Kaspersky Security Center 10.0

Manuel d'implantation

VERSION DE L'APPLICATION : 10.0

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.

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

Date d'édition : 12/12/2012

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

TABLE DES MATIERES

A PROPOS DE CE MANUEL

Ce document est le Manuel d'implantation de Kaspersky Security Center 10.0 (ci-après Kaspersky Security Center).

Il est destiné aux techniciens chargés d'installer et d'administrer Kaspersky Security Center et d'offrir une assistance technique aux sociétés qui utilisent Kaspersky Security Center.

Ce guide poursuit les objectifs suivants :

- Décrire les principes de fonctionnement de Kaspersky Security Center, la configuration requise, les scénarios de déploiement type et les particularités de l'intégration à d'autres applications.
- Aider à la planification du déploiement de Kaspersky Security sur le réseau de l'entreprise.
- Décrire la préparation de l'installation de Kaspersky Security Center, l'installation et l'activation de l'application.
- Donner les recommandations sur la prise en charge et l'administration de Kaspersky Security Center après l'installation.
- Présenter les sources complémentaires d'informations sur l'application et les modes d'obtention du Support Technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Le Manuel d'implantation de Kaspersky Security Center contient l'introduction, les sections qui décrivent l'installation des modules 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 sur l'application (cf. page 10)

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Security Center (à la page 12)

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 13)

Cette section contient la description des modules de Kaspersky Security Center et de la logique de leur interaction.

Configurations matérielles et logicielles (à la page 14)

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 17)

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

Schémas de déploiement type du système de protection (à la page 20)

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

Déploiement du système de protection à l'intérieur de l'entreprise (à la page 21)

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

Déploiement du système de protection dans le réseau de l'entreprise-cliente (à la page 24)

Cette section décrit les processus de déploiement du système de protection dans le réseau de l'entreprise-cliente, qui correspondent aux schémas typiques de déploiement.

Déploiement du Serveur d'administration (cf. page 27)

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

Configuration du système de protection du réseau de l'entreprise-cliente (à la page 45)

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

Installation à distance des applications (cf. page 49)

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 (cf. page 64)

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

Connexion des appareils nomades au Serveur d'administration

Cette section décrit la connexion au Serveur d'administration des périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync® et iOS Mobile Device Management(iOS MDM).

Configuration de l'envoi SMS dans Kaspersky Security Center (à la page 75)

Cette section décrit l'installation de l'utilitaire Kaspersky SMS Broadcasting sur le périphérique mobile, la synchronisation de l'utilitaire avec le Serveur d'administration et la configuration de l'envoi SMS dans la Console d'administration.

Charge sur le réseau (cf. page 78)

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 du Serveur d'administration par les événements (à la page 82)

Cette section décrit les exemples de la vitesse de remplissage de la base de données du Serveur d'administration par les événements survenus pendant le fonctionnement des applications administrées.

Contacter le Support Technique

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

Glossaire

La section reprend les termes utilisés dans ce document.

Kaspersky Lab (cf. page 91)

Cette section reprend les informations sur Kaspersky Lab.

Informations sur le code tiers (cf. page 92)

Cette section contient les informations sur le code tiers utilisé dans l'application Kaspersky Security Center.

Notifications sur les marques de commerce (à la page 93)

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

Le texte du document est suivi des significations sur lesquelles nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les significations. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

Exemple de texte	Description des conventions
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte d'informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'aide. Il peut s'agir par exemple de conseils utiles, de recommandations, de valeurs importantes de paramètres ou de cas particuliers importants pour le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés dans les groupes sous le titre "Exemple".

Exemple de texte	Description des conventions
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les significations suivantes sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison de touches **Option**+**N**.	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. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères gras.
➡ *Pour créer un fichier de trace, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et présentent l'icône "flèche".
Dans la ligne de commande, saisissez le texte kav update Les informations suivantes s'affichent : Indiquez la date au format JJ:MM:AA.	La police spéciale (Courier) désigne les types de texte suivants : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<Nom d'utilisateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable à chaque fois. Par ailleurs, les chevrons sont omis.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi 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 INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour une recherche indépendante des informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site Internet du Support Technique (Base de connaissances) ;
- aide électronique ;
- La documentation.

Si vous ne parvenez pas à résoudre vous-même le problème, il est conseillé de contacter le Service de support technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 83).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

Page sur le site Web de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page spéciale pour chaque application.

La page (http://www.kaspersky.com/fr/security-center) fournit des informations générales sur l'application, ces possibilités et ses particularités.

La page http://www.kaspersky.com/fr/ contient le lien vers la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

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

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour utiliser les applications de Kaspersky Lab. La Base de connaissances est composée d'articles d'aide regroupés par thèmes.

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

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Security Center, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support Technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et les liens vers les tâches dans lesquelles ces paramètres sont utilisés.

L'aide complète contient des informations sur la gestion de la protection, la configuration des paramètres de l'application et l'exécution des tâches principales pour l'utilisateur.

Documentation

La distribution de l'application contient les documents qui vous aideront à installer et activer l'application sur les ordinateurs du réseau de l'entreprise et à configurer les paramètres de fonctionnement ou à obtenir des informations sur les principes de fonctionnement de l'application.

FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.fr).

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

CONTACTER LE SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Si vous avez des questions sur la documentation de l'application, vous pouvez contacter les membres du Groupe de rédaction de la documentation. Vous pouvez par exemple faire parvenir à nos experts vos commentaires sur la documentation.

KASPERSKY SECURITY CENTER

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

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau de l'entreprise. L'application offre à l'utilisateur l'accès aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise et permet de configurer tous les modules de la protection construite sur la base des applications de Kaspersky Lab.

L'application Kaspersky Security Center est un outil destiné aux administrateurs de réseaux d'entreprise et aux responsables de la sécurité.

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

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

- Former une hiérarchie des Serveurs d'administration pour administrer le réseau de votre propre entreprise, ainsi que les réseaux des postes distants ou des entreprises clientes.

  Les *entreprises-clientes* font référence aux entreprises dont la protection antivirus est assurée par le prestataire de services.

- Former une hiérarchie des groupes d'administration pour gérer les périphériques (les postes clients et les machines virtuelles) comme un ensemble.

- Administrer le système de protection antivirus formé à partir des applications de Kaspersky Lab.

- Créer de manière centralisée les images des systèmes d'exploitation et les déployer sur les postes clients par le réseau, ainsi qu'exécuter l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs de logiciels.

- Administrer à distance les applications de Kaspersky Lab et d'autres éditeurs installées sur les postes clients : installer les mises à jour, rechercher et corriger les vulnérabilités.

- Diffuser de manière centralisée les clés des applications de Kaspersky Lab sur les postes clients, suivre l'utilisation des clés et prolonger la durée de validité des licences.

- Recevoir les statistiques et les rapports de fonctionnement des applications et des périphériques.

- Recevoir les notifications pour les événements critiques survenus pendant le fonctionnement des applications de Kaspersky Lab.

- Contrôler l'accès des périphériques dans le réseau de l'entreprise à l'aide des règles de restriction d'accès et à l'aide de la liste "blanche" des périphériques. Les agents NAC sont utilisés pour administrer l'accès des périphériques dans le réseau de l'entreprise.

- Administrer les périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync® et iOS Mobile Device Management (iOS MDM).

- Administrer le chiffrement des informations enregistrées sur les disques durs et les disques amovibles, et administrer l'accès des utilisateurs aux données chiffrées.

- Faire l'inventaire du matériel connecté au réseau de l'entreprise.

- Travailler de façon centralisée avec les objets, placés en quarantaine ou dans le dossier de sauvegarde par les applications antivirus, aussi qu'avec les fichiers dont le traitement est différé par les applications antivirus.

ARCHITECTURE DE L'APPLICATION

Cette section contient la description des modules de Kaspersky Security Center et de la logique de leur interaction.

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

- **Serveur d'administration** (ci-après aussi *Serveur*). Est un entrepôt centralisé d'informations rélatives aux applications 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 module est un module unique pour toutes les applications développées 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.

- **Serveur des périphériques mobiles**. Offre l'accès aux périphériques mobiles et permet de les administrer via la Console d'administration. Le Serveur des périphériques mobiles exécute la collecte des informations sur les périphériques mobiles, ainsi que l'enregistrement de leurs profils.

- **Kaspersky Security Center Web-Console**. Conçu pour contrôler l'état du système de protection de l'entreprise cliente se trouvant sous l'administration de Kaspersky Security Center.

CONFIGURATIONS LOGICIELLES ET MATERIELLES

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

Serveur d'administration et Kaspersky Security Center Web-Console

Tableau 2. Configurations logicielles au Serveur d'administration et à Kaspersky Security Center Web-Console

MODULE	EXIGENCES
Système d'exploitation	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 Vista x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows 7 ; Microsoft Windows 7 x64 ; Microsoft Windows 8 ; Microsoft Windows 8 x64 ; 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 Server 2012.
Data Access Components	Microsoft Data Access Components (MDAC) version 2.8 ou supérieure ; 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, 5.087 Service Pack 1, 5.091 ; MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.

Tableau 3. Configurations matérielles au Serveur d'administration et à Kaspersky Security Center Web-Console

SYSTEME D'EXPLOITATION	FREQUENCE DU PROCESSEUR, GHZ	VOLUME DE MEMOIRE VIVE, GO	VOLUME D'ESPACE LIBRE SUR LE DISQUE, GO
Microsoft Windows, 32-bits	1 ou plus	4	10
Microsoft Windows, 64-bits	1,4 ou plus	4	10

Console d'administration

Tableau 4. Configurations logicielles pour la Console d'administration

MODULE	EXIGENCES
Système d'exploitation	Microsoft Windows (la version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration).
Console d'administration	Microsoft Management Console version 2.0 et supérieure.
Navigateur	Microsoft Internet Explorer® 7.0 et plus lors du fonctionnement avec Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 ou Microsoft Windows Vista ; Microsoft Internet Explorer 8.0 et plus lors du fonctionnement avec Microsoft Windows 7 ; Microsoft Internet Explorer 10.0 et plus lors du fonctionnement avec Microsoft Windows 8.

Tableau 5. Configurations matérielles pour la Console d'administration

SYSTEME D'EXPLOITATION	FREQUENCE DU PROCESSEUR, GHZ	VOLUME DE MEMOIRE VIVE, MO	VOLUME D'ESPACE LIBRE SUR LE DISQUE, GO
Microsoft Windows, 32-bits	1 ou plus	512	1
Microsoft Windows, 64-bits	1,4 ou plus	512	1

Lors de l'utilisation de la fonctionnalité de l'Administration système, le volume d'espace libre sur le disque doit être au moins Go.

Serveur des périphériques mobiles iOS Mobile Device Management

Tableau 6. Configurations logicielles au Serveur des périphériques mobiles iOS MDM

MODULE	EXIGENCES
Système d'exploitation	Microsoft Windows (la version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration).

Tableau 7. Configurations matérielles au Serveur des périphériques mobiles iOS MDM

SYSTEME D'EXPLOITATION	FREQUENCE DU PROCESSEUR, GHZ	VOLUME DE MEMOIRE VIVE, GO	VOLUME D'ESPACE LIBRE SUR LE DISQUE, GO
Microsoft Windows, 32-bits	1 ou plus	2	2
Microsoft Windows, 64-bits	1,4 ou plus	2	2

Le Serveur des périphériques mobiles Exchange ActiveSync

Les configurations logicielles et matérielles pour le Serveur des périphériques mobiles Exchange ActiveSync sont entièrement incluses dans les exigences pour le serveur Microsoft Exchange Server.

Agent d'administration et agent de mises à jour

Tableau 8. Configurations logicielles pour l'Agent d'administration et l'agent de mises à jour

MODULE	EXIGENCES
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.

Tableau 9. Configurations matérielles pour l'Agent d'administration et l'agent de mises à jour

SYSTEME D'EXPLOITATION	FREQUENCE DU PROCESSEUR, GHZ	VOLUME DE MEMOIRE VIVE, GO	VOLUME D'ESPACE LIBRE SUR LE DISQUE POUR L'AGENT D'ADMINISTRATION, GO	VOLUME D'ESPACE LIBRE SUR LE DISQUE POUR L'AGENT DE MISES A JOUR, GO
Microsoft Windows, 32-bits	1 ou plus	0,5	1	4
Microsoft Windows, 64-bits	1,4 ou plus	0,5	1	4
Linux, 32-bits	1 ou plus	1	1	4
Linux, 64-bits	1,4 ou plus	1	1	4
Mac OS	1	1	1	4

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 10. 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 11. 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.

SELECTION DU SYSTEME DE PROTECTION DE L'ENTREPRISE

La sélection de la structure du système de protection de l'entreprise est définie par les facteurs suivants :

- La topologie du réseau de l'entreprise.
- La structure d'organisation.
- Le nombre d'employés qui sont responsables de la protection du réseau et de la diffusion des obligations entre eux.
- Les ressources matérielles qui peuvent être indiquées pour installer les modules d'administration de la protection.
- La capacité de transmission des voies de communication qui peuvent être indiquées pour le fonctionnement des modules de la protection dans le réseau d'une entreprise.
- Le temps d'exécution disponible des opérations administratives importantes dans le réseau de l'entreprise. Les opérations administratives importantes sont des opérations telles que la diffusion des mises à jour des bases antivirus et la modification des stratégies pour les postes clients.

Lors de la sélection de la structure de la protection, il est recommandé de définir tout d'abord les ressources matérielles et réseau existantes qui peuvent être utilisées pour le fonctionnement du système centralisé de protection.

Afin d'analyser l'infrastructure de réseau et matérielle, la succession suivante d'actions est prévue :

1. Définir les paramètres suivants du réseau à déployer la protection :
   - nombre de segments du réseau ;
   - vitesse des liaisons entre les segments du réseau particuliers ;
   - nombre d'ordinateurs administrés dans chacun des segments du réseau ;
   - capacité de transmission de chaque liaison qui peut être indiquée pour le fonctionnement de la protection.
2. Définir une période d'exécution des opérations administratives clés pour tous les ordinateurs administrés.
3. Analyser les informations des points 1 et 2, ainsi que les données du test de charge du système d'administration (cf. section "Charge sur le réseau" à la page 78). Répondre aux questions sur la base de l'analyse réalisée :
   - Est-il possible de maintenir tous les clients par un seul Serveur d'administration ou faut-il avoir une hiérarchie des Serveurs d'administration ?
   - Quelle configuration matérielle des Serveurs d'administration est requise pour maintenir tous les clients pendant le temps défini dans le point 2 ?
   - Faut-il utiliser les agents de mises à jour pour diminuer la charge sur les canaux de liaison ?

Après avoir répondu aux questions citées, vous pouvez composer l'ensemble des structures accessibles de la protection de l'entreprise.

Le réseau de l'entreprise permet d'utiliser une des structures types de la protection :

- Un Serveur d'administration. Tous les postes clients sont connectés à un seul Serveur d'administration. Le Serveur d'administration joue rôle de l'agent de mises à jour.

- Un Serveur d'administration avec les agents de mise à jour. Tous les postes clients sont connectés à un seul Serveur d'administration. Les postes clients qui jouent le rôle des agents de mises à jour sont indiqués dans le réseau.

- Hiérarchie des Serveurs d'administration. Pour chaque segment du réseau, un Serveur d'administration séparé inclus dans la hiérarchie partagée des Serveurs d'administration est indiqué. Le Serveur d'administration principal joue rôle de l'agent de mises à jour.

- Une hiérarchie des Serveurs d'administration avec les agents de mise à jour. Pour chaque segment du réseau, un Serveur d'administration séparé inclus dans la hiérarchie partagée des Serveurs d'administration est indiqué. Les postes clients qui jouent le rôle des agents de mises à jour sont indiqués dans le réseau.

SCHEMAS TYPIQUES DE DEPLOIEMENT DU SYSTEME DE PROTECTION

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

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

- Le déploiement du système de protection via les outils de Kaspersky Security Center à l'aide d'un des moyens suivants :
  - à l'aide de la Console d'administration ;
  - à l'aide de 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 sont effectuées automatiquement à l'aide de Kaspersky Security Center.

  Le schéma principal de déploiement est le déploiement du système de protection 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 du système de protection 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 le système de protection à l'aide des stratégies de groupe Active Directory®. Pour plus d'informations, cf. l'aide de Kaspersky Security Center.

DEPLOIEMENT DU SYSTEME DE PROTECTION A L'INTERIEUR DE L'ENTREPRISE

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

DANS CETTE SECTION

DEPLOIEMENT DU SYSTEME DE PROTECTION 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 nécessaire. 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. 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 nécessaires 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 DU SYSTEME DE PROTECTION 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 nécessaire. 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. 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.

   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 crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications nécessaires de Kaspersky Lab.
5. 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 DU SYSTEME DE PROTECTION A L'INTERIEUR DE L'ENTREPRISE

L'administrateur de Kaspersky Security Center (ci-après, l'administrateur) effectue l'installation manuelle du logiciel nécessaire 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. 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 nécessaires 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 DU SYSTEME DE PROTECTION DANS LE RESEAU DE L'ENTREPRISE-CLIENTE

Cette section décrit les processus de déploiement du système de protection dans le réseau de l'entreprise-cliente, qui correspondent aux schémas typiques de déploiement.

DANS CETTE SECTION

DEPLOIEMENT DU SYSTEME DE PROTECTION VIA LA CONSOLE D'ADMINISTRATION DANS LE RESEAU DE L'ENTREPRISE-CLIENTE

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

1. L'administrateur de 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. 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-cliente.

3. L'administrateur de 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.

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

5. L'administrateur de 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 DU SYSTEME DE PROTECTION A L'AIDE DES OUTILS DE KASPERSKY SECURITY CENTER WEB-CONSOLE DANS LE RESEAU DE L'ENTREPRISE-CLIENTE

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

1. L'administrateur de 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. 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-cliente.

3. L'administrateur de l'entreprise-cliente 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 de Kaspersky Security Center crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications nécessaire de Kaspersky Lab.

5. L'administrateur de l'entreprise-cliente lance l'installation des applications sélectionnées sur les postes clients dans Kaspersky Security Center Web-Console.

6. En fonction des besoins, l'administrateur de 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 DU SYSTEME DE PROTECTION DANS LE RESEAU DE L'ENTREPRISE-CLIENTE

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

1. L'administrateur de 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. 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-cliente.

3. L'administrateur de l'entreprise-cliente 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 de Kaspersky Security Center crée et configure sur le Serveur d'administration virtuel les paquets d'installation de l'Agent d'administration et des applications nécessaire de Kaspersky Lab.

5. L'administrateur de 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 protéger le réseau 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 du système de protection pour les prestataires de services.

Kaspersky Security Center offre la possibilité d'intégration dans Microsoft Network Access Protection (NAP) qui permet de régler l'accès des postes clients au réseau. Pour assurer l'analyse de la puissance du système d'exploitation lors du fonctionnement en commun de l'application Kaspersky Security Center avec Microsoft NAP, il faut complémentairement installer le module System Health Validator (cf. section "Installation et configuration de Kaspersky Security Center SHV" à la page 40).

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

DANS CETTE SECTION

ETAPES 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. Configurez les paramètres du Serveur d'administration.

ETAPES DE DEPLOIEMENT DU SERVEUR D'ADMINISTRATION POUR LA PROTECTION DU RESEAU DE L'ENTREPRISE-CLIENTE

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

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

MISE A JOUR DE LA VERSION PRECEDENTE DE KASPERSKY SECURITY CENTER

Vous pouvez installer le Serveur d'administration de la version 10.0 sur l'ordinateur sur lequel la version précédente du Serveur d'administration est installée. Lors de la mise à jour jusqu'à la version 10.0, les données et les paramètres de la version précédente du Serveur d'administration sont enregistrés.

Pour actualiser le Serveur d'administration de version 9.0 jusqu'à la version 10.0, procédez comme suit :

1. Lancez le fichier exécutable setup.exe pour la version 10.0.

   Lancez l'Assistant d'installation qui vous proposera de créer une copie de sauvegarde des données du Serveur d'administration pour Kaspersky Security Center 9.0.

   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.

2. S'il faut créer une copie de sauvegarde, dans la fenêtre ouverte **Création de la copie de sauvegarde du Serveur d'administration**, cochez la case **Créer la copie de sauvegarde du Serveur d'administration**.

   La copie de sauvegarde des données du Serveur d'administration est créée à l'aide de l'utilitaire klbackup. Cet utilitaire fait partie du distributif de l'application et se trouve dans la racine du dossier d'installation Kaspersky Security Center.

   Les informations détaillées sur le fonctionnement de l'utilitaire de la copie de sauvegarde et de la restauration des données sont fournies dans l'Aide de Kaspersky Security Center dans la section "Applications".

3. Installez le Serveur d'administration de version 10.0, en suivant les consignes de l'Assistant d'installation.

   L'interruption du processus de mise à jour à l'étape d'installation du Serveur d'administration peut amener au dysfonctionnement de Kaspersky Security Center 9.0.

4. Pour les ordinateurs avec l'Agent d'administration de version précédente installé, créez et lancez la tâche d'installation à distance de la nouvelle version de l'Agent d'administration (cf. section "Installation des applications à l'aide de la tâche d'installation à distance" à la page 50).

   Après l'exécution de la tâche d'installation à distance, 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 ET SUPPRESSION DE KASPERSKY SECURITY CENTER

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

- **Standard**. Dans ce cas, l'ensemble minimal de modules 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 modules 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 est possible (cf. section "Installation des applications à l'aide de la tâche d'installation à distance" à la page 50). 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

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 et à la Console d'administration (cf. section "Configurations logicielles et matérielles" à la page 14).

Kaspersky Security Center garde l'information dans la base de données du serveur SQL. Dans ce cas, l'application Microsoft SQL Server 2008 R2 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 matérielles et logicielles" à la page 14). 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 modules de l'application fonctionnent correctement, tous les ports requis doivent être ouverts sur les ordinateurs (cf. tableau ci-après).

Tableau 12. Ports utilisés par Kaspersky Security Center

NUMERO DE PORT	PROTOCOLE	DESCRIPTION
Ordinateur avec le Serveur d'administration installé		
8060	HTTP	Utilisé pour la connexion au serveur Internet pour le fonctionnement de Kaspersky Security Center Web-Console et pour l'organisation du portail interne de l'entreprise.
8061	HTTPS	Utilisé pour la connexion au serveur Internet pour le fonctionnement de Kaspersky Security Center Web-Console et pour l'organisation du portail interne de l'entreprise. Le chiffrement est utilisé lors de la connexion.
13000	TCP	Utilisé pour les buts suivants : • l'obtention de données des postes clients ; • la connexion des agents de mises à jour ; • la connexion des Serveurs d'administration secondaires. Dans ce cas, la connexion SSL sécurisée est utilisée.
13000	UDP	Utilisé pour le transfert d'informations sur la désactivation des ordinateurs.
13111	TCP	Utilisé pour la connexion au serveur proxy KSN.
13291	TCP	Utilisé pour la connexion de la Console d'administration au Serveur d'administration. Dans ce cas, la connexion SSL sécurisée est utilisée.
13292	TCP	Est utilisé pour la connexion des périphériques mobiles.
14000	TCP	Utilisé pour les buts suivants : • l'obtention de données des postes clients ; • la connexion des agents de mises à jour ; • la connexion des Serveurs d'administration secondaires. Dans ce cas, la connexion SSL sécurisée n'est pas utilisée.
17000	TCP	Utilisé pour la connexion au serveur proxy d'activation. Dans ce cas, la connexion SSL sécurisée est utilisée.
17100	TCP	Utilisé pour la connexion au serveur proxy d'activation pour activer les clients mobiles.
18000	HTTP	Est utilisé pour l'obtention des données par le Serveur d'administration du serveur d'authentification Cisco® NAC.
Ordinateur nommé l'agent de mises à jour		
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.
Ordinateur avec l'Agent d'administration installé		
7	UDP	Est utilisé par Wake On Lan.

NUMERO DE PORT	PROTOCOLE	DESCRIPTION
67	UDP	Utilisés sur l'ordinateur qui est désigné en tant que serveur PXE lors du déploiement des images des systèmes d'exploitation.
69	UDP	
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.

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. Lancer 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 sur votre ordinateur se poursuivra.

3. Sélectionnez le type d'installation **Standard** et cliquez sur le bouton **Suivant**.

Finalement, l'Assistant d'installation dépaquètera 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 l'Assistant d'installation, les modules 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 2008 R2 Express Edition.

INSTALLATION PERSONNALISEE

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

  lancez le fichier exécutable setup.exe.

L'Assistant d'installation de l'application se lance. 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. CONSULTATION 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 sur votre ordinateur se poursuivra.

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

ETAPE 2. SELECTION DU TYPE D'INSTALLATION

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

ETAPE 3. SELECTION DES MODULES POUR L'INSTALLATION

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

- **Kaspersky Lab Cisco NAC Posture Validation Server**. Le module 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 périphériques mobiles**. Ce module assure la gestion de la protection des périphériques mobiles par Kaspersky Security Center.

- **Agent de SNMP**. Recueille les données statistiques pour le Serveur d'administration par le protocole SNMP. Le module 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 module sélectionné et sur le volume du disque nécessaire à son installation.

Les modules Agent d'administration et Console d'administration ne s'affichent pas dans la liste des modules. Ces modules 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 module 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 sut 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 modules du Serveur d'administration. Par défaut, les modules 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 13. 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 **Sécurité** 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*). Voir les informations détaillées dans le *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 sut 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 5000, il est possible d'utiliser Microsoft SQL Express 2005/2008. Si le nombre dépasse 5000, nous conseillons 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 2008 R2 Express Edition**.

    L'Assistant d'installation de l'application installera Microsoft SQL Server 2008 R2 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 matérielles et logicielles" à la page 14).

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 si ce mode est sélectionné. 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 lorsqu'un ordinateur avec la base de données ne se trouve 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 PARTAGE

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 module 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 lorsque 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 si vous avez sélectionné le module **Prise en charge des périphériques mobiles** 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 modules 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 modules 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. Le tableau indique aussi les attributs d'autres services exécutés sur l'ordinateur après l'installation du Serveur d'administration.

Le service du serveur des stratégies (Posture Validation Server) de Kaspersky Lab pour Cisco NAC 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 14. Attributs des services

MODULE	NOM DE SERVICE	NOM DE SERVICE AFFICHE	TYPE DE LANCEMENT	COMPTE
Serveur d'administration	kladminserver	Serveur d'administration Kaspersky Security Center	Automatique au démarrage du système d'exploitation.	Compte de type KL-AK-* indiqué par l'utilisateur ou compte spéciale créée lors de l'installation
Kaspersky Lab Cisco NAC Posture Validation Server	klnacserver	Kaspersky Lab Cisco NAC Posture Validation Server	Automatique au démarrage du système d'exploitation.	Système local
Agent d'administration	klnagent	Agent d'administration Kaspersky Security Center	Automatique au démarrage du système d'exploitation.	Système local
Serveur Internet pour le fonctionnement de la console Internet et pour l'organisation du portail interne de l'entreprise	klwebsrv	Serveur Internet de Kaspersky Lab	Automatique au démarrage du système d'exploitation.	Compte spécial non privilégié de type KlScSvc-*
Serveur proxy d'activation	klactprx	Serveur proxy d'activation de Kaspersky Lab	Automatique au démarrage du système d'exploitation.	Compte spécial non privilégié de type KlScSvc-*
Portail Internet d'autorisation d'accès	klnsacwsrv	Portail d'autorisation de Kaspersky Lab	Mode manuel	Système local
Serveur proxy KSN	ksnproxy	Serveur proxy Kaspersky Security Network	Mode manuel	Compte spécial non privilégié de type KlScSvc-*
Serveur iOS MDM	KLIOSMdmServiceSrv2	iOS MDM Mobile devices server	Automatique au démarrage du système d'exploitation.	Network Service
Objet COM+ pour l'interaction avec le serveur Exchange	KasperskyMdmService	Kaspersky MDM for Exchange	Automatique lors de l'appel à l'objet	Compte utilisateur faisant partie des groupes Domain User et KLMDM Role Group (KLMDM Secure Group)

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 modules 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 éventuels conflits survenus pendant le fonctionnement des modules 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 se lance 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.

Pour configurer les notifications par courrier, l'administrateur peut avoir besoin d'un compte sur le serveur de courrier pour l'authentification ESMTP.

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 modules 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.

   L'Assistant d'installation se lance. 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. Par défaut c'est <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. 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 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.

Pour installer Kaspersky Security Center SHV sur un ordinateur d'une manière locale, procédez comme suit :

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

   L'Assistant d'installation se lance. 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 l'application à partir du CD de distribution.

2. Définissez le dossier de destination. Par défaut c'est <Disque>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV. 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 de l'Assistant, Kaspersky Security Center SHV s'installera 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. Dans ce cas, l'Assistant se lance. Comme résultat de son fonctionnement, tous les modules 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 l'application à partir du CD de distribution.

ETAPES DE L'ASSISTANT

ETAPE 1. CONSULTATION 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.

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

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 sur votre ordinateur se poursuivra.

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

L'installation à distance de Kaspersky Security Center Web-Console à l'aide du paquet d'installation ou l'installation locale en mode non interactif signifie l'acceptation automatique des conditions du Contrat de licence sur l'application installée. Il est possible de consulter le Contrat de licence de l'application concrète dans la distribution de cette application ou sur le site de l'assistance technique de Kaspersky Lab.

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 A 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 43).

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 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 de Apache HTTP Server 2.2 sont exécutées sur cette étape de l'Assistant.

Avant l'installation, indiquez le certificat que Kaspersky Security Center Web-Console utilisera pour la connexion avec le serveur Apache. 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 un 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 lance. 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, cette 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 dans le dossier **Stockages** dans le dossier joint **Clés** du Serveur d'administration principal, une clé Kaspersky Security Center ou Kaspersky Security Center SPE à l'aide d'un des moyens suivants :
   - 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-cliente sous l'administration du Serveur virtuel sélectionné va lancer Kaspersky Security Center Web-Console SPE 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-cliente 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-cliente 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 de Kaspersky Security Center*.

CONFIGURATION DU SYSTEME DE PROTECTION DU RESEAU DE L'ENTREPRISE-CLIENTE

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

La configuration du système de protection est une partie du processus de déploiement de la protection dans le réseau de l'entreprise-cliente. La procédure de configuration du système de protection 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-cliente.
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 nécessaires de Kaspersky Lab sur les ordinateurs de l'entreprise-cliente.

   Cette section analyse les conditions nécessaires pour installer à distance des applications sur les ordinateurs de l'entreprise-cliente. 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 49).

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

DANS CETTE SECTION

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

Si les ordinateurs de l'entreprise-cliente 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 sélectionnez 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. Pour l'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 65

Installation à distance des applications 49

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

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 49).

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

- Avant la première installation des applications sur les ordinateurs de l'entreprise-cliente, 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. Pour l'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 de 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 émises (cf. section "Configurations matérielles et logicielles" à la page 14).

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 60).

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 10 for Windows ;
- Kaspersky Endpoint Security 8 for Smartphone ;
- Kaspersky Endpoint Security 8 for Mac ;
- Kaspersky Endpoint Security 8 for Linux.
- Kaspersky Endpoint Security 10 pour les périphériques mobiles ;
- Kaspersky Security for Virtualization 1.1 ;
- Kaspersky Security pour les environnements protégés 2.0.

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 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 ensembles 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 60).

DANS CETTE SECTION

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 ensembles 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**.

   Une fois l'Assistant de création de la tâche terminé, 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 ensembles 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**.

   Une fois l'Assistant de création de la tâche terminé, 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 DE L'APPLICATION A L'AIDE DES STRATEGIES DE GROUPE ACTIVE DIRECTORY

Kaspersky Security Center permet d'installer les applications de Kaspersky Lab à l'aide des stratégies de groupe Active Directory.

L'installation des applications à l'aide des stratégies de groupe Active Directory est possibles uniquement lors de l'utilisation des paquets d'installation incluant l'Agent d'administration.

Pour installer l'application à l'aide des stratégies de groupe Active Directory, procédez comme suit :

1. Lancez le processus de création de la tâche de groupe d'installation à distance ou de la tâche d'installation à distance pour l'ensemble d'ordinateurs.

2. Dans la fenêtre de l'Assistant de création de la tâche **Paramètres**, cochez la case **Fixer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**.

3. Lancez la tâche créée d'installation à distance ou attendez son lancement programmé.

Finalement, le mécanisme suivant de l'installation à distance sera lancé :

1. Après le lancement de la tâche dans chaque domaine, qui comprend les postes clients de l'ensemble, les objets suivants seront créés :

   - la stratégie de groupe avec le nom **Kaspersky_AK{GUID}** ;

   - le groupe de sécurité **Kaspersky_AK{GUID}** lié avec la stratégie de groupe. Ce groupe de sécurité contient les postes clients sur lesquels la tâche se diffuse. La composition du groupe de sécurité détermine la zone d'action de la stratégie de groupe.

2. L'installation des applications sur les postes clients s'opère directement depuis le dossier partagé Kaspersky Security Center KLSHARE. Dans ce cas, dans le dossier d'installation Kaspersky Security Center un dossier secondaire joint sera créé. Ce dossier contient le fichier avec extension mst pour l'application à installer.

3. Lors de l'ajout de nouveaux ordinateurs dans la zone d'action d'une tâche, ils seront ajoutés au groupe de protection après le lancement suivant d'une tâche. Si dans la programmation d'une tâche, la case **Lancer les tâches non exécutées** est cochée, les ordinateurs seront immédiatement ajoutés au groupe de protection.

4. Lors de la suppression des ordinateurs depuis la zone d'action d'une tâche, leur suppression depuis le groupe de sécurité se déroulera lors du prochain lancement d'une tâche.

5. Lors de la suppression d'une tâche depuis Active Directory, la stratégie sera supprimée, ainsi que le lien vers cette stratégie et le groupe de protection lié avec une tâche.

Si vous voulez utiliser un autre schéma d'installation via Active Directory, vous pouvez manuellement configurer les paramètres d'installation. Cela peut être utile, par exemple, dans les cas suivants :

- quand l'administrateur de protection antivirus ne possède pas les privilèges d'apporter les modifications de certains domaines dans Active Directory ;
- s'il est nécessaire de placer le distributif d'origine sur une ressource de réseau à part ;
- pour raccorder une stratégie de groupe à des sous-divisions concrètes Active Directory.

Les options suivantes d'utilisation d'un autre schéma d'installation via Active Directory sont disponibles :

- Si l'installation doit se dérouler directement depuis le dossier partagé de Kaspersky Security Center, dans les propriétés d'une stratégie de groupe d'Active Directory il est nécessaire d'indiquer le fichier avec extension msi, situé dans le dossier joint exec dans le dossier du paquet d'installation de l'application requise.
- Si le paquet d'installation doit être placé dans une autre ressource de réseau, il faut y copier tout le contenu du dossier exec, puisque, excepté le fichier avec extension msi, ce dossier contient les fichiers de configuration formés au moment de création du paquet d'installation. Pour que la clé soit installée avec l'application, il faut aussi copier le fichier de licence dans ce dossier.

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 diffusion du paquet d'installation (cf. section "Diffusion des paquets d'installation sur les Serveurs d'administration secondaires" à la page 57).
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 51).
   - Si vous voulez créer la tâche pour l'ensemble des 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 51).

   Finalement, l'Assistant de création de la tâche d'installation à distance se lance. 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**.

   Une fois l'Assistant de création de la tâche terminé, 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 60).

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 à distance**.

   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 **Installation à distance** 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 ensembles 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 une 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 quand l'application antivirus est installée sur cet ordinateur et la protection permanente fonctionne.

DESINSTALLATION A DISTANCE DES APPLICATIONS

Kaspersky Security Center permet de supprimer les applications incompatibles qui peuvent provoquer les conflits survenus pendant 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 ensembles d'ordinateurs*. Tâches créées pour les postes clients sélectionnés peu importe l'appartenance des ordinateurs à un groupe d'administration quelconque.

DANS CETTE SECTION

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**.

   Une fois l'Assistant de création de la tâche terminé, 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 ensembles 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**.

   Une fois l'Assistant de création de la tâche terminé, la tâche de désinstallation à distance de l'application pour l'ensemble d'ordinateurs sélectionné sera créée. La tâche créée s'affiche dans la zone de travail du dossier **Tâches pour les ensembles 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.

UTILISATION DES 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 **Installation à distance** 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

GENERATION DU PAQUET D'INSTALLATION

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

1. Connectez-vous au Serveur d'administration nécessaire.
2. Dans l'arborescence de la console **Installation à distance**, sélectionnez le dossier joint **Paquets d'installation**.
3. Lancez le processus de création d'un paquet d'installation via l'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.

   L'Assistant de création d'un paquet d'installation se lance. 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.

DIFFUSION 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 diffusion 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**.

Une fois l'Assistant de création de la tâche terminé, la tâche de diffusion 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.

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

Vous pouvez utiliser les agents de mises à jour pour la diffusion 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 DE L'INSTALLATION DE L'APPLICATION

Après la création du paquet d'installation de l'application, vous pouvez configurer le paquet d'installation de telle manière pour que les informations diagnostiques sur les résultats d'installation de l'application soient transmises dans Kaspersky Security Center. Pour les paquets d'installation des applications de Kaspersky Lab, le transfert des informations diagnostiques sur les résultat d'installation de l'application est configuré par défaut et la configuration complémentaire n'est pas requise.

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.

2. 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.

3. 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 de l'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.

4. 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.

5. 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.

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

Les informations sur les résultats de l'installation de l'application, indiquées par l'utilisateur, seront enregistrées dans les journaux de Kaspersky Security Center et affichées dans la liste des événements, dans les rapports et dans les résultats de l'exécution des tâches.

RECUPERATION DES VERSIONS 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 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 détecte 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 **Installation à distance** 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** disparait 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 **Installation à distance** 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

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 problèmes, 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

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**.

   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 de du mot de passe sera affichée lors de la création du compte. 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 su 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 10 for Windows ;
- Kaspersky Security for Virtualization 1.1

DANS CETTE SECTION

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. L'Assistant d'installation de l'Agent d'administration se lance. 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.

A la fin 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 lorsque 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 45).

L'installation à distance de l'Agent d'administration à l'aide du paquet d'installation ou l'installation locale en mode non interactif signifie l'acceptation automatique des conditions du Contrat de licence sur l'application installée. Il est possible de consulter le Contrat de licence de l'application concrète dans la distribution de cette application ou sur le site de l'assistance technique de Kaspersky Lab.

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 Kaspersky Security Center
  2. Dans l'arborescence de la console **Installation à distance** 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. Dans ce cas, 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.

   Le lancement du fichier exécutable avec la clé EULA=1 signifie que vous acceptez les conditions du Contrat de licence. Le texte du Contrat de licence est inclut dans la distribution de Kaspersky Security Center. L'acceptation des dispositions du Contrat de licence est une condition indispensable pour installer l'application ou pour actualiser la version précédente de l'application.

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. La 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 **Installation à distance**, 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 via l'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.

   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.

CONNEXION DES APPAREILS NOMADES AU SERVEUR D'ADMINISTRATION

Cette section décrit la connexion au Serveur d'administration des périphériques mobiles qui prennent en charge les protocoles Exchange ActiveSync et iOS Mobile Device Management (iOS MDM) et qui fonctionnent sous les systèmes d'exploitation suivants :

- Windows Mobile ;
- Windows CE ;
- Windows Phone 7 ;
- Android™ ;
- Symbian ;
- Bada ;
- Apple iOS.

DANS CETTE SECTION

SERVEURS DES PERIPHERIQUES MOBILES

La collecte d'informations sur les périphériques mobiles et la conservation de leurs profils est exécutée par Serveurs des périphériques mobiles. Le *Serveur des périphériques mobiles* est un module de Kaspersky Security Center qui offre à l'administrateur l'accès aux périphériques mobiles et qui permet de les administrer via Console d'administration.

Il existe deux types des Serveurs des périphériques mobiles :

- Le Serveur des périphériques mobiles Exchange ActiveSync. Il est installer sur le poste client avec le serveur déjà installé Microsoft Exchange et permet de recevoir les données depuis le serveur Microsoft Exchange et de les transmettre sur le Serveur d'administration. Ce Serveur des périphériques mobiles est utilisé pour administrer les périphériques mobiles qui prennent en charge le protocole Exchange ActiveSync.

- Le Serveur des périphériques mobiles iOS MDM. S'installe sur le poste client et permet de connecter les périphériques mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

Après l'installation sur les postes clients, les Serveurs des périphériques mobiles s'affichent dans la Console d'administration dans le dossier **Serveurs des périphériques mobiles** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.

Les Serveurs des périphériques mobiles de Kaspersky Security Center permettent d'administrer les objets suivants :

- périphérique mobile séparé ;
- quelques périphériques mobiles ;
- plusieurs périphériques mobiles connectés au cluster des serveurs simultanément. Lors de la connexion au cluster des serveurs, le Serveur des périphériques mobiles installé sur ce cluster s'affiche dans la Console d'administration comme un serveur.

CONNEXION DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Kaspersky Security Center permet d'administrer les périphériques mobiles Exchange ActiveSync. Les *périphériques mobiles Exchange ActiveSync* sont des périphériques mobiles qui se connectent aux boîtes aux lettres du serveur Microsoft Exchange et sont administrés par le protocole ActiveSync.

Le protocole ActiveSync prend en charge les systèmes d'exploitation suivants :

- Windows Mobile ;
- Windows CE ;
- Windows Phone 7 ;
- Android ;
- Symbian ;
- Bada.

La connexion des périphériques mobiles Exchange ActiveSync au Serveur d'administration est exécutée dans la suite suivante :

1. L'administrateur installe le Serveur des périphériques mobiles Exchange ActiveSync sur le poste client avec le serveur installé Microsoft Exchange. L'installation du Serveur des périphériques mobiles Exchange ActiveSync est exécutée par les moyens titulaires du système d'exploitation.
2. Le Serveur connecté des périphériques mobiles Exchange ActiveSync s'affiche dans la Console d'administration dans le dossier **Serveurs des périphériques mobiles** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.
3. L'utilisateur se connecte à la boîte aux lettres Microsoft Exchange et il est notifié que la boîte aux lettres sélectionnée se trouve sous l'administration d'un profil qui impose les restrictions sur le périphérique mobile connecté.
4. Le périphérique mobile de l'utilisateur connecté au serveur Microsoft Exchange s'affiche dans le dossier **Périphériques mobiles Exchange ActiveSync** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.

Après la connexion du périphérique mobile Exchange ActiveSync au Serveur des périphériques mobiles Exchange ActiveSync, l'administrateur peut administrer les périphériques mobiles connectés Exchange ActiveSync. Les informations sur l'administration des périphériques mobiles Exchange ActiveSync sont présentées dans le Manuel de l'administrateur de Kaspersky Security Center.

DANS CETTE SECTION

INSTALLATION DU SERVEUR DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Pour installer le Serveur des périphériques mobiles Exchange ActiveSync, procédez comme suit :

1. Dans le paquet d'installation Kaspersky Security Center dans le dossier MDM4Exchange, lancez le fichier d'installation setup.

2. Suivez les étapes de l'Assistant d'installation.

CREATION DU PROFIL D'ADMINISTRATION DES PERIPHERIQUES EXCHANGE ACTIVESYNC

Pour créer un profil d'administration des périphériques mobiles Exchange ActiveSync, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Périphériques mobiles**, sélectionnez le dossier joint **Serveurs des périphériques mobiles**.

2. Dans la zone de travail du dossier **Serveurs des périphériques mobiles**, sélectionnez le Serveur des périphériques mobiles Exchange ActiveSync.

3. Dans le menu contextuel du Serveur des périphériques mobiles Exchange ActiveSync, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du serveur des périphériques mobiles Exchange ActiveSync s'ouvre.

4. Dans la fenêtre des propriétés du serveur des périphériques mobiles Exchange ActiveSync, sélectionnez la section **Boîtes aux lettres**.

5. Sélectionnez une boîte aux lettres et cliquez sur le bouton **Modifier les profils**.

   Le fenêtre **Profils des paramètres** s'ouvre.

6. Dans la fenêtre **Profils des paramètres**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouveau profil** s'ouvre.

7. Exécutez la configuration des paramètres du profil dans les sections de la fenêtre **Nouveau profil**.

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

   Le profil s'affichera dans la liste des profils dans la fenêtre **Profils**.

9. Si vous voulez que le profil créé soit un profil par défaut, sélectionnez-le dans la liste dans la fenêtre **Profils** et cliquez sur le bouton **Faire comme le profil par défaut**.

CONNEXION DES PERIPHERIQUES MOBILES IOS MDM

Kaspersky Security Center permet d'administrer les périphériques mobiles sous iOS. Les périphériques mobiles iOS connectés au Serveur des périphériques mobiles iOS MDM et se trouvant sous l'administration du Serveur d'administration sont appelés *Périphériques mobiles iOS MDM.* La connexion des périphériques mobiles iOS MDM est exécutée dans la suite suivante :

1. L'administrateur installe le Serveur des périphériques mobiles iOS MDM sur le poste client sélectionné. L'installation du Serveur des périphériques mobiles iOS MDM est exécutée par les moyens titulaires du système d'exploitation.

2. L'administrateur installe le certificat Apple Push Notification Service (APNs) sur le Serveur d'administration.

3. L'administrateur envoie à l'utilisateur du périphérique mobile iOS le lien pour télécharger le profil iOS MDM (cf. section "Installation du profil iOS MDM sur le périphérique mobile iOS" à la page 72). *Le profil iOS MDM* est utilisé pour connecter les périphériques mobiles iOS MDM au Serveur des périphériques mobiles iOS MDM.

4. L'utilisateur installe le profil iOS MDM sur le périphérique mobile iOS.

5. Le périphérique mobile se connecte au Serveur des périphériques mobiles iOS MDM. Les périphériques mobiles connectés iOS MDM s'affichent dans le dossier **Périphériques mobiles iOS MDM** joint dans le dossier **Périphériques mobiles** de l'arborescence de la console.

Les informations sur l'administration des périphériques mobiles iOS MDM sont présentées dans le Manuel de l'administrateur de Kaspersky Security Center.

INSTALLATION DU SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour installer le Serveur des périphériques mobiles iOS MDM, procédez comme suit :

1. Dans le paquet d'installation Kaspersky Security Center dans le dossier MDM4iOS, lancez le fichier d'installation setup.

   L'Assistant d'installation du Serveur d'administration iOS MDM sera lancé.

2. La fenêtre de l'Assistant **Paramètres de connexion au Serveur des périphériques mobiles iOS MDM** permet de connecter les paramètres suivants :

   - **Port de connexion à l'Agent d'administration**. Indiquez dans le champ le port de connexion du service iOS MDM à l'Agent d'administration. Le numéro de port par défaut est 9799.

   - **Port de connexion local au service iOS MDM**. Indiquez dans le champ le port de connexion local de l'Agent d'administration au service iOS MDM. Le numéro de port par défaut est 9899.

   - **Port de connexion externe au service iOS MDM**. Indiquez dans le champ le port de connexion externe des périphériques mobiles au service iOS MDM. Le numéro de port par défaut est 443.

   Il est conseillé d'utiliser les valeurs par défaut.

3. Dans la fenêtre de l'Assistant **Sélection du certificat**, sélectionnez le certificat qui sera utilisé lors de la connexion du Serveur des périphériques mobiles iOS MDM au Serveur d'administration :

   - **Nouveau**. Sélectionnez cette option si vous voulez créer un nouveau certificat. Dans le champ **Adresse URL de la connexion à distance avec le Serveur des périphériques mobiles**, saisissez l'adresse du poste client avec le Serveur installé des périphériques mobiles. Ce poste client doit être accessible pour connecter les périphériques mobiles iOS MDM à celui-ci.

   - **Sélectionnez un fichier de certification**. Sélectionnez cette option si vous voulez utiliser le certificat existant. Dans le champ **Chemin au fichier**, indiquez le chemin d'accès au fichier du certificat.

Une fois l'Assistant terminé, l'installation du Serveur des périphériques mobiles iOS MDM sur le poste client local sera exécutée.

OBTENTION DU CERTIFICAT APNS

Pour obtenir le certificat APNs, procédez comme suit :

1. Créez une demande sur l'obtention du certificat APNs dans l'application Internet Information Services (IIS).
2. Enregistrez la clé pour le Serveur des périphériques mobiles iOS MDM dans l'espace personnel de l'utilisateur sur le portail de Kaspersky Lab.

   Après l'enregistrement, le lien **Signer la demande sur le certificat** devient disponible.
3. Demandez la signature du certificat dans l'espace personnel de l'utilisateur sur le site de Kaspersky Lab à l'aide du lien **Signer la demande sur le certificat**.

   Quand la demande signée sera prête, vous recevrez une notification sur la disponibilité de la demande signée.
4. Téléchargez la demande signée sur le certificat depuis le site de Kaspersky Lab.
5. Téléchargez la demande signée sur le certificat sur le site Apple Inc., en utilisant Apple ID aléatoire.

   Il n'est pas recommandé d'utiliser l'Apple ID personnalisé. Créez un Apple ID séparé pour l'utiliser en tant que corporatif. Attachez l'Apple ID créé à la boîte aux lettres de la société et non pas à un employé séparé.
6. Téléchargez le certificat APNs depuis le site Apple Inc.

INSTALLATION DU CERTIFICAT APN SUR LE SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour installer le certificat APN sur le Serveur des périphériques mobiles iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Périphériques mobiles**, sélectionnez le dossier joint **Serveurs des périphériques mobiles**.
2. Dans la zone de travail du dossier **Serveurs des périphériques mobiles**, sélectionnez le Serveur des périphériques mobiles iOS MDM.
3. Dans le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur des périphériques mobiles iOS MDM s'ouvre.
4. Dans la fenêtre des propriétés du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Certificats**.
5. Dans la section **Certificats** dans le groupe des paramètres **Certificat Apple Push Notification**, cliquez sur le bouton **Installer**.

L'installation du certificat APNs sera exécutée.

INSTALLATION DU PROFIL IOS MDM SUR LE PERIPHERIQUE MOBILE IOS

Pour installer le profil iOS MDM sur le périphérique mobile, procédez comme suit :

1. Sélectionnez le dossier **Comptes utilisateurs** dans l'arborescence de la console.
2. Sélectionnez le compte utilisateur sur le périphérique duquel vous voulez installer le profil iOS MDM.
3. Dans le menu contextuel du compte utilisateur du périphérique mobile, sélectionnez l'option **Installer le profil iOS MDM sur l'appareil mobile de l'utilisateur**.

   La fenêtre **Installation du profil iOS MDM** s'ouvre.
4. Dans la fenêtre **Installation du profil iOS MDM** dans le champ **Liste des Serveurs disponibles des périphériques mobiles iOS MDM**, sélectionnez le Serveur des périphériques mobiles iOS MDM pour lequel il faut créer un profil iOS MDM.
5. Dans la fenêtre **Installation du profil iOS MDM**, indiquez le mode d'envoi de la notification sur l'installation du profil iOS MDM sur le périphérique mobile :

   - **A l'aide de SMS**. Cochez la case pour envoyer à l'utilisateur un SMS avec le lien vers le téléchargement du profil MDM. Dans le champ **Texte SMS**, saisissez le message pour l'utilisateur ou utilisez le message par défaut. Dans la liste déroulante à côté du champ de saisie **Texte SMS**, saisissez l'option **Mot de passe à usage unique** et indiquez le mot de passe de l'utilisateur.

   - **Par courrier électronique**. Cochez la case pour envoyer à l'utilisateur par courrier électronique une notification qui contient le lien vers le téléchargement du profil MDM et du code QR créé spécialement pour ce message. Dans le champ **Objet**, indiquez l'objet du message. Dans le champ **Texte du message**, saisissez le message pour l'utilisateur. Dans la liste déroulante à côté du champ **Texte du message**, sélectionnez l'option **Mot de passe à usage unique** et saisissez le mot de passe de l'utilisateur.
6. Cliquez sur le bouton **OK**.

Suite à ces actions, l'utilisateur du périphérique mobile reçoit une notification avec le lien vers le téléchargement du profil iOS MDM du portail Internet. L'utilisateur indépendamment l'installation du profil iOS MDM sur le périphérique iOS.

AJOUT DU PROFIL DE CONFIGURATION SUR LE SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour ajouter le profil de configuration sur le Serveur des périphériques mobiles iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Périphériques mobiles**, sélectionnez le dossier joint **Serveurs des périphériques mobiles**.
2. Dans la zone de travail du dossier **Serveurs des périphériques mobiles**, sélectionnez le Serveur des périphériques mobiles iOS MDM.
3. Dans le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur des périphériques mobiles s'ouvre.
4. Dans la fenêtre des propriétés du **Serveur des périphériques mobiles**, sélectionnez la section **Profils**.
5. Dans la section **Profils**, cliquez sur le bouton **Créer**.

   La fenêtre **Ajout du nouveau profil de configuration** s'ouvre.

6. Dans la fenêtre **Ajout du nouveau profil de configuration**, indiquez le nom du profil dans le champ **Nom du profil de configuration**.

7. Dans la fenêtre **Ajout du profil de configuration** dans le champ **Identificateur du profil de configuration**, indiquez l'identificateur du profil de configuration créé.

Pour créer un profil de configuration, l'application iPhone Configuration Utility doit être installée sur l'ordinateur. L'application s'installe par les outils titulaires Windows.

Le profil de configuration ajouté s'affiche dans la section **Profils** dans la fenêtre des propriétés du Serveur des périphériques mobiles iOS MDM.

INSTALLATION DU PROFIL DE CONFIGURATION SUR LE PERIPHERIQUE MOBILE IOS MDM

Pour installer le profil de configuration sur le périphérique mobile iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le dossier joint **Périphériques mobiles iOS MDM**.

2. Dans le dossier **Périphériques mobiles iOS MDM**, sélectionnez le périphérique mobile sur lequel vous voulez installer le profil de configuration.

3. Dans le menu contextuel du périphérique mobile, sélectionnez l'option **Installer le profil sur le périphérique** ou utilisez l'option analogue dans le menu **Actions**.

   La fenêtre **Sélection du profil pour l'installation** s'ouvre.

4. Dans la fenêtre **Sélection du profil pour l'installation**, sélectionnez le profil de configuration.

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

Le profil de configuration sera installé sur le périphérique mobile iOS MDM.

AJOUT DU PROFIL PROVISIONING SUR LE SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour ajouter le profil provisioning sur le Serveur des périphériques mobiles iOS MDM, procédez comme suit :

1. Créez le profil provisioning sur le portail Internet Apple Inc. dans le Centre d'élaboration des applications iOS.

2. Dans l'arborescence de la console dans le dossier **Gestion des périphériques mobiles**, sélectionnez le dossier joint **Serveurs des périphériques mobiles**.

3. Dans la zone de travail du dossier **Serveurs des périphériques mobiles**, sélectionnez le Serveur des périphériques mobiles iOS MDM.

4. Dans le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur des périphériques mobiles s'ouvre.

5. Dans la fenêtre des propriétés du **Serveur des périphériques mobiles**, cliquez sur le bouton **Importer** et indiquez le chemin d'accès au fichier du profil provisioning.

Le profil sera ajouté dans les paramètres du Serveur des périphériques mobiles iOS MDM.

INSTALLATION DU PROFIL PROVISIONING SUR LE PERIPHERIQUE MOBILE IOS MDM

Pour installer le profil provisioning sur le périphérique iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le dossier joint **Périphériques mobiles iOS MDM**.

2. Dans la zone de travail du dossier **Périphériques mobiles iOS MDM**, sélectionnez le périphérique mobile sur lequel vous voulez installer le profil provisioning.

3. Dans le menu contextuel du périphérique, sélectionnez l'option **Installer le profil provisioning sur le périphérique** ou utilisez l'option analogue dans le menu **Actions**.

   La fenêtre **Sélection du profil provisioning pour l'installation** s'ouvre.

4. Dans la fenêtre **Sélection du profil provisioning pour l'installation**, indiquez le profil provisioning que vous voulez installer sur le périphérique mobile.

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

Le profil provisioning sera installé sur le périphérique mobile.

CONFIGURATION DE L'ENVOI SMS DANS KASPERSKY SECURITY CENTER

Kaspersky Security Center peut être utilisé pour envoyer des notifications SMS aux utilisateurs des périphériques mobiles.

L'envoi SMS peut être utilisé dans les cas suivants :

- Pour recevoir par l'administrateur des notifications SMS sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications installées sur les postes clients.
- Pour installer les application sur les périphériques mobiles des utilisateurs. L'utilisateur du périphérique mobile reçoit un SMS qui contient le lien pour télécharger l'application à installer.
- Pour notifier les employés de l'entreprise.

Le déploiement de l'envoi SMS est exécuté dans la séquence suivante :

1. L'administrateur installe l'utilitaire Kaspersky SMS Broadcasting sur le périphérique mobile Android.

   L'utilitaire Kaspersky SMS Broadcasting s'installe uniquement sur les périphériques mobiles sous Android.

2. Après l'installation de l'utilitaire Kaspersky SMS Broadcasting sur le périphérique mobile, l'administrateur synchronise le périphérique mobile avec le Serveur d'administration.
3. L'administrateur désigne le périphérique mobile avec l'utilitaire Kaspersky SMS Broadcasting installé comme l'expéditeur des SMS dans la Console d'administration.

DANS CETTE SECTION

RECEPTION ET INSTALLATION DE L'UTILITAIRE KASPERSKY SMS BROADCASTING

L'utilitaire SMS Broadcasting est inclus dans le paquet d'installation Kaspersky Endpoint Security 10 pour les périphériques mobiles. Vous pouvez télécharger le paquet d'installation Kaspersky Endpoint Security 10 pour les périphériques mobiles depuis le site de Kaspersky Lab.

Pour Installer l'utilitaire Kaspersky SMS Broadcasting, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le dossier joint **Paquets d'installation**.
2. Dans la zone de travail du dossier **Paquets d'installation** à l'aide du lien **Administrer les paquets d'applications mobiles**, ouvrez la fenêtre **Administration des paquets des applications mobiles**.

3. Dans la fenêtre **Administration des paquets des applications mobiles**, vous pouvez sélectionnez le paquet de l'application mobile qui contient l'utilitaire Kaspersky SMS Broadcasting.

   Si le paquet n'a pas été créé, cliquez sur le bouton **Nouveau** et créez le paquet de l'application mobile pour l'utilitaire Kaspersky SMS Broadcasting.

4. Dans la fenêtre **Administration des paquets des applications mobiles**, cliquez sur le bouton **Publier sur le serveur Internet**.

   Le lien pour télécharger le paquet de l'application mobile avec l'utilitaire Kaspersky SMS Broadcasting sera publié sur le serveur Internet.

5. Dans la fenêtre **Administration des paquets des applications mobiles**, cliquez sur le bouton **Envoyer par courrier** pour envoyer à l'utilisateur du périphérique mobile le lien pour télécharger le paquet des applications mobiles qui contient l'utilitaire Kaspersky SMS Broadcasting.

6. Téléchargez sur le périphérique mobile depuis le serveur Internet le paquet des applications mobiles qui contient l'utilitaire Kaspersky SMS Broadcasting.

7. Exécutez l'installation de l'utilitaire Kaspersky SMS Broadcasting par les outils titulaires du périphérique mobile.

Vous pouvez également télécharger l'utilitaire Kaspersky SMS Broadcasting sur le périphérique mobile depuis le site de Kaspersky Lab ou connecter le périphérique mobile à l'ordinateur et copier sur le périphérique mobile l'utilitaire Kaspersky SMS Broadcasting déjà téléchargé.

SYNCHRONISATION DU PERIPHERIQUE MOBILE AVEC LE SERVEUR D'ADMINISTRATION

Pour synchroniser le périphérique mobile avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center dans le menu contextuel du dossier **Serveur d'administration**, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Dans la fenêtre des propriétés du Serveur d'administration dans la section **Paramètres**, cochez la case **Ouvrir le port pour les périphériques mobiles**.

3. Dans la section **Paramètres** dans le champ **Port pour les périphériques mobiles**, indiquez le port de synchronisation du périphérique mobile avec le Serveur d'administration. Le numéro de port par défaut est 13292.

4. Lancez l'utilitaire Kaspersky SMS Broadcasting sur le périphérique mobile.

5. Dans la fenêtre principale de l'utilitaire Kaspersky SMS Broadcasting, cliquez sur le bouton **Paramètres de synchronisation**.

6. Dans la fenêtre **Paramètres de synchronisation**, indiquez l'adresse IP du Serveur dans le champ **Adresse du serveur**.

7. Dans le champ **Port**, indiquez le port de connexion au Serveur d'administration. Le numéro de port par défaut est 13292.

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

Quand le périphérique mobile est synchronisé avec le Serveur d'administration, vous pouvez désigner ce périphérique mobile comme l'expéditeur des messages SMS.

DESIGNATION DU PERIPHERIQUE MOBILE COMME EXPEDITEUR DES MESSAGES SMS

Pour désigner le périphérique mobile comme expéditeur des messages SMS, procédez comme suit :

1. Dans l'arborescence de la console dans le menu contextuel du dossier **Rapports et notifications**, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : Rapports et notifications** s'ouvre.

2. Dans la fenêtre **Propriétés : Rapports et notifications**, sélectionnez la section **Expéditeurs des SMS**.

3. Dans le section **Expéditeurs des SMS**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection du périphérique** s'ouvre.

4. Dans la fenêtre **Sélection du périphérique**, indiquez le périphérique mobile qui sera utilisé en tant qu'expéditeur des messages SMS.

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

L'utilitaire Kaspersky SMS Broadcasting doit être installé sur le périphérique-expéditeur des SMS.

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

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 10.0 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 15. 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 diffusion 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 16. Débit du trafic

SCENARIO	MISE A JOUR INITIALE DES BASES ANTIVIRUS[1]
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 au moment où se déroule la synchronisation active des données entre les postes clients et le Serveur d'administration. 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.

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

[1] Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases.

Tableau 17. 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.[2]
SYNCHRONISATION INITIALE[3] AVANT LA MISE A JOUR DES BASES SUR LE POSTE CLIENT	368,6	463,7	832,3
SYNCHRONISATION INITIALE[4] APRES LA MISE A JOUR DES BASES SUR LE POSTE CLIENT	1 748,3	34 388,3	36 136,6
SYNCHRONISATION LORS DE L'ABSENCE DE MODIFICATIONS SUR LE POSTE CLIENT ET SUR LE SERVEUR D'ADMINISTRATION	8,7	6,6	15,3
SYNCHRONISATION LORS DE LA MODIFICATION D'UN PARAMETRE DANS LA STRATEGIE DU GROUPE[5]	11,1	13,3	24,4
SYNCHRONISATION LORS DE LA MODIFICATION D'UN PARAMETRE DANS LA TACHE DE GROUPE	10,0	12,5	22,5
SYNCHRONISATION FORCEE LORS DE L'ABSENCE DE MODIFICATIONS SUR LE POSTE CLIENT	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 18. Débit du trafic

SCENARIO	MISE A JOUR D'INCREMENTATION DES BASES ANTIVIRUS[6]
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.[7]	10 416,1

[2] Le volume du trafic varie essentiellement en fonction de l'utilisation de la 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.

[3] 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 des stratégies et des tâches, créées pour le groupe par défaut, au poste client.

[4] 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 des stratégies et des tâches, créées pour le groupe par défaut, au poste client.

[5] Le tableau indique le volume du trafic lors de la modification d'un des paramètres de protection par un mot de passe inclus dans les paramètres de la stratégie de Kaspersky Endpoint Security. Les données pour d'autres paramètres de la stratégie peuvent être différents des données présentées dans le tableau.

[6] Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases.

[7] Le volume du trafic varie essentiellement en fonction de l'utilisation de la 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 détecté" dont les informations sont transmises sur le Serveur d'administration et enregistrées dans la base de données (cf. tableau ci-après).

Tableau 19. Débit du trafic

SCENARIO[8]	TRANSFERT DES DONNEES SUR LE SERVEUR D'ADMINISTRATION QUAND L'EVENEMENT "VIRUS DETECTE" SURGIT.	TRANSFERT DES DONNEES SUR LE SERVEUR D'ADMINISTRATION QUAND NEUFS EVENEMENTS "VIRUS DETECTE" 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 LES VINGT-QUATRE HEURES

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

Tableau 20. Débit du trafic

SCENARIO	ETAT DE "REPOS" DU SYSTEME D'ADMINISTRATION[9]
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

[8] 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.

[9] Les données, affichées dans le tableau, caractérisent l'état du réseau après l'installation standard de Kaspersky Security Center et après la fin de l'Assistant de configuration initiale. La période de synchronisation entre le poste client et le Serveur d'administration est de 20 minutes, le téléchargement des mises à jour dans le stockage du Serveur d'administration est effectué toutes les heures.

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

Cette section décrit les exemples de la vitesse de remplissage de la base de données du Serveur d'administration par les événements survenus pendant le fonctionnement des applications administrées.

Les informations sur les événements survenus pendant le fonctionnement des applications administrées sont transmises depuis le périphérique client et sont enregistrées dans la base de données du Serveur d'administration.

La base de données reçoit (Ne*Nh) événements par jour (cf. tableau ci-après). Ici, Nh est le nombre de périphériques clients avec les applications administrées installées, Ne est le nombre d'événements par jour, sur lesquels les informations sont transmises par l'application administrée installée depuis le périphérique client avec l'application administrée installée.

Tableau 21. Vitesse de remplissage de la base de données par les événements

NOMBRE DE PERIPHERIQUES AVEC LES APPLICATIONS ADMINISTREES INSTALLEES	NOMBRE D'EVENEMENTS TRANSMIS CHAQUE JOUR DANS LA BASE DE DONNEES
100	2 000
1000	20 000
10 000	200 000

Le tableau reprend les données pour le fonctionnement titulaire des applications administrées, quand pas plus de 20 événements sont reçus par jour depuis un périphérique client.

Le nombre maximal des événements, conservés dans la base de données, se défini 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

Cette section reprend les informations sur les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Support Technique.

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé comment résoudre votre problème dans la documentation de l'application ou dans une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 10), veuillez contacter le Support technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

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

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- Par téléphone. Vous pouvez contacter les experts du Support Technique en France.
- Envoyer une demande via système Kaspersky CompanyAccount sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique francophones (http://support.kaspersky.com/fr/support/international).

Avant de contacter le Support Technique, veuillez prendre connaissances des Règles d'octroi du Support Technique (http://support.kaspersky.com/support/details). Ceci permettra nos experts à vous venir en aide le plus vite possible.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount est un service Internet (https://companyaccount.kaspersky.com) prévu à l'envoi et à la surveillance des demandes dans Kaspersky Lab.

Pour accéder à Kaspersky CompanyAccount, il faut s'enregistrer sur la page d'enregistrement (https://support.kaspersky.com/companyaccount/registration) et recevoir l'identifiant et le mot de passe. Pour ce faire, vous devez indiquer le code d'activation ou le fichier clé.

Kaspersky CompanyAccount permet de réaliser les actions suivantes :

- Envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- Communiquer avec le Support Technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel.
- Consulter l'historique complet de votre interaction avec le Support Technique.
- Obtenir une copie du fichier clé en cas de perte ou de suppression de celui-ci.

Formulaire de soumission de demande du Support Technique

Vous pouvez envoyer une demande par email au Support Technique en anglais, en français et en autres langues.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- type de demande ;
- Nom et numéro de version de l'application ;
- texte de la demande.

S'il faut, vous pouvez aussi attacher les fichiers à la forme électronique de la demande.

L'expert du Support Technique répond via Kaspersky CompanyAccount, en envoyant un message électronique à l'adresse indiquée lors de l'enregistrement.

Demande électronique adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivantes au Laboratoire d'étude des virus :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Security Center ne détecte aucune infection.

  Les experts du Laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de détection d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky Security Center considère un certain fichier comme infecté mais vous êtes convaincu que ce n'est pas le cas.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Kaspersky CompanyAccount. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application. La priorité des demandes créés via formulaire de demande est inférieure aux demandes créées via Kaspersky CompanyAccount.

GLOSSAIRE

A

Administrateur de Kaspersky Security Center

Personne qui gère les travaux du programme grâce à un 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 par l'interface locale.

Agent d'administration

Module 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 module est un module unique pour toutes les applications de l'entreprise pour Windows. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab fonctionnant sur Novell, Unix et Mac.

Agent des mises a jour

Ordinateur qui joue le rôle d'intermédiaire entre le centre 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 n'est pas compatible avec l'administration par Kaspersky Security Center.

B

Bases

Bases de données contenant les informations sur des menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les enregistrements dans les bases permettent de détecter le code malveillant dans les objets analysés. Les bases se forment par les experts de Kaspersky Lab et s'actualisent 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 en cours de l'installation du Serveur d'administration et sauvegardé sur le Serveur d'administration dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Client du Serveur d'administration (poste client)

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

Cle active

Clé utilisée au moment actuel pour faire fonctionner l'application.

CLE COMPLEMENTAIRE

Clé qui confirme le droit d'utilisation de l'application, mais non utilisée au moment actuel.

CONSOLE D'ADMINISTRATION

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

D

DEGRE D'IMPORTANCE DE L'EVENEMENT

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

Critique.

Erreur.

Avertissement.

Message d'information.

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

DUREE DE VALIDITE DE LA LICENCE

Durée de validité de la licence est une période pendant laquelle 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 caractérise le niveau de la protection de l'ordinateur.

F

FICHIER CLE

Le fichier de type xxxxxxx.key qui permet d'utiliser l'application de Kaspersky Lab sur les conditions de la licence d'évaluation ou commerciale. Vous pouvez utiliser l'application uniquement lors de la présence du fichier clé.

G

GROUPE D'ADMINISTRATION

Ensemble d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion dans son ensemble. Le groupe peut contenir d'autres groupes. Les stratégies de groupe et les tâches de groupe peuvent être créées pour chaque application installée dans le groupe.

I

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 réussir la tâche à l'aide de la méthode de l'installation forcée, le compte utilisateur employé pour le lancement de la tâche doit jouir des privilèges d'exécution à distance des applications sur les

postes clients. 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.

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 l'exécution de la tâche d'installation à distance à un compte utilisateur (ou plusieurs comptes) concret. Lorsque l'utilisateur s'enregistre dans le domaine, le système tente d'installer l'application sur le poste client depuis lequel l'utilisateur s'est enregistré. Cette méthode est recommandée pour l'installation des applications de la société sur les ordinateurs tournant sous Microsoft Windows 98/Me.

K

KASPERSKY SECURITY CENTER SYSTEM HEALTH VALIDATOR (SHV)

Le module de l'application Kaspersky Security Center conçu pour vérifier la puissance du système d'exploitation lors de l'utilisation simultanée de l'application Kaspersky Security Center avec Microsoft NAP.

L

LE SERVEUR DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Module de Kaspersky Security Center qui s'installe sur le poste client et qui permet de connecter les périphériques mobiles Exchange ActiveSync au Serveur d'administration.

LE SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Module de Kaspersky Security Center qui s'installe sur le poste client et qui permet de connecter les périphériques mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

M

MISE A JOUR

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

MISE A JOUR DISPONIBLE

Paquet des mises à jour des modules de l'application Kaspersky Lab qui contient les mises à jour urgentes recueillies au cours d'un intervalle de temps et les modifications dans 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 avec les extensions .kpd et .kud, inclus dans le distributif 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 L'APPLICATION

Paramètres de fonctionnement de l'application, communs pour l'ensemble de ses types de tâches et responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres des performances de l'application, les paramètres de génération des rapports et les paramètres du dossier de sauvegarde.

PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches.

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

Module 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 spécifique 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 module 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.

PROFIL

Ensemble des paramètres de comportement des périphériques mobiles Exchange ActiveSync lors de la connexion au serveur Microsoft Exchange.

PROFIL DE CONFIGURATION

Stratégie qui contient l'ensemble de paramètres et de restrictions pour le périphérique mobile iOS MDM.

PROFIL IOS MDM

L'ensemble des paramètres de connexion des périphériques mobiles iOS au Serveur d'administration. Le profil iOS MDM est installé par l'utilisateur sur le périphérique mobile, après quoi le périphérique mobile se connecte au Serveur d'administration.

PROFIL PROVISIONING

L'ensemble des paramètres pour utiliser les applications sur les périphériques mobiles iOS. Le profil provisioning contient les informations sur la licence et il est lié à l'application concrète.

PERIPHERIQUE MOBILE EXCHANGE ACTIVESYNC

Périphérique mobile qui se connecte au Serveur d'administration via protocole Exchange ActiveSync.

PERIPHERIQUE MOBILE IOS MDM

Périphérique mobile sous iOS qui se trouvant sous l'administration du Serveur des périphériques mobiles iOS MDM (cf. section “Serveur des périphériques mobiles iOS MDM” à la page 89).

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 de la structure du groupe d'administration et des postes clients ;

le stockage des paquets d'installation des applications pour l'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 de la structure du groupe d'administration et des postes clients ;
- le stockage des paquets d'installation des applications pour l'installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;
- le certificat du Serveur d'administration.

SERVEUR D'ADMINISTRATION

Module 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 la société, et d'un outil efficace de gestion de ces applications.

SERVEUR DES PERIPHERIQUES MOBILES

Module de Kaspersky Security Center qui offre l'accès aux périphériques mobiles et qui permet de les administrer via la Console d'administration.

SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab depuis lesquels l'application de Kaspersky Lab reçoit les mises à jour des bases et des modules de l'application.

SEUIL DE L'ACTIVITE DE VIRUS

Nombre d'événements d'un type donné et générés 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 virale. Ces données peuvent être utiles en période d'épidémie et permettent à l'administrateur de réagir opportunément à la menace d'une attaque de virus.

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 le 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 qui se présente 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 et exécutée sur tous les postes clients de ce groupe d'administration.

TACHE LOCALE

Tâche définie et exécutée sur un poste client particulier.

TACHE POUR UNE SELECTION D'ORDINATEURS

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

U

UTILISATEUR DE KASPERSKY SECURITY CENTER

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les 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 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 combinée à des outils d'administration centralisés 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 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 mises à jour toutes les heures*, tandis que *Les bases antispam sont mises à jour 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 (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-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 plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien 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 officiel de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire Anti-Virus :	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 demandes auprès des experts en virus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

NOTIFICATION SUR LES MARQUES DE COMMERCE

Les noms et les marques déposés appartiennent à leurs propriétaires respectifs.

Cisco est une marque de Cisco Systems, Inc. déposée aux Etats-Unis et aux autres pays, et/ou de ses sociétés affiliées.

Active Directory, ActiveSync, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et aux autres pays.

Intel, Core, Xeon sont des marques d'Intel Corporation déposées aux Etats-Unis et aux autres pays.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et aux autres pays.

Apple, iPhone, Mac, Mac OS sont des marques déposées d'Apple Inc.

Android est une marque de Google, Inc.

Le propriétaire de la marque de commerce Symbian est Symbian Foundation Ltd.

Novell, Netware sont des marques de Novell, Inc. déposées aux Etats-Unis et/ou dans d'autres pays.

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

INDEX

K

L

M

P

R

S

T

U