installer Kaspersky Security via Kaspersky Security Center (cf. page [80](#)) peuvent se trouver dans le même domaine que le serveur d'administration ou dans un autre domaine. Ils peuvent même n'appartenir à aucun domaine.

Installation centralisée via les stratégies de groupe Active Directory

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

Vous pouvez installer Kaspersky Security uniquement avec les paramètres par défaut.

Les serveurs sur lesquels vous installez Kaspersky Security via des stratégies de groupe Active Directory doivent se trouver dans le même domaine et dans la même unité d'organisation. L'installation a lieu après le démarrage du serveur avant l'entrée dans Microsoft Windows.

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

Cette section explique la procédure d'installation et de suppression de Kaspersky Security et de la console de Kaspersky Security sur le serveur protégé à l'aide de l'Assistant d'installation. Elle fournit également des informations sur la configuration complémentaire de Kaspersky Security et sur les actions à réaliser après l'installation de Kaspersky Security.

Dans cette section

Installation à l'aide de l'Assistant d'installation	51
Modification de la liste des composants et restauration de Kaspersky Security	68
Suppression à l'aide de l'Assistant d'installation.....	70

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

Les rubriques suivantes décrivent l'installation de Kaspersky Security et la console de Kaspersky Security.

► *Pour installer et utiliser Kaspersky Security, procédez comme suit :*

1. Installez Kaspersky Security sur le serveur protégé (cf. section « Installation de Kaspersky Security sur le serveur protégé » à la page [52](#)).
2. Installez la console de Kaspersky Security sur les ordinateurs sur lesquels vous avez l'intention d'administrer Kaspersky Security (cf. section « Installation de la console de Kaspersky Security » à la page [56](#)).

3. Si vous avez installé la console de Kaspersky Security sur un autre ordinateur, et non sur le serveur protégé, procédez à la configuration avancée pour que les utilisateurs de la console puissent administrer à distance Kaspersky Security (cf. section « Configuration avancée après l'installation de la console de Kaspersky Security sur un autre ordinateur » à la page [58](#)).
4. Réalisez les actions requises après l'installation de Kaspersky Security (page [64](#)).

Dans cette section

Installation de Kaspersky Security sur le serveur protégé	52
Installation de la console de Kaspersky Security	56
Configuration avancée après l'installation de la Console de Kaspersky Security sur un autre ordinateur	58
Actions après l'installation de Kaspersky Security.....	64

Installation de Kaspersky Security sur le serveur protégé

Avant d'installer Kaspersky Security, réalisez les actions suivantes :

- Assurez-vous qu'aucun autre logiciel anti-virus n'est installé sur le serveur. Vous pouvez installer Kaspersky Security sans supprimer la version de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition qui serait déjà installée.
- Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté est enregistré dans le groupe des administrateurs sur le serveur protégé.

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

Vous pouvez lire des informations plus détaillées sur les paramètres d'installation (de suppression) (cf. page [30](#)).

► *Pour installer Kaspersky Security à l'aide de l'Assistant d'installation, procédez comme suit :*

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

La fenêtre **Contrat de Licence Utilisateur Final** s'ouvre.

4. Lisez les dispositions du contrat de licence, puis cochez la case **J'accepte les termes du Contrat de Licence Utilisateur Final** pour poursuivre l'installation. Cliquez sur **Suivant**.

Si Kaspersky Anti-Virus for Windows Servers Enterprise Edition est installé sur le serveur, la fenêtre **Découverte d'une version antérieure de l'application** s'ouvre.

Si aucune version antérieure de l'application n'est détectée, passez à l'étape 6.

5. Pour mettre à niveau une version antérieure de l'application, cliquez sur **Installer**. L'Assistant d'installation effectue la mise à jour vers Kaspersky Security, tout en conservant les paramètres compatibles dans la nouvelle version (cf. section « Migration depuis une version antérieure de l'application » à la page [93](#)). Lorsque la mise à jour de l'application est terminée, la fenêtre **Fin de l'installation** s'ouvre (passez à l'étape 15 des présentes instructions).

Fenêtre **Analyse rapide avant l'installation** s'ouvre.

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

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

Pour voir exactement les fichiers qui ont été analysés, cliquez sur le bouton **Liste des objets traités**.

7. Dans la fenêtre **Analyse rapide avant l'installation**, cliquez sur **Suivant**.

La fenêtre **Type d'installation** s'ouvre.

8. Sélectionnez une des options suivantes :

- **Installation recommandée** pour installer par défaut tous les composants logiciels de Kaspersky Security à l'exception du composant Analyse des scripts. Passez à l'étape 11 des présentes instructions.
- **Installation personnalisée** afin de sélectionner les composants dans la liste des composants logiciels de Kaspersky Security.

9. Si vous avez sélectionné le type d'installation **Installation personnalisée**, la fenêtre **Installation personnalisée** s'ouvre.

Par défaut, tous les composants logiciels de Kaspersky Security sont sélectionnés à l'exception du composant Analyse des scripts.

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

Sélectionnez les composants que vous souhaitez installer. Pour annuler toutes les modifications de la fenêtre **Installation personnalisée**, cliquez sur le bouton **Réinitialiser**. Ensuite, cliquez sur **Suivant**.

10. Exécutez les actions suivantes dans la fenêtre **Sélection du dossier d'installation** qui s'ouvre :

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

Cliquez sur **Suivant**.

11. Dans la fenêtre **Paramètres avancés d'installation** qui s'ouvre, définissez les paramètres d'installation suivants :

- **Activer la protection en temps réel après l'installation de l'application.**
- **Ajouter les exclusions recommandées par Microsoft.**
- **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions.**
- **Ajouter les objets correspondant au masque not-a-virusRemoteAdmin* aux exclusions.**

Cliquez sur **Suivant**.

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

Si vous souhaitez importer les paramètres de Kaspersky Security depuis un fichier de configuration existant créé dans Kaspersky Anti-Virus 8.0 for Windows Servers, désignez le fichier de configuration. Cliquez sur **Suivant**.

13. Dans la fenêtre **Activation de l'application** qui s'ouvre, exécutez l'une des actions suivantes :

- Si vous souhaitez activer l'application, sélectionnez le fichier clé de Kaspersky Security.
- Si vous souhaitez activer l'application plus tard, cliquez sur **Suivant**.
- si vous aviez enregistré le fichier clé dans le répertoire \server de la distribution, le nom de ce fichier apparaîtra dans le champ **Clé**.
- Si vous souhaitez ajouter une licence à l'aide d'un fichier clé qui se trouve dans un autre dossier, spécifiez le fichier clé.

Vous ne pouvez pas activer l'application à l'aide d'un code d'activation dans l'Assistant d'installation. Si vous souhaitez activer l'application à l'aide d'un code d'activation, vous pourrez en ajouter un après l'installation de l'application. Vous trouverez plus d'informations sur l'activation de l'application dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

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

Cliquez sur **Suivant** pour appliquer la clé dans l'application.

14. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**. L'Assistant lance l'installation des composants de Kaspersky Security.

15. La fenêtre **L'installation est terminée** s'ouvre à la fin de l'installation.

16. Cochez la case **Lire les notes de publication** afin de consultez les informations relatives à la version après la fin de l'Assistant d'installation.

17. Cliquez sur **OK**.

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

Installation de la console de Kaspersky Security

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

► *Pour installer la console de Kaspersky Security, procédez comme suit :*

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

La fenêtre de bienvenue de l'application s'ouvre.

3. Cliquez sur le lien **Installer la console de Kaspersky Security**.

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

4. Dans la fenêtre **Contrat de Licence Utilisateur Final** qui s'ouvre, lisez les dispositions du contrat de licence, puis cochez la case **J'accepte les termes du Contrat de Licence Utilisateur Final** pour poursuivre l'installation. Cliquez sur **Suivant**.

5. Dans la fenêtre **Type d'installation** qui s'ouvre, sélectionnez l'une des options suivantes :

- **Installation complète** pour installer l'ensemble des composants logiciels « Outils d'administration » sur l'ordinateur. Cela comprend la console de Kaspersky Security, le fichier d'aide et les guides. Passez à l'étape 7 des présentes instructions.
- **Installation personnalisée** pour sélectionner les composants dans la liste. Cliquez sur **Suivant**.

Vous pouvez obtenir de plus amples informations sur les composants logiciels de Kaspersky Security (cf. page [24](#)).

6. Si vous avez sélectionné le type d'installation **Installation personnalisée**, la fenêtre **Installation personnalisée** s'ouvre.

Tous les composants de la sélection « Outils d'administration » sont repris par défaut dans la liste des composants à installer. Sélectionnez les composants que vous souhaitez installer. Cliquez sur **Suivant**.

7. Exécutez les actions suivantes dans la fenêtre **Sélection du dossier d'installation** qui s'ouvre :

Le cas échéant, désignez un autre dossier pour la conservation des fichiers installés. Cliquez sur **Suivant**.

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

Si vous avez l'intention d'administrer Kaspersky Security sur un ordinateur distant à l'aide la console de Kaspersky Security, cochez la case **Autoriser l'accès à distance**. Cliquez sur **Suivant**.

9. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**. L'Assistant lance l'installation des composants sélectionnés.

10. La fenêtre **L'installation est terminée** s'ouvre à la fin de l'installation.

11. Cliquez sur **OK**.

La fenêtre de l'Assistant d'installation se ferme. La Console de Kaspersky Security sera installée sur le serveur protégé.

Si vous avez installé la console de Kaspersky Security non pas sur le serveur à protéger mais sur un autre ordinateur, procédez à une configuration complémentaire (cf. rubrique « Configuration avancée après l'installation de la console de Kaspersky Security sur un autre ordinateur » à la page [58](#)).

Configuration avancée après l'installation de la console de Kaspersky Security sur un autre ordinateur

Si vous avez installé la console de Kaspersky Security non pas sur le serveur à protéger mais sur un autre ordinateur, il faudra réaliser les actions suivantes afin que les utilisateurs puissent administrer Kaspersky Security à distance :

- Sur le serveur protégé, ajoutez les utilisateurs de Kaspersky Security au groupe KAVWSEE Administrators.
- Si le serveur protégé est équipé du système Microsoft Windows Server 2008 / 2012 / 2012 R2, autorisez les connexions réseau pour le service Kaspersky Security Management Service (kavfsgt.exe).
- Si lors de l'installation de Kaspersky Security sur un ordinateur tournant sous Microsoft Windows vous n'avez pas coché la case **Autoriser les connexions réseau pour la Console de Kaspersky Security**, autorisez manuellement les connexions réseau pour la console de Kaspersky Security via le pare-feu sur cet ordinateur.

Dans cette section

À propos des autorisations d'accès au service Kaspersky Security Management.....	59
Autorisation des connexions réseau pour le service Kaspersky Security Management Service	60
Autorisation des connexions de réseau pour la Console de Kaspersky Security dans Microsoft Windows.....	61

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

Vous pouvez consulter la liste des services de Kaspersky Security (cf. rubrique « Modifications dans le système après l'installation de Kaspersky Security » à la page [41](#)).

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

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

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

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

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

Autorisation des connexions réseau pour le service Kaspersky Security Management Service

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

Pour établir une connexion entre la console de Kaspersky Security et Kaspersky Security Management Service, il faut autoriser les connexions réseau pour le service via le pare-feu sur le serveur protégé.

Vous devez configurer les connexions réseau si Kaspersky Security tourne sous Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2.

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

1. Sur le serveur Windows protégé, sélectionnez **Démarrer** → **Panneau de configuration** → **Sécurité** → **Pare-feu Windows**.
2. Dans la fenêtre **Paramètres du pare-feu Windows**, choisissez la commande **Modifier les paramètres**.
3. Sur l'onglet **Exclusions** dans la liste des exclusions prédéfinies, cochez les cases **COM + Accès réseau**, **Windows Management Instrumentation (WMI)** et **Remote Administration**.
4. Cliquez sur **Ajouter programme**.
5. Dans la boîte de dialogue **Ajout de programme**, désignez le fichier kavfsgt.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de Kaspersky Security.
6. Cliquez sur **OK**.
7. Cliquez sur le bouton **OK** dans la boîte de dialogue **Paramètres du pare-feu Windows**.

Les connexions réseau pour le service Kaspersky Security Management seront autorisées.

Autorisation des connexions de réseau pour la Console de Kaspersky Security dans Microsoft Windows

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

La console de Kaspersky Security utilise le protocole DCOM pour obtenir les informations relatives au fonctionnement de l'application (objets analysés, tâches effectuées, etc.) du service d'administration de Kaspersky Security sur le serveur distant.

Si l'ordinateur sur lequel est installée la console de Kaspersky Security est équipé de Microsoft Windows XP Service Pack 2 ou d'une version supérieure de Microsoft Windows Vista / 7 / 8 / 8.1, vous devrez autoriser les connexions réseau via le pare-feu sur cet ordinateur afin d'établir des connexions entre la console de Kaspersky Security et le service d'administration de Kaspersky Security.

► *Pour établir la connexion entre la console et le service Kaspersky Security Management, procédez comme suit :*

1. Assurez-vous que l'accès à distance anonyme aux applications COM est autorisé (mais pas le lancement à distance et l'activation des applications COM).
2. Dans le pare-feu Windows, ouvrez le port TCP 135 et autorisez les connexions de réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Security kavfsrcn.exe. Les informations entre l'ordinateur sur lequel la console de Kaspersky Security est installée et le serveur protégé sur lequel Kaspersky Security est installé sont échangées via le port TCP 135.

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

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

1. Sur l'ordinateur où la console de Kaspersky Security est installée, ouvrez la console **Service des composants** : sélectionnez **Démarrer** → **Exécuter**, saisissez la commande **dcomcnfg**, puis cliquez sur **OK**.
2. Dans la console **Services des composants** de l'ordinateur, déployez le nœud **Ordinateurs**, ouvrez le menu contextuel du nœud **Poste de travail** et sélectionnez la commande **Propriétés**.
3. Dans l'onglet **Sécurité COM** de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les restrictions** du groupe de paramètres **Autorisations d'accès**.
4. Dans la fenêtre **Autorisation d'accès**, vérifiez que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur **ANONYMOUS LOGON**.
5. Cliquez sur **OK**.

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

1. Sur l'ordinateur distant, fermez la console de Kaspersky Security.
2. Réalisez les actions suivantes en fonction du système d'exploitation de l'ordinateur :
 - Sous Microsoft Windows XP SP2 ou une version supérieure, procédez comme suit :
 - a. Choisissez l'option **Démarrer** → **Panneau de configuration** → **Pare-feu Windows**.
 - b. Dans la fenêtre **Pare-feu Windows** (onglet **Exclusions**), cliquez sur le bouton **Ajouter un programme**.
 - Sous Microsoft Windows Vista, procédez comme suit :
 - a. Choisissez l'option **Démarrer** → **Panneau de configuration** → **Pare-feu Windows** et dans la fenêtre **Pare-feu Windows**, choisissez l'option **Modifier les paramètres**.
 - b. Sur l'onglet **Exclusions** de la fenêtre **Pare-feu Windows (Paramètres du pare-feu Windows)**, cliquez sur le bouton **Ajouter port**.

- c. Dans le champ **Nom** , indiquez le nom du port RPC (TCP/135) ou définissez un autre nom, par exemple DCOM Kaspersky Security et dans le champ **Numéro de port**, indiquez le numéro du port : 135.
 - d. Sélectionnez le protocole **TCP**.
 - e. Cliquez sur **OK**.
 - f. Sur l'onglet **Exclusions**, cliquez sur le bouton **Ajouter programme**.
- Sous Microsoft Windows 7, procédez comme suit :
 - a. Sélectionnez **Démarrer** → **Panneau de configuration** → **Pare-feu Windows** dans la fenêtre **Pare-feu Windows** sélectionnez **Autoriser le lancement de l'application ou du composant depuis Pare-feu Windows**.
 - b. Dans la fenêtre **Autoriser un programme via le Pare-feu Windows**, cliquez sur le bouton **Autoriser un autre programme**.
3. Dans la fenêtre **Ajout de programme**, désignez le fichier kavfsrnc.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de la console de Kaspersky Security. Par défaut, le chemin d'accès complet au fichier est le suivant :
- Dans la version 32 bits de Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\kavfsrnc.exe ;
 - Dans la version 64 bits de Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\kavfsrnc.exe.
4. Cliquez sur **OK**.
5. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu Windows (Paramètres du pare-feu Windows)**.

Actions après l'installation de Kaspersky Security

Kaspersky Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si vous avez sélectionné **Activer la protection en temps réel après l'installation de l'application** lors de l'installation, Kaspersky Security analyse les objets du système de fichiers du serveur lorsque vous accédez à ce dernier. Kaspersky Security analyse le code des scripts exécutés si vous avez installé le composant Analyse des scripts au moment de l'installation personnalisée. Chaque vendredi à 20h00, Kaspersky Security lance la tâche Analyse des zones critiques.

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

- Lancer la tâche de mise à jour des bases de données de Kaspersky Security. Une fois installé, Kaspersky Security analyse les objets à l'aide des bases livrées avec le logiciel.

Il est conseillé de les actualiser immédiatement car les bases sont peut-être obsolètes.

Par la suite, l'application mettra à jour les bases toutes les heures conformément à la planification définie dans la tâche par défaut.

- Lancer l'analyse des zones critiques du serveur, si le serveur protégé n'était pas équipé d'un logiciel anti-virus avec fonction de protection des fichiers en temps réel avant l'installation de Kaspersky Security.
- Configurer les notifications de l'administrateur concernant les événements de Kaspersky Security.

Vous trouverez plus d'informations sur le lancement de la tâche et la configuration de ses paramètres, ainsi que des instructions sur la configuration des notifications de l'administrateur dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Dans cette section

Configuration et lancement de la tâche de mise à jour des bases de données de Kaspersky Security	65
Analyse rapide	67

Configuration et lancement de la tâche de mise à jour des bases de données de Kaspersky Security

Pour mettre à jour les bases de données après l'installation de l'application, vous devez :

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

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

1. Ouvrez la console de Kaspersky Security sur l'ordinateur. Pour cela, cliquez sur **Démarrer** → **Programmes** → **Kaspersky Security 10 for Windows Server** → **Outils d'administration** → **Console de Kaspersky Security**.
2. Si vous avez lancé la console de Kaspersky Security non pas sur le serveur protégé, mais sur un autre ordinateur, connectez-vous au serveur protégé : ouvrez le menu contextuel de l'entrée **Kaspersky Security** dans l'arborescence de la console, sélectionnez **Se connecter à un autre ordinateur**, puis dans la boîte de dialogue **Sélection d'ordinateur**, sélectionnez **Autre ordinateur**, et dans le champ de saisie, indiquez le nom de réseau du serveur protégé.

Si le compte utilisateur employé pour accéder à Microsoft Windows ne jouit pas des privilèges d'accès au service d'administration de Kaspersky Security sur le serveur, indiquez un compte qui jouit de tels privilèges. Vous pouvez obtenir des informations sur les comptes qui peuvent fournir un accès à Kaspersky Security Management Service (cf. section « À propos des autorisations d'accès au service Kaspersky Security Management » à la page [59](#)).

La fenêtre de la console de Kaspersky Security s'ouvre.

3. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
4. Sélectionnez la sous-entrée **Mise à jour des bases de l'application**.

5. Dans le panneau de résultats, passez au lien **Propriétés**.
6. Dans la fenêtre **Paramètres de la tâche** qui s'ouvre, ouvrez l'onglet **Paramètres de connexion**.
7. Exécutez les actions suivantes :
 - a. Si le protocole Web Proxy Auto-Discovery Protocole (WPAD) pour la reconnaissance automatique des paramètres du serveur proxy par le réseau local n'est pas configuré, définissez les paramètres du serveur proxy : dans la section **Paramètres du serveur proxy**, sélectionnez **Utiliser les paramètres du serveur proxy indiqué** et saisissez l'adresse dans le champ **Adresse** et le numéro de port du serveur proxy dans le champ **Port**.
 - b. Si votre réseau requiert une authentification au moment de l'accès au serveur proxy, sélectionnez la méthode requise dans la liste déroulante de la section **Paramètres d'authentification du serveur proxy** :
 - **Utiliser l'authentification NTLM** si le serveur proxy prend en charge l'analyse intégrée de l'authenticité dans Microsoft Windows (NTLM authentication). Kaspersky Security accèdera au serveur proxy à l'aide du compte utilisateur indiqué dans la tâche (par défaut la tâche est exécutée sous le compte **Système local (SYSTEM)**).
 - **Utiliser l'authentification NTLM avec utilisateur et mot de passe** si le serveur prend en charge la vérification intégrée de l'authenticité dans Microsoft Windows. Kaspersky Security utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy.

Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
 - **Utiliser le nom d'utilisateur et le mot de passe** pour choisir l'authentification traditionnelle (Basic authentication). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
8. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

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

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

1. Dans l'arborescence de la Console de Kaspersky Security, développez l'entrée **Mise à jour**.
2. Dans le menu contextuel de la sous-entrée **Mise à jour des bases de l'application**, sélectionnez la commande **Démarrer**.

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

Une fois que la tâche est terminée, vous pouvez consulter la date d'édition des dernières mises à jour des bases de données installées le nœud **Kaspersky Security**.

Analyse rapide

Une fois que les bases de Kaspersky Security ont été actualisées, recherchez la présence éventuelle de programmes malveillants sur le serveur à l'aide de la tâche Analyse des zones critiques.

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

1. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
2. Dans le menu contextuel de la sous-entrée **Analyse rapide**, sélectionnez la commande **Démarrer**.

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

► *Pour consulter le journal d'exécution des tâches,*

dans le panneau des résultats **Analyse rapide**, cliquez sur le lien **Ouvrir le journal d'exécution**.

Modification de la liste des composants et restauration de Kaspersky Security

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



► *Pour modifier la liste des composants de Kaspersky Security, procédez comme suit :*

1. Sur le serveur protégé sur lequel est installé Kaspersky Security, exécutez le fichier de l'application d'accueil setup.exe.
2. Dans la section **Installation** de la fenêtre qui s'ouvre, cliquez sur le lien **Kaspersky Security**.

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

3. Sélectionnez **Modification de la liste des composants de l'application**. Cliquez sur **Suivant**.

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

4. Dans la liste des composants disponibles de la fenêtre **Installation personnalisée**, sélectionnez les composants que vous souhaitez ajouter à Kaspersky Security ou que vous souhaitez supprimer de l'application. Pour ce faire, procédez comme suit :
 - Pour installer de nouveaux composants, cliquez sur le bouton  situé près du nom du composant sélectionné, et, dans le menu contextuel, sélectionnez :
 - l'option **Le composant sera installé sur un disque dur local** si vous souhaitez installer un composant ;
 - l'option **Le composant et ses sous-composants seront installés sur le disque dur local** si vous souhaitez installer un groupe de composants.
 - Pour supprimer des composants installés, cliquez sur le bouton  situé près du nom du composant sélectionné, et, dans le menu contextuel, sélectionnez l'option **Le composant sera inaccessible**.

Cliquez sur **Installer**.

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

La liste des composants de Kaspersky Security sera modifiée conformément aux paramètres définis.

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

► *Pour restaurer Kaspersky Security après un arrêt forcé, procédez comme suit :*

1. Sur le serveur protégé sur lequel est installé Kaspersky Security, exécutez le fichier de l'application d'accueil setup.exe.
2. Dans la section **Installation** de la fenêtre qui s'ouvre, cliquez sur le lien **Kaspersky Security**.

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

3. Sélectionnez **Restauration des composants installés**. Cliquez sur **Suivant**.

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

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

Kaspersky Security sera restaurée conformément aux paramètres définis.

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

Cette section contient des instructions pour supprimer Kaspersky Security et la console de Kaspersky Security du serveur protégé à l'aide de l'Assistant d'installation.

Dans cette section

Suppression de Kaspersky Security sur le serveur protégé	70
Suppression de la console de Kaspersky Security	71

Suppression de Kaspersky Security sur le serveur protégé

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

Vous pouvez supprimer Kaspersky Security du serveur protégé à l'aide de l'Assistant d'installation/de suppression.

Le redémarrage du serveur sera peut-être requis après la suppression de Kaspersky Security. Il est possible de reporter le redémarrage à plus tard.

► *Pour supprimer la console de Kaspersky Security, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes** → **Kaspersky Security 10** → **Modification ou suppression**.

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

2. Sélectionnez **Suppression des composants de l'application**. Cliquez sur **Suivant**.

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

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

- Cochez la case **Exporter les objets en quarantaine** pour que Kaspersky Security exporte les objets en quarantaine. Cette case est décochée par défaut.
- Cochez la case **Exporter les objets de sauvegarde** pour que Kaspersky Security exporte les objets de la sauvegarde. Cette case est décochée par défaut.
- Cliquez sur le bouton **Enregistrer dans** et indiquez le dossier vers lequel vous souhaitez exporter les objets restaurés. Par défaut, les objets sont exportés vers le dossier %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Uninstall.

Cliquez sur **Suivant**.

4. Dans la fenêtre **Prêt pour la suppression**, confirmez l'opération de suppression en cliquant sur **Supprimer**.

5. Dans la fenêtre qui s'ouvre lorsque la suppression est terminée, cliquez sur **OK**.

Kaspersky Security est supprimé du serveur protégé.

Suppression de la console de Kaspersky Security

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

Vous pouvez supprimer la console de Kaspersky Security sur l'ordinateur à l'aide de l'Assistant d'installation/de suppression.

Il n'est pas nécessaire de redémarrer l'ordinateur après la suppression de la console de Kaspersky Security.

► *Pour supprimer la console de Kaspersky Security, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Tous les programmes** → **Kaspersky Security 10** → **Outils d'administration** → **Modification ou suppression**.

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

Choisissez l'option **Suppression des composants de l'application**, puis cliquez sur **Suivant**.

3. La fenêtre **Prêt pour la suppression** s'ouvre. Cliquez sur **Supprimer**.

La fenêtre **Désinstallation terminée** s'ouvre.

4. Cliquez sur **OK**.

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

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

Cette section décrit les particularités de l'installation et de la suppression de Kaspersky Security via la ligne de commande. Elle fournit également des exemples de commande pour l'installation et la suppression de Kaspersky Security et des exemples de commande pour l'ajout et la suppression de modules de Kaspersky Security.

Dans cette section

Présentation de l'installation et de la suppression de Kaspersky Security via la ligne de commande.....	74
Exemples d'instructions pour l'installation de Kaspersky Security	74
Actions après l'installation de Kaspersky Security.....	76
Ajout et suppression de composants Exemples d'instructions	78
Suppression de Kaspersky Security. Exemples d'instructions	78
Codes de retour	79

Présentation de l'installation et de la suppression de Kaspersky Security via la ligne de commande

Vous pouvez installer et supprimer Kaspersky Security, ajouter ou supprimer des composants en exécutant les fichiers du paquet d'installation `\server\ks4ws_x86(x64).msi` via la ligne de commande et en précisant les paramètres d'installation à l'aide d'une clé.

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

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

Si vous exécutez l'un des fichiers `\server\ks4ws_x86(x64).msi` sur le serveur protégé sans clé additionnelle, Kaspersky Security sera installé avec les paramètres d'installation par défaut (cf. page [30](#)).

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

Exemples d'instructions pour l'installation de Kaspersky Security

Cette rubrique présente des exemples d'instructions pour l'installation de Kaspersky Security.

Sur un ordinateur fonctionnant sous Microsoft Windows 32 bits, exécutez les fichiers de la distribution dont le suffixe est `x86`. Sur un ordinateur fonctionnant sous Microsoft Windows 64 bits, exécutez les fichiers de la distribution dont le suffixe est `x64`.

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

Exemples d'instructions d'installation de Kaspersky Security : lancement du fichier setup.exe

- *Pour installer Kaspersky Security selon les paramètres par défaut sans intervention de l'utilisateur, saisissez l'instruction :*

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

- *Pour installer Kaspersky Security avec les paramètres suivants :*

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

saisissez l'instruction suivante :

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

- *Exemples d'instructions pour l'installation : exécution du fichier msi du paquet d'installation*

- *Pour installer Kaspersky Security selon les paramètres par défaut sans intervention de l'utilisateur, saisissez l'instruction :*

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

- *Pour installer Kaspersky Security avec les paramètres par défaut en affichant l'interface d'installation, saisissez l'instruction :*

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

- *Pour installer Kaspersky Security avec une activation à l'aide du fichier clé C:\0000000A.key :*

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

- *Pour installer Kaspersky Security avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux de l'ordinateur, saisissez l'instruction :*

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

- *Pour installer Kaspersky Security en enregistrant les fichiers dans le dossier d'installation C:\KWS, saisissez l'instruction suivante :*

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

- Pour installer Kaspersky Security, enregistrer le fichier journal appelé ksws.log dans le répertoire où se trouve le fichier msi de la distribution de Kaspersky Security, saisissez l'instruction suivante :

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

- Pour installer la console de Kaspersky Security, saisissez l'instruction suivante :

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

- Pour installer Kaspersky Security avec une activation à l'aide du fichier clé C:\0000000A.key ; ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions ; configurer Kaspersky Security conformément aux paramètres du fichier de configuration C:\settings.xml, saisissez l'instruction suivante :

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

Voir également

Actions après l'installation de Kaspersky Security.....	76
Paramètres d'installation et de suppression et arguments correspondant pour le service	
Windows Installer.....	30

Actions après l'installation de Kaspersky Security

Kaspersky Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si l'option **Activer la protection en temps réel après l'installation de l'application** a été sélectionnée lors de l'installation, Kaspersky Security analyse les objets du système de fichiers du serveur lorsque vous accédez à ce dernier. Kaspersky Security analyse le code des scripts exécutés si vous avez installé le composant Analyse des scripts au moment de l'installation personnalisée. Chaque vendredi à 20h00, Kaspersky Security lance la tâche Analyse des zones critiques.

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

- Lancer la tâche de mise à jour des bases de données de Kaspersky Security. Une fois installé, Kaspersky Security analyse les objets à l'aide des bases livrées avec le logiciel. Il est conseillé de les actualiser immédiatement. Pour ce faire, vous devez lancer la tâche Mise à jour des bases de l'application. Par la suite, la mise à jour des bases de données sera exécutée toutes les heures selon la planification définie par défaut.

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

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

Dans ce cas, les mises à jour des bases de données de Kaspersky Security seront téléchargées des serveurs de mise à jour de Kaspersky Lab. La connexion à la source des mises à jour s'opère via le serveur proxy (adresse du proxy : proxy.company.com, port : 8080) et utilise l'authentification intégrée de Microsoft Windows pour accéder au serveur (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser ; mot de passe : 123456).

Pour en savoir plus sur l'administration de Kaspersky Security via la ligne de commande, lisez le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

- Lancer l'analyse des zones critiques du serveur, si le serveur protégé n'était pas équipé d'un logiciel anti-virus avec fonction de protection des fichiers en temps réel avant l'installation de Kaspersky Security.

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

```
KAVSHELL SCANCritical /W:scancritical.log
```

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

- Configurer les notifications de l'administrateur sur les événements de Kaspersky Security (cf. document » *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*).

Ajout et suppression de composants

Exemples d'instructions

Si vous souhaitez ajouter de nouveaux composants à la liste des composants de Kaspersky Security installés précédemment, assurez-vous que la liste des valeurs de la clé ADDLOCAL contient non seulement les codes des composants que vous souhaitez installer, mais aussi les codes des composants déjà installés. Dans le cas contraire, les composants déjà installés seront supprimés.

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

- *Pour ajouter le composant Analyse des scripts aux composants déjà installés, exécutez la commande suivante :*

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,ScriptChecker /qn EULA=1
```

ou

```
\server\setup.exe /s /p "ADDLOCAL=Oas,ScriptChecker EULA=1"
```

Suppression de Kaspersky Security.

Exemples d'instructions

- *Pour supprimer Kaspersky Security du serveur protégé, saisissez l'instruction suivante :*

```
msiexec /x ks4ws.msi /qn EULA=1
```

- *Pour supprimer la console de Kaspersky Security, saisissez l'instruction suivante :*

```
msiexec /x ks4wstools.msi /qn EULA=1
```

Codes de retour

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

Tableau 12. Codes de retour

Code	Description
25001	Privilèges insuffisants pour l'installation de l'application.
25002	La suppression de la version antérieure de l'application n'est pas terminée.
25003	L'application installée ne correspond pas à la version du système d'exploitation.
25004	Une application incompatible a été découverte.

Installation et suppression de Kaspersky Anti-Virus via Kaspersky Security Center

Cette section fournit des informations d'ordre général sur l'installation de Kaspersky Security via Kaspersky Security Center, décrit les procédures d'installation et de désinstallation de Kaspersky Security via Kaspersky Security Center et présente également les opérations à réaliser après l'installation de l'application.

Dans cette section

Présentation générale de l'installation via Kaspersky Security Center	80
Privilèges pour l'installation ou la suppression de Kaspersky Security	81
Procédure d'installation de Kaspersky Security via Kaspersky Security Center	82
Actions après l'installation de Kaspersky Security.....	84
Installation de la console de Kaspersky Security via Kaspersky Security Center	88
Suppression de Kaspersky Security via Kaspersky Security Center	89

Présentation générale de l'installation via Kaspersky Security Center

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

Une fois que cette tâche aura été exécutée, Kaspersky Security sera installé sur plusieurs ordinateurs avec les mêmes paramètres.

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

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

Le *Manuel de l'administrateur de Kaspersky Security Center* contient des informations supplémentaires sur la tâche d'installation à distance.

Privilèges pour l'installation ou la suppression de Kaspersky Security

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

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

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

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

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

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

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

Procédure d'installation de Kaspersky Security via Kaspersky Security Center

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

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

- Sur l'ordinateur où est installé le Serveur d'administration de Kaspersky Security Center, le plug-in d'administration de Kaspersky Security est installé (fichier `\server\klcfginst.exe` de la distribution de Kaspersky Security).
- Sur les serveurs protégés, l'Agent d'administration de Kaspersky Security Center est installé. Si les serveurs protégés ne sont pas dotés de l'Agent d'administration de Kaspersky Security Center, vous pouvez l'installer en même temps que Kaspersky Security dans la tâche d'installation à distance.

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

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

1. Lancez la console d'administration Kaspersky Security Center.
2. Dans Kaspersky Security Center, développez l'entrée **Installation à distance** et dans la sous-entrée **Paquets d'installation**, créez un nouveau paquet d'installation en désignant le fichier ks4ws.kud de la distribution en tant que fichier du paquet d'installation.
3. Le cas échéant, dans les propriétés du paquet d'installation créé, modifiez la sélection des composants installés de Kaspersky Security (cf. section « Modification de la liste des composants et restauration de Kaspersky Security » à la page [68](#)). Si nécessaire, modifiez les paramètres d'installation par défaut (cf. section « Paramètres d'installation et de suppression et arguments correspondants pour le service Windows Installer » à la page [30](#)).

Dans Kaspersky Security Center, développez l'entrée **Installation à distance** et dans la sous-entrée **Paquets d'installation**, dans l'espace de travail, ouvrez le menu contextuel du paquet d'installation créé pour Kaspersky Security et choisissez l'option **Propriétés**. Dans le groupe **Configuration** de la fenêtre **Propriétés: <nom du paquet d'installation>**, réalisez les opérations suivantes :

- a. Dans le groupe de paramètres **Composants installés**, cochez les cases en regard du nom des composants de Kaspersky Security que vous souhaitez installer.
- b. Pour désigner un répertoire d'installation différent du répertoire sélectionné par défaut, indiquez le nom du répertoire et son chemin d'accès dans le champ **Dossier cible**.

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

- c. Dans le groupe de paramètres **Paramètres avancés d'installation**, définissez les valeurs suivantes :
- Rechercher la présence éventuelle de virus sur l'ordinateur avant de lancer l'installation.
 - Activer la protection en temps réel après l'installation de l'application.
 - Ajouter les exclusions recommandées par Microsoft.

- Tenir compte des exclusions recommandées par Kaspersky Lab.
 - Ajouter les objets correspondant au masque not-a-virus:RemoteAdmin* aux exclusions.
- d. Si vous souhaitez importer les paramètres de Kaspersky Security depuis un fichier de configuration existant créé dans Kaspersky Anti-Virus 6.0 for Windows Servers, désignez le fichier de configuration.
 - e. Dans la boîte de dialogue **Propriétés: <nom du paquet d'installation>**, cliquez sur **OK**.
4. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la Console de Kaspersky Security sur les ordinateurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

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

5. Lancez la tâche créée d'installation à distance de Kaspersky Security.

Kaspersky Security sera installé sur les ordinateurs indiqués dans la tâche.

Voir également

Actions après l'installation de Kaspersky Security.....	84
Vérification des fonctions de Kaspersky Security. Utilisation du virus d'essai EICAR.....	96

Actions après l'installation de Kaspersky Security

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

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

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

Vous pouvez également configurer les notifications de l'administrateur sur les événements de Kaspersky Security (cf. document » *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*).

Le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server* contient des informations supplémentaires sur la configuration des paramètres de Kaspersky Security via Kaspersky Security Center.

Dans cette section

Création et lancement de la tâche de groupe de mise à jour des bases de données de l'application.....	86
Création et lancement de la tâche de groupe d'analyse des serveurs et attribution de l'état de tâche d'analyse des zones critiques.....	87

Création et lancement de la tâche de groupe de mise à jour des bases de données de l'application

Une fois que vous avez défini la source des mises à jour via la stratégie, créez la tâche de groupe Mise à jour des bases de Kaspersky Security et lancez-la. Lors de la création de la tâche, vous pouvez configurer son lancement selon la fréquence **Après réception des mises à jour par le serveur d'administration**.

► *Pour créer une tâche de groupe de mise à jour des bases de l'application, procédez comme suit :*

1. Lancez l'Assistant de création de tâches de groupe : dans l'arborescence de la console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**, sélectionnez le groupe pour les serveurs duquel vous souhaitez créer la tâche. Ouvrez le menu contextuel du dossier **Tâches** et sélectionnez la commande **Créer** → **Tâche**.
2. Dans la fenêtre **Définition du nom de la tâche** de l'Assistant de création des tâches, saisissez un nom pour la tâche, par exemple Mise à jour des bases de données sur les serveurs du groupe.
3. Dans la fenêtre **Sélection du type de tâche**, sélectionnez sous l'onglet **Kaspersky Security 10** le type de tâche à créer : Mise à jour des bases de données de l'application.
4. Dans la fenêtre **Configuration**, choisissez l'option **Créer**.
5. Dans la fenêtre **Source des mises à jour**, sélectionnez l'option **Serveur d'administration Kaspersky Security Center**.
6. Dans la fenêtre **Planification**, cochez la case **Exécuter de manière planifiée** et dans la liste **Fréquence**, choisissez l'option **Après réception des mises à jour par le serveur d'administration**.
7. Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

La tâche de groupe Mise à jour des bases de données de l'application sera créée.

Création et lancement de la tâche de groupe d'analyse des serveurs et attribution de l'état de tâche d'analyse des zones critiques

► *Pour créer une tâche de groupe d'analyse des zones critiques des serveurs dans la console d'administration de Kaspersky Security Center et lui attribuer l'état de tâche d'analyse des zones critiques, procédez comme suit :*

1. Lancez l'Assistant de création de tâches de groupe : dans l'arborescence de la console d'administration de Kaspersky Security Center, développez l'entrée **Ordinateurs administrés**, sélectionnez le groupe pour les serveurs duquel vous souhaitez créer la tâche. Ouvrez le menu contextuel du dossier **Tâches** et sélectionnez la commande **Créer** → **Tâche**.
2. Dans la fenêtre **Définition du nom de la tâche** de l'Assistant de création des tâches, saisissez un nom pour la tâche, par exemple Analyse des zones critiques sur les serveurs du groupe.
3. Dans la fenêtre **Sélection du type de tâche**, sélectionnez sous l'onglet **Kaspersky Security 10** le type de tâche à créer : Analyse à la demande.
4. Dans la fenêtre **Configuration**, choisissez l'option **Créer**.
5. Dans la fenêtre **Zone d'analyse**, introduisez le cas échéant des modifications à la zone d'analyse. La zone d'analyse reprend par défaut les secteurs critiques du serveur.
6. Dans la fenêtre **Paramètres**, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide de l'ordinateur**.
7. Dans la fenêtre **Planification**, programmez l'exécution de la tâche :
 - a. Cochez la case **Exécuter de manière planifiée**.
 - b. Définissez la fréquence d'exécution de la tâche, par exemple, une fois par semaine.
 - c. Dans le champ **Heure de démarrage**, indiquez l'heure de l'exécution de la tâche.
 - d. Dans le champ **A partir de**, saisissez la date du jour en tant que date d'entrée en vigueur de la planification.
 - e. Cliquez sur **OK**.

8. Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

La tâche de groupe d'analyse des serveurs ayant le statut de la tâche d'analyse des zones critiques sera créée.

Installation de la console de Kaspersky Security via Kaspersky Security Center

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

► *Pour installer la Console de Kaspersky Security à l'aide d'une tâche d'installation à distance, procédez comme suit :*

1. Dans la console d'administration Kaspersky Security Center, développez l'entrée **Installation à distance** et dans la sous-entrée **Paquets d'installation**, créez un nouveau paquet d'installation à partir du fichier client\setup.exe. Création d'un paquet d'installation :
 - Dans la fenêtre **Sélectionnez le type de paquet d'installation**, sélectionnez l'option **Créer package d'installation pour l'application spécifiée par l'utilisateur** et sélectionnez le fichier client\setup.exe dans le dossier de distribution.
 - Le cas échéant, modifiez la liste des composants à installer dans le champ **Paramètres de lancement du fichier exécutable (facultatif)** à l'aide de l'argument ADDLOCAL et modifiez le dossier cible.

Par exemple, pour réaliser l'installation dans C:\KasperskyConsole de la console de Kaspersky Security sans le fichier d'aide et la documentation, saisissez l'instruction suivante :

```
\server\setup.exe /s /p  
"ADDLOCAL=MmcSnapin INSTALLDIR=c:\KasperskyConsole EULA=1 "
```


2. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la Console de Kaspersky Security sur les ordinateurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

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

3. Lancez la tâche créée d'installation à distance.

La console de Kaspersky Security sera installée sur les ordinateurs désignés dans la tâche.

Suppression de Kaspersky Security via Kaspersky Security Center

- *Pour supprimer Kaspersky Security, procédez comme suit dans la console d'administration de Kaspersky Security Center.*

1. Dans la console d'administration Kaspersky Security Center, créez et lancez une tâche de suppression de l'application.
2. Dans la tâche, sélectionnez la méthode de suppression (de la même manière que vous aviez choisi la méthode d'installation, cf. point précédent) et désignez le compte sous les privilèges duquel le serveur d'administration communiquera avec les ordinateurs. Vous pouvez supprimer Kaspersky Security uniquement selon les paramètres de suppression par défaut (cf. section « Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer » à la page [30](#)).

Installation et suppression de Kaspersky Anti-Virus via les stratégies de groupe Active Directory

Cette section décrit l'installation et la suppression de Kaspersky Security via des stratégies de groupe Active Directory et présente les actions à réaliser après l'installation de l'application via les stratégies de groupe d'Active Directory.

Dans cette section

Installation de Kaspersky Security via les stratégies de groupe Active Directory	90
Actions après l'installation de Kaspersky Security	91
Suppression de Kaspersky Security via les stratégies de groupe Active Directory	92

Installation de Kaspersky Security via les stratégies de groupe Active Directory

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

Les ordinateurs sur lesquels vous souhaitez installer Kaspersky Security (la console de Kaspersky Security) doivent appartenir au même domaine et à la même unité d'organisation.

Les systèmes d'exploitation des ordinateurs sur lesquels vous souhaitez installer Kaspersky Security à l'aide de la stratégie doivent tous être de la même édition (32 ou 64 bits).

Vous devez posséder les autorisations d'administrateur de domaine.

Pour installer Kaspersky Security, utilisez les paquets d'installation ks4ws_x86(x64).msi. Pour installer la Console de Kaspersky Security, utilisez le paquet d'installation ks4wstools.msi.

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

► *Pour installer la console de Kaspersky Security (la console de Kaspersky Security), procédez comme suit :*

1. Enregistrez le fichier msi du paquet d'installation de la version correspondante du système d'exploitation de Microsoft Windows dans un dossier partagé sur le contrôleur de domaine.
2. Sur le contrôleur de domaine, créez une nouvelle stratégie de groupe dans laquelle les serveurs sont réunis.
3. À l'aide du **Group Policy Object Editor**, créez un nouveau paquet d'installation dans le nœud **Configuration des ordinateurs**. Saisissez le chemin d'accès au fichier msi du paquet d'installation de Kaspersky Security (de la console de Kaspersky Security) au format UNC (Universal Naming Convention).
4. Cochez la case **Always install with elevated privileges** du service Windows Installer aussi bien dans le nœud **Configuration des ordinateurs** que dans le nœud **Configuration des utilisateurs** du groupe sélectionné.
5. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

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

Actions après l'installation de Kaspersky Security

Après l'installation de Kaspersky Security sur les serveurs protégés, il est conseillé de procéder immédiatement à la mise à jour des bases de l'application et de lancer l'analyse des zones critiques du serveur. Vous pouvez exécuter ces actions à partir de la console de Kaspersky Security (cf. section « Actions après l'installation de Kaspersky Security » à la page [64](#)).

Vous pouvez également configurer les notifications de l'administrateur sur les événements de Kaspersky Security (cf. document « Manuel de l'administrateur de Kaspersky Security 10 for Windows Server »).

Suppression de Kaspersky Security via les stratégies de groupe Active Directory

Si vous avez installé Kaspersky Security (la console de Kaspersky Security) sur les ordinateurs du groupe en utilisant une stratégie de groupe Active Directory, vous pouvez utiliser cette stratégie afin de supprimer Kaspersky Security (la console de Kaspersky Security).

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

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

► *Pour supprimer Kaspersky Security (la console de Kaspersky Security), procédez comme suit :*

1. Sur le contrôleur de domaine, choisissez une unité d'organisation reprenant les ordinateurs desquels vous souhaitez supprimer Kaspersky Security ou la Console de Kaspersky Security.
2. Sélectionnez la stratégie créée pour l'installation de Kaspersky Security et dans **Editeur des stratégies de groupe**, nœud **Software Installation (Configuration des ordinateurs → Configuration des programmes → Software Installation)** ouvrez le menu contextuel du paquet d'installation de Kaspersky Security (de la console de Kaspersky Security) et sélectionnez la commande **Toutes les tâches → Supprimer**.
3. Sélectionnez la méthode de suppression **Supprimer immédiatement le programme de tous les ordinateurs**.
4. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Security est supprimé des ordinateurs du groupe après leur redémarrage, avant d'entrer dans Microsoft Windows.

Migration depuis une version antérieure de l'application

Vous pouvez installer Kaspersky Security 10 sans supprimer les versions antérieures de l'application installées sur l'ordinateur, pour autant qu'il s'agisse d'une des versions suivantes de Kaspersky Security :

- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ;
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Cette section contient des informations sur l'enregistrement, le transfert et l'application des paramètres des applications installées lors de l'installation de Kaspersky Security 10 for Windows Server sans suppression de Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ou de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Lors de la mise à jour de l'application vers la version Kaspersky Security 10 for Windows Server, il faudra peut-être redémarrer l'ordinateur.

Dans cette section

Migration des paramètres de Kaspersky Anti-Virus 6.0 for Windows Servers MP4.....	94
Migration des paramètres de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1	95

Migration des paramètres de Kaspersky Anti-Virus 6.0 for Windows Servers MP4

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 et Kaspersky Security 10 for Windows Server sont des applications distinctes et l'ensemble de leurs modules opérationnels, ainsi que les paramètres configurables pour ces deux applications sont différents.

Lorsque Kaspersky Security 10 est installé en écrasant Kaspersky Anti-Virus 6.0, il est possible de transférer une partie des paramètres suivants configurés lors de l'utilisation de Kaspersky Anti-Virus 6.0 :

- paramètres généraux de l'application et paramètres des services enregistrés de Windows ;
- paramètres d'analyse à la demande ;
- paramètres de la zone de confiance ;
- paramètres de la mise à jour .

Après la mise à jour de Kaspersky Anti-Virus 6.0 vers Kaspersky Security 10, il est recommandé d'effectuer une vérification des paramètres de l'application transférés de Kaspersky Anti-Virus vers Kaspersky Security.

Vous pouvez également appliquer les stratégies et les tâches de groupe créées avec Kaspersky Anti-Virus 6.0 dans Kaspersky Security.

Les stratégies et les tâches de groupe de Kaspersky Security Center ne sont pas converties automatiquement et elles sont prises en charge sans réinstallation du plug-in d'administration de Kaspersky Security.

- *Pour utiliser les stratégies ou les tâches de groupe créées à l'aide de Kaspersky Anti-Virus 6.0,*

importez la stratégie ou la tâche enregistrée précédemment lors de la création d'une nouvelle stratégie ou d'une nouvelle tâche au cours de la première étape de l'Assistant dans le plug-in d'administration de Kaspersky Security 10.

Migration des paramètres de Kaspersky Anti-Virus 8.0 for Servers Enterprise Edition Service Pack 1

Lors de la migration de Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1 vers Kaspersky Security 10 for Windows Server, tous les paramètres locaux sont conservés sans modification.

Les stratégies et les tâches de groupe de Kaspersky Security Center ne sont pas converties automatiquement et elles sont prises en charge sans réinstallation du plug-in d'administration de Kaspersky Security.

- *Pour utiliser les stratégies ou les tâches de groupe créées à l'aide de Kaspersky Anti-Virus 8.0,*

importez la stratégie ou la tâche enregistrée précédemment lors de la création d'une nouvelle stratégie ou d'une nouvelle tâche au cours de la première étape de l'Assistant dans le plug-in d'administration de Kaspersky Security 10.

Le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server* et le *Manuel de l'administrateur de Kaspersky Security Center* contient des informations supplémentaires sur la procédure d'importation des stratégies et des tâches de groupe.

Vérification des fonctions de Kaspersky Security. Utilisation du virus d'essai EICAR

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

Dans cette section

Présentation du virus d'essai EICAR.....	96
Vérification des fonctions « Protection en temps réel » et « Analyse à la demande 98 » de Kaspersky Security	

Présentation du virus d'essai EICAR

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

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

Le fichier qui contient le virus d'essai s'appelle eicar.com. Vous pouvez le télécharger sur la page du site **EICAR** http://www.eicar.org/anti_virus_test_file.htm.

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

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

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

Pour que Kaspersky Security traite le fichier eicar.com avec un préfixe, dans la section des paramètres de sécurité **Protection des objets**, indiquez la valeur **Tous les objets** pour la tâche Protection des fichiers en temps réel de Kaspersky Security et pour la tâche d'analyse à la demande. Cf. instructions dans le *Manuel de l'administrateur de Kaspersky Security 10 for Windows Server*.

Tableau 13. Préfixe des fichiers EICAR

Préfixe	Etat du fichier après l'analyse et l'action de Kaspersky Security
Sans préfixe	Kaspersky Security attribue l'état Infecté à l'objet et le supprime.
SUSP–	Kaspersky Security attribue l'état potentiellement infecté à l'objet (découvert à l'aide de l'analyseur heuristique) et le supprime (les objets potentiellement infectés ne sont pas réparés).
WARN–	Kaspersky Security attribue l'état potentiellement infecté à l'objet (le code de l'objet correspond en partie à un code malveillant connu) et le supprime (les objets potentiellement infectés ne sont pas réparés).
CURE–	Kaspersky Security attribue l'état Infecté à l'objet et le répare. Si la réparation a réussi, tout le texte du fichier est remplacé par le mot « CURE ».

Vérification des fonctions « Protection en temps réel » et « Analyse à la demande » de Kaspersky Security

Après l'installation de Kaspersky Security, vous pouvez confirmer que Kaspersky Security est en mesure d'identifier les objets contenant du code malveillant. Pour l'analyse, vous pouvez utiliser le virus d'essai **EICAR** (cf. la section « **Présentation du virus d'essai EICAR** » à la page [96](#)).

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

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

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

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

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

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

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

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

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

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

2. Ouvrez la console de Kaspersky Security.

3. Exécutez les actions suivantes :

- a. Dans l'arborescence de la console de Kaspersky Security, développez le nœud **Analyse à la demande**.
- b. Sélectionnez la sous-entrée **Analyse rapide**.
- c. Sous l'onglet **Configuration de la zone d'analyse**, ouvrez le menu contextuel du nœud **Emplacements réseau**, puis choisissez **Ajouter un fichier de réseau**.
- d. Saisissez le chemin d'accès au fichier eicar.com sur l'ordinateur distant au format UNC (Universal Naming Convention).
- e. Cochez la case afin d'inclure le chemin de réseau dans la zone d'analyse.
- f. Lancez la tâche Analyse des zones critiques.

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

- Le fichier eicar.com est supprimé du disque de l'ordinateur.
- Dans la console de Kaspersky Security, le journal de l'exécution de la tâche a reçu l'état **Critique** ; le journal de l'exécution de la tâche **Analyse rapide** reprend une ligne d'information sur la menace dans le fichier eicar.com. (Pour consulter le journal d'exécution de la tâche dans l'arborescence de la console de Kaspersky Security, développez l'entrée **Analyse à la demande**, sélectionnez la tâche **Analyse rapide** et dans le volet des résultats de l'entrée, cliquez sur le lien **Ouvrir le journal d'exécution**).

Schémas de déploiement de Kaspersky Security

Cette section décrit les schémas de déploiement dans le cadre de l'utilisation de Kaspersky Security pour protéger des stockages DAS, des clusters, des serveurs de terminaux et des stockages réseau.

Dans cette section

Protection des stockages à connexion directe (DAS)	102
Protection des clusters	103
Protection des serveurs de terminaux	105
Protection des stockages réseau	106

Protection des stockages à connexion directe (DAS)

Kaspersky Security protège les périphériques de stockage de données connectés directement au serveur (stockage DAS) (cf. ill. ci-après).

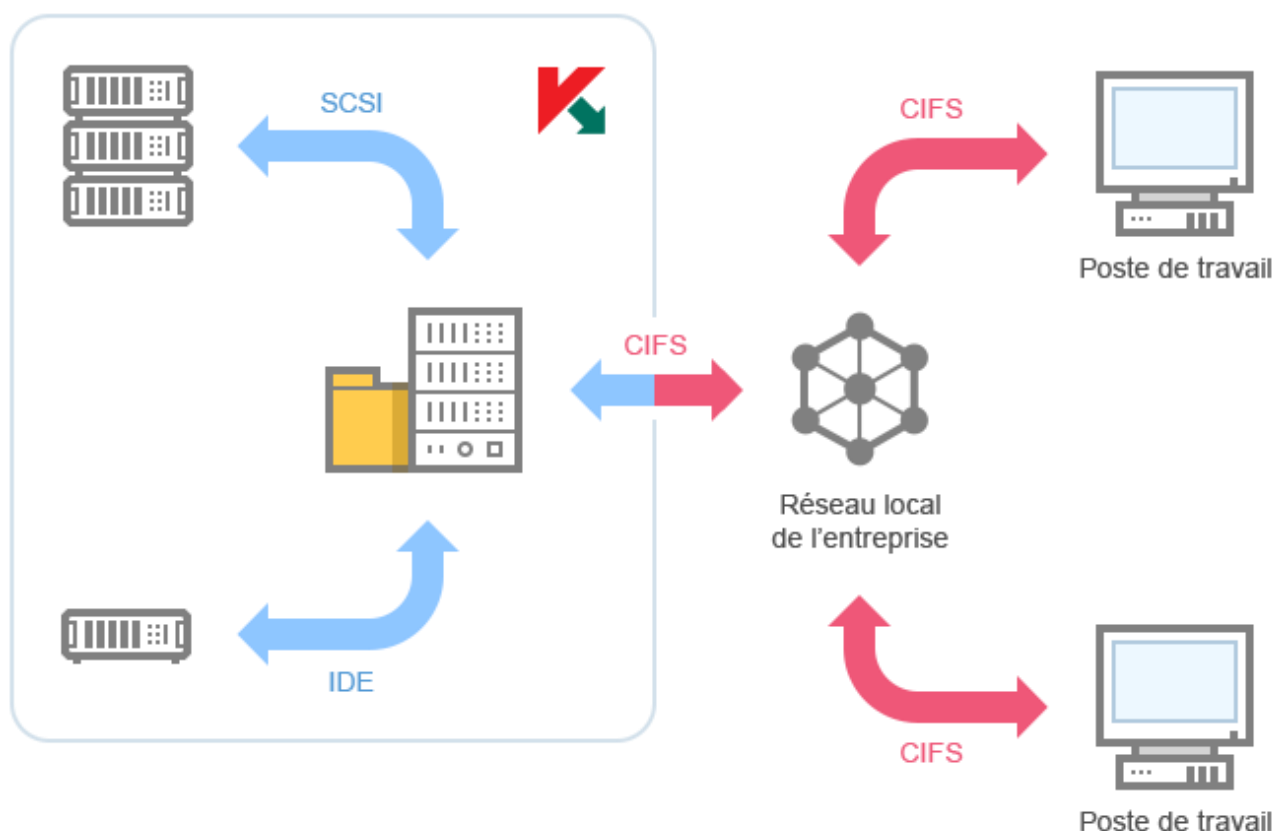


Illustration 1. Schéma de la protection des stockages à connexion directe

Kaspersky Security contrôle les opérations exécutées sur les fichiers qui se trouvent dans les stockages DAS. Kaspersky Security identifie le DAS comme une ressource fichier locale du serveur.

Protection des clusters

Kaspersky Security peut être installé sur des clusters de serveurs qui fonctionnent sous les modes **Actif / Actif** et **Actif / Passif** (cf. ill. ci-après).

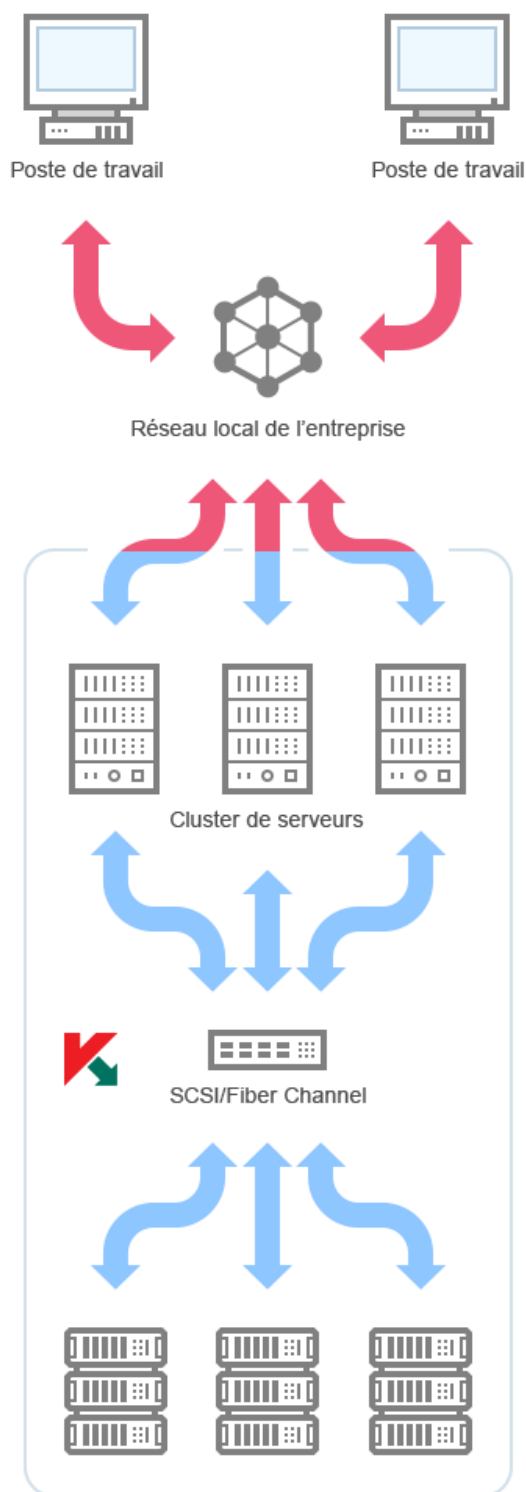


Illustration 2. Schéma de protection d'un cluster de serveurs

Kaspersky Security garantit le bon fonctionnement du serveur lors de la migration des ressources en cluster (**failover** / **failback**).

Le cluster est complètement protégé uniquement si Kaspersky Security est installé sur chaque nœud. Kaspersky Security protège les disques locaux du système de fichiers du serveur ainsi que les disques partagés du cluster appartenant au nœud protégé. Les ressources fichier qui appartiennent à un nœud de cluster non protégé ne sont pas protégées.

Protection des serveurs de terminaux

Kaspersky Security protège les serveurs de terminaux (cf. ill. ci-dessous).

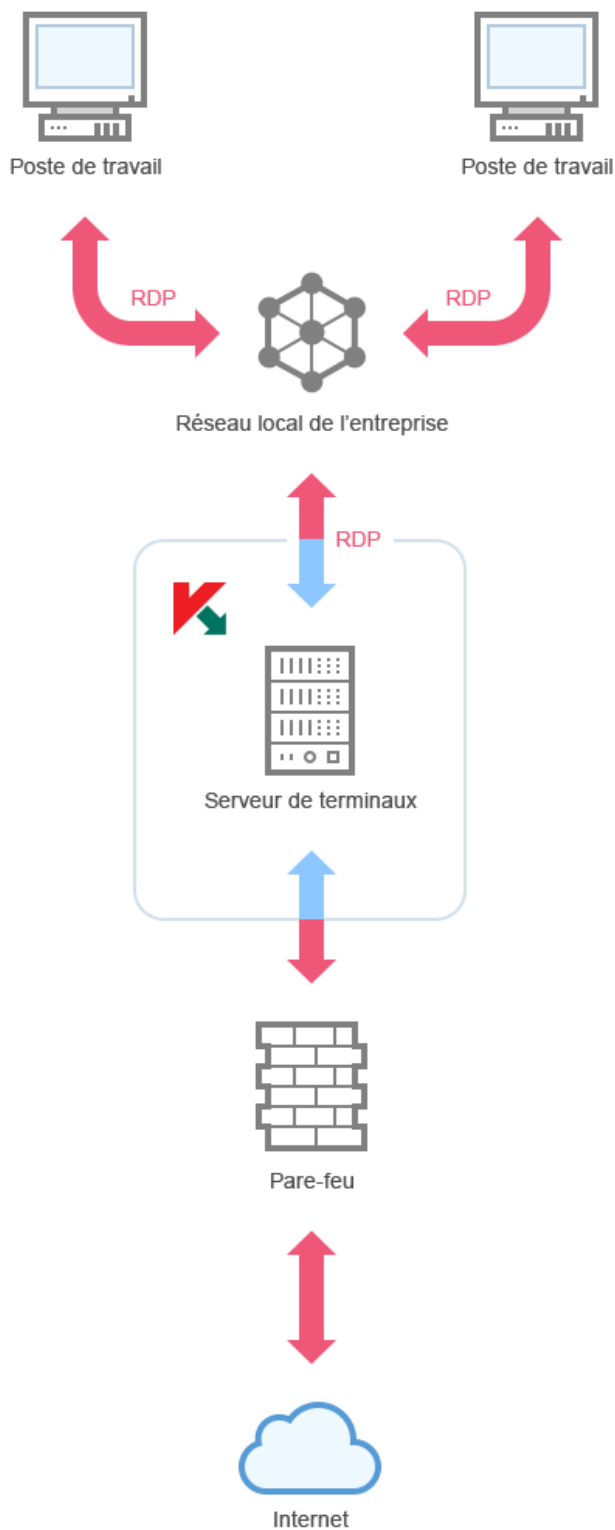


Illustration 3. Schéma de protection de serveurs de terminaux

Kaspersky Security offre les possibilités suivantes :

- protection des utilisateurs des terminaux qui travaillent en mode de publication du bureau et des applications ;
- notification des utilisateurs des terminaux à l'aide des services des terminaux ;
- audit des actions réalisées sur les fichiers et les scripts des utilisateurs des terminaux.

Protection des stockages réseau

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

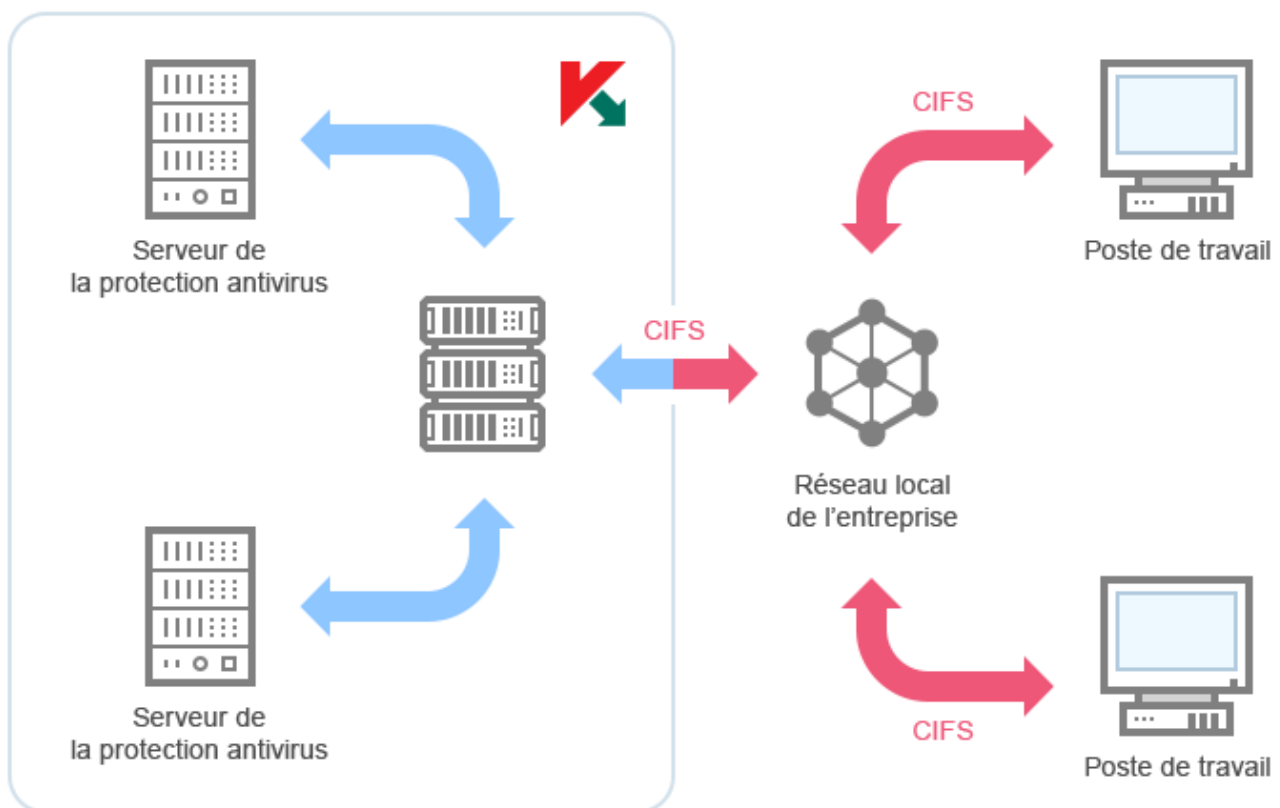


Illustration 4. Schéma de protection des stockages réseau.

Kaspersky Security analyse les fichiers placés dans les dossiers partagés du stockage réseau en cas de tentative de lecture ou de modification de ces fichiers depuis des postes de travail.

Le stockage réseau autorisera la lecture ou la modification du fichier uniquement si Kaspersky Security l'a considéré comme un fichier sain. Si Kaspersky Security considère que le fichier est infecté ou probablement infecté, le stockage réseau interdit la lecture ou la modification du fichier. Kaspersky Security permet de configurer les actions que l'application doit exécuter sur les fichiers infectés ou probablement infectés. Kaspersky Security répare par défaut les objets infectés et si la réparation est impossible, il les supprime (si cette action est disponible dans le stockage réseau). Les fichiers infectés sont placés quant à eux en quarantaine. Avant de réparer ou de supprimer un fichier, Kaspersky Security place une copie de celui-ci dans la sauvegarde.

Vous trouverez de plus amples informations dans le *Manuel d'implantation de Kaspersky Security 10 for Windows Server pour la protection des stockages réseau*.

Contacteur le Support Technique

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

Dans cette section

Modes d'obtention de l'assistance technique	108
Assistance technique via Kaspersky CompanyAccount	109
Assistance technique par téléphone.....	110
Utilisation du fichier de trace et du script AVZ.....	110

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 (<http://support.kaspersky.com/fr/support/rules>).

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

- appeler le Support Technique par téléphone (<http://support.kaspersky.com/fr/b2b>).

- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

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 Kaspersky CompanyAccount. Un compte permet de gérer de manière centralisée les requêtes électroniques des employés inscrits chez Kaspersky Lab ainsi que de gérer les autorisations de ces employés au sein du Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

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

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

Assistance technique par téléphone

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

Avant de contacter le Support Technique, prenez connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/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 à envoyer au Support Technique. Les experts du Support Technique peuvent également vous demander de créer *un fichier de trace*. Le fichier de trace permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

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

Glossaire

A

Agent d'administration

Composant de Kaspersky Security Center qui assure l'interaction entre le serveur d'administration et les applications de Kaspersky Lab installées sur un nœud particulier du réseau (poste de travail ou serveur). Ce module est unique pour toutes les applications Windows du portefeuille de la société.

Analyse heuristique

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

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

Analyse sur la base de signatures

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

Analyseur heuristique

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 potentiellement infectés. Par exemple, un fichier qui contient une succession de commandes propres à des objets malveillants (ouverture d'un fichier, écriture dans le fichier) pourrait être considéré comme potentiellement infecté.

Archive

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

B

Bases antivirus

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

C

Clé active

Clé utilisée actuellement par l'application.

Clé additionnelle

Clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée actuellement.

Fans

Faux positif

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

Fichier clé

Fichier xxxxxxxx.key qui permet d'activer l'application de Kaspersky Lab selon les conditions de la licence par le biais de l'ajout d'une clé.

Fichier infecté

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

Fichier potentiellement infectable

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

Fichier probablement infecté

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

G

Groupe d'administration

Ensemble d'ordinateurs regroupés selon leurs fonctions et les applications de Kaspersky Lab installées sur ceux-ci. Les ordinateurs sont regroupés pour en faciliter la gestion au sein d'un ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

M

Masque de fichier

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

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

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

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

Mise à jour

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

O

Objets exécutés au démarrage du système

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

Objet OLE

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

P

Paramètres de la tâche

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

Paramètres de l'application

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

Q

Quarantaine

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

R

Réparation des objets

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

S

Sauvegarde

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

Serveur d'administration

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

T

Tâche

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

V

Vulnérabilité

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

AO KASPERSKY LAB

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

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

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

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

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

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

Les experts antivirus de Kaspersky Lab travaillent 24 heures sur 24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et

de neutralisation de ces menaces et ajoutent les signatures de ces menaces aux bases utilisées par les applications de Kaspersky Lab.

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

RESULTATS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a remporté des centaines de récompenses. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 400 millions de personnes. Kaspersky Lab compte plus de 270 000 entreprises parmi ses clients.

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

Informations sur le code tiers

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

Avis de marques déposées

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

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

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

Radmin – sont des marques déposées de Famatech.

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

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

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

Index

A

AO	117
----------	-----

G

Groupes d'administration	113
--------------------------------	-----

S

Script AVZ.....	110
-----------------	-----

Serveur d'administration.....	116
-------------------------------	-----

T

Trace	
fichier de trace.....	110