

Kaspersky Security Center 9.0

**KASPERSKY** **lab**

Manuel  
d'implantation

VERSION DE L'APPLICATION : 9.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que ce document vous aidera dans votre travail et répondra à la plupart des problèmes émergents.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, 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, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous un format quelconque et la diffusion, y compris la traduction, de n'importe quel document ne sont admises que par autorisation écrite de Kaspersky Lab.

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

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

Kaspersky Lab ne peut être tenu 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. Kaspersky Lab n'assume pas non plus de responsabilité en cas de dommages liés à l'utilisation de ces textes.

Date d'édition : 22/03/12

© 2012 Kaspersky Lab ZAO. Tous droits réservés.

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

# TABLE DES MATIERES

A PROPOS DE CE MANUEL.....	5
Dans ce document.....	5
Conventions.....	7
SOURCES D'INFORMATIONS COMPLEMENTAIRES.....	8
Sources d'informations pour les recherches indépendantes .....	8
Discussion sur les applications de Kaspersky Lab sur le forum .....	9
Contacter le Groupe de rédaction de la documentation pour les utilisateurs.....	9
KASPERSKY SECURITY CENTER.....	10
ARCHITECTURE DE L'APPLICATION.....	11
CONFIGURATIONS LOGICIELLE ET MATERIELLE .....	12
INFORMATIONS SUR LA PRODUCTIVITE DU SERVEUR D'ADMINISTRATION.....	15
SCHEMAS TYPIQUES DE DEPLOIEMENT DE LA PROTECTION ANTIVIRUS .....	16
DEPLOIEMENT DE LA PROTECTION ANTIVIRUS A L'INTERIEUR DE L'ENTREPRISE.....	17
Déploiement de la protection antivirus via la Console d'administration à l'intérieur de l'entreprise.....	17
Déploiement de la protection antivirus à l'aide des outils de Kaspersky Security Center Web-Console à l'intérieur de l'entreprise.....	18
Déploiement manuel de la protection antivirus à l'intérieur de l'entreprise .....	18
DEPLOIEMENT DE LA PROTECTION ANTIVIRUS DANS LE RESEAU DE L'ENTREPRISE-CLIENT .....	20
Déploiement de la protection antivirus via la Console d'administration dans le réseau de l'entreprise-client.....	20
Déploiement de la protection antivirus via la Kaspersky Security Center Web-Console dans le réseau de l'entreprise-client.....	21
Déploiement manuel de la protection antivirus dans le réseau de l'entreprise-client.....	22
DEPLOIEMENT DU SERVEUR D'ADMINISTRATION .....	23
Étapes de déploiement du Serveur d'administration à l'intérieur de l'entreprise .....	23
Étapes de déploiement du Serveur d'administration pour la protection antivirus de l'entreprise-client.....	24
Mise à jour d'une version antérieure de l'application Kaspersky Security Center .....	24
Installation de Kaspersky Security Center .....	25
Préparation de l'installation .....	25
Installation standard.....	27
Installation personnalisée.....	27
Modifications dans le système après l'installation .....	34
Suppression de l'application .....	35
Installation de la Console d'administration sur le poste de travail de l'administrateur.....	35
Installation et configuration de Kaspersky Security Center SHV .....	36
Installation de Kaspersky Security Center Web-Console .....	36
Étape 1. Lecture du contrat de licence.....	37
Étape 2. Sélection du dossier d'installation.....	37
Étape 3. Sélection des ports .....	37
Étape 4. Connexion au Kaspersky Security Center .....	38
Étape 5. Sélection d'installation du serveur Apache .....	38
Étape 6. Installation du serveur Apache .....	38
Étape 7. Lancement de l'installation de Kaspersky Security Center Web-Console.....	39
Étape 8. Fin de l'Assistant de Kaspersky Security Center Web-Console.....	39

Configuration du fonctionnement du Serveur d'administration avec Kaspersky Security Center Web-Console .....	39
CONFIGURATION DU SYSTEME DE PROTECTION ANTIVIRUS DE L'ENTREPRISE-CLIENT .....	41
Désignation de l'ordinateur en tant que l'agent de mises à jour. Configuration des paramètres de l'agent de mises à jour .....	41
Installation locale de l'Agent d'administration sur l'agent de mises à jour.....	43
Conditions nécessaires pour installer les applications sur les ordinateurs de l'entreprise-client .....	43
Création d'une hiérarchie des groupes d'administration soumis au Serveur d'administration virtuel .....	44
INSTALLATION A DISTANCE DES APPLICATIONS .....	45
Installation des applications à l'aide de la tâche d'installation à distance .....	47
Installation de l'application sur les postes clients sélectionnés .....	47
Installation des applications sur les postes clients du groupe d'administration .....	48
Installation des applications sur les Serveurs d'administration secondaires .....	48
Installation des applications à l'aide de l'Assistant d'installation à distance .....	49
Consultation du rapport de déploiement de la protection .....	50
Désinstallation à distance des applications .....	50
Désinstallation à distance de l'application avec les postes clients du groupe d'administration .....	51
Désinstallation à distance de l'application des postes clients sélectionnés.....	51
Fonctionnement avec les paquets d'installation .....	52
Génération du paquet d'installation.....	52
Propagation des paquets d'installation sur les Serveurs d'administration secondaires.....	53
Propagation des paquets d'installation à l'aide des agents de mise à jour .....	53
Transfert dans Kaspersky Security Center des informations sur les résultats d'installation de l'application .....	53
Récupération des version actuelles des applications .....	55
Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe .....	56
Préparation de l'ordinateur à l'installation à distance en mode interactif .....	56
Préparation de l'ordinateur à l'installation à distance en mode non interactif .....	57
INSTALLATION LOCALE DES APPLICATIONS .....	59
Installation locale de l'Agent d'administration .....	60
Installation locale du plug-in d'administration de l'application .....	60
Installation de l'application en mode non interactif.....	60
Installation de l'application à l'aide des paquets autonomes.....	61
CHARGE SUR LE RESEAU .....	62
Déploiement initial de la protection antivirus.....	62
Mise à jour initiale des bases antivirus .....	63
Synchronisation du client avec le Serveur d'administration .....	63
Mise à jour complémentaire des bases antivirus .....	64
Traitement des événements des clients par le Serveur d'administration .....	65
Débit du trafic pendant vingt-quatre heures.....	65
VITESSE DE REMPLISSAGE DE LA BASE DE DONNEES PAR LES EVENEMENTS DE KASPERSKY ENDPOINT SECURITY .....	66
CONTACTER LE SUPPORT TECHNIQUE .....	67
GLOSSAIRE .....	68
KASPERSKY LAB ZAO .....	73
NOTIFICATION SUR LES MARQUES DE COMMERCE .....	74
INDEX .....	75

# A PROPOS DE CE MANUEL

Ce document décrit l'installation des composants de l'application Kaspersky Security Center 9.0 (ci-après – Kaspersky Security Center), ainsi que l'installation à distance et locale des applications Kaspersky Lab dans un réseau informatique des entreprises tierces.

Le document s'adresse aux administrateurs de protection antivirus des réseaux des entreprises et aux entreprises offrant des services SaaS (ci-après – *prestataires de services*).

Dans les cas, quand les actions du prestataire de services sont différentes des actions de l'administrateur du réseau de l'entreprise, les actions du prestataire de services sont décrites séparément.

## DANS CETTE SECTION

---

Dans ce document .....	<a href="#">5</a>
Conventions .....	<a href="#">7</a>

## DANS CE DOCUMENT

Le Manuel d'implantation de Kaspersky Security Center contient l'introduction, les sections qui décrivent l'installation des composants de l'application et les paramètres de leur interaction décrivant le déploiement de la protection antivirus du réseau, les sections avec les informations sur le test de charge, ainsi que le glossaire des termes.

### Sources d'informations complémentaires (à la page [8](#))

Cette section reprend les informations où vous pouvez obtenir des informations sur l'application, excepté les documents livrés avec l'application.

### Kaspersky Security Center (à la page [10](#))

Cette section reprend les informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Security Center.

### Architecture de l'application (à la page [11](#))

Cette section décrit les composants internes de l'application Kaspersky Security Center et la logique de leur interaction.

### Configurations matérielles et logicielles (à la page [12](#))

Cette section contient les informations sur les configurations matérielles et logicielles des ordinateurs du réseau.

### Informations sur la productivité du Serveur d'administration (à la page [15](#))

La section reprend les résultats du test de productivité du Serveur d'administration pour différentes configurations matérielles.

### Schémas typiques de déploiement de la protection antivirus (à la page [16](#))

Cette section décrit les schémas typiques de déploiement de la protection antivirus dans le réseau de l'entreprise à l'aide de Kaspersky Security Center.

### **Déploiement de la protection antivirus à l'intérieur de l'entreprise (à la page [17](#))**

Cette section décrit les processus de déploiement de la protection antivirus à l'intérieur de l'entreprise, qui correspondent aux schémas typiques de déploiement.

### **Déploiement de la protection antivirus dans le réseau de l'entreprise-client (à la page [20](#))**

Cette section décrit les processus de déploiement de la protection antivirus dans le réseau de l'entreprise-client, qui correspondent aux schémas typiques de déploiement.

### **Déploiement du Serveur d'administration (à la page [23](#))**

Cette section décrit les étapes de déploiement du Serveur d'administration.

### **Configuration de la protection antivirus du réseau de l'entreprise-client (à la page [41](#))**

Cette section décrit les particularités de la configuration du système de protection antivirus via la Console d'administration dans le réseau de l'entreprise-client.

### **Installation à distance des applications (à la page [45](#))**

Cette section décrit les moyens de l'installation à distance des applications de Kaspersky Lab ou leur suppression depuis les ordinateurs du réseau.

### **Installation locale des applications (à la page [59](#))**

Cette section décrit la procédure d'installation des applications qui peuvent être installées sur les ordinateurs uniquement d'une manière locale.

### **Charge sur le réseau (à la page [62](#))**

Cette section contient l'information sur le volume du trafic réseau que les postes clients et le Serveur d'administration échangent entre eux-mêmes lors de l'exécution des opérations clés administratives.

### **Vitesse de remplissage de la base de données par les événements de Kaspersky Endpoint Security (à la page [66](#))**

Cette section reprend les exemples de vitesse de remplissage de la base de données du Serveur d'administration par les événements.

### **Contacter le service du Support Technique (à la page [67](#))**

Cette section décrit les règles des appels au service du Support Technique.

### **Glossaire**

La section reprend les termes utilisés dans ce document.

### **Kaspersky Lab ZAO (à la page [73](#))**

Cette section reprend les informations sur Kaspersky Lab ZAO.

### **Notifications sur les marques de commerce (à la page [74](#))**

Cette section reprend les notifications sur les marques de commerce déposées.

## Index

Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

# CONVENTIONS

Les conventions décrites dans le tableau ci-dessous sont utilisées dans le document.

Tableau 1. Conventions

EXEMPLE DU TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance.
<b>Exemple:</b> ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La <i>mise à jour</i> , c'est ...	Les nouveaux termes sont en italique.
<b>ALT+F4</b>	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.
<b>Activer</b>	Les noms des éléments de l'interface sont en caractères mi-gras : les champs de saisie, les commandes du menu, les boutons.
➡ <i>Pour planifier une tâche, procédez comme suit :</i>	Les phrases d'introduction sont en italique.
help	Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux.
<adresse IP de votre ordinateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable à chaque fois. Par ailleurs, les parenthèses angulaires sont omises.

# SOURCES D'INFORMATIONS COMPLEMENTAIRES

Cette section reprend les informations où vous pouvez obtenir des informations sur l'application, excepté les documents livrés avec l'application.

Si vous avez des questions sur le choix, l'achat, l'installation ou l'utilisation de Kaspersky Security Center, vous pouvez obtenir des réponses rapidement.

Kaspersky Lab offre de nombreuses sources d'informations sur l'application. Vous pouvez choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

## DANS CETTE SECTION

---

Sources d'informations pour les recherches indépendantes .....	<a href="#">8</a>
Discussion sur les applications de Kaspersky Lab sur le forum .....	<a href="#">9</a>
Contacteur le Groupe de rédaction de la documentation pour les utilisateurs .....	<a href="#">9</a>

## SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

- page consacrée à l'application sur le site Internet de Kaspersky Lab ;
- page consacrée à l'application sur le site Internet du service du Support Technique (dans la Base de connaissances) ;
- système d'aide électronique ;
- documentation.

### Page sur le site Internet de Kaspersky Lab

<http://www.kaspersky.com/fr/security-center>

Cette page fournit des informations générales sur l'application, ses possibilités et ses particularités.

### Page sur le site Internet du service du Support Technique (Base de connaissances)

[http://support.kaspersky.com/fr/remote\\_adm](http://support.kaspersky.com/fr/remote_adm)

Cette page propose des articles publiés par les experts du service du Support Technique.

Ces articles contiennent des informations utiles, des recommandations et les réponses aux questions les plus souvent posées sur l'achat, l'installation et l'utilisation de l'application Kaspersky Security Center. Ils sont regroupés par thèmes tels que "Manipulation des fichiers clés", "Mise à jour des bases" ou "Résolution des problèmes". Les articles peuvent répondre à des questions concernant non seulement cette application Kaspersky Security Center, mais également d'autres logiciels de Kaspersky Lab. Ils peuvent aussi contenir des informations sur le service du Support Technique dans son ensemble.

## Systeme d'aide électronique

Une aide complète est livrée avec l'application.

Celle-ci propose une description détaillée des fonctions proposées par l'application.

Pour ouvrir l'aide, sélectionnez l'élément **Rubriques de l'aide** dans le menu **Aide** de la console.

Si vous avez des questions sur une fenêtre en particulier de l'application, vous pouvez consulter l'aide contextuelle.

Pour ouvrir l'aide contextuelle, appuyez sur la touche **F1** dans la fenêtre qui vous intéresse.

## Documentation

La documentation qui accompagne cette application contient la majorité des informations indispensables pour son utilisation. Elle contient des documents suivants :

- **Le Manuel de l'administrateur** décrit le but, les notions principales, les fonctions et le mode de fonctionnement général de Kaspersky Security Center.
- **Le Manuel d'implantation** décrit l'installation des composants de Kaspersky Security Center, ainsi que l'installation à distance des applications dans un réseau informatique de configuration simple.
- **Guide de démarrage** contient une description des étapes qui permettront à l'administrateur de la sécurité antivirus de l'entreprise de commencer à utiliser rapidement Kaspersky Security Center et de déployer la protection antivirus dans tout le réseau sur la base des applications de Kaspersky Lab.

Ces documents sont en format PDF et sont livrés avec Kaspersky Security Center.

Vous pouvez télécharger la documentation depuis les pages consacrées à l'application sur le site Internet de Kaspersky Lab.

Les informations sur l'interface de l'application d'administration (API) Kaspersky Security Center s'affichent dans le fichier klakaut.chm situé dans le dossier d'installation de l'application.

## DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum à l'adresse <http://forum.kaspersky.fr>.

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

## CONTACTER LE GROUPE DE REDACTION DE LA DOCUMENTATION POUR LES UTILISATEURS

Si vous avez des questions concernant la documentation, ou vous y avez trouvé une erreur, ou vous voulez laisser un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs.

En passant par le lien **Envoyer des commentaires** situé en haut à droite de la fenêtre de l'aide, vous pouvez ouvrir la fenêtre du client de messagerie utilisé par défaut sur votre ordinateur. L'adresse du groupe de rédaction de la documentation – docfeedback@kaspersky.com sera indiquée dans la fenêtre ouverte, et dans le sujet du message – "Kaspersky Help Feedback: Kaspersky Security Center". Sans modifier le sujet du message, écrivez votre commentaire et envoyez le message.

# KASPERSKY SECURITY CENTER

Cette section reprend les informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Security Center.

Le logiciel est proposé dans deux versions :

- Kaspersky Security Center 9.0 (ci-après – Kaspersky Security Center) est proposé gratuitement avec toutes les applications de Kaspersky Lab de la suite Kaspersky Open Space Security (version vendue en boîte). Il peut également être téléchargé depuis le site de Kaspersky Lab (<http://www.kaspersky.fr>).
- Kaspersky Security Center 9.0, Service Provider Edition (ci-après – Kaspersky Security Center SPE) est livré sous les conditions particulières aux partenaires de Kaspersky Lab. Pour plus d'informations, visitez le site Internet de Kaspersky Lab, à la page <http://www.kaspersky.com/fr/partners>.

L'application Kaspersky Security Center est un précurseur de l'application Kaspersky Security Center.

L'application Kaspersky Security Center a été développée pour l'exécution centralisée des principales tâches d'administration de la gestion de la sécurité antivirus des réseaux informatiques des entreprises qui repose sur l'emploi des applications reprises dans la suite logicielle Kaspersky Open Space Security. Kaspersky Security Center prend en charge toutes les configurations réseau utilisant le protocole TCP/IP.

L'application Kaspersky Security Center est un outil pour les administrateurs de réseaux d'entreprise et pour les responsables de la sécurité antivirus.

La version SPE est un outil pour les entreprises offrant les services SaaS (ci-après – *prestataires de services*).

A l'aide de Kaspersky Security Center, vous pouvez :

- Créer les Serveurs d'administration virtuels pour assurer une protection antivirus des bureaux à distance ou des réseaux des entreprises-clients.

Sous les *entreprises-clients*, les entreprises, dont la protection antivirus est assurée par le prestataire de services, sont ici sous-entendues.

- Former une hiérarchie de groupes d'administration qui assure une protection antivirus de l'entreprise. Les groupes d'administration permettent d'administrer la sélection d'ordinateurs comme un tout unique.
- Effectuer l'installation et la désinstallation à distance des applications de Kaspersky Lab.
- Effectuer à distance l'administration centralisée des applications de Kaspersky Lab.
- Recevoir et diffuser de façon centralisée sur les postes clients les mises à jour des bases et des modules des applications de Kaspersky Lab.
- Recevoir les notifications sur les événements critiques dans le fonctionnement des applications de Kaspersky Lab.
- Recevoir les statistiques et les rapports de fonctionnement des applications de Kaspersky Lab.
- Administrer les clés des applications installées de Kaspersky Lab.
- Travailler de façon centralisée avec les fichiers, placés en quarantaine ou dans le dossier de sauvegarde par les applications antivirus, aussi qu'avec les objets dont le traitement est différé.
- Travailler de façon centralisée avec les applications des éditeurs tiers, installées sur les postes clients.

# ARCHITECTURE DE L'APPLICATION

Cette section décrit les composants internes de l'application Kaspersky Security Center et la logique de leur interaction.

L'application Kaspersky Security Center inclut les composants principaux suivants :

- **Serveur d'administration** (ci-après aussi *Serveur*). Est un entrepôt centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau local de la société et un outil efficace de gestion de ces applications.
- **Agent d'administration** (ci-après aussi *Agent*). Coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste du réseau (lui-même un poste de travail ou un serveur). Ce composant est unique pour toutes les applications qui font partie des produits Kaspersky Open Space Security, élaborés pour les systèmes Microsoft® Windows®. Pour les applications Kaspersky Lab, élaborées pour les systèmes Novell® et Unix®, des versions isolées de l'Agent d'administration existent.
- **Console d'administration** (ci-après aussi *Console*). Fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur et de l'Agent d'administration. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console). La Console d'administration permet de se connecter au Serveur d'administration distant par Internet.
- **Kaspersky Security Center Web-Console**. Conçu pour contrôler l'état de la protection antivirus de l'entreprise cliente se trouvant sous l'administration de Kaspersky Security Center.

# CONFIGURATIONS LOGICIELLE ET MATERIELLE

Cette section contient les informations sur les configurations matérielles et logicielles des ordinateurs du réseau.

## Serveur d'administration et Kaspersky Security Center Web-Console

- Configuration logicielle :
  - Microsoft Data Access® Components (MDAC) de version 2.8 ou supérieure ou Microsoft Windows DAC 6.0.
  - Système de gestion des bases de données : Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, MySQL versions 5.0.67, 5.0.77, 5.0.85, 5.0.87 Service Pack 1, 5.0.91 ou MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.
  - Microsoft Windows Server® 2003 et supérieur ; Microsoft Windows Server 2003 x64 et supérieur ; Microsoft Windows Server 2008 ; Microsoft Windows Server 2008 déployé en mode Server Core ; Microsoft Windows Server 2008 x64 avec Service Pack 1 et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows Server 2008 R2 ; Microsoft Windows Server 2008 R2 déployé en mode Server Core ; Microsoft Windows XP Professional avec Service Pack 2 et supérieur ; Microsoft Windows XP Professional x64 et supérieur ; Microsoft Windows Vista® avec Service Pack 1 et supérieur, Microsoft Windows Vista x64 avec Service Pack 1 et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows 7 ; Microsoft Windows 7 x64.
- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.
  - Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
    - Processeur avec 1,4 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.

## Console d'administration

- Configuration logicielle :
  - Système d'exploitation Microsoft Windows.  
  
La version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration.
  - Microsoft Management Console version 2.0 et supérieure.

- Lors du fonctionnement sous Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 ou Microsoft Windows Vista : la présence du navigateur installé Microsoft Internet Explorer® 7.0 ou suivant est requise.
- L'utilisation sous Microsoft Windows 7 requiert Microsoft Internet Explorer 8.0 ou suivant.
- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.
  - Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
    - Processeur avec 1,4 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.

### Agent d'administration et agent de mises à jour

- Configuration logicielle :
  - Système d'exploitation :
    - Microsoft Windows.
    - Linux®.
    - Mac OS.

La version du système d'exploitation pris en charge est définie selon les exigences des applications dont l'administration est accessible via Kaspersky Security Center.

- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
  - Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
    - Processeur avec 1,4 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.

- Pendant le fonctionnement sous le système d'exploitation Linux 32 bits :
  - Processeur avec 1 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation Linux 64 bits :
  - Processeur avec 1,4 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation Mac OS :
  - Processeur avec 1 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.

# INFORMATIONS SUR LA PRODUCTIVITE DU SERVEUR D'ADMINISTRATION

La section reprend les résultats du test de productivité du Serveur d'administration pour différentes configurations matérielles.

Les résultats des tests de productivité du Serveur d'administration ont permis de définir les nombres maximaux des postes clients avec lesquels le Serveur d'administration peut exécuter la synchronisation pour les délais indiqués. Cette information peut être utilisée pour sélectionner les schémas optimaux de déploiement de la protection antivirus dans les réseaux informatiques des entreprises.

Les configurations matérielles suivantes du Serveur d'administration ont été utilisées pour le test :

- Système d'exploitation 32 bits (processeur à 2 noyaux Intel® Core®2 Duo E8400, 3.00 GHz, 4 Go RAM, disque dur SATA 500 Go) ;
- Système d'exploitation 64 bits (processeur à 4 noyaux Intel Xeon® E5450, 3.00 GHz, 8 Go RAM, disque dur SAS 2x320 RAID 0).

Le serveur des bases de données Microsoft SQL 2005x32 Enterprise Edition a été installé sur le même ordinateur que le Serveur d'administration.

Le Serveur d'administration de deux configurations matérielles avait pris en charge la création de 200 Serveurs d'administration virtuels.

Tableau 2. Résultats généralisés du test de charge du Serveur d'administration sous le système d'exploitation de 32 bits

Période de synchronisation, min.	Nombre d'ordinateurs administrés
15	5 000
30	10 000
45	15 000
60	20 000

Tableau 3. Résultats généralisés du test de charge du Serveur d'administration sous le système d'exploitation de 64 bits

Période de synchronisation, min.	Nombre d'ordinateurs administrés
15	10 000
30	20 000
45	30 000
60	40 000

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL et SQL Express, il n'est pas recommandé d'utiliser l'application pour administrer plus de 5 000 ordinateurs.

Ce document reprend aussi les informations détaillées sur les résultats du test de productivité du Serveur d'administration.

# SCHEMAS TYPIQUES DE DEPLOIEMENT DE LA PROTECTION ANTIVIRUS

Cette section décrit les schémas typiques de déploiement de la protection antivirus dans le réseau de l'entreprise à l'aide de Kaspersky Security Center.

Vous pouvez déployer la protection antivirus dans le réseau de l'entreprise à l'aide de Kaspersky Security Center, en utilisant les schémas suivants de déploiement :

- Le déploiement de la protection antivirus via les outils de Kaspersky Security Center à l'aide d'un des moyens suivants :
  - à l'aide de la Console d'administration ;
  - par Kaspersky Security Center Web-Console.

L'installation des applications Kaspersky Lab sur les postes clients et la connexion des postes clients au Serveur d'administration se passent automatiquement à l'aide de Kaspersky Security Center.

Le schéma principal de déploiement est le déploiement de la protection antivirus via la Console d'administration. L'utilisation de Kaspersky Security Center Web-Console permet de lancer l'installation des applications de Kaspersky Lab via le navigateur.

- Le déploiement manuel de la protection antivirus à l'aide des paquets autonomes d'installation, formés dans Kaspersky Security Center.

L'installation des applications Kaspersky Lab sur les postes clients et sur le poste administrateur s'opère manuellement. Les paramètres de connexion des postes clients au Serveur d'administration seront définis lors de l'installation de l'Agent d'administration.

Cette option de déploiement est recommandée dans les cas, quand l'installation à distance n'est pas possible.

Kaspersky Security Center permet aussi de déployer la protection antivirus à l'aide des stratégies de groupe Active Directory®. Pour plus d'informations, cf. l'aide de Kaspersky Security Center.

# DEPLOIEMENT DE LA PROTECTION ANTIVIRUS A L'INTERIEUR DE L'ENTREPRISE

Cette section décrit les processus de déploiement de la protection antivirus à l'intérieur de l'entreprise, qui correspondent aux schémas typiques de déploiement.

## DANS CETTE SECTION

---

Déploiement de la protection antivirus via la Console d'administration à l'intérieur de l'entreprise .....	<a href="#">17</a>
Déploiement de la protection antivirus à l'aide des outils de Kaspersky Security Center Web-Console à l'intérieur de l'entreprise.....	<a href="#">18</a>
Déploiement manuel de la protection antivirus à l'intérieur de l'entreprise.....	<a href="#">18</a>

## DEPLOIEMENT DE LA PROTECTION ANTIVIRUS VIA LA CONSOLE D'ADMINISTRATION A L'INTERIEUR DE L'ENTREPRISE

L'administrateur de Kaspersky Security Center (ci-après, l'administrateur) effectue l'installation à distance du logiciel antivirus. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - c. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. configure les paramètres du Serveur d'administrateur.
2. S'il faut, l'administrateur crée une hiérarchie des Serveurs d'administration dans Kaspersky Security Center.
3. L'administrateur forme une structure des groupes d'administration et diffuse les postes clients de l'entreprise selon les groupes d'administration.
4. L'administrateur crée et configure dans Kaspersky Security Center les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.
5. L'administrateur choisit dans le Console d'administration les ordinateurs à installer les applications sélectionnées.
6. L'administrateur crée et lance les tâches d'installation à distance des applications sélectionnées via la Console d'administration.
7. En fonction des besoins, l'administrateur exécute une configuration complémentaire des applications installées via la Console d'administration : à l'aide des stratégies et des paramètres locaux des applications.

## DEPLOIEMENT DE LA PROTECTION ANTIVIRUS A L'AIDE DES OUTILS DE KASPERSKY SECURITY CENTER WEB-CONSOLE A L'INTERIEUR DE L'ENTREPRISE

L'administrateur de Kaspersky Security Center (ci-après, l'administrateur) effectue l'installation à distance du logiciel antivirus. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe Kaspersky Security Center Web-Console sur le même ordinateur ;
  - c. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - e. configure le Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console.
2. L'administrateur crée le Serveur d'administration virtuel dans Kaspersky Security Center pour gérer les postes clients.
3. L'administrateur choisit l'ordinateur dans le réseau, qui jouera le rôle de l'agent de mises à jour, et installe localement l'Agent d'administration sur celui-ci.
 

Enfin, Kaspersky Security Center désigne automatiquement le poste client avec l'Agent d'administration installé en tant que l'agent de mises à jour et le configure en tant que la passerelle des connexions lors de la première connexion avec le Serveur d'administration.
4. L'administrateur crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.
5. L'administrateur lance Kaspersky Security Center Web-Console.
6. L'administrateur lance l'installation des applications sélectionnées sur les postes clients dans Kaspersky Security Center Web-Console.
7. En fonction des besoins, l'administrateur exécute une configuration complémentaire des applications installées via la Console d'administration : à l'aide des stratégies et des paramètres locaux des applications.

## DEPLOIEMENT MANUEL DE LA PROTECTION ANTIVIRUS A L'INTERIEUR DE L'ENTREPRISE

L'administrateur de Kaspersky Security Center (ci-après, l'administrateur) effectue l'installation manuelle du logiciel antivirus à l'aide des paquets autonomes d'installation. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - c. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. configure les paramètres du Serveur d'administrateur.

2. S'il faut, l'administrateur crée une hiérarchie des Serveurs d'administration dans Kaspersky Security Center.
3. L'administrateur crée une structure des groupes d'administration.
4. L'administrateur crée et configure dans Kaspersky Security Center les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.
5. L'administrateur crée les paquets autonomes d'installation pour les applications sélectionnées.
6. L'administrateur transmet les paquets autonomes d'installation sur les postes clients, par exemple, en publiant le lien vers les paquets autonomes.
7. Les utilisateurs des postes clients lancent l'installation des applications à l'aide des paquets autonomes reçus d'installation.
8. Après l'établissement du lien avec le Serveur d'administration, les postes clients se déplacent dans les groupes d'administration indiqués dans les propriétés des paquets autonomes d'installation.

# DEPLOIEMENT DE LA PROTECTION ANTIVIRUS DANS LE RESEAU DE L'ENTREPRISE-CLIENT

Cette section décrit les processus de déploiement de la protection antivirus dans le réseau de l'entreprise-client, qui correspondent aux schémas typiques de déploiement.

## DANS CETTE SECTION

---

Déploiement de la protection antivirus via la Console d'administration dans le réseau de l'entreprise-client.....	<a href="#">20</a>
Déploiement de la protection antivirus via la Kaspersky Security Center Web-Console dans le réseau de l'entreprise-client.....	<a href="#">21</a>
Déploiement manuel de la protection antivirus dans le réseau de l'entreprise-client .....	<a href="#">21</a>

## DEPLOIEMENT DE LA PROTECTION ANTIVIRUS VIA LA CONSOLE D'ADMINISTRATION DANS LE RESEAU DE L'ENTREPRISE-CLIENT

L'installation à distance du logiciel antivirus via Kaspersky Security Center Web-Console est effectuée par l'administrateur de Kaspersky Security Center conjointement avec l'administrateur de l'entreprise-client. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur Kaspersky Security Center déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe Kaspersky Security Center Web-Console sur le même ordinateur ;
  - c. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - e. configure le Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console.
2. L'administrateur de Kaspersky Security Center crée dans Kaspersky Security Center le Serveur d'administration virtuel pour gérer les postes clients de l'entreprise-client.
3. L'administrateur Kaspersky Security Center choisit l'ordinateur dans le réseau, qui jouera le rôle de l'agent de mises à jour, et installe localement l'Agent d'administration sur celui-ci.

Enfin, Kaspersky Security Center désigne automatiquement le poste client avec l'Agent d'administration installé en tant que l'agent de mises à jour et le configure en tant que la passerelle des connexions lors de la première connexion avec le Serveur d'administration.

4. L'administrateur Kaspersky Security Center crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.

5. L'administrateur Kaspersky Security Center choisit dans le Console d'administration les ordinateurs à installer les applications sélectionnées.
6. L'administrateur crée et lance les tâches d'installation à distance des applications sélectionnées via la Console d'administration.
7. En fonction des besoins, l'administrateur exécute une configuration complémentaire des applications installées via la Console d'administration : à l'aide des stratégies et des paramètres locaux des applications.

## **DEPLOIEMENT DE LA PROTECTION ANTIVIRUS VIA LA KASPERSKY SECURITY CENTER WEB-CONSOLE DANS LE RESEAU DE L'ENTREPRISE-CLIENT**

L'installation à distance du logiciel antivirus via Kaspersky Security Center Web-Console est effectuée par l'administrateur de Kaspersky Security Center conjointement avec l'administrateur de l'entreprise-client. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur Kaspersky Security Center déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe Kaspersky Security Center Web-Console sur le même ordinateur ;
  - c. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - e. configure le Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console.
2. L'administrateur de Kaspersky Security Center crée dans Kaspersky Security Center le Serveur d'administration virtuel pour gérer les postes clients de l'entreprise-client.
3. L'administrateur de l'entreprise-client choisit l'ordinateur dans le réseau, qui jouera le rôle de l'agent de mises à jour, et installe localement l'Agent d'administration sur celui-ci.

Finalement, Kaspersky Security Center désigne automatiquement le poste client avec l'Agent d'administration installé en tant que l'agent de mises à jour et le configure en tant que la passerelle des connexions lors de la première connexion avec le Serveur d'administration.

4. L'administrateur Kaspersky Security Center crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.
5. L'administrateur de l'entreprise-client lance l'installation des applications sélectionnées sur les postes clients dans Kaspersky Security Center Web-Console.
6. En fonction des besoins, l'administrateur Kaspersky Security Center exécute une configuration complémentaire des applications installées via la Console d'administration : à l'aide des stratégies et des paramètres locaux des applications.

## DEPLOIEMENT MANUEL DE LA PROTECTION ANTIVIRUS DANS LE RESEAU DE L'ENTREPRISE-CLIENT

L'installation manuelle du logiciel antivirus à l'aide des paquets autonomes d'installation est effectuée par l'administrateur de Kaspersky Security Center conjointement avec l'administrateur de l'entreprise-client. Dans ce cas, le processus de déploiement se compose des étapes principales suivantes :

1. L'administrateur Kaspersky Security Center déploie le Serveur d'administration de manière suivante :
  - a. installe Kaspersky Security Center sur l'ordinateur sélectionné ;
  - b. installe Kaspersky Security Center Web-Console sur le même ordinateur ;
  - c. installe la Console d'administration sur le poste de travail de l'administrateur (si nécessaire) ;
  - d. installe la Kaspersky Security Center SHV sur le poste de travail de l'administrateur (si nécessaire) ;
  - e. configure le Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console.
2. L'administrateur de Kaspersky Security Center crée dans Kaspersky Security Center le Serveur d'administration virtuel pour gérer les postes clients de l'entreprise-client.
3. L'administrateur de l'entreprise-client choisit l'ordinateur dans le réseau, qui jouera le rôle de l'agent de mises à jour, et installe localement l'Agent d'administration sur celui-ci.

Finalement, Kaspersky Security Center désigne automatiquement le poste client avec l'Agent d'administration installé en tant que l'agent de mises à jour et le configure en tant que la passerelle des connexions lors de la première connexion avec le Serveur d'administration.

4. L'administrateur Kaspersky Security Center crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications antivirus de Kaspersky Lab.
5. L'administrateur Kaspersky Security Center crée les paquets autonomes d'installation pour les applications sélectionnées.
6. L'administrateur de Kaspersky Security Center transmet à l'entreprise desservie le paquet autonome d'installation, par exemple, en publiant le lien vers le paquet autonome d'installation dans Kaspersky Security Center Web-Console.
7. L'administrateur de l'entreprise desservie transmet le paquet autonome d'installation sur les ordinateurs sélectionnés via Kaspersky Security Center Web-Console.
8. Les utilisateurs des postes clients lancent l'installation de l'application à l'aide du paquet autonome d'installation obtenu.
9. Après l'établissement du lien avec le Serveur d'administration, les postes clients se déplacent dans le groupe d'administration indiqué dans les propriétés du paquet autonome d'installation.

# DEPLOIEMENT DU SERVEUR D'ADMINISTRATION

Cette section décrit les étapes de déploiement du Serveur d'administration.

Les étapes de déploiement sont décrites pour deux options de travail avec l'application :

- le déploiement du Serveur d'administration à l'intérieur de l'entreprise ;
- le déploiement du Serveur d'administration pour la protection antivirus de l'entreprise client (lors du travail avec les versions SPE de l'application).

S'il vous faut déployer le Serveur d'administration à l'intérieur de l'entreprise qui inclut les bureaux à distance ne faisant pas partie du réseau de l'entreprise, vous pouvez suivre l'ordre de déploiement de la protection antivirus pour les prestataires de services.

La section décrit ci-après les actions qui font partie des étapes de déploiement de la protection.

## DANS CETTE SECTION

Étapes de déploiement du Serveur d'administration à l'intérieur de l'entreprise.....	<a href="#">23</a>
Étapes de déploiement du Serveur d'administration pour la protection antivirus de l'entreprise-client .....	<a href="#">24</a>
Mise à jour d'une version antérieure de l'application Kaspersky Security Center.....	<a href="#">24</a>
Installation de Kaspersky Security Center.....	<a href="#">25</a>
Installation de la Console d'administration sur le poste de travail de l'administrateur .....	<a href="#">35</a>
Installation et configuration de Kaspersky Security Center SHV .....	<a href="#">36</a>
Installation de Kaspersky Security Center Web-Console .....	<a href="#">36</a>
Configuration du fonctionnement du Serveur d'administration avec Kaspersky Security Center Web-Console.....	<a href="#">39</a>

## ÉTAPES DE DEPLOIEMENT DU SERVEUR D'ADMINISTRATION A L'INTERIEUR DE L'ENTREPRISE

➤ *Pour déployer le Serveur d'administration à l'intérieur de l'entreprise, procédez comme suit :*

1. Installez Kaspersky Security Center sur le poste de travail de l'administrateur.
2. S'il faut, installez Kaspersky Security Center SHV sur le poste de travail de l'administrateur.
3. Configurez les paramètres du Serveur d'administration.

## ÉTAPES DE DEPLOIEMENT DU SERVEUR D'ADMINISTRATION POUR LA PROTECTION ANTIVIRUS DE L'ENTREPRISE-CLIENT

➤ Pour déployer le Serveur d'administration pour la protection antivirus de l'entreprise client, procédez comme suit :

1. Installez Kaspersky Security Center sur le poste de travail de l'administrateur.
2. S'il faut, installez Kaspersky Security Center SHV sur le poste de travail de l'administrateur.
3. Installez Kaspersky Security Center Web-Console sur le poste de travail de l'administrateur.
4. Configurez les paramètres du Serveur d'administration pour le fonctionnement avec Kaspersky Security Center Web-Console.

## MISE A JOUR D'UNE VERSION ANTERIEURE DE L'APPLICATION KASPERSKY SECURITY CENTER

Kaspersky Security Center prend en charge la restauration des données de la copie de sauvegarde des données du Serveur d'administration, formée par la version de l'application antérieure.

➤ Pour actualiser le Serveur d'administration de version 8.0 jusqu'à la version 9.0, procédez comme suit :

1. Pour Kaspersky Administration Kit 8.0 créez une copie de réserve des données du Serveur d'administration à l'aide de l'utilitaire *klbackup*. Cette utilitaire fait partie du distributif de l'application et se trouvent dans la racine du dossier d'installation Kaspersky Administration Kit.

Pour une restauration complète des données du Serveur d'administration lors de la création de la copie de sauvegarde des données, il faut enregistrer le certificat du Serveur d'administration. Le certificat du Serveur d'administration est nécessaire pour le fonctionnement de l'utilitaire *klbackup*.

Les informations détaillées sur le fonctionnement de l'utilitaire de la copie de sauvegarde et de la restauration des données sont fournies dans le *Manuel de l'administrateur de Kaspersky Security Center*.

2. Installez le Serveur d'administration de version 9.0 sur l'ordinateur sur lequel la version précédente du Serveur d'administration est installée. Lors de la mise à jour jusqu'à la version 9.0, les données et les paramètres de version précédente du Serveur d'administration sont enregistrés.

L'interruption du processus de mise à jour à l'étape d'installation du Serveur d'administration peut amener au dysfonctionnement de Kaspersky Administration Kit 8.0.

3. Pour les ordinateurs sélectionnés, créez et lancez une tâche d'installation à distance pour la nouvelle version de l'Agent d'administration. Après sa fin réussie, la version de l'Agent d'administration sera actualisée.

En cas de problèmes lors de l'installation, vous pouvez restaurer la version précédente du Serveur d'administration, en utilisant la copie de sauvegarde des données du Serveur créée avant la mise à jour.

Si dans le réseau au moins un Serveur d'administration de nouvelle version est installé, la mise à jour d'autres Serveurs d'administration dans le réseau peut être effectuée à l'aide de la tâche d'installation à distance qui utilise le paquet du Serveur d'administration.

# INSTALLATION DE KASPERSKY SECURITY CENTER

La procédure d'installation locale des composants de Kaspersky Security Center. Les deux types d'installation dont disponibles :

- **Standard.** Dans ce cas, l'ensemble minimal de composants nécessaires de l'application sera installé. Ce type d'installation est recommandé pour les réseaux contenant moins de 200 ordinateurs.
- **Personnalisée.** En ce cas vous pouvez sélectionner des composants particuliers pour l'installation et configurer les paramètres complémentaires de l'application. Ce type d'installation est recommandé pour les réseaux contenant plus de 200 ordinateurs. L'installation personnalisée est recommandé pour les utilisateurs expérimentés.

Si dans le réseau au moins un Serveur d'administration est installé, les Serveurs peuvent être installés sur d'autres ordinateurs à l'aide de la tâche d'installation à distance avec la méthode d'installation forcée (cf. section "Installation des applications à l'aide de la tâche d'installation à distance" à la page [46](#)). Lors de la formation de la tâche d'installation à distance, il faut utiliser le paquet d'installation du Serveur d'administration.

## DANS CETTE SECTION

---

Préparation de l'installation .....	<a href="#">25</a>
Installation standard .....	<a href="#">27</a>
Installation personnalisée.....	<a href="#">27</a>
Modifications dans le système après l'installation .....	<a href="#">34</a>
Suppression de l'application.....	<a href="#">35</a>

## PREPARATION DE L'INSTALLATION

Avant l'installation il est nécessaire de s'assurer que la configuration logicielle et matérielle de l'ordinateur correspond aux exigences émises au Serveur d'administration et à la Console d'administration (cf. section "Configurations logicielle et matérielle" à la page [12](#)).

Kaspersky Security Center garde l'information dans la base de données du serveur SQL. Avec cela, l'application Microsoft SQL Server 2005 Express Edition s'installe par défaut avec Kaspersky Security Center. Pour garder l'information vous pouvez aussi utiliser d'autres serveurs SQL (cf. section "Configurations logicielle et matérielle" à la page [12](#)). En ce cas, ils doivent être installés dans le réseau avant l'installation de Kaspersky Security Center.

Pour installer Kaspersky Security Center il est nécessaire d'avoir les privilèges d'administrateur local sur l'ordinateur, où l'installation a lieu.

Afin que tous les composants de l'application fonctionnent correctement, tous les ports requis doivent être ouverts sur les ordinateurs (cf. tableau ci-après).

Tableau 4. Ports utilisés par Kaspersky Security Center

NUMERO DE PORT	PROTOCOLE	DESCRIPTION
<b>Ordinateur avec le Serveur d'administration installé</b>		
13000	TCP	Utilisé pour les buts suivants : <ul style="list-style-type: none"> <li>• l'obtention de données des postes clients ;</li> <li>• la connexion des agents de mises à jour ;</li> <li>• la connexion des Serveurs d'administration secondaires.</li> </ul> Avec cela, la connexion SSL sécurisée est utilisée.
14000	TCP	Utilisé pour les buts suivants : <ul style="list-style-type: none"> <li>• l'obtention de données des postes clients ;</li> <li>• la connexion des agents de mises à jour ;</li> <li>• la connexion des Serveurs d'administration secondaires.</li> </ul> Avec cela, la connexion SSL sécurisée n'est pas utilisée.
13000	UDP	Utilisé pour le transfert d'informations sur la désactivation des ordinateurs.
13292	TCP	Est utilisé pour la connexion des périphériques mobiles.
18000	HTTP	Est utilisé pour l'obtention des données par le Serveur d'administration du serveur d'authentification Cisco® NAC.
<b>Ordinateur nommé l'agent de mises à jour</b>		
13000	TCP	Est utilisé pour la connexion à l'agent de mises à jour par les postes clients.
13001	TCP	Est utilisé pour la connexion par les postes clients, si l'ordinateur avec le Serveur d'administration installé se présente comme l'agent de mises à jour.
14000	TCP	Est utilisé pour la connexion à l'agent de mises à jour par les postes clients.
14001	TCP	Est utilisé pour la connexion par les postes clients, si l'ordinateur avec le Serveur d'administration installé se présente comme l'agent de mises à jour.
<b>Ordinateur avec l'Agent d'administration installé</b>		
15000	UDP	Est utilisé pour l'obtention de la demande sur la connexion au Serveur d'administration, ce qui permet de recevoir les informations sur l'ordinateur en temps réel.
15001	UDP	Utilisé pour l'interaction avec l'agent de mises à jour.
7	UDP	Est utilisé par Wake On Lan.

La plage de ports 1024-5000 (protocole TCP) est utilisée pour les connexions sortantes des postes clients avec le Serveur d'administration et les agents de mises à jour. Dans Microsoft Windows Vista et Windows Server 2008 la plage sortante est par défaut : 49152-65535 (protocole TCP).

## INSTALLATION STANDARD

► Pour exécuter l'installation standard de Kaspersky Security Center sur l'ordinateur local, procédez comme suit :

1. Lancez le fichier exécutable setup.exe. L'Assistant d'installation vous proposera de réaliser une configuration des paramètres de l'application. Suivez les instructions de l'Assistant.
2. Lisez attentivement le contrat de licence et si vous en acceptez toutes les dispositions, cochez la case **J'accepte les termes du contrat de licence**. L'installation de l'application se poursuivra.
3. Sélectionnez le type d'installation **Standard** et cliquez sur le bouton **Suivant**.

Finalement, l'Assistant d'installation dépaquetera les fichiers nécessaires du distributif et les enregistrera sur le disque dur de l'ordinateur.

Dans la dernière fenêtre nous vous proposerons de lancer la Console d'administration. Lors du premier lancement vous pouvez exécuter l'installation initiale de l'application (cf. *Manuel de l'administrateur de Kaspersky Security Center*).

A la fin du fonctionnement de l'Assistant d'installation, les composants suivants de l'application seront installés sur le disque dur avec le système d'exploitation installé :

- Serveur d'administration (avec la version serveur de l'Agent d'administration) ;
- Console d'administration ;
- les plug-ins accessibles d'administration des applications compris dans le paquet d'installation.

Aussi les applications suivantes seront installées, si elles n'étaient pas installées auparavant :

- Microsoft Windows Installer 3.1 ;
- Microsoft Data Access Component 2.8 ;
- Microsoft .NET Framework 2.0 ;
- Microsoft SQL Server 2005 Express Edition.

## INSTALLATION PERSONNALISEE

► Pour exécuter l'installation personnalisée de Kaspersky Security Center sur un ordinateur local,

lancez le fichier exécutable setup.exe.

Finalement l'Assistant d'installation de l'application se lancera. Suivez les instructions de l'Assistant.

Ensuite, les étapes de l'Assistant d'installation de l'application sont décrites, ainsi que les actions que vous pouvez exécuter à chaque de ces étapes.

## ETAPES DE L'ASSISTANT

---

Etape 1. Lecture du contrat de licence .....	<a href="#">28</a>
Etape 2. Sélection du type d'installation .....	<a href="#">28</a>
Etape 3. Sélection des composants pour l'installation .....	<a href="#">28</a>
Etape 4. Sélection de la taille du réseau .....	<a href="#">29</a>
Etape 5. Sélection d'un compte .....	<a href="#">30</a>
Etape 6. Sélection de la base de données .....	<a href="#">31</a>
Etape 7. Configuration des paramètres du serveur SQL .....	<a href="#">31</a>
Etape 8. Sélection de la méthode d'authentification .....	<a href="#">32</a>
Etape 9. Définition du dossier public .....	<a href="#">32</a>
Etape 10. Configuration des paramètres de connexion au Serveur d'administration .....	<a href="#">33</a>
Etape 11. Création de l'adresse du Serveur d'administration .....	<a href="#">33</a>
Etape 12. Configuration des paramètres pour les périphériques mobiles .....	<a href="#">33</a>
Etape 13. Sélection des plug-ins d'administration des applications .....	<a href="#">33</a>
Etape 14. Fin de l'installation .....	<a href="#">34</a>

## ETAPE 1. LECTURE DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation requiert la prise de connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat de licence et si vous en acceptez toutes les dispositions, cochez la case **J'accepte les termes du contrat de licence**. L'installation de l'application se poursuivra.

Si vous n'êtes pas d'accord avec le contrat de licence, alors annulez l'installation de l'application en cliquant sur le bouton **Annuler**.

Pour utiliser l'application Kaspersky Security Center Web-Console sous Linux, la licence Kaspersky Security Center Web-Console, Service Provider Edition est requise.

## ETAPE 2. SELECTION DU TYPE D'INSTALLATION

Indiquez le type d'installation **Personnalisée**.

## ETAPE 3. SELECTION DES COMPOSANTS POUR L'INSTALLATION

Sélectionnez les composants du Serveur d'administration de Kaspersky Security Center que vous voulez installer :

- **Kaspersky Lab Cisco NAC Posture Validation Server.** Le composant standard de Kaspersky Lab qui autorise l'ensemble de mandats pour le fonctionnement avec Cisco NAC. Vous pouvez configurer les paramètres de l'action réciproque avec CISCO NAC dans les propriétés ou dans la stratégie du Serveur d'administration (cf. *Manuel de l'administrateur de Kaspersky Security Center*).
- **Prise en charge des appareils nomades.** Ce composant assure la gestion de la protection des périphériques mobiles par Kaspersky Security Center.
- **L'agent de SNMP.** Recueille les données statistiques pour le Serveur d'administration par le protocole SNMP. Le composant est accessible lors de l'installation de l'application sur l'ordinateur par le protocole SNMP.

Après avoir installé Kaspersky Security Center, les fichiers mib, nécessaires pour recueillir les données statistiques, seront situés dans le dossier d'installation de l'application dans le sous-dossier SNMP.

La boîte de dialogue de la fenêtre de l'Assistant reprend l'aide sur le composant sélectionné et sur le volume du disque nécessaire à son installation.

Les composants Agent d'administration et Console d'administration ne s'affichent pas dans la liste des composants. Ces composants s'installent automatiquement, il est impossible d'annuler leur installation.

La version serveur de l'Agent d'administration sera installée sur l'ordinateur avec le composant Serveur d'administration. Son installation conjointe avec la version standard de l'Agent d'administration est impossible. Si la version de serveur de l'Agent d'administration a déjà été installée sur votre ordinateur, il faut la supprimer et relancer l'installation du Serveur d'administration.

A cette étape de l'Assistant, il faut aussi indiquer le dossier pour installer les composants du Serveur d'administration. Par défaut, les composants s'installent dans le dossier <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Si le dossier avec ce nom n'existe pas, il sera automatiquement créé pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

## ETAPE 4. SELECTION DE LA TAILLE DU RESEAU

Indiquez la taille du réseau à installer Kaspersky Security Center. Selon le nombre d'ordinateurs dans le réseau, l'Assistant configure les paramètres d'installation et l'affichage de l'interface de l'application.

Le tableau ci-dessous énumère les paramètres d'installation de l'application et d'affichage de l'interface lors de la sélection des tailles différentes du réseau.

Tableau 5. Dépendance des paramètres d'installation de la sélection des tailles du réseau

PARAMETRES	1-100 ORDINATEURS	100-1000 ORDINATEURS	1000-5000 ORDINATEURS	PLUS DE 5000 ORDINATEURS
Affichage de l'entrée des Serveurs d'administration virtuels et secondaires et de tous les paramètres, liés avec les Serveurs virtuels et secondaires, dans l'arborescence de la console	absent	absent	présent	présent
Affichage des sections <b>Sécurité</b> dans les fenêtres des propriétés du Serveur et des groupes d'administration	absent	absent	présent	présent
Création de la stratégie de l'Agent d'administration à l'aide de l'Assistant de démarrage rapide	absent	absent	présent	présent
Répartition aléatoire du temps de lancement de la tâche de mise à jour sur les postes clients	absent	dans l'intervalle 5 minutes	dans l'intervalle 10 minutes	dans l'intervalle 10 minutes

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL et SQL Express, il n'est pas recommandé d'utiliser l'application pour administrer plus de 5 000 ordinateurs.

## ETAPE 5. SELECTION D'UN COMPTE

Sélectionnez le compte sous lequel le Serveur d'administration sera lancé comme le service sur cet ordinateur :

- **Compte du système local.** Le Serveur d'administration sera lancé sous le compte et avec les privilèges *Compte du système local*.

Pour que Kaspersky Security Center fonctionne correctement, il faut que le compte possède les droits d'accès d'administrateur des ressources pour le placement de la base des informations du Serveur d'administration au démarrage du Serveur d'administration.

Le Serveur d'administration ne peut pas être installé sous le compte de système sous Microsoft Windows Vista et les systèmes d'exploitation Microsoft Windows des versions plus avancées. Dans ces cas, l'option **Compte créé automatiquement (<Nom du compte>)** est accessible.

- **Compte d'utilisateur.** Le Serveur d'administration sera lancé sous un compte utilisateur. Dans ce cas, le Serveur d'administration initiera toutes les opérations avec les privilèges de ce compte. A l'aide du bouton **Parcourir** définissez l'utilisateur, dont le compte sera utilisé, et saisissez le mot de passe.

Lors de l'utilisation du serveur SQL en mode d'authentification du compte d'utilisateur par les outils Microsoft Windows, il faut assurer l'accès à la base des données. Le compte utilisateur doit posséder la base de données de Kaspersky Anti-Virus. Par défaut, il faut utiliser le schéma dbo.

Si vous voulez changer ultérieurement le compte du Serveur d'administration, vous pourrez utiliser l'utilitaire de changement du compte du Serveur d'administration (*klsrvswch*). Pour plus d'informations, cf. *Manuel de l'administrateur de Kaspersky Security Center*.

## ETAPE 6. SELECTION DE LA BASE DE DONNEES

Cette étape de l'Assistant d'installation requiert la sélection de la ressource Microsoft SQL Server (SQL Express) ou MySQL qui sera utilisée pour l'emplacement de la base d'informations des données du Serveur d'administration.

Si vous installez Kaspersky Security Center sur le serveur qui joue le rôle du contrôleur du domaine uniquement pour la lecture (RODC), la possibilité d'installer Microsoft SQL Server (SQL Express) existe pour ce serveur. Dans ce cas pour une installation correcte de Kaspersky Security Center, il est recommandé d'utiliser la ressource MySQL.

La structure de la base de données du Serveur d'administration est décrite dans le fichier klakdb.chm situé dans le dossier d'installation de l'application Kaspersky Security Center.

## ETAPE 7. CONFIGURATION DES PARAMETRES DU SERVEUR SQL

La configuration des paramètres du serveur SQL est exécutée sur cette étape de l'Assistant d'installation.

Selon la base de données sélectionnée, les options suivantes de configuration des paramètres du serveur SQL sont possibles :

- Si à l'étape précédente vous avez sélectionné SQL Express ou Microsoft SQL Server, sélectionnez une des options suivantes :
- Si le Serveur SQL est installé dans le réseau de l'entreprise, indiquez son nom dans le champ **Nom du serveur SQL**.

Dans le champ **Nom du serveur SQL** le nom du serveur SQL se met automatiquement, s'il est détecté sur l'ordinateur, où Kaspersky Security Center s'installe. Le bouton **Parcourir** permet d'afficher la liste de tous les serveurs SQL installés dans le réseau.

Si le Serveur d'administration sera lancé sous le compte administrateur local ou sous le compte système, le bouton **Parcourir** n'est pas accessible.

Indiquez le nom de la base de données qui sera créée pour le placement de l'information du Serveur d'administration, dans le champ **Nom de la base de données**. Par défaut, la base de données est créée sous le nom **KAV**.

Si, à l'aide de Kaspersky Security Center, vous envisagez d'administrer les ordinateurs en nombre moins de 5 000, il est possible d'utiliser Microsoft SQL Express 2005 / 2008. Si le nombre dépasse 5 000, on conseille d'utiliser Microsoft SQL 2005 / 2008.

- Si dans le réseau de la société le serveur SQL n'est pas installé, sélectionnez l'option **Installer Microsoft SQL Server 2005 Express Edition**.

L'Assistant d'installation de l'application installera Microsoft SQL Server 2005 Express Edition. Les paramètres nécessaires seront configurés automatiquement.

- Si à l'étape précédente vous avez sélectionné le serveur MySQL, indiquez son nom dans le champ **Nom du serveur SQL** (par défaut, l'adresse IP de l'ordinateur, où Kaspersky Security Center s'installe, est utilisée) et le port de connexion dans le champ **Port** (le numéro de port par défaut est 3306).

Dans le champ **Nom de la base de données** saisissez le nom de la base de données qui sera créée pour le placement des informations du Serveur d'administration (par défaut, la base de données est créée sous le nom **KAV**).

Si vous voulez installer à la main le serveur SQL sur l'ordinateur duquel vous effectuez l'installation de Kaspersky Security Center, il vous faut interrompre l'installation et la lancer de nouveau après l'installation du serveur SQL. Les serveurs SQL entretenus sont énumérés dans les exigences au système (cf. section "Configurations logicielle et matérielle" à la page [12](#)).

Si vous voulez installer le serveur SQL à la main sur l'ordinateur à distance, il n'est pas requis d'interrompre l'Assistant d'installation de Kaspersky Security Center. Installez le serveur SQL et retournez à l'installation de Kaspersky Security Center.

## ETAPE 8. SELECTION DE LA METHODE D'AUTHENTIFICATION

Définissez la méthode d'authentification à utiliser lors de la connexion du Serveur d'administration au serveur SQL.

Selon la base de données sélectionnée, vous pouvez sélectionner les modes suivants d'authentification :

- Pour SQL Express ou Microsoft SQL Server, sélectionnez une des options suivantes :
  - **Mode d'authentification Microsoft Windows.** Dans ce cas lors de la vérification des privilèges le compte sera utilisé pour le lancement du Serveur d'administration.
  - **Mode d'authentification du serveur SQL.** Le compte indiqué dans la fenêtre sera utilisé dans le cas de sélection de ce mode. Remplissez les champs **Compte**, **Mot de passe** et **Confirmation du mot de passe**.

Si la base de données du Serveur d'administration se trouvent sur un autre ordinateur et le compte du Serveur d'administration n'a aucun droit d'accès au serveur de la base de données, lors de l'installation ou de la mise à jour du Serveur d'administration, il faut utiliser le mode d'authentification du serveur SQL. Cela peut être dans le cas, quand un ordinateur avec la base de données se trouve non pas dans le domaine, ou le Serveur d'administration est installé sous le compte Système local.

- Pour le serveur MySQL, indiquez le compte et le mot de passe.

## ETAPE 9. DEFINITION DU DOSSIER PUBLIC

Définissez le placement et le nom du dossier public, qui sera utilisé pour :

- la sauvegarde des fichiers pour l'installation à distance des applications (les fichiers sont copiés sur le Serveur d'administration lors de la création des paquets d'installation) ;
- le stockage des mises à jour copiées depuis la source sur le Serveur d'administration.

L'accès public pour la lecture pour tous les utilisateurs sera ouvert à cette ressource.

Choisissez l'une des deux options suivantes :

- **Créer un dossier partagé.** Création du nouveau dossier. Indiquez le chemin d'accès au dossier dans le champ ci-après.
- **Sélectionner un dossier partagé existant.** La sélection du dossier partagé parmi les dossiers déjà existants.

Le dossier partagé peut être local sur l'ordinateur duquel vous effectuez l'installation ou distant, sur n'importe lequel des postes clients faisant partie du réseau de l'entreprise. Vous pouvez indiquer le dossier partagé à l'aide du bouton **Parcourir**, aussi que manuellement, en saisissant le chemin UNC dans le champ correspondant (par exemple, \\server\KLSHARE).

Le dossier local KLSHARE est créé par défaut dans le dossier défini pour l'installation du composant Kaspersky Security Center.

## ETAPE 10. CONFIGURATION DES PARAMETRES DE CONNEXION AU SERVEUR D'ADMINISTRATION

Configurez les paramètres de connexion au Serveur d'administration :

- **Numéro de port.** Le numéro de port pour se connecter au Serveur d'administration. Le numéro de port par défaut est 14000.
- **Numéro du port SSL.** Le numéro du port pour établir une connexion sécurisée avec le Serveur d'administration via le protocole SSL. Le numéro de port par défaut est 13000.

Si le Serveur d'administration fonctionne sous Microsoft Windows XP avec Service Pack 2, alors le pare-feu intégré bloque les ports TCP avec les numéros 13000 et 14000. C'est pourquoi pour assurer l'accès sur l'ordinateur, sur lequel le Serveur d'administration est installé, il est nécessaire d'ouvrir ces ports manuellement.

## ETAPE 11. CREATION DE L'ADRESSE DU SERVEUR D'ADMINISTRATION

Définissez l'adresse du Serveur d'administration. Vous avez le choix parmi les options suivantes :

- **Nom DNS.** Cette option est utilisée dans le cas, quand le serveur DNS est présent dans le réseau, et les postes clients peuvent l'obtenir à l'aide de l'adresse du Serveur d'administration.
- **Nom NETBIOS.** Il est utilisé si les postes clients obtiennent l'adresse du Serveur d'administration via le protocole NetBIOS, ou si un serveur WINS est présent dans le réseau.
- **Adresse IP.** Cette option est utilisée si le serveur a une adresse IP fixe qui ne sera pas modifiée par la suite.

Lors de l'installation de la version SPE de l'application, il est recommandé d'utiliser le nom DNS ou l'adresse IP en tant que l'adresse du Serveur. Lors de la création du Serveur d'administration virtuel, l'adresse, saisie sur cette étape de l'Assistant d'installation, est utilisée par défaut en tant que l'adresse du Serveur d'administration principal.

## ETAPE 12. CONFIGURATION DES PARAMETRES POUR LES PERIPHERIQUES MOBILES

Cette étape de l'Assistant d'installation est disponible dans le cas si vous avez sélectionné le composant **Prise en charge des appareils nomades** pour installer.

Indiquez le nom du Serveur d'administration pour connecter les appareils mobiles.

Lors de l'installation de la version SPE de l'application, il est recommandé d'utiliser le nom DNS ou l'adresse IP en tant que l'adresse du Serveur. Lors de la création du Serveur d'administration virtuel, l'adresse, saisie sur cette étape de l'Assistant d'installation, est utilisée par défaut en tant que l'adresse du Serveur d'administration principal.

## ETAPE 13. SELECTION DES PLUG-INS D'ADMINISTRATION DES APPLICATIONS

Sélectionnez les plug-ins d'administration des applications Kaspersky Lab qui requièrent l'installation conjointement avec Kaspersky Security Center.

## ETAPE 14. FIN DE L'INSTALLATION

A la fin de la configuration des paramètres d'installation des composants de Kaspersky Security Center, vous pouvez lancer l'installation.

Si les applications supplémentaires sont nécessaires pour lancer l'installation, l'Assistant d'installation vous en notifiera avant l'installation de Kaspersky Security Center dans la fenêtre **Installation des composants nécessaires**. Les applications nécessaires seront automatiquement installées après avoir cliqué sur le bouton **Suivant**.

## MODIFICATIONS DANS LE SYSTEME APRES L'INSTALLATION

Finalement, après l'installation de la Console d'administration sur votre ordinateur, dans le menu **Démarrer** → **Applications** → **Kaspersky Security Center** l'icône pour son lancement s'affichera.

Le Serveur d'administration et l'Agent d'administration seront installés sur l'ordinateur en tant que services avec les attributs spécifiés dans le tableau ci-après. Aussi dans le tableau les attributs du service du serveur des stratégies (Posture Validation Server) de Kaspersky Lab pour Cisco NAC sont spécifiés. Ce service sera exécuté sur l'ordinateur si le Serveur des stratégies de Kaspersky Lab pour Cisco NAC a été installé conjointement avec le Serveur d'administration.

Tableau 6. Attributs des services

ATTRIBUT	SERVEUR D'ADMINISTRATION	KASPERSKY LAB CISCO NAC POSTURE VALIDATION SERVER	AGENT D'ADMINISTRATION
Nom de service	CSAdminServer	nacserver	klagent
Nom de service affiché	Serveur d'administration Kaspersky Security Center	Kaspersky Lab Cisco NAC Posture Validation Server	Agent d'administration Kaspersky Security Center
Type de lancement	Automatique au démarrage du système d'exploitation.		
Compte	Système local ou spécifié par l'utilisateur.		

La version Serveur de l'Agent d'administration sera installée sur l'ordinateur avec le Serveur d'administration. Elle fait partie du Serveur d'administration, est installée et supprimée, et peut coopérer uniquement avec le Serveur d'administration installé localement. La configuration des paramètres de connexion de l'Agent réseau n'est pas requise. Elle est réalisée par le programme en tenant compte des composants installés sur un ordinateur. Ces paramètres ne seront pas accessibles aussi dans les paramètres locaux de l'Agent d'administration sur cet ordinateur. Telle configuration permet d'éviter la configuration complémentaire des paramètres et des possibles conflits dans le fonctionnement des composants lors de leur installation séparée.

La version serveur de l'Agent d'administration s'installe avec les mêmes attributs et exécute les mêmes fonctions d'administration des applications que l'Agent d'administration standard. La stratégie de groupe d'administration va agir cette version. Cette stratégie inclut le poste client du Serveur d'administration. Toutes les tâches, prévues pour l'Agent d'administration excepté la tâche de changement du Serveur, seront créées pour la version serveur de l'Agent d'administration.

L'installation séparée de l'Agent d'administration sur l'ordinateur du Serveur d'administration n'est pas requise. La version serveur de l'Agent d'administration exécute ses fonctions.

Vous pouvez consulter les propriétés des services du Serveur, de l'Agent d'administration et du Serveur des stratégies de Kaspersky Lab, ainsi que suivre leur fonctionnement à l'aide des moyens d'administration standards Microsoft Windows : Administration de l'ordinateur\Services. L'information sur le fonctionnement des services du Serveur d'administration s'enregistre dans le journal Microsoft Windows sur l'ordinateur, où le Serveur d'administration est installé, dans la branche séparée du journal Kaspersky Event Log.

Les groupes locaux d'utilisateurs KLAdmins et KLOperators sont aussi automatiquement créés sur l'ordinateur où le Serveur d'administration est installé. Si le Serveur d'administration est lancé sous le compte utilisateur, appartenant au domaine, alors les groupes des utilisateurs KLAdmins et KLOperators sont ajoutés dans la liste des groupes d'utilisateurs de domaine. La modification du contenu du groupe des utilisateurs s'effectue à l'aide des moyens standards d'administration Microsoft Windows.

## SUPPRESSION DE L'APPLICATION

Vous pouvez supprimer Kaspersky Security Center à l'aide des moyens standards d'installation et de suppression des applications Microsoft Windows. L'Assistant se lance pour supprimer l'application. Comme résultat de son fonctionnement, tous les composants de l'application (y compris les plug-ins) seront supprimés de l'ordinateur. Si lors du fonctionnement de l'Assistant vous n'avez pas défini la suppression du dossier partagé (KLSHARE), alors après la fin de toutes les tâches liées, vous pouvez le supprimer manuellement.

L'Assistant de suppression de l'application vous proposera d'enregistrer la copie de sauvegarde du Serveur d'administration.

Lors de la suppression de l'application sous Microsoft Windows 7 et Microsoft Windows 2008, une terminaison anticipée du logiciel de suppression peut se produire. Afin d'éviter ceci, désactivez le service de contrôle des comptes (UAC) dans le système d'exploitation et redémarrez la suppression de l'application.

## INSTALLATION DE LA CONSOLE D'ADMINISTRATION SUR LE POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Vous pouvez installer la Console d'administration séparément sur le poste de travail de l'administrateur et gérer le Serveur d'administration par le réseau à l'aide de cette Console.

► *Pour installer la Console d'administration sur le poste de travail de l'administrateur, procédez comme suit :*

1. Lancez le fichier exécutable setup.exe, situé sur le CD de distribution de l'application Kaspersky Security Center dans le dossier Console.

Finalement l'Assistant d'installation se lancera. Suivez les instructions de l'Assistant.

Le processus d'installation de la Console d'administration à partir du fichier de distribution obtenu par Internet correspond au processus d'installation de la Console d'administration à partir du CD de distribution.

2. Sélectionnez le dossier de destination. C'est <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console par défaut. Si ce dossier n'existe pas, alors il sera créé automatiquement pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.
3. Dans la fenêtre finale de l'Assistant d'installation, cliquez sur le bouton **Commencer** pour commencer le processus d'installation de la Console d'administration.

A la fin du fonctionnement de l'Assistant, la Console d'administration sera installée sur le poste de travail de l'administrateur.

Après l'installation de la Console d'administration il est nécessaire de se connecter au Serveur d'administration. Pour cela, il faut lancer la Console d'administration et dans la fenêtre ouverte indiquer le nom de l'ordinateur sur lequel le Serveur d'administration est installé, et les paramètres du compte pour se connecter. Après l'établissement de la connexion avec le Serveur d'administration, il est possible d'administrer le système de protection antivirus à l'aide de cette Console d'administration.

Vous pouvez supprimer la Console d'administration à l'aide des moyens standards d'installation et de suppression des applications Microsoft Windows.

# INSTALLATION ET CONFIGURATION DE KASPERSKY SECURITY CENTER SHV

Kaspersky Security Center offre la possibilité d'intégration dans la plate-forme Microsoft Network Access Protection (NAP). Microsoft NAP permet de régler l'accès des postes clients au réseau. Microsoft NAP suppose que dans le réseau, le serveur avec le système d'exploitation Microsoft Windows Server 2008 est choisi, et que le service PVS (Posture Validation Server) est installé sur ce système. Il suppose aussi que les systèmes d'exploitation NAP-compatibles sont installés sur les postes clients : Microsoft Windows Vista, Microsoft Windows XP avec Service Pack 3, Microsoft Windows 7.

Lors du fonctionnement collectif de l'application Kaspersky Security Center avec Microsoft NAP, System Health Validator (ci-après Kaspersky Security Center SHV) exécute l'analyse de capacité de travail du système d'exploitation.

➤ Afin d'installer localement Kaspersky Security Center SHV sur l'ordinateur, procédez comme suit :

1. Lancez le fichier setup.exe, situé sur le CD de distribution de l'application Kaspersky Security Center SHV.

Enfin l'Assistant d'installation se lancera. Suivez les instructions de l'Assistant.

Le processus d'installation de Kaspersky Security Center SHV à partir du fichier de distribution obtenu par Internet correspond au processus d'installation de Kaspersky Security Center SHV à partir du CD de distribution.

2. Définissez le dossier de destination. C'est <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV par défaut. Si ce dossier n'existe pas, alors il sera créé automatiquement pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.
3. Dans la fenêtre finale de l'Assistant d'installation, cliquez sur le bouton **Commencer** pour commencer le processus d'installation de Kaspersky Security Center SHV.

A la fin du fonctionnement de l'Assistant Kaspersky Security Center SHV sera installé sur votre ordinateur.

Vous pouvez supprimer Kaspersky Security Center SHV à l'aide des moyens standards d'installation et de suppression des applications Microsoft Windows. Avec cela l'Assistant se lance. Comme résultat de son fonctionnement, tous les composants de l'application seront supprimés de l'ordinateur.

## INSTALLATION DE KASPERSKY SECURITY CENTER WEB-CONSOLE

➤ Pour installer Kaspersky Security Center Web-Console sur un ordinateur local,

Lancez le fichier setup.exe, situé sur le CD de distribution de l'application Kaspersky Security Center Web-Console. L'installation est accompagnée de l'Assistant. L'Assistant d'installation vous proposera de réaliser une configuration des paramètres d'installation. Suivez les instructions de l'Assistant.

Le processus d'installation de Kaspersky Security Center Web-Console à partir du fichier de distribution obtenu par Internet correspond au processus d'installation de SHV à partir du CD de distribution.

## ETAPES DE L'ASSISTANT

Etape 1. Lecture du contrat de licence .....	<a href="#">37</a>
Etape 2. Sélection du dossier d'installation .....	<a href="#">37</a>
Etape 3. Sélection des ports .....	<a href="#">37</a>
Etape 4. Connexion au Kaspersky Security Center .....	<a href="#">37</a>
Etape 5. Sélection d'installation du serveur Apache.....	<a href="#">38</a>
Etape 6. Installation du serveur Apache.....	<a href="#">38</a>
Etape 7. Lancement de l'installation de Kaspersky Security Center Web-Console .....	<a href="#">39</a>
Etape 8. Fin de l'Assistant de Kaspersky Security Center Web-Console .....	<a href="#">39</a>

## ETAPE 1. LECTURE DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation requiert la prise de connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat de licence et si vous en acceptez toutes les dispositions, cochez la case **J'accepte les termes du contrat de licence**. L'installation de l'application se poursuivra.

Si vous n'êtes pas d'accord avec le contrat de licence, alors annulez l'installation de l'application en cliquant sur le bouton **Annuler**.

Pour utiliser l'application Kaspersky Security Center Web-Console sous Linux, la licence Kaspersky Security Center Web-Console, Service Provider Edition est requise.

## ETAPE 2. SELECTION DU DOSSIER D'INSTALLATION

Définissez le dossier de destination pour installer Kaspersky Security Center Web-Console. Par défaut, le dossier de destination est le dossier <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console. Si ce dossier n'existe pas, alors il sera créé automatiquement. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

## ETAPE 3. SELECTION DES PORTS

Définissez les paramètres suivants :

- **Numéro du port SSL.** Le numéro du port pour établir une connexion sécurisée de l'ordinateur avec le Serveur d'administration via le protocole SSL. Le numéro de port par défaut est 13291.
- **Numéro de port.** Numéro de port pour connecter l'ordinateur au serveur Apache. Le numéro de port par défaut est 9000.

## ETAPE 4. CONNEXION AU KASPERSKY SECURITY CENTER

Sélectionnez le mode de connexion de Kaspersky Security Center Web-Console à Kaspersky Security Center. Les modes suivants de connexion sont accessibles :

- **Utiliser le serveur Apache installé sur l'ordinateur local.** Si cette option a été sélectionnée, la connexion de Kaspersky Security Center Web-Console à Kaspersky Security Center sera exécutée via le serveur Apache installé sur l'ordinateur local (il est possible de sélectionner l'installation du serveur Apache à l'étape suivante).
- **Utiliser le serveur Apache installé sur l'ordinateur à distance.** Vous pouvez sélectionner cette option si le serveur Apache est déjà installé sur l'ordinateur à distance sous Linux. Dans ce cas, uniquement la partie serveur de Kaspersky Security Center Web-Console sera localement installée. Pour connecter Kaspersky Security Center Web-Console à Kaspersky Security Center, il faut installer la partie client de Kaspersky Security Center Web-Console sur l'ordinateur à distance. Lorsque vous sélectionnez cette option, l'Assistant d'installation passe à Etape 7 (cf. section "Etape 7. Lancement de l'installation de Kaspersky Security Center Web-Console" à la page [39](#)).

➔ *Pour installer la partie client de Kaspersky Security Center Web-Console sur l'ordinateur à distance sous Linux, selon le type de système, lancez un des fichiers suivants :*

- Pour les systèmes de 32 bits :
  - kscwebconsole-9.<numéro\_de\_version>.i386.rpm ;
  - kscwebconsole\_9.<numéro\_de\_version>\_i386.deb.
- Pour les systèmes de 64 bits :
  - kscwebconsole-9.<numéro\_de\_version>.x86\_64.rpm ;
  - kscwebconsole\_9.<numéro\_de\_version>\_x86\_64.deb.

## ETAPE 5. SELECTION D'INSTALLATION DU SERVEUR APACHE

Si le serveur Apache n'a pas été installé sur l'ordinateur, cette étape de l'Assistant vous propose d'installer Apache HTTP Server 2.2.

L'option d'installation d'Apache HTTP Server 2.2 est sélectionnée par défaut. Si vous ne voulez pas installer le serveur Apache à l'aide de l'Assistant d'installation de Kaspersky Security Center Web-Console, décochez la case **Installer Apache HTTP Server 2.2**.

*Le redémarrage de l'ordinateur peut être requis durant l'installation du serveur Apache.*

## ETAPE 6. INSTALLATION DU SERVEUR APACHE

L'installation et la configuration d'Apache HTTP Server 2.2 sont exécutées sur cette étape de l'Assistant.

Avant l'installation, indiquez le certificat que l'application Kaspersky Security Center Web-Console utilisera pour la connexion avec le serveur Apache (cf. ill. ci-après). Sélectionnez l'une des options ci-dessous :

- **Former le nouveau.** Former le certificat pour le fonctionnement selon HTTPS.

- **Sélectionner l'existant.** Utiliser le certificat existant pour le fonctionnement selon HTTPS. Définissez le certificat à l'aide d'un des modes proposés :
  - **Sélectionner le fichier du certificat.** Vous pouvez sélectionner le certificat existant, en cliquant sur le bouton **Parcourir**.
  - **Sélectionner le fichier de la clé fermée.** Vous pouvez créer le certificat par le fichier de sa clé fermée, en cliquant sur le bouton **Parcourir**.

Après la sélection du certificat, cliquez sur le bouton **Suivant**. Finalement, l'Assistant d'installation Apache HTTP Server 2.2 se lancera. Suivez les instructions de l'Assistant.

## ETAPE 7. LANCEMENT DE L'INSTALLATION DE KASPERSKY SECURITY CENTER WEB-CONSOLE

Cliquez sur le bouton **Commencer** pour lancer l'installation de Kaspersky Security Center Web-Console.

Le processus d'installation s'affiche dans la fenêtre de l'Assistant.

## ETAPE 8. FIN DE L'ASSISTANT DE KASPERSKY SECURITY CENTER WEB-CONSOLE

Si le serveur Apache 2 de version 2.2.9 ou supérieure a été déjà installé sur l'ordinateur ou l'installation automatique du serveur Apache s'est terminée avec erreur, la dernière étape de l'Assistant d'installation de Kaspersky Security Center Web-Console vous proposera d'ouvrir le fichier avec les instructions sur la configuration du serveur Apache. Pour ouvrir le fichier avec les instructions après la fin de l'Assistant, il faut cocher la case **Ouvrir le fichier readme.txt**.

Pour compléter l'Assistant d'installation, cliquez sur **Terminer**.

## CONFIGURATION DU FONCTIONNEMENT DU SERVEUR D'ADMINISTRATION AVEC KASPERSKY SECURITY CENTER WEB-CONSOLE

➔ *Pour configurer le fonctionnement du Serveur d'administration avec Kaspersky Security Center Web-Console, procédez comme suit :*

1. Ajoutez la clé de Kaspersky Security Center ou de Kaspersky Security Center SPE dans le dossier **Stockages**, dans le dossier joint **Clés** du Serveur d'administration principal d'une des manières suivantes :
  - A l'aide de l'Assistant de démarrage rapide du Serveur d'administration (pour lancer l'Assistant, sélectionnez l'option **Toutes les tâches** → **Assistant de démarrage rapide**) dans le menu contextuel du Serveur d'administration).
  - A l'aide du lien **Ajouter une clé** dans le dossier **Clés**.
  - Ajoutez une clé en tant que clé active dans les propriétés du Serveur d'administration principal dans la fenêtre des propriétés du Serveur d'administration principal, dans la section **Clés**, à l'aide du bouton **Modifier**.
2. Créez une hiérarchie des Serveurs d'administration, si nécessaire.
3. S'il faut, créez des Serveurs d'administration virtuels, en les incluant dans la hiérarchie des Serveurs d'administration.

Configurez les paramètres du Serveur virtuel, en procédant comme suit :

- a. Sélectionnez le compte administrateur du Serveur virtuel parmi les comptes proposés par l'application, ou créez un nouveau compte. Sous le nom de ce compte, l'administrateur du réseau de l'entreprise-client sous l'administration du Serveur virtuel sélectionné va lancer Kaspersky Security Center Web-Console pour consulter les informations sur l'état de la protection antivirus du réseau.

Dans le cas de nécessité, vous pouvez créer plusieurs comptes des administrateurs pour un Serveur virtuel.

L'administrateur du Serveur d'administration virtuel est un utilisateur interne de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

- b. Créez le fichier du contrat de licence eula.txt ou eula.html et le fichier de la foire aux questions faq.txt ou faq.html.

Placez les fichiers créés eula.txt (eula.html) et faq.txt (faq.html) dans le dossier d'installation du serveur Apache dans le dossier joint htdocs\help. Les liens sur ces fichiers s'affichent dans la fenêtre principale de l'application Kaspersky Security Center Web-Console.

- c. Transmettez dans chaque entreprise-client les informations suivantes :

- L'adresse du serveur avec Kaspersky Security Center Web-Console installé (sous forme de l'adresse URL ou l'adresse IP).
- Le nom du Serveur d'administration virtuel sous lequel le réseau de l'entreprise-client se trouve.
- Le nom de l'utilisateur et le mot de passe du compte de l'administrateur du Serveur d'administration virtuel.

➡ *Pour que le logo de votre entreprise s'affiche dans l'interface de Kaspersky Security Center Web-Console, procédez comme suit :*

1. Préparez le fichier du logo répondant aux critères suivants :

- Format du fichier : PNG ;
- Nom du fichier : logo.png ;
- Taille du fichier : toute ;
- Résolution : 220×72 pixels.

2. Placez le fichier du logo dans le dossier d'installation du serveur Apache.

- Si le serveur Apache est installé sous Microsoft Windows, le chemin d'accès au dossier d'installation par défaut : C:\Program Files\Apache Software Foundation\Apache2.2\htdocs\images\custom\_logo.
- Si le serveur Apache est installé sous Linux, le chemin d'accès au dossier d'installation par défaut : /opt/kaspersky/kscwebconsole/share\htdocs/images/custom\_logo.

Pour plus d'informations sur la configuration du fonctionnement du Serveur d'administration avec Kaspersky Security Center Web-Console, cf. *Manuel de l'administrateur Kaspersky Security Center*.

# CONFIGURATION DU SYSTEME DE PROTECTION ANTIVIRUS DE L'ENTREPRISE-CLIENT

Cette section décrit les particularités de la configuration du système de protection antivirus via la Console d'administration dans le réseau de l'entreprise-client.

La configuration du système de protection antivirus est une partie du processus de déploiement de la protection antivirus dans le réseau de l'entreprise-client. La procédure de configuration du système de protection antivirus inclut les étapes suivantes :

1. Sélection de l'ordinateur qui jouera le rôle de l'agent de mises à jour dans le réseau de l'entreprise-client.
2. Installation locale de l'Agent d'administration sur l'agent de mises à jour.
3. Installation à distance de l'Agent d'administration et des applications antivirus de Kaspersky Lab sur les ordinateurs de l'entreprise-client.

Cette section analyse les conditions nécessaires pour installer à distance des applications sur les ordinateurs de l'entreprise-client. La procédure d'installation à distance de l'Agent d'administration et des applications antivirus de Kaspersky Lab est décrite en détails dans la section Installation à distance des applications (à la page [45](#)).

4. Création d'une hiérarchie des groupes d'administration soumis au Serveur d'administration virtuel.

## DANS CETTE SECTION

Désignation de l'ordinateur en tant que l'agent de mises à jour. Configuration des paramètres de l'agent de mises à jour .....	<a href="#">41</a>
Installation locale de l'Agent d'administration sur l'agent de mises à jour .....	<a href="#">42</a>
Conditions nécessaires pour installer les applications sur les ordinateurs de l'entreprise-client .....	<a href="#">43</a>
Création d'une hiérarchie des groupes d'administration soumis au Serveur d'administration virtuel.....	<a href="#">44</a>

## DESIGNATION DE L'ORDINATEUR EN TANT QUE L'AGENT DE MISES A JOUR. CONFIGURATION DES PARAMETRES DE L'AGENT DE MISES A JOUR

Si les ordinateurs de l'entreprise-client ne possèdent pas de connexion directe avec le Serveur d'administration virtuel, vous pouvez les gérer via la passerelle des connexions. Le rôle de la passerelle des connexions pour le groupe d'administration peut être exécuté par l'agent de mises à jour du groupe.


Pour désigner le poste client en tant que l'agent de mises à jour, exécutant le rôle de la passerelle des connexions pour le groupe d'administration, il suffit d'installer l'Agent d'administration sur cet ordinateur. Lors de la première connexion de cet ordinateur avec le Serveur d'administration, Kaspersky Security Center le désigne automatiquement en tant que l'agent de mises à jour du groupe et le configure comme la passerelle des connexions.

Vous pouvez aussi sélectionner l'agent de mises à jour et le configurer manuellement comme la passerelle des connexions.

➔ Pour désigner un ordinateur en tant que l'agent de mises à jour du groupe d'administration, procédez comme suit :

1. Sélectionnez le groupe d'administration dans l'arborescence de la console.
2. Ouvrez la section **Agents de mise à jour** de la fenêtre des propriétés du groupe sélectionné à l'aide d'un des moyens suivants :
  - Dans le menu contextuel du groupe d'administration, sélectionnez l'option **Propriétés**. Dans la fenêtre ouverte **Propriétés**, sélectionnez la section **Agents de mise à jour**.
  - A l'aide du lien **Configurer les agents de mises à jour pour le groupe** dans la zone de travail du groupe d'administration.
3. Sélectionnez l'ordinateur et ajoutez-le en tant que l'agent de mises à jour pour le groupe.

Pour ajouter un ordinateur en tant qu'agent de mise à jour, cliquez sur **Ajouter** et cochez le nom du poste client nécessaire du dossier **Ordinateurs administrés**. Vous pouvez sélectionner plusieurs ordinateurs simultanément. Ils seront tous ajoutés à la liste.

Il est possible de sélectionner le mode d'ajout de l'agent de mises à jour en ouvrant la liste à l'aide du bouton  situé à droite du bouton **Ajouter**. Les moyens suivants d'ajout de l'ordinateur sont disponibles :

- **Ajouter l'ordinateur du groupe**. L'ajout de l'ordinateur du dossier **Ordinateurs administrés**.
- **Ajouter l'ordinateur selon l'adresse**. Saisie de l'adresse IP de l'ordinateur.

Cette option doit être utilisée pour ajouter l'ordinateur, protégé par le pare-feu, en tant que l'agent de mises à jour, parce qu'il est impossible d'ajouter cet ordinateur directement dans le groupe d'administration.

Suite à l'ajout de l'agent de mises à jour selon l'adresse IP, le Serveur d'administration le découvre lors du balayage suivant du réseau et le place dans le dossier **Ordinateurs non définis**. Puisque l'agent de mises à jour est protégé par le pare-feu, les actions suivantes sont requises pour configurer son fonctionnement :

1. Ajouter cet ordinateur au groupe d'administration sélectionné.
2. Ouvrir à nouveau la fenêtre des propriétés du groupe sélectionné dans la section **Agents de mise à jour**.
3. Supprimer l'ordinateur, ajouté selon l'adresse, de la liste des agents de mises à jour.
4. Ajouter le même ordinateur du dossier **Ordinateurs administrés** à l'aide du bouton **Ajouter** ou **Ajouter l'ordinateur du groupe**.
5. Dans la fenêtre des propriétés de cet agent de mises à jour, dans la section **Avancé**, vérifier si les cases **Passerelle des connexions** et **Initier la création de la connexion avec la passerelle du côté du Serveur d'administration** sont cachées.

Finalement, l'ordinateur sélectionné sera désigné comme l'agent de mise à jour du groupe d'administration.

## INSTALLATION LOCALE DE L'AGENT D'ADMINISTRATION SUR L'AGENT DE MISES A JOUR

Pour que l'ordinateur, sélectionné par l'agent de mises à jour, puisse se connecter directement avec le Serveur d'administration virtuel pour exécuter le rôle de la passerelle des connexions, l'installation locale de l'Agent d'administration est requise sur cet ordinateur.

L'ordre d'installation locale de l'Agent d'administration sur l'ordinateur, sélectionné par l'agent de mises à jour, coïncide avec l'ordre d'une installation locale de l'Agent d'administration sur n'importe quel ordinateur du réseau.

Les conditions suivantes doivent être exécutées pour l'ordinateur sélectionné par l'agent de mises à jour :

- Lors d'une installation locale de l'Agent d'administration, dans la fenêtre de l'Assistant d'installation **Serveur d'administration**, dans le champ **Adresse du serveur**, il faut indiquer l'adresse du Serveur d'administration virtuel sous l'administration duquel l'ordinateur se trouve. En guise d'adresse de l'ordinateur, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur sur le réseau Windows.

La forme suivante de l'enregistrement de l'adresse du Serveur virtuel est utilisée : **<Adresse complète du Serveur d'administration physique auquel le Serveur virtuel est soumis>/<Nom du Serveur d'administration virtuel>**.

- Pour exécuter le rôle de la passerelle des connexions, tous les ports nécessaires pour la connexion avec le Serveur d'administration doivent être ouverts sur l'ordinateur.

Suite à l'installation sur l'ordinateur de l'Agent d'administration avec les paramètres indiqués, l'application Kaspersky Security Center exécute automatiquement les actions suivantes :

- Inclut cet ordinateur dans le groupe **Ordinateurs administrés** du Serveur d'administration virtuel.
- Désigne cet ordinateur en tant que l'agent de mises à jour du groupe **Ordinateurs administrés** du Serveur d'administration virtuel.

Il est nécessaire et suffisant d'exécuter l'installation de l'Agent d'administration sur l'ordinateur, désigné comme l'agent de mises à jour du groupe **Ordinateurs administrés** dans le réseau de l'entreprise. Sur les ordinateurs, jouant le rôle des agents de mises à jour dans les groupes d'administration joints, l'Agent d'administration peut être installé à distance, en utilisant l'agent de mises à jour du groupe **Ordinateurs administrés** en tant que la passerelle des connexions.

### VOIR EGALEMENT

Installation locale de l'Agent d'administration .....	<a href="#">60</a>
Installation à distance des applications .....	<a href="#">45</a>

## CONDITIONS NECESSAIRES POUR INSTALLER LES APPLICATIONS SUR LES ORDINATEURS DE L'ENTREPRISE-CLIENT

Le processus d'installation à distance des applications sur les ordinateurs de l'entreprise cliente coïncide avec le processus d'installation à distance des applications à l'intérieur de l'entreprise (cf. section Installation à distance du logiciel (à la page [45](#))).

Pour installer les applications sur les ordinateurs de l'entreprise-client, il faut exécuter les conditions suivantes :

- Avant la première installation des applications sur les ordinateurs de l'entreprise-client, l'installation de l'Agent d'administration sur ces ordinateurs est requise.

Lors de la configuration du paquet d'installation de l'Agent d'administration du côté du prestataire de services dans l'application Kaspersky Security Center dans la fenêtre des propriétés du paquet d'installation, il faut configurer les paramètres suivants :

- Dans la section **Connexion**, dans la ligne **Adresse du serveur**, il faut indiquer la même adresse du Serveur d'administration virtuel que lors d'une installation locale de l'Agent d'administration sur l'agent de mises à jour.
- Dans la section **Avancé**, il faut cocher la case **Se connecter au Serveur d'administration via la passerelle des connexions**. Dans la ligne **Adresse de la passerelle des connexions**, il faut indiquer l'adresse de l'agent de mises à jour. En guise d'adresse de l'ordinateur, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur sur le réseau Windows.
- En tant que le mode de téléchargement du paquet d'installation de l'Agent d'administration, il faut sélectionner **Via les outils Microsoft Windows à l'aide des agents de mises à jour**. La sélection du mode de téléchargement s'effectue d'une manière suivante :
  - Lors de l'installation des applications à l'aide des tâches d'installation à distance, le mode de téléchargement peut être sélectionné par deux moyens :
    - lors de la création de la tâche d'installation à distance dans la fenêtre **Paramètres** ;
    - dans la fenêtre des propriétés de la tâche d'installation à distance dans la section **Paramètres**.
  - Lors de l'installation des applications à l'aide de l'Assistant d'installation à distance, le mode de téléchargement peut être sélectionné dans la fenêtre de l'Assistant **Paramètres**.
- Le compte, sous lequel l'agent de mises à jour fonctionne, doit avoir l'accès à la ressource Admin\$ sur les postes clients.

## CREATION D'UNE HIERARCHIE DES GROUPES D'ADMINISTRATION SOUMIS AU SERVEUR D'ADMINISTRATION VIRTUEL

Après la création du Serveur d'administration virtuel, il contient, par défaut, un groupe d'administration **Ordinateurs administrés**.

La procédure de création de la hiérarchie des groupes d'administration, soumis au Serveur d'administration virtuel, coïncide avec la procédure de création de la hiérarchie des groupes d'administration, soumis au Serveur d'administration physique. Cette procédure est décrite dans le *Manuel de l'administrateur Kaspersky Security Center*.

Il est impossible d'ajouter les Serveurs d'administration virtuels et secondaires aux groupes d'administration soumis au Serveurs d'administration virtuels. Cela dépend des restrictions des Serveurs d'administration virtuels. Ces restrictions sont décrites dans le *Manuel de l'administrateur de Kaspersky Security Center*.

# INSTALLATION A DISTANCE DES APPLICATIONS

Cette section décrit les moyens de l'installation à distance des applications de Kaspersky Lab ou leur suppression depuis les ordinateurs du réseau.

Avant l'installation des applications sur les postes clients, il faut s'assurer que la configuration logicielle et matérielle de l'ordinateur correspond aux exigences (cf. section "Configurations logicielle et matérielle" à la page [12](#)) émises.

Cette section décrit l'installation à distance des applications via la Console d'administration.

L'Agent d'administration assure le lien entre le Serveur d'administration et le poste client. Par conséquent, il doit être installé sur chaque poste client qui sera connecté au système d'administration centralisé distant.

Uniquement la version serveur de l'Agent d'administration peut être utilisée sur l'ordinateur avec le Serveur d'administration installé. Elle est incluse dans le Serveur d'administration et s'installe et est supprimée ensemble avec lui. L'installation de l'Agent d'administration sur cet ordinateur n'est pas requise.

L'installation de l'Agent d'administration s'effectue de la même façon que l'installation des applications, et peut être réalisée à distance aussi que localement. Lors de l'installation centralisée des applications antivirus via la Console d'administration, vous pouvez installer l'Agent d'administration conjointement avec les applications antivirus.

Les Agents d'administration peuvent se différer d'après les applications de Kaspersky Lab, avec lesquelles ils doivent être installés pour le fonctionnement collectif. Dans certains cas uniquement l'installation locale de l'Agent d'administration est possible (cf. Manuel des applications appropriées). L'Agent d'administration s'installe sur le poste client une fois.

L'administration des applications Kaspersky Lab via la Console d'administration est exécutée à l'aide des plug-ins d'administration. Par conséquent, pour recevoir l'accès à l'administration de l'application via Kaspersky Security Center, le plug-in d'administration de cette application doit être installé sur le bureau d'administrateur.

Vous pouvez exécuter l'installation à distance des applications depuis le bureau d'administrateur dans la fenêtre principale de l'application Kaspersky Security Center.

Certaines applications de Kaspersky Lab peuvent être installées sur les postes clients seulement localement (cf. Manuel des applications appropriées). L'administration à distance de ces applications à l'aide de Kaspersky Security Center est disponible.

Pour l'installation à distance du logiciel, il faut créer la tâche d'installation à distance.

La tâche formée d'installation à distance sera exécutée selon sa programmation. Vous pouvez interrompre la procédure d'installation, en arrêtant manuellement l'exécution de la tâche.

Si l'installation à distance de l'application se termine par erreur, vous pouvez vérifier la cause de ce problème et l'éliminer à l'aide de l'utilitaire de préparation de l'ordinateur à l'installation à distance (cf. section "Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe" à la page [56](#)).

Vous pouvez suivre le processus d'installation des applications antivirus de Kaspersky Lab à l'aide du rapport de déploiement.

Kaspersky Security Center soutient l'administration à distance par les applications de Kaspersky Lab suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition ;
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition ;
- Kaspersky Anti-Virus 8.0 pour la sauvegarde des données ;
- Kaspersky Anti-Virus 5.7 for Novell NetWare ;
- Kaspersky Anti-Virus 6.0 Second Opinion Solution ;
- Kaspersky Anti-Virus 8.0 for Linux File Server ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security 8 for Smartphone ;
- Kaspersky Endpoint Security 8 for Mac ;
- Kaspersky Endpoint Security 8 for Linux.
- Kaspersky Security for Virtualization 1.1.

Les informations détaillées sur l'administration des applications dénombrées via Kaspersky Security Center sont fournies dans les Manuels correspondants aux applications.

**DANS CETTE SECTION**

Installation des applications à l'aide de la tâche d'installation à distance .....	<a href="#"><u>46</u></a>
Installation des applications à l'aide de l'Assistant d'installation à distance .....	<a href="#"><u>49</u></a>
Consultation du rapport de déploiement de la protection .....	<a href="#"><u>50</u></a>
Désinstallation à distance des applications .....	<a href="#"><u>50</u></a>
Fonctionnement avec les paquets d'installation .....	<a href="#"><u>52</u></a>
Récupération des versions actuelles des applications .....	<a href="#"><u>54</u></a>
Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe .....	<a href="#"><u>56</u></a>

# INSTALLATION DES APPLICATIONS A L'AIDE DE LA TACHE D'INSTALLATION A DISTANCE

Vous pouvez installer à distance des applications sur les postes clients, en lançant les tâches d'installation à distance. Kaspersky Security Center permet de créer la tâche d'installation à distance des types suivants :

- *Tâches de groupe.* Tâches créées pour les postes clients des groupes d'administration sélectionnés.
- *Tâches pour les sélections d'ordinateurs.* Tâches créées pour les postes clients sélectionnés peu importe l'appartenance des ordinateurs à un groupe d'administration quelconque.

Pour que la tâche d'installation à distance fonctionne correctement sur le poste client, sur lequel l'Agent d'administration n'est pas installé, il est nécessaire d'ouvrir les ports TCP 139 et 445, UDP 137 et 138. Ces ports sont ouverts par défaut sur tous les postes clients inclus dans le domaine. Ils s'ouvrent automatiquement à l'aide de l'utilitaire de préparation de l'ordinateur à l'installation à distance (cf. section "Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe" à la page 56).

## DANS CETTE SECTION

Installation de l'application sur les postes clients sélectionnés .....	<a href="#">47</a>
Installation des applications sur les postes clients du groupe d'administration .....	<a href="#">48</a>
Installation des applications sur les Serveurs d'administration secondaires .....	<a href="#">48</a>

## INSTALLATION DE L'APPLICATION SUR LES POSTES CLIENTS SELECTIONNES

► Pour installer l'application sur les postes clients sélectionnés, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les ordinateurs nécessaires.
2. Dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
3. Lancez le processus de création d'une tâche en utilisant le lien **Création d'une tâche**.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center**, sélectionnez le type de tâche **Installation à distance de l'application**.

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche d'installation à distance de l'application pour l'ensemble sélectionné d'ordinateurs sera créée. La tâche créée s'affiche dans la zone de travail du dossier **Tâches pour les sélections d'ordinateurs**.

4. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera installée sur les postes clients sélectionnés.

## INSTALLATION DES APPLICATIONS SUR LES POSTES CLIENTS DU GROUPE D'ADMINISTRATION

➔ Pour installer l'application sur les postes clients du groupe d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.
2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.
3. Dans la zone de travail du groupe, sélectionnez l'onglet **Tâches**.
4. Lancez le processus de création d'une tâche en utilisant le lien **Création d'une tâche**.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center**, sélectionnez le type de tâche **Installation à distance de l'application**.

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche de groupe d'installation à distance de l'application sélectionnée sera créée. La tâche créée s'affiche dans la zone de travail du groupe d'administration, sous l'onglet **Tâches**.

5. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera installée sur les postes clients du groupe d'administration.

## INSTALLATION DES APPLICATIONS SUR LES SERVEURS D'ADMINISTRATION SECONDAIRES

➔ Pour installer l'application sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.
2. Assurez-vous que le paquet d'installation correspondant à l'application à installer se trouve sur chaque Serveur d'administration secondaire sélectionné. Si le paquet d'installation n'est présent sur aucun Serveur secondaire, diffusez-le à l'aide de la tâche de propagation du paquet d'installation (cf. section "Propagation des paquets d'installation sur les Serveurs d'administration secondaires" à la page [53](#)).
3. Lancez la création de la tâche d'installation de l'application sur les Serveurs d'administration secondaires à l'aide d'un des moyens suivants :
  - Si vous voulez former la tâche pour les Serveurs secondaires du groupe d'administration sélectionné, lancez la création de la tâche de groupe d'installation à distance pour ce groupe (cf. section "Installation des applications sur les postes clients du groupe d'administration" à la page [48](#)).
  - Si vous voulez former la tâche pour l'ensemble de Serveurs secondaires, lancez la création de la tâche d'installation à distance pour l'ensemble d'ordinateurs. (cf. section "Installation de l'application sur les postes clients sélectionnés" à la page [47](#))

Finalement, l'Assistant de création de la tâche d'installation à distance se lancera. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center** dans le dossier **Avancé**, sélectionnez le type de tâche **Installation à distance de l'application sur les Serveurs d'administration secondaires**.

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche d'installation à distance de l'application sélectionnée sur les Serveurs d'administration secondaire sera créée.

4. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera installée sur les Serveurs d'administration secondaires.

## INSTALLATION DES APPLICATIONS A L'AIDE DE L'ASSISTANT D'INSTALLATION A DISTANCE

Pour l'installation des applications de la société, vous pouvez utiliser l'Assistant d'installation à distance. L'Assistant d'installation à distance permet de réaliser l'installation à distance des applications, en utilisant les paquets d'installation formés, aussi que directement des distributifs.

Pour que la tâche d'installation à distance fonctionne correctement sur le poste client, sur lequel l'Agent d'administration n'est pas installé, il est nécessaire d'ouvrir les ports suivants : TCP 139 et 445 ; UDP 137 et 138. Ces ports sont ouverts par défaut pour tous les ordinateurs inclus dans le domaine, et s'ouvrent automatiquement à l'aide de l'utilitaire de préparation de l'ordinateur à l'installation à distance. (cf. section "Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe" à la page 56)

► Pour installer l'application à l'aide de l'Assistant d'installation à distance, procédez comme suit :

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.
2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.
3. Dans la zone de travail du groupe, sélectionnez l'onglet **Groupes**.
4. Lancez l'installation de l'application à l'aide du lien **Commencer l'installation** dans le groupe **Installation distante**.

Finalement, l'Assistant d'installation à distance se lance. Suivez les instructions de l'Assistant.

A la dernière étape de l'Assistant, cliquez sur le bouton **Suivant** pour créer et lancer la tâche d'installation à distance sur les ordinateurs sélectionnés.

Kaspersky Security Center exécute les actions suivantes suite au fonctionnement de l'Assistant d'installation à distance :

- Crée le paquet d'installation pour installer l'application (s'il n'a pas été créé auparavant). Le paquet d'installation se place dans le dossier **Stockages** dans le dossier joint **Paquets d'installation** avec le nom correspondant au nom et à la version de l'application. Vous pouvez utiliser ce paquet d'installation pour installer l'application ultérieurement.
- Crée et lance la tâche d'installation à distance pour la sélection d'ordinateurs ou pour le groupe d'administration. La tâche formée d'installation à distance se place dans le dossier **Tâches pour les sélections d'ordinateurs** ou s'ajoute aux tâches du groupe d'administration pour lequel elle a été créée. Vous pouvez manuellement lancer cette tâche par la suite. Le nom de la tâche correspond au nom du paquet d'installation pour l'installation de l'application : **Installation <Nom du d'installation sélectionné>**.

## CONSULTATION DU RAPPORT DE DEPLOIEMENT DE LA PROTECTION

Pour suivre le processus de déploiement de la protection dans le réseau, il est possible d'utiliser **Rapport sur le déploiement de la protection**.

► Pour consulter le rapport sur le déploiement de la protection, procédez comme suit :

1. Connectez-vous au Serveur d'administration pour lequel il faut consulter le rapport sur le déploiement.
2. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**.
3. Dans le dossier **Rapports et notifications**, sélectionnez le modèle du rapport "**Rapport de déploiement de la protection**".

Le rapport sera créé dans la barre des résultats. Ce rapport contient l'information sur le déploiement de la protection sur tous les postes clients du réseau.

Vous pouvez former un nouveau rapport de déploiement de la protection et indiquer quel type d'information il faut y inclure :

- pour un groupe d'administration ;
- pour une liste des postes clients ;
- pour la sélection de postes clients ;
- pour tous les postes clients.

Vous pouvez consulter les informations détaillées sur la création de nouveau rapport dans *Manuel de l'administrateur de Kaspersky Security Center*.

Dans le cadre de Kaspersky Security Center il est considéré que l'application antivirus est déployée sur l'ordinateur dans le cas, quand l'application antivirus est installée sur cet ordinateur et la protection permanente fonctionne.

## DESINSTALLATION A DISTANCE DES APPLICATIONS

Il est aussi possible de supprimer les applications incompatibles qui peuvent provoquer les conflits dans le fonctionnement des applications de Kaspersky Lab administrées via Kaspersky Security Center.

Vous pouvez exécuter la désinstallation à distance des applications des postes clients, en lançant les tâches de désinstallation à distance. Kaspersky Security Center permet de créer la tâche de désinstallation à distance des types suivants :

- *Tâches de groupe*. Tâches créées pour les postes clients des groupes d'administration sélectionnés.
- *Tâches pour les sélections d'ordinateurs*. Tâches créées pour les postes clients sélectionnés peu importe l'appartenance des ordinateurs à un groupe d'administration quelconque.

### DANS CETTE SECTION

Désinstallation à distance de l'application avec les postes clients du groupe d'administration .....	<a href="#">51</a>
Désinstallation à distance de l'application des postes clients sélectionnés .....	<a href="#">51</a>

## DESINSTALLATION A DISTANCE DE L'APPLICATION AVEC LES POSTES CLIENTS DU GROUPE D'ADMINISTRATION

➤ *Pour désinstaller à distance l'application des postes clients du groupe d'administration, procédez comme suit :*

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.
2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.
3. Dans la zone de travail du groupe, sélectionnez l'onglet **Tâches**.
4. Lancez le processus de création d'une tâche en utilisant le lien **Création d'une tâche**.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center** dans le dossier **Avancé**, sélectionnez le type de tâche "**Tâche de désinstallation à distance de l'application**".

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche de groupe de désinstallation à distance de l'application sélectionnée sera créée. La tâche créée s'affiche dans la zone de travail du groupe d'administration, sous l'onglet **Tâches**.

5. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche de désinstallation à distance, l'application sélectionnée sera supprimée des postes clients du groupe d'administration.

## DESINSTALLATION A DISTANCE DE L'APPLICATION DES POSTES CLIENTS SELECTIONNES

➤ *Pour désinstaller à distance l'application des postes clients sélectionnés, procédez comme suit :*

1. Connectez-vous au Serveur d'administration qui gère les ordinateurs nécessaires.
2. Dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
3. Lancez le processus de création d'une tâche en utilisant le lien **Création d'une tâche**.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center** dans le dossier **Avancé**, sélectionnez le type de tâche "**Tâche de désinstallation à distance de l'application**".

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche de désinstallation à distance de l'application pour l'ensemble sélectionné d'ordinateurs sera créée. La tâche créée s'affiche dans la zone de travail du dossier **Tâches pour les sélections d'ordinateurs**.

4. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera supprimée des postes clients sélectionnés.

## FONCTIONNEMENT AVEC LES PAQUETS D'INSTALLATION

Lors de la création de la tâche d'installation à distance, les paquets d'installation sont utilisés. Ces paquets contiennent un ensemble de paramètres nécessaires à l'installation de l'application. Vous pouvez utiliser le même paquet d'installation plusieurs fois.

Les paquets d'installation formés pour les Serveurs d'administration se placent dans l'arborescence de la console dans le dossier **Stockages** dans le dossier joint **Paquets d'installation**. Sur le Serveur d'administration les paquets d'installation sont sauvegardés dans le dossier partagé spécifié, dans le dossier de service Packages.

### DANS CETTE SECTION

Génération du paquet d'installation .....	<a href="#">52</a>
Propagation des paquets d'installation sur les Serveurs d'administration secondaires .....	<a href="#">53</a>
Propagation des paquets d'installation à l'aide des agents de mise à jour .....	<a href="#">53</a>
Transfert dans Kaspersky Security Center des informations sur les résultats d'installation de l'application .....	<a href="#">53</a>

## GENERATION DU PAQUET D'INSTALLATION

➤ Afin de créer le paquet d'installation, procédez comme suit :

1. Connectez-vous au Serveur d'administration nécessaire.
2. Dans l'arborescence de la console **Stockages**, sélectionnez le dossier joint **Paquets d'installation**.
3. Lancez le processus de création d'un paquet d'installation par un des moyens suivants :
  - dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez l'option **Créer** → **Paquet d'installation** ;
  - dans le menu contextuel de la liste des paquets d'installation, sélectionnez l'option **Créer** → **Paquet d'installation** ;
  - à l'aide du lien **Créer un paquet d'installation** dans le groupe de gestion avec la liste des paquets d'installation.

Finalement l'Assistant de création d'un paquet d'installation se lancera. Suivez les instructions de l'Assistant.

Après la fin de l'Assistant, le paquet d'installation créé sera affiché dans la zone de travail du dossier **Paquets d'installation**.

Il ne faut pas créer manuellement le paquet d'installation pour l'installation à distance de l'Agent d'administration. Il se forme automatiquement lors de l'installation de l'application Kaspersky Security Center et se situe dans le dossier **Paquets d'installation**. Si le paquet pour l'installation à distance de l'Agent d'administration a été supprimé, alors il faut sélectionner le fichier nagent9.kud, situé dans le dossier NetAgent de distribution Kaspersky Security Center, pour sa création réitérée en tant que fichier avec la description.

Lors de la création du paquet d'installation du Serveur d'administration, il faut sélectionner le fichier sc9.kud, situé à la racine du dossier de distribution Kaspersky Security Center, en tant que fichier avec description.

## PROPAGATION DES PAQUETS D'INSTALLATION SUR LES SERVEURS D'ADMINISTRATION SECONDAIRES

➔ Pour propager les paquets d'installation sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.
2. Lancez la création de la tâche de propagation du paquet d'installation sur les Serveurs d'administration secondaires à l'aide d'un des moyens suivants :
  - Si vous voulez former la tâche pour les Serveurs secondaires du groupe d'administration sélectionné, lancez la création de la tâche de groupe pour ce groupe.
  - Si vous voulez former la tâche pour l'ensemble de Serveurs secondaires, lancez la création de la tâche pour l'ensemble d'ordinateurs.

Ceci permet de lancer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.

Dans la fenêtre **Type de tâche** de l'Assistant de création de la tâche dans l'entrée **Serveur d'administration Kaspersky Security Center** dans le dossier **Avancé**, sélectionnez le type de tâche **Diffusion du paquet d'installation**.

Suite au fonctionnement de l'Assistant de création de la tâche, la tâche de propagation des paquets d'installation sélectionnés sur les Serveurs d'administration secondaire sera créée.

3. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiqué dans les paramètres de la tâche.

Suite à l'exécution de la tâche, les paquets d'installation sélectionnés seront copiés sur les Serveurs d'administration secondaires.

## PROPAGATION DES PAQUETS D'INSTALLATION A L'AIDE DES AGENTS DE MISE A JOUR

Vous pouvez utiliser les agents de mises à jour pour la propagation de paquets d'installation dans le cadre du groupe d'administration.

Après la récupération des paquets d'installation depuis le Serveur d'administration, les agents de mises à jour les diffusent automatiquement sur les postes clients à l'aide d'une diffusion IP multiadresse. La diffusion IP de nouveaux paquets d'installation dans le cadre du groupe d'administration est effectuée une fois. Si au moment de la diffusion le poste client a été désactivé du réseau de la société, alors lors du lancement de la tâche d'installation, l'Agent d'administration du poste client télécharge automatiquement le paquet d'installation nécessaire de l'agent de mises à jour.

## TRANSFERT DANS KASPERSKY SECURITY CENTER DES INFORMATIONS SUR LES RESULTATS D'INSTALLATION DE L'APPLICATION

➔ Pour configurer la transmission de l'information diagnostique dans Kaspersky Security Center sur le résultat d'installation de l'application, procédez comme suit :

1. Passez dans le dossier du paquet d'installation formé par les moyens de Kaspersky Security Center pour l'application sélectionnée. Ce dossier est situé dans le dossier partagé qui était indiqué lors de l'installation de Kaspersky Security Center.

- Ouvrez le fichier avec l'extension kpd ou kud pour la rédaction (par exemple, à l'aide du traitement de texte Notepad Microsoft Windows). Le fichier a le format du fichier ini de configuration ordinaire.
- Ajouter les lignes suivantes dans le fichier :

```
[SetupProcessResult]

Wait=1
```

Cette commande configure l'application Kaspersky Security Center de telle manière, pour qu'elle attende la fin d'installation de l'application, pour laquelle le paquet d'installation est formé, et pour qu'elle analyse le code de retour du programme d'installation. S'il faut désactiver la transmission de l'information diagnostique, saisissez la valeur 0 pour la clé Wait.

- Introduisez la description des codes de retour de l'installation réussite. Pour ce faire, ajoutez les lignes suivantes dans le fichier :

```
[SetupProcessResult_SuccessCodes]

<code de retour>=[<description>]

<code de retour 1>=[<description>]

...
```

Les valeurs facultatives figurent entre crochets.

Syntaxe des lignes :

- <code de retour>. N'importe quel nombre correspondant au code de retour du programme d'installation. Le nombre des codes de retour peut être aléatoire.
- <description>. La description de texte du résultat d'installation. La description peut être absente.

- Introduisez la description des codes de retour pour l'installation erronée. Pour ce faire, ajoutez les lignes suivantes dans le fichier :

```
[SetupProcessResult_ErrorCodes]

<code de retour>=[<description>]

<code de retour 1>=[<description>]

...
```

La syntaxe des lignes correspond à la syntaxe des codes de retour lors de l'installation réussite.

- Fermer le fichier kpd ou .kud, en sauvegardant toutes les modifications accomplies.

Finalement, l'information sur les résultats d'installation de l'application, indiquée par l'utilisateur, sera enregistrée dans les journaux de Kaspersky Security Center et sera affichée dans la liste des événements, dans les rapports et dans les résultats d'exécution des tâches.

## RECUPERATION DES VERSION ACTUELLES DES APPLICATIONS

Kaspersky Security Center permet de récupérer les versions actuelles des applications corporatives exposées sur les serveurs Web de Kaspersky Lab.

► Pour recevoir des versions actuelles des applications corporatives de Kaspersky Lab, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application Kaspersky Security Center.
2. Ouvrez la fenêtre **Versions actuelles des applications** à l'aide du lien **Nouvelles versions des applications de Kaspersky Lab** dans le groupe **Déploiement**.

Le lien **Nouvelles versions des applications de Kaspersky Lab** devient accessible quand le Serveur d'administration découvre une nouvelle version de l'application corporative sur le serveur Web de Kaspersky Lab.

3. Sélectionnez dans la liste l'application nécessaire.
4. Télécharger le distributif de l'application à l'aide du lien dans la ligne **URL de la distribution**.

Si pour l'application sélectionnée, le bouton **Télécharger les applications et créer les paquets d'installation** s'affiche, vous pouvez cliquer sur ce bouton pour télécharger le distributif de l'application et pour créer automatiquement le paquet d'installation. Dans ce cas, Kaspersky Security Center télécharge le distributif de l'application sur le Serveur d'administration dans le dossier partagé indiqué lors de l'installation de Kaspersky Security Center. Le paquet d'installation, créé automatiquement, s'affiche dans le dossier **Stockages** de l'arborescence de la console, dans le dossier joint **Paquets d'installation**.

Après la fermeture de la fenêtre **Versions actuelles des applications**, le lien **Nouvelles versions des applications de Kaspersky Lab** disparaît du groupe **Déploiement**.

Vous pouvez créer les paquets d'installation des nouvelles versions des applications et travailler avec les paquets d'installation créés dans le dossier **Stockages** de l'arborescence de la console, dans le dossier joint **Paquets d'installation**.

Vous pouvez aussi ouvrir la fenêtre **Versions actuelles des applications** à l'aide du lien **Nouvelles versions des applications de Kaspersky Lab** dans la zone de travail du dossier **Paquets d'installation**.

### VOIR EGALEMENT

Installation des applications à l'aide de la tâche d'installation à distance .....	<a href="#">46</a>
Installation des applications à l'aide de l'Assistant d'installation à distance .....	<a href="#">49</a>
Consultation du rapport de déploiement de la protection .....	<a href="#">50</a>
Désinstallation à distance des applications .....	<a href="#">50</a>
Fonctionnement avec les paquets d'installation .....	<a href="#">52</a>
Préparation de l'ordinateur à l'installation à distance. Utilitaire riprep.exe .....	<a href="#">56</a>
Génération du paquet d'installation .....	<a href="#">52</a>

## PREPARATION DE L'ORDINATEUR A L'INSTALLATION A DISTANCE. UTILITAIRE RIPREP.EXE

L'installation à distance de l'application sur un poste client peut se terminer avec erreur pour des raisons suivantes :

- La tâche a déjà réussi sur cet ordinateur. En ce cas, son exécution n'est pas requise de nouveau.
- Pendant le lancement de la tâche l'ordinateur a été arrêté. Dans ce cas, il faut démarrer l'ordinateur et lancer la tâche encore une fois.
- L'échec de connexion entre le Serveur d'administration et l'Agent d'administration, installé sur le poste client. Pour déterminer les causes du problème, vous pouvez utiliser l'utilitaire de diagnostic à distance de l'ordinateur (klactgui). Pour plus d'informations sur cet utilitaire reportez-vous au *Manuel de l'administrateur de Kaspersky Security Center*.
- Si l'Agent d'administration n'est pas installé sur l'ordinateur, les problèmes suivants peuvent survenir lors de l'installation à distance de l'application :
  - Sur le poste client, le mode **L'accès partagé simple aux fichiers** est activé.
  - Le service Server ne fonctionne pas sur le poste client.
  - Tous les ports nécessaires sont fermés sur le poste client.
  - Le compte sous lequel la tâche est exécutée ne jouit pas assez de privilèges.

Pour résoudre les problèmes survenus lors de l'installation de l'application sur le poste client sur lequel l'Agent d'administration n'a pas été installé, vous pouvez utiliser l'utilitaire de préparation de l'ordinateur à l'installation à distance (riprep).

L'utilitaire de préparation de l'ordinateur à l'installation à distance (riprep) est décrit dans cette section. Il est situé dans le dossier d'installation Kaspersky Security Center sur l'ordinateur avec le Serveur d'administration installé.

L'utilitaire de préparation de l'ordinateur à l'installation à distance ne fonctionne pas sous le système d'exploitation Microsoft Windows XP Home Edition.

### DANS CETTE SECTION

Préparation de l'ordinateur à l'installation à distance en mode interactif ..... [56](#)

Préparation de l'ordinateur à l'installation à distance en mode non interactif ..... [57](#)

## PREPARATION DE L'ORDINATEUR A L'INSTALLATION A DISTANCE EN MODE INTERACTIF

➤ Pour préparer l'ordinateur à l'installation à distance en mode interactif, procédez comme suit :

1. Lancez le fichier riprep.exe sur le poste client.
2. Dans la fenêtre principale ouverte de l'utilitaire de préparation à l'installation à distance, cochez les cases suivantes :
  - **Désactiver l'accès partagé simple aux fichiers.**
  - **Lancer le service Server.**

- **Ouvrir les ports.**
- **Ajouter un compte.**
- **Désactiver le contrôle des comptes utilisateur (UAC).** Ce paramètre est accessible pour les systèmes d'exploitation Microsoft Windows Vista, Microsoft Windows 7 et Microsoft Windows Server 2008.

3. Cliquez sur le bouton **Démarrer**.

Finalement, les étapes de préparation de l'ordinateur à l'installation à distance s'affichent dans la partie inférieure de la fenêtre principale de l'utilitaire.

Si vous avez coché la case **Ajouter un compte**, la demande de saisie du nom du compte et du mot de passe sera affichée lors de la création du compte. Finalement, un compte local, appartenant au groupe des administrateurs locaux, sera créé.

Si vous avez coché la case **Désactiver le contrôle des comptes utilisateur**, la tentative de désactivation du contrôle des comptes sera exécutée même si le contrôle des comptes a été désactivé avant le lancement de l'utilitaire. Après la désactivation du contrôle des comptes la demande de redémarrage de l'ordinateur sera affichée.

## PREPARATION DE L'ORDINATEUR A L'INSTALLATION A DISTANCE EN MODE NON INTERACTIF

► *Pour préparer l'ordinateur à l'installation à distance en mode non interactif,*

sur le poste client lancer le fichier riprep.exe de la ligne de commande avec l'ensemble nécessaire des paramètres.

Syntaxe de l'utilitaire :

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Description des paramètres :

- `-silent` : lancement de l'utilitaire en mode non interactif.
- `-cfg CONFIG_FILE` : définition de configuration de l'utilitaire, où `CONFIG_FILE` : chemin d'accès au fichier de configuration (fichier avec extension .ini).
- `-tl traceLevel` : définition du niveau de traçage, où `traceLevel` : nombre de 0 à 5. Si le paramètre n'est pas indiqué, alors la valeur 0 est utilisée.

Suite au lancement de l'utilitaire en mode non interactif, vous pouvez exécuter des tâches suivantes :

- Désactivation du mode d'accès partagé simple aux fichiers.
- Lancement du système Server sur le poste client.
- Ouverture des ports.
- Création d'un compte local.
- Désactivation du contrôle des comptes utilisateur (UAC).

Vous pouvez définir les paramètres de préparation de l'ordinateur à l'installation à distance dans le fichier de configuration indiqué dans la clé `-cfg`. Afin d'ajouter ces paramètres, il faut ajouter les informations suivantes dans le fichier de configuration :

- dans la section `Common` spécifier les tâches à exécuter :
  - `DisableSFS` : désactivation du mode d'accès partagé simple aux fichiers (0 – tâche désactivée ; 1 – tâche activée) ;
  - `StartServer` : démarrage du service Server (0 – tâche désactivée ; 1 – tâche activée) ;
  - `OpenFirewallPorts` : ouverture des ports nécessaires (0 – tâche désactivée ; 1 – tâche activée) ;
  - `DisableUAC` : désactivation du contrôle des comptes utilisateur (0 – tâche désactivée ; 1 – tâche activée) ;
  - `RebootType` : définition du comportement en cas de nécessité de redémarrage lors de la désactivation du contrôle des comptes. Vous pouvez utiliser les valeurs suivantes du paramètre :
    - 0 – ne jamais redémarrer l'ordinateur ;
    - 1 – redémarrer l'ordinateur, si avant le lancement de l'utilitaire le contrôle des comptes a été activé ;
    - 2 – redémarrage forcé l'ordinateur, si avant le lancement de l'utilitaire le contrôle des comptes a été activé ;
    - 4 – redémarrer toujours l'ordinateur ;
    - 5 – redémarrage toujours forcé de l'ordinateur.
- dans la section `UserAccount` saisir le nom du compte (`user`) et son mot de passe (`Pwd`).

L'exemple du contenu du fichier de configuration :

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

A la fin du fonctionnement de l'utilitaire, les fichiers suivants se créent dans le dossier de lancement :

- `riprep.txt` : rapport de fonctionnement, où les étapes de fonctionnement de l'utilitaire avec les causes de leur comportement sont énumérées.
- `riprep.log` : fichier de traçage (se crée, si le niveau de traçage est plus de 0).

# INSTALLATION LOCALE DES APPLICATIONS

Cette section décrit la procédure d'installation des applications qui peuvent être installées sur les ordinateurs uniquement d'une manière locale.

Pour réaliser l'installation locale des applications sur le poste client sélectionné, il vous faut posséder des privilèges d'administrateur sur cet ordinateur.

► *Pour installer les applications d'une manière locale sur le poste client sélectionné, procédez comme suit :*

1. Installez l'Agent d'administration sur le poste client et configurez la connexion du poste client avec le Serveur d'administration.
2. Installez sur l'ordinateur les applications nécessaires selon les descriptions exposées dans les Manuels pour ces applications.
3. Installez sur le bureau d'administrateur le plug-in d'administration pour chaque application installée.

Kaspersky Security Center prend aussi en charge la possibilité d'installation locale des applications à l'aide du paquet d'installation autonome.

La création des paquets autonomes d'installation est accessible pour les applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition ;
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition ;
- Kaspersky Anti-Virus 8.0 pour la sauvegarde des données ;
- Kaspersky Anti-Virus 6.0 Second Opinion Solution ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security Data Protection Suite ;
- Kaspersky Security for Virtualization 1.1.

## DANS CETTE SECTION

---

Installation locale de l'Agent d'administration .....	<a href="#">60</a>
Installation locale du plug-in d'administration de l'application.....	<a href="#">60</a>
Installation de l'application en mode non interactif .....	<a href="#">60</a>
Installation de l'application à l'aide des paquets autonomes .....	<a href="#">61</a>

## INSTALLATION LOCALE DE L'AGENT D'ADMINISTRATION

► Pour installer l'Agent d'administration sur l'ordinateur d'une manière locale,

lancez le fichier exécutable setup.exe, situé sur le CD de distribution de l'application Kaspersky Security Center dans le dossier Packages\NetAgent. Finalement, l'Assistant d'installation de l'Agent d'administration se lancera. Suivez les instructions de l'Assistant.

Le processus d'installation de l'Agent d'administration à partir du fichier de distribution obtenu par Internet correspond au processus d'installation de l'Agent d'administration à partir du CD de distribution.

À la fin du fonctionnement de l'Assistant d'installation, l'Agent d'administration sera installé sur votre ordinateur.

Vous pouvez consulter les propriétés du service de l'Agent d'administration Kaspersky Security Center, lancer, arrêter et suivre le fonctionnement de l'Agent d'administration à l'aide des moyens standards d'administration Microsoft Windows : Administration de l'ordinateur\Services.

Le plug-in pour le fonctionnement avec Cisco Network Admission Control (NAC) s'installe sur l'ordinateur conjointement avec l'Agent d'administration. Ce plug-in fonctionne dans le cas où l'application Cisco Trust Agent est installée sur l'ordinateur.

Si vous voulez utiliser l'ordinateur, sur lequel l'Agent d'administration est installé, en tant que la passerelle des connexions pour le groupe d'administration sélectionné, il faut indiquer, que l'ordinateur, sur lequel l'Agent d'administration est installé, est l'agent de mises à jour pour ce groupe et il est utilisé en tant que la passerelle des connexions (cf. section " Désignation de l'ordinateur en tant que l'agent de mises à jour. Configuration des paramètres de l'agent de mises à jour " à la page [41](#)).

## INSTALLATION LOCALE DU PLUG-IN D'ADMINISTRATION DE L'APPLICATION

► Afin de lancer le plug-in d'administration de l'application,

sur l'ordinateur avec la Console d'administration préinstallée, lancez le fichier exécutable klcfginst.exe qui fait partie du paquet de distribution de cette application. Le fichier klcfginst.exe fait partie de toutes les applications administrées par Kaspersky Security Center. L'installation est suivie de l'Assistant et ne demande aucune configuration des paramètres.

## INSTALLATION DE L'APPLICATION EN MODE NON INTERACTIF

► Afin d'effectuer l'installation de l'application en mode non interactif, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application Kaspersky Security Center
2. Dans l'arborescence de la console **Stockages** dans le dossier joint **Paquets d'installation**, sélectionnez le paquet d'installation de l'application nécessaire ou formez un nouveau paquet d'installation pour cette application.

Le paquet d'installation sera enregistré sur le Serveur d'administration dans le dossier partagé dans le dossier de service Packages. Avec cela, le sous-dossier isolé correspond à chaque paquet d'installation.

3. Ouvrez le dossier du paquet d'installation nécessaire grâce à un des modes suivants :
  - Copiez le dossier, correspondant au paquet d'installation nécessaire, du Serveur d'administration sur le poste client. Ensuite, ouvrez le dossier copié sur le poste client.
  - Ouvrez le dossier partagé du poste client sur le Serveur d'administration. Ce dossier correspond au paquet d'installation nécessaire.

Si le dossier partagé se trouve sur l'ordinateur avec le système d'exploitation Microsoft Windows Vista préinstallé, il faut établir la valeur **Désactivé** pour le paramètre **Administration des comptes utilisateurs : tous les administrateurs travaillent en mode d'approbation par l'administrateur (Démarrer → Panneau de configuration → Administration → Stratégie locale de la sécurité → Paramètres de la sécurité)**.

4. Selon l'application sélectionnée, procédez comme suit :
  - Pour Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers et Kaspersky Security Center passez au sous-dossier exec et lancez le fichier exécutable (fichier avec extension .exe) avec la clé /s.
  - Pour autres applications de Kaspersky Lab lancez du dossier ouvert le fichier exécutable (fichier avec extension .exe) avec la clé /s.

## INSTALLATION DE L'APPLICATION A L'AIDE DES PAQUETS AUTONOMES

Kaspersky Security Center permet de former les paquets autonomes d'installation des applications. Le paquet autonome d'installation représente le fichier exécutable qui peut être placé sur le serveur Web, envoyé par courrier ou transmis vers le poste client par un autre moyen. Le fichier reçu peut être lancé localement sur l'ordinateur pour exécuter l'installation de l'application sans la participation de Kaspersky Security Center.

➤ *Pour installer l'application à l'aide du paquet autonome d'installation, procédez comme suit :*

1. Connectez-vous au Serveur d'administration nécessaire.
2. Dans le dossier de l'arborescence de la console **Stockages**, sélectionnez le dossier joint **Paquets d'installation**.
3. Dans la zone de travail, sélectionnez le paquet d'installation de l'application nécessaire.
4. Lancez le processus de création d'un paquet autonome d'installation par un des moyens suivants :
  - dans le menu contextuel du paquet d'installation, sélectionnez l'option **Créer un paquet d'installation autonome** ;
  - à l'aide du lien **Créer un paquet d'installation autonome** dans le groupe de travail avec le paquet d'installation.

Finalement, l'Assistant de création du paquet d'installation autonome se lance. Suivez les instructions de l'Assistant.

A la dernière étape de l'Assistant, sélectionnez le mode de transfert du paquet d'installation autonome sur le poste client.

5. Transmettez le paquet d'installation autonome sur le poste client.
6. Lancez le paquet d'installation autonome sur le poste client.

Finalement, l'application sera installée sur le poste client avec les paramètres indiqués dans le paquet autonome.

# CHARGE SUR LE RESEAU

Cette section contient l'information sur le volume du trafic réseau que les postes clients et le Serveur d'administration échangent entre eux-mêmes lors de l'exécution des scénarios clés administratifs.

La charge principale sur le réseau est liée avec l'exécution des scénarios d'administration suivants :

- déploiement initial de la protection antivirus ;
- mise à jour initiale des bases antivirus ;
- synchronisation du poste client avec le Serveur d'administration ;
- mise à jour régulière des bases antivirus ;
- traitement des événements sur les postes clients par le Serveur d'administration.

## DANS CETTE SECTION

Déploiement initial de la protection antivirus .....	<a href="#">62</a>
Mise à jour initiale des bases antivirus .....	<a href="#">63</a>
Synchronisation du client avec le Serveur d'administration.....	<a href="#">63</a>
Mise à jour complémentaire des bases antivirus.....	<a href="#">64</a>
Traitement des événements des clients par le Serveur d'administration.....	<a href="#">65</a>
Débit du trafic pendant vingt-quatre heures .....	<a href="#">65</a>

## DEPLOIEMENT INITIAL DE LA PROTECTION ANTIVIRUS

Cette section reprend le débit du trafic lors de l'installation sur le poste client de l'Agent d'administration de version 9.0 et de Kaspersky Endpoint Security 8 for Windows (cf. tableau ci-après).

L'Agent d'administration s'installe à l'aide de l'installation forcée, quand les fichiers requis pour l'installation sont copiés par le Serveur d'administration dans le dossier partagé sur le poste client. Après l'installation l'Agent d'administration reçoit le distributif de Kaspersky Endpoint Security 8 for Windows, en utilisant la connexion avec le Serveur d'administration.

Tableau 7. Débit du trafic

SCENARIO	INSTALLATION DE L'AGENT D'ADMINISTRATION POUR UN POSTE CLIENT	INSTALLATION DE KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS POUR UN POSTE CLIENT (AVEC LES BASES ACTUALISEES)	INSTALLATION COLLECTIVE DE L'AGENT D'ADMINISTRATION ET DE KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS
Trafic du poste client au Serveur d'administration, Ko.	386,70	1 841,3	2 253,8
Trafic du Serveur d'administration au poste client, Ko.	14 801,13	269 994,5	284 768,7
Trafic général (pour un poste client), Ko.	15 187,83	271 835,8	287 022,5

Après avoir installé les Agents d'administration sur les postes clients, vous pouvez spécifier un des ordinateurs dans le groupe d'administration en tant qu'agent de mises à jour. Il sera utilisé pour la propagation des paquets d'installation. En ce cas, le volume du trafic transmis lors du déploiement initial de la protection antivirus diffère essentiellement en fonction de l'utilisation de la diffusion IP multiadresse.

Dans le cas d'utilisation de la diffusion IP multiadresse, les paquets d'installation seront diffusés une fois sur tous les ordinateurs inclus dans le groupe d'administration. De cette façon, le trafic général se réduira à peu près dans N fois, où N - le nombre général des ordinateurs inclus dans le groupe d'administration. Si la diffusion IP multiadresse n'est pas utilisée, le trafic général coïncide avec le fait d'obtention des paquets d'installation du Serveur d'administration, et ce n'est pas le Serveur d'administration qui est la source des paquets d'installation, mais c'est l'agent de mises à jour.

## MISE A JOUR INITIALE DES BASES ANTIVIRUS

Cette section reprend les informations sur le débit du trafic lors du premier lancement de la tâche de mise à jour des bases sur le poste client (cf. tableau ci-après).

Tableau 8. Débit du trafic

SCENARIO	MISE A JOUR INITIALE DES BASES ANTIVIRUS <sup>1</sup>
Trafic du poste client au Serveur d'administration, Ko.	1 357,1
Trafic du Serveur d'administration au poste client, Ko.	33 917,0
Trafic général (pour un poste client), Ko.	35 274,1

## SYNCHRONISATION DU CLIENT AVEC LE SERVEUR D'ADMINISTRATION

Ce scénario caractérise l'état du système d'administration dans le cas, quand la synchronisation active des données entre les postes clients et le Serveur d'administration se passe. Les postes clients se connectent au Serveur d'administration avec une période, spécifiée par l'administrateur. Le Serveur d'administration compare l'état des données sur le poste client avec l'état des données sur le Serveur et enregistre l'information sur la dernière connexion du poste client dans la base de données et synchronise les données.

La section reprend les informations sur le débit du trafic pour les scénarios d'administration généraux lors de la connexion du client au Serveur d'administration avec la synchronisation (cf. tableau ci-après).

<sup>1</sup> Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases.

Tableau 9. Débit du trafic

SCENARIO	Trafic des postes clients au Serveur d'administration, Ko	Trafic du Serveur d'administration aux postes clients, Ko.	Trafic général (pour un poste client), Ko. <sup>2</sup>
<b>SYNCHRONISATION INITIALE<sup>3</sup> AVANT LA MISE A JOUR DES BASES SUR LE POSTE CLIENT</b>	368,6	463,7	832,3
<b>SYNCHRONISATION INITIALE<sup>4</sup> APRES LA MISE A JOUR DES BASES SUR LE POSTE CLIENT</b>	1 748,3	34 388,3	36 136,6
<b>SYNCHRONISATION LORS DE L'ABSENCE DES MODIFICATIONS SUR LE POSTE CLIENT ET SUR LE SERVEUR D'ADMINISTRATION</b>	8,7	6,6	15,3
<b>SYNCHRONISATION LORS DE LA MODIFICATION D'UN PARAMETRE DANS LA STRATEGIE DU GROUPE</b>	11,1	13,3	24,4
<b>SYNCHRONISATION LORS DE LA MODIFICATION D'UN PARAMETRE DANS LA TACHE DE GROUPE</b>	10,0	12,5	22,5
<b>SYNCHRONISATION FORCEEE LORS DE L'ABSENCE DES MODIFICATIONS SUR LE POSTES CLIENT</b>	47,3	15,5	62,8

## MISE A JOUR COMPLEMENTAIRE DES BASES ANTIVIRUS

Cette section reprend les informations sur le débit du trafic lors de la mise à jour d'incrémentation des bases antivirus dans 20 heures après la dernière mise à jour (cf. tableau ci-après).

Tableau 10. Débit du trafic

SCENARIO	MISE A JOUR D'INCREMENTATION DES BASES ANTIVIRUS <sup>5</sup>
Trafic du poste client au Serveur d'administration, Ko.	436,9
Trafic du Serveur d'administration au poste client, Ko.	9 979,2
Trafic général (pour un poste client), Ko. <sup>6</sup>	10 416,1

<sup>2</sup> Le volume du trafic varie essentiellement en fonction de l'utilisation d'une diffusion IP multiadresse à l'intérieur des groupes d'administration. Dans le cas d'utilisation d'une diffusion IP multiadresse, le trafic général pour le groupe se réduit à peu près dans N fois, où N- le nombre général des ordinateurs inclus dans le groupe d'administration.

<sup>3</sup> Installation de l'Agent d'administration et de l'application antivirus sur le poste client, déplacement du poste client dans le groupe d'administration, application au poste client de la stratégie et des tâches créées pour le groupe par défaut.

<sup>4</sup> Installation de l'Agent d'administration et de l'application antivirus sur le poste client, déplacement du poste client dans le groupe d'administration, application au poste client de la stratégie et des tâches créées pour le groupe par défaut.

<sup>5</sup> Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases.

<sup>6</sup> Le volume du trafic varie essentiellement en fonction de l'utilisation d'une diffusion IP multiadresse à l'intérieur des groupes d'administration. Dans le cas d'utilisation d'une diffusion IP multiadresse, le trafic général pour le groupe se réduit à peu près dans N fois, où N- le nombre général des ordinateurs inclus dans le groupe d'administration.

## TRAITEMENT DES EVENEMENTS DES CLIENTS PAR LE SERVEUR D'ADMINISTRATION

Cette section reprend le débit du trafic lors de l'apparition sur le poste client de l'événement "Virus découvert" dont les informations sont transmises sur le Serveur d'administration et enregistrées dans la base de données (cf. tableau ci-après).

Tableau 11. Débit du trafic

SCENARIO <sup>7</sup>	TRANSFERT DES DONNEES SUR LE SERVEUR D'ADMINISTRATION QUAND L'EVENEMENT "VIRUS DECOUVERT" SURGIT.	TRANSFERT DES DONNEES SUR LE SERVEUR D'ADMINISTRATION QUAND NEUFS EVENEMENTS "VIRUS DECOUVERT" SURGISSENT.
Trafic du poste client au Serveur d'administration, Ko.	27,2	100,4
Trafic du Serveur d'administration au poste client, Ko.	25,8	52,5
Trafic général (pour un poste client), Ko.	53,0	152,9

## DEBIT DU TRAFIC PENDANT VINGT-QUATRE HEURES

Cette section reprend les informations sur le débit du trafic pendant vingt-quatre heures de fonctionnement du système d'administration en état de "repos", quand aucun changement des données ne se passe, ni du côté des postes clients, ni du côté du Serveur d'administration (cf. tableau ci-après).

Tableau 12. Débit du trafic

SCENARIO	ÉTAT DE "REPOS" DU SYSTEME D'ADMINISTRATION <sup>8</sup>
Trafic du poste client au Serveur d'administration, Ko.	2 922,1
Trafic du Serveur d'administration au poste client, Ko.	15 140,5
Trafic général (pour un poste client), Ko.	18 062,6

<sup>7</sup> Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle de l'application antivirus, et en fonction des événements notamment spécifiés dans la stratégie de l'application antivirus comme ceux qui demandent l'enregistrement dans la base de données du Serveur d'administration.

<sup>8</sup> Les données, citées dans le tableau, caractérisent l'état du réseau après l'installation standard de Kaspersky Security Center et après la fin de fonctionnement de l'Assistant de configuration initiale. La période de synchronisation du poste client avec le Serveur d'administration durait 20 minutes, le téléchargement des mises à jour dans le stockage du Serveur d'administration se passait chaque heure.

# VITESSE DE REMPLISSAGE DE LA BASE DE DONNEES PAR LES EVENEMENTS DE KASPERSKY ENDPOINT SECURITY

Cette section reprend les exemples de vitesse de remplissage de la base de données du Serveur d'administration par les événements.

La base de données reçoit ( $N_e * N_h$ ) événements par jour (cf. tableau ci-après). Ici,  $N_h$  est le nombre de postes clients avec Kaspersky Endpoint Security installé,  $N_e$  est le nombre d'événements par jour, sur lesquels les informations sont transmises par Kaspersky Endpoint Security depuis le poste client avec Kaspersky Endpoint Security installé.

Tableau 13. Vitesse de remplissage de la base de données par les événements

<b>NOMBRE D'ORDINATEURS AVEC KASPERSKY ENDPOINT SECURITY INSTALLE</b>	<b>NOMBRE D'EVENEMENTS TRANSMIS CHAQUE JOUR DANS LA BASE DE DONNEES</b>
100	$\leq 2\ 000$
1000	$\leq 20\ 000$
10 000	$\leq 200\ 000$

Le tableau reprend les données pour le fonctionnement titulaire de Kaspersky Endpoint Security, quand pas plus de 20 événements sont reçus par jour depuis un poste client.

Le nombre maximal des événements, conservés dans la base de données, se définit dans la section **Paramètres** de la fenêtre des propriétés du Serveur d'administration. Par défaut, la base de données ne dépasse pas 400 000 événements conservés.

# CONTACTER LE SUPPORT TECHNIQUE

Vous pouvez obtenir des informations sur l'application auprès des experts du service du Support Technique par téléphone ou par Internet. Lorsque vous contactez le service du Support Technique, indiquez les informations sur la licence de l'application Kaspersky Security Center.

Les experts du service du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application qui ne sont pas traitées dans l'aide. En cas d'infection de votre ordinateur, ils vous aideront à éliminer dans la mesure du possible les programmes malveillants, ainsi qu'à surmonter leurs effets.

Avant de contacter le service du Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique (<http://support.kaspersky.com/fr/support/entreprises/rules>).

## Demande adressée par email au Support Technique

Vous pouvez poser vos questions aux experts du service du Support Technique en remplissant le formulaire en ligne du Helpdesk (<http://support.kaspersky.ru/helpdesk.html?LANG=fr>).

Vous pouvez envoyer votre demande en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une demande électronique, vous devez indiquer votre **numéro client** obtenu lors de l'enregistrement sur le site Internet du service du Support Technique et le **mot de passe**.

Si vous n'êtes pas un utilisateur enregistré des applications de Kaspersky Lab, remplissez le formulaire d'enregistrement (<https://my.kaspersky.com/fr>). Lors de l'enregistrement, indiquez *le code d'activation* de l'application ou *le fichier clé*.

Vous recevrez la réponse de l'expert du service du Support Technique dans votre Espace personnel (<https://my.kaspersky.com/fr>) et à l'adresse électronique indiquée dans la demande.

Dans le formulaire en ligne de demande, décrivez le problème rencontré avec le plus de détails possible. Dans les champs obligatoires, indiquez :

- **Type de la demande.** Les questions le plus souvent posées par les utilisateurs sont regroupées par thème ; par exemple "Problème d'installation / de suppression d'un logiciel" ou "Problème de recherche / de suppression de virus". Si vous ne trouvez pas le sujet qui vous concerne, sélectionnez "Question générale".
- **Nom et version de l'application.**
- **Texte de la demande.** Décrivez le problème rencontré avec le plus de détails possibles.
- **Numéro de client et mot de passe.** Saisissez le numéro de client et le mot de passe que vous avez reçu lors de l'enregistrement sur le site Internet du service du Support Technique.
- **Adresse électronique.** Les experts du service du Support Technique vous enverront la réponse à votre question.

## Support Technique par téléphone

Si le problème est urgent, vous pouvez toujours appeler le Support Technique local de Kaspersky Lab. Ou encore si vous disposez d'un Contrat de Support Kaspersky, référez-vous aux coordonnées (<http://support.kaspersky.com/fr/support/details>) indiquées sur celui-ci. Ceci aidera nos experts à vous venir en aide le plus rapidement possible.

# GLOSSAIRE

## A

### **ADMINISTRATEUR DE KASPERSKY SECURITY CENTER**

Personne qui gère le fonctionnement de l'application via le système d'administration centralisé à distance de Kaspersky Security Center.

### **ADMINISTRATION CENTRALISEE DE L'APPLICATION**

Administration à distance de l'application à l'aide des services d'administration proposés par Kaspersky Security Center.

### **ADMINISTRATION DIRECTE DE L'APPLICATION**

Administration de l'application via l'interface locale.

### **AGENT D'ADMINISTRATION**

Composant de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant est unique pour toutes les applications développées sous Windows par la société. Il existe des versions distinctes de l'Agent d'administration destinées aux versions des applications développées par Kaspersky Lab pour Novell, Unix et Mac.

### **AGENT DES MISES A JOUR**

Ordinateur qui joue le rôle de centre intermédiaire de diffusion des mises à jour et des paquets d'installation dans les limites du groupe d'administration.

### **APPLICATION INCOMPATIBLE**

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Security Center.

## B

### **BASES**

Les bases de données qui contiennent les descriptions des menaces informatiques connues de Kaspersky Lab au jour d'édition des bases. Les enregistrements dans les bases permettent de détecter le code malveillant dans les objets analysés. Les bases sont formées par les experts de Kaspersky Lab et sont actualisées chaque heure.

## C

### **CERTIFICAT DU SERVEUR D'ADMINISTRATION**

Certificat qui sert à l'authentification du Serveur d'administration lors de la connexion de la Console d'administration et de l'échange d'informations avec les postes client. Le certificat du Serveur d'administration est créé au cours de l'installation du Serveur d'administration et est enregistré sur le Serveur d'administration dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

### **CLE ACTIVE**

Clé utilisée actuellement par l'application.

### **CLE COMPLEMENTAIRE**

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

### **CLIENT DU SERVEUR D'ADMINISTRATION (POSTE CLIENT)**

L'ordinateur, serveur ou poste de travail, sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab.

## CONSOLE D'ADMINISTRATION

Composant de l'application Kaspersky Security Center qui offre une interface utilisateur pour les services d'administration du Serveur d'administration et de l'Agent d'administration.

## D

### DEGRE D'IMPORTANTCE DE L'EVENEMENT

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky Lab. Il existe 4 degrés d'importance :

- Critique.
- Erreur.
- Avertissement.
- Message d'information.

Les événements d'un même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

### DUREE DE VALIDITE DE LA LICENCE

La durée de validité de la licence est un intervalle de temps pendant lequel vous pouvez utiliser les fonctions de l'application et les services complémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

## E

### ETAT DE LA PROTECTION

Etat actuel de la protection qui définit le niveau de protection de l'ordinateur.

## F

### FICHER CLÉ

Le fichier de type xxxxxxxx.key qui permet d'utiliser une application de Kaspersky Lab selon les termes d'une licence d'évaluation ou commerciale. Le fichier clé est créé par l'application sur la base du code d'activation. Le fichier de licence est indispensable à l'utilisation de l'application.

## G

### GROUPE D'ADMINISTRATION

Regroupement d'ordinateurs sur la base des fonctions exécutées et des applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion en tant qu'ensemble unique. Le groupe peut contenir d'autres groupes. Il est possible de créer des stratégies de groupe et des tâches de groupe pour chacune des applications installées dans le groupe.

## I

### INSTALLATION A DISTANCE

Installation des applications de Kaspersky Lab à l'aide des services offerts par l'application Kaspersky Security Center.

### INSTALLATION A L'AIDE D'UN SCRIPT D'OUVERTURE DE SESSION

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou à plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancée. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs fonctionnant sous Microsoft Windows 98/Me.

## INSTALLATION FORCEE

Méthode d'installation à distance des applications de Kaspersky Lab qui permet de réaliser l'installation à distance d'un logiciel sur des postes clients définis. Pour garantir la réussite de la tâche lancée à l'aide de la méthode de l'installation forcée, le compte utilisateur employé pour le lancement de la tâche doit jouir des droits d'exécution à distance des applications sur les postes client. Cette méthode est recommandée pour l'installation des applications sur les ordinateurs fonctionnant sous les systèmes d'exploitation Microsoft Windows NT / 2000 / 2003 / XP compatibles avec cette possibilité ou sur les ordinateurs fonctionnant sous Microsoft Windows 98 / Me sur lesquels l'Agent d'administration est installé.

## M

### MISE A JOUR

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

### MISE A JOUR DISPONIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

## P

### PAQUET D'INSTALLATION

Sélection des fichiers pour l'installation à distance de l'application Kaspersky Lab à l'aide du système d'administration à distance Kaspersky Security Center. Le paquet d'installation est créé sur la base des fichiers spéciaux portant les extensions .kpd et .kud, inclus dans la distribution de l'application, et contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut.

### PARAMETRES DE LA TACHE

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

### PARAMETRES 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.

### PLUG-IN D'ADMINISTRATION DE L'APPLICATION

Composant spécial, qui fait office d'interface pour l'administration du fonctionnement de l'application par la Console d'administration. Le plug-in d'administration est propre à chaque application. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Security Center.

### POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Ordinateur sur lequel le composant qui fait office d'interface pour l'administration de l'application est installé. Pour les logiciels antivirus, il s'agit de la Console Anti-Virus, pour l'application Kaspersky Security Center – de la Console d'administration.

Depuis le poste de travail de l'administrateur, il est possible de réaliser la configuration et l'administration de la partie Serveur de l'administration, et pour Kaspersky Security Center, d'élaborer et d'administrer la protection antivirus centralisée du réseau de l'entreprise sur la base des applications de Kaspersky Lab.

## R

### RESTAURATION DES DONNEES DU SERVEUR D'ADMINISTRATION

Il s'agit de la restauration des données du Serveur d'administration à l'aide d'un utilitaire de sauvegarde sur la base des informations présentes dans le dossier de sauvegarde. L'utilitaire permet de restaurer :

- la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;
- les données de configuration sur la structure du groupe d'administration et des postes clients ;
- le stockage des paquets d'installation des applications pour une installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;
- le certificat du Serveur d'administration.

## S

### SAUVEGARDE DES DONNEES DU SERVEUR D'ADMINISTRATION

Copie des données du Serveur d'administration pour la sauvegarde et la restauration ultérieure, réalisée à l'aide de l'utilitaire de copie de sauvegarde. L'utilitaire permet d'enregistrer :

- la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;
- les données de configuration sur la structure du groupe d'administration et des postes clients ;
- le stockage des paquets d'installation des applications pour une installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;
- le certificat du Serveur d'administration.

### SERVEUR D'ADMINISTRATION

Composant de l'application Kaspersky Security Center qui remplit la fonction d'enregistrement centralisé des informations sur les applications Kaspersky Lab installées sur le réseau local de l'entreprise, et d'un outil efficace de gestion de ces applications.

### SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Les serveurs HTTP et FTP de Kaspersky Lab depuis lesquels l'application de Kaspersky Lab récupère les mises à jour des bases et des modules de l'application.

### SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et survenus dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque de virus. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

### STOCKAGE DES COPIES DE SAUVEGARDE

Dossier spécial pour la conservation des copies des données du Serveur d'administration, créées à l'aide de l'utilitaire de copie de sauvegarde.

### STRATEGIE

Sélection des paramètres de fonctionnement de l'application dans un groupe d'administration en cas d'administration à l'aide de Kaspersky Security Center. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre à chaque application peut être définie. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

## T

### TACHE

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

### TACHE DE GROUPE

Tâche définie pour un groupe d'administration et exécutée sur tous les postes client de ce groupe d'administration.

### TACHE LOCALE

Tâche définie et exécutée sur un poste client particulier.

### TACHE POUR UNE SÉLECTION D'ORDINATEURS

Tâche définie pour une sélection de postes client parmi des groupes d'administration aléatoires et exécutée sur ceux-ci.

## U

### UTILISATEUR DE KASPERSKY SECURITY CENTER

Utilisateur chargé de surveiller l'état et le fonctionnement du système de protection administré à l'aide de Kaspersky Security Center.

# KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale de systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et 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 "). Selon les résultats d'une étude réalisée par KomKon TGI-Russia en 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

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

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions en combinaison avec des outils d'administration centralisée permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et ils sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures, tandis que les bases antispam sont actualisées toutes les 5 minutes.*

**Technologies.** Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment Safenet (E-U), Alt-N Technologies (E-U), Blue Coat Systems (E-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (E-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security(E-U), GFI (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), NETASQ (France), NETGEAR (E-U), Parallels (Russie), SonicWALL (E-U), WatchGuard Technologies (E-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

**Réalisations.** Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu la note la plus élevée Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien renommé AV-Comparatives. 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 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site de Kaspersky Lab :

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

Encyclopédie des virus :

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

Laboratoire antivirus :

newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>

(pour les questions aux experts antivirus)

Forum Internet de Kaspersky Lab :

<http://forum.kaspersky.fr>

# NOTIFICATION SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Cisco – la marque Cisco Systems, Inc. déposée aux Etats-Unis et aux autres pays, et/ou ses compagnies affiliées.

Active Directory, Data Access, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server et Windows Vista – les marques Microsoft Corporation déposées aux Etats-Unis et aux autres pays.

Intel, Core, Xeon – les marques Intel Corporation déposées aux Etats-Unis et aux autres pays.

Linux – la marque Linus Torvalds déposée aux Etats-Unis et aux autres pays.

Mac, Mac OS – les marques déposées Apple Inc.

Novell – la marque Novell, Inc. déposée aux Etats-Unis et aux autres pays.

UNIX – la marque déposée aux Etats-Unis et aux autres pays, la licence délivrée par la société X/Open Company Limited.

# INDEX

## A

Agent d'administration.....	29, 34
installation.....	43, 60
Agent de SNMP .....	29
Agents de mise à jour.....	41, 43, 53, 68
Ajout	
Serveur d'administration .....	39, 44
Assistant d'installation à distance.....	49

## B

BASES DE DONNEES.....	12
Bases de données .....	31

## C

Cisco Network Admission Control .....	29
Compte du système local.....	30
Compte utilisateur .....	30
Configuration	
fichier kpd .....	53
CONFIGURATION LOGICIELLE .....	12
CONFIGURATION MATERIELLE .....	12
Console d'administration .....	29
Construction de la protection.....	17

## D

Diffusion du paquet d'installation.....	53
Dossier partagé.....	32

## F

Fichier avec la description de l'application .....	53
fichier kpd.....	53

## G

Groupes d'administration .....	44, 69
--------------------------------	--------

## I

Installation	
forcée.....	47
Kaspersky Security Center .....	25
mode silencieux.....	60
paquet autonome.....	61
personnalisée .....	27
script d'ouverture de session .....	47
sélection des composants .....	29
Serveur d'administration secondaire.....	48
INSTALLATION	
A DISTANCE .....	45
ACTIVE DIRECTORY.....	45
LOCALE .....	59
PAQUET AUTONOME .....	45
TACHE .....	45

Installation forcée .....	47
Installation personnalisée .....	27
Installation standard .....	27
<b>K</b>	
KASPERSKY LAB .....	73
KASPERSKY LAB ZAO .....	73
klbackup .....	24
klsrvswch .....	30
<b>M</b>	
Mise à jour de l'application .....	24
<b>P</b>	
Packages .....	52
Paquet d'installation .....	43, 52, 70
diffusion .....	53
Paquet d'installation autonome .....	61
PAQUET D'INSTALLATION AUTONOME .....	45
Passerelle des connexions .....	18, 43, 60
Périphériques mobiles .....	33
Ports .....	25
<b>R</b>	
Rapports .....	50
riprep .....	56
<b>S</b>	
Sauvegarde .....	71
Schémas de déploiement .....	17
Script d'ouverture de session .....	47
Serveur d'administration .....	29, 34, 71
Serveur des stratégies .....	29, 34
Serveur SQL .....	31
Serveurs secondaires	
ajout .....	44
Service	
Agent d'administration .....	34
Serveur d'administration .....	34
serveur des stratégies .....	34
SHV Kaspersky Lab .....	29
Sondage du réseau .....	41
Stockages	
dossier de sauvegarde .....	71
Stratégies .....	71
Support des périphériques mobiles .....	29
Suppression	
Kaspersky Security Center .....	35
tâche .....	50
<b>T</b>	
Tâches .....	47
de groupe .....	72
Taille du réseau .....	29
Test de charge .....	17

## U

UTILITAIRE DE PREPARATION DE L'ORDINATEUR A L'INSTALLATION A DISTANCE .....	45
Utilitaire de préparation de l'ordinateur à l'installation à distance .....	49, 56