Kaspersky Security Center 10.0

Manuel de l'administrateur

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 guide de l'utilisateur 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 :

- Aider à configurer et à utiliser Kaspersky Security Center.
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'utilisation de Kaspersky Security Center.
- 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 de l'administrateur de Kaspersky Security Center contient l'introduction, les sections décrivant l'interface de l'application, ses paramètres et les services, les sections décrivant les résolutions des problèmes généraux, ainsi que les glossaires des termes.

Sources d'informations sur l'application (cf. page 13)

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 15)

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

Interface de l'application (cf. page 21)

Cette section décrit les paramètres principaux de l'interface Kaspersky Security Center.

Licence de l'application (cf. page 36)

Cette section présente les notions principales relatives à l'activation de l'application. Elle explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

Assistant de configuration initiale (à la page 41)

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale de Kaspersky Security Center.

Administration d'accès des périphériques dans le réseau de l'entreprise (NAC) (à la page 135)

Cette section reprend les informations sur le contrôle d'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.

Inventaire du matériel détecté dans le réseau (à la page 141)

Cette section reprend les informations sur l'inventaire du matériel connecté au réseau de l'entreprise.

Mise à jour des bases et des modules d'application (à la page 143).

Cette section décrit le téléchargement et la diffusion des mises à jour des bases et des modules d'application à l'aide de Kaspersky Security Center.

Travail avec les clés des applications (à la page 151)

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés des applications administrées de Kaspersky Lab.

Stockages des données (à la page 154)

Cette section contient les informations sur les données enregistrées sur le Serveur d'administration et utilisées pour suivre les états des postes clients et leur service.

Contacter le Service du Support Technique (à la page 160)

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.

Glossaire

La section reprend les termes utilisés dans ce document.

Kaspersky Lab (cf. page 166)

Cette section reprend les informations sur Kaspersky Lab.

Informations sur le code tiers (cf. page 167)

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 168)

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".
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 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 160).

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 sur la boutique en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page sur le site Internet 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.

DANS CETTE SECTION

NOUVEAUTES

Modifications apportées dans l'application Kaspersky Security Center 10.0 par rapport à la version 9.0 :

- La fonctionnalité de prise et de déploiement des images des systèmes d'exploitation a été ajoutée.
- La possibilité d'installer à distance d'une manière centralisée des applications tierces a été réalisée.
- La possibilité d'installer à distance d'une manière centralisée des mises à jour des systèmes d'exploitation et des applications a été réalisée.
- La fonctionnalité Windows Server® Update Services est incluse dans le Serveur d'administration.
- La fonctionnalité de contrôle des restrictions de licence a été ajoutée et la fonctionnalité du registre des applications a été élargie.
- La fonctionnalité d'utilisation du registre du matériel a été ajoutée.
- La possibilité de contrôler l'accès des périphériques au réseau de l'entreprise à l'aide des règles et à l'aide de la liste blanche des périphériques – Network Access Control a été réalisée.
- La possibilité d'accès partagé au bureau du poste client a été ajoutée et la fonctionnalité du bureau distant a été élargie.
- Le Serveur des périphériques mobiles Exchange ActiveSync a été réalisé.
- Le Serveur des périphériques mobiles iOS MDM a été réalisé.
- La possibilité d'envoi des messages SMS aux utilisateurs des périphériques mobiles a été réalisée.
- La fonctionnalité d'installation centralisée des applications sur les périphériques mobiles administrés a été réalisée.
- La fonctionnalité d'installation centralisée des certificats sur les périphériques mobiles administrés a été réalisée.
- La prise en charge du chiffrement des données pour l'application Kaspersky Endpoint Security 10 for Windows® a été ajoutée.
- Les possibilités de contrôle des applications ont été élargies, les fonctions suivantes ont été ajoutées : l'analyse statistique des règles de contrôle des applications, la création des catégories sur la base de l'ensemble des fichiers exécutables sur les ordinateurs de référence, l'affichage de plusieurs catégories pour un fichier exécutable.
- La possibilité de publier des paquets autonomes arbitraires sur le serveur Internet intégré au Serveur d'administration a été réalisée.
- La sélection des agents de mises à jour est incluse dans l'ensemble des sélections créées par défaut.

- La barre d'informations avec l'état des agents de mises à jour a été ajoutée.
- La possibilité de filtrage dans les listes centralisées de la quarantaine, du dossier de sauvegarde et des fichiers en traitement différé.
- La fonctionnalité d'utilisation de la liste centralisée des utilisateurs a été ajoutée.
- La possibilité d'exclure les sous-sections séparées depuis la recherche selon Active Directory.
- La possibilité de programmer le lancement de la tâche un jour précis dans le mois a été ajoutée.
- La définition automatique de la période de répartition du lancement des tâches a été réalisée.
- La possibilité d'utiliser la négation lors de la définition des critères de recherche dans les sélections d'ordinateurs a été réalisée.
- La possibilité d'indiquer la base vide déjà existante en tant que base de données du Serveur d'administration lors de l'installation a été réalisée.
- La possibilité d'indiquer les groupes en tant que critères de recherche dans les sélections d'ordinateurs a été ajoutée.
- La possibilité d'indiquer dans les paramètres de l'agent de mises à jour ce qu'il diffuse (les paquets d'installation, les mises à jour ou les deux) a été ajoutée.
- La possibilité de recherche d'ordinateurs selon les noms des utilisateurs ou selon la session a été ajoutée, ainsi que le rapport sur les utilisateurs des ordinateurs.
- L'utilitaire graphique d'administration de l'Agent d'administration a été réalisé.
- L'affichage séparé de la date d'expiration de la licence et de la date du délai de validité de la clé a été ajouté dans les propriétés de la clé et dans le rapport sur l'utilisation des clés.
- L'affichage des informations sur le volume total de données enregistrées dans la base de données du Serveur d'administration et sur le volume des événements enregistrés dans la base de données a été ajouté.
- La possibilité de définir les critères à l'aide de l'opérateur "ou" dans les règles de déplacement des ordinateurs dans les groupes d'administration a été ajoutée.

DISTRIBUTION

L'application peut être acheté dans la boutique en ligne de Kaspersky Lab (par exemple http://www.kaspersky.com/fr, section **Boutique en ligne**) ou chez nos partenaires.

En achetant Kaspersky Security Center dans la boutique en ligne, vous copiez l'application depuis le site Internet de la boutique en ligne. Les informations indispensables à l'activation de l'application vous seront envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre Service Ventes.

CONFIGURATIONS LOGICIELLE ET MATERIELLE

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

INTERFACE DE L'APPLICATION

Cette section décrit les paramètres principaux de l'interface Kaspersky Security Center.

La consultation, la création, la modification et la configuration des groupes d'administration, l'administration centralisée du fonctionnement des applications de Kaspersky Lab installées sur les postes clients sont exécutées depuis le poste administrateur. La Console d'administration correspond à l'interface d'administration. Elle représente un outil autonome centralisé intégré à Microsoft Management Console (MMC), c'est pourquoi l'interface de Kaspersky Security Center est standard pour MMC.

La Console d'administration permet de se connecter au Serveur d'administration distant par Internet.

Pour travailler localement avec les postes clients, l'application prévoit la possibilité d'installer une connexion à distance avec l'ordinateur par la Console d'administration à l'aide de l'application standard Microsoft Windows "Connexion en cours au poste de travail distant".

Afin d'utiliser cette possibilité, il est nécessaire d'autoriser la connexion à distance au poste de travail sur le poste client.

DANS CETTE SECTION

FENETRE PRINCIPALE DE L'APPLICATION

La fenêtre principale de l'application (cf. ill. ci-dessous) contient le menu, la barre d'outils, la barre de consultation et la zone de travail.

Le menu permet de gérer les fenêtres et d'accéder à l'aide. L'option du menu **Action** reprend les commandes du menu contextuel pour l'objet de l'arborescence de la console.

La barre de consultation reflète l'étendue des noms de **Kaspersky Security Center** dans l'arborescence de la console (cf. section "Arborescence de la console" à la page 23).

L'ensemble des boutons dans la barre d'outils assure un accès direct à certains points du menu principal. Les boutons dans la barre d'outils changent selon l'entrée ou le dossier de l'arborescence de la console sélectionné.

Le type de zone de travail de la fenêtre principale dépend de l'entrée (du dossier) de l'arborescence de la console à laquelle il/elle appartient et les fonctions qu'il/elle assure.

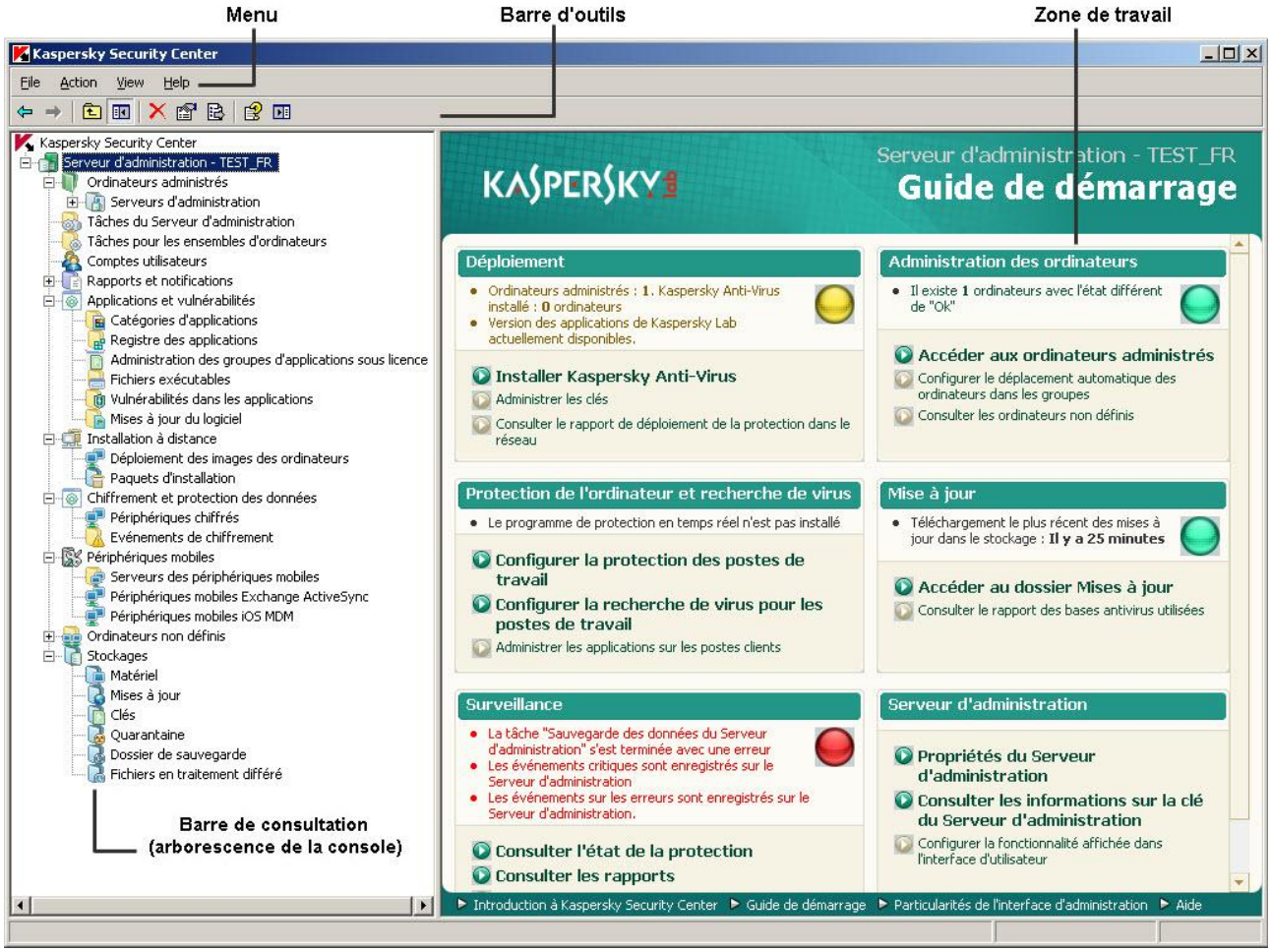

Illustration 1. Fenêtre principale de Kaspersky Security Center

ARBORESCENCE DE LA CONSOLE

L'arborescence de la console (cf. ill. ci-dessous) est conçue pour refléter la hiérarchie (formée dans le réseau) des Serveurs d'administration, de la structure de leurs groupes d'administration, ainsi que d'autres objets de l'application, tels que **Stockages** et **Rapports et notifications**. L'étendue des noms de Kaspersky Security Center peut inclure plusieurs sections avec les noms des serveurs qui correspondent aux Serveurs d'administration installés et inclus dans la structure du réseau.

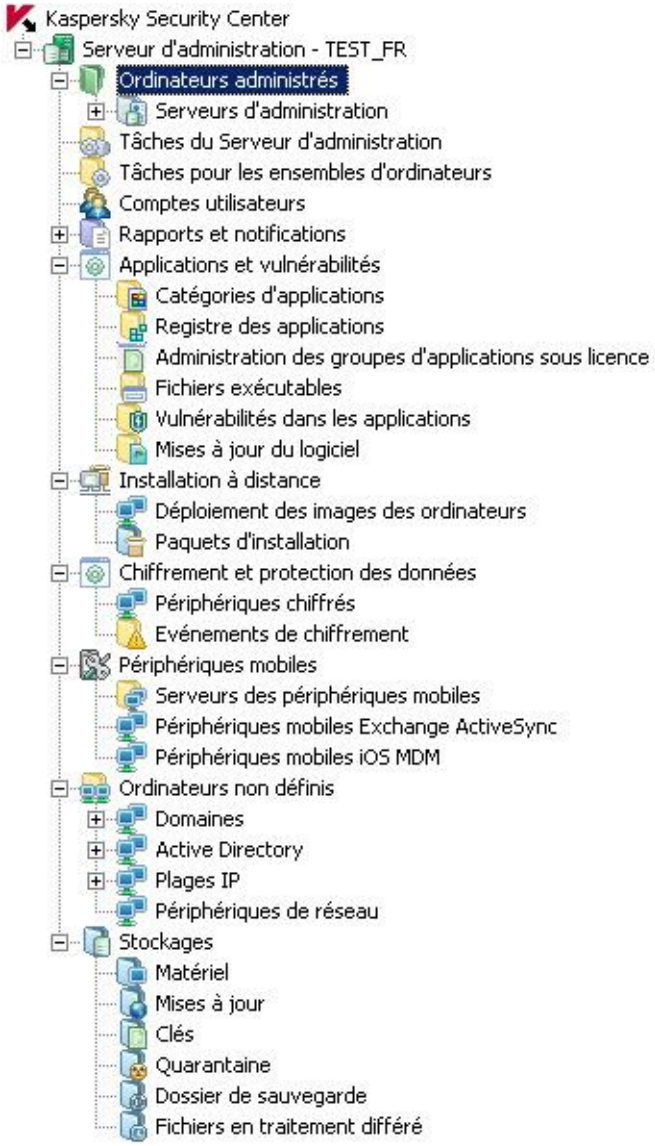

Illustration 2. Arborescence de la console

La section **Serveur d'administration : <Nom de l'ordinateur>** est un conteneur et reflète la structure du Serveur d'administration indiqué. Le conteneur **Serveur d'administration – <Nom de l'ordinateur>** inclut les dossiers suivants :

- **Ordinateurs administrés**.
- **Comptes utilisateurs**.
- **Rapports et notifications**.
- **Tâches du Serveur d'administration**.
- **Tâches pour les ensembles d'ordinateurs**.

- **Applications et vulnérabilités**.
- **Installation à distance**.
- **Périphériques mobiles**.
- **Chiffrement et protection des données**.
- **Ordinateurs non définis**.
- **Stockages**.

Le dossier **Ordinateurs administrés** est conçu pour conserver, refléter, configurer et modifier la structure des groupes d'administration, les stratégies de groupe et les tâches de groupe.

Le dossier **Comptes utilisateurs** contient les informations sur les comptes utilisateurs dans le réseau.

Le dossier **Rapports et notifications** contient l'ensemble des modèles pour former les rapports d'état du système de protection sur les postes clients des groupes d'administration. Le dossier **Rapports et notifications** contient aussi les sous-dossiers suivants :

- **Sélections d'ordinateurs**. Conçu pour la recherche des postes clients selon les critères définis.
- **Evénements**. Contient les sélections d'événements qui présentent les informations sur les événements enregistrés pendant le fonctionnement des applications, ainsi que sur les résultats de l'exécution de la tâche.

Le dossier **Tâches du Serveur d'administration** contient l'ensemble de tâches, désignées pour le Serveur d'administration.

Le dossier **Tâches pour les ensembles d'ordinateurs** contient les tâches pour les sélections d'ordinateurs dans le groupe d'administration ou dans le dossier **Ordinateurs non définis**. Ces tâches sont désignées pour les petits groupes de postes clients qui ne peuvent pas être unis dans un groupe d'administration séparé.

Le dossier **Applications et vulnérabilités** est conçu pour administrer les applications installées sur les ordinateurs du réseau. Il contient les sous-dossiers suivants :

- **Catégories des applications**. Conçu pour travailler avec les catégories d'utilisateurs des applications.
- **Registre des applications**. Contient la liste des applications installées sur les postes clients sur lesquels l'Agent d'administration est installé.
- **Fichiers exécutables**. Contient la liste des fichiers exécutables enregistrés sur les postes clients avec l'Agent d'administration installé.
- **Vulnérabilités dans les applications**. Contient la liste des vulnérabilités des applications sur les postes clients avec l'Agent d'administration installé.
- **Mises à jour du logiciel**. Contient la liste des mises à jour des applications reçues par le Serveur d'administration qui peuvent être déployées sur les postes client.

Le dossier **Installation à distance** est conçu pour administrer l'installation à distance des systèmes d'exploitation et des applications. Les sous-dossiers suivants le composent :

- **Déploiement des images des ordinateurs** Conçu pour déployer les images des systèmes d'exploitation sur les postes clients.
- **Paquets d'installation**. Contient la liste des paquets d'installation qui peuvent être utilisés pour l'installation à distance des applications sur les postes clients.

Le dossier **Périphériques mobiles** est conçu pour administrer les périphériques mobiles Exchange ActiveSync et iOS MDM.

Le dossier **Chiffrement et protection des données** est conçu pour administrer le processus de chiffrement des données d'utilisateur sur les disques et les supports amovibles.

Le dossier **Ordinateurs non définis** est conçu pour afficher le réseau d'ordinateurs où le Serveur d'administration est installé. Le Serveur d'administration obtient les informations relatives à la structure du réseau et aux ordinateurs qui en font partie lors des requêtes fréquentes adressées au réseau Windows, aux sous-réseaux IP ou Active Directory® créés dans le réseau informatique de l'entreprise. Les résultats des sondages sont affichés dans les zones d'informations des sous-dossiers correspondants : **Domaines**, **Plages IP** et **Active Directory**.

Le dossier **Stockages** permet de manipuler les objets utilisés pour la surveillance de l'état des postes client et les entretenir. Les données suivantes le composent :

- **Mises à jour**. Contient la liste des mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les postes clients.
- **Matériel**. Contient la liste du matériel connecté au réseau de l'entreprise.
- **Clés**. Contient la liste des clés sur les postes clients.
- **Quarantaine**. Contient la liste des objets placés par les applications antivirus dans les dossiers de quarantaine des postes client.
- **Dossier de sauvegarde**. Contient la liste des copies de sauvegarde des objets placés dans le dossier de sauvegarde.
- **Fichiers en traitement différé**. Contient la liste des fichiers pour lesquels les applications antivirus ont décidé le traitement ultérieur.

ZONE DE TRAVAIL

La *Zone de travail* est une zone de la fenêtre principale de l'application Kaspersky Security Center située à droite de l'arborescence de la console (cf. ill. ci-après). Elle contient la description des objets de l'arborescence de la console et des fonctions qu'ils exécutent. Le contenu de la zone de travail correspond à l'objet sélectionné dans l'arborescence de la console.

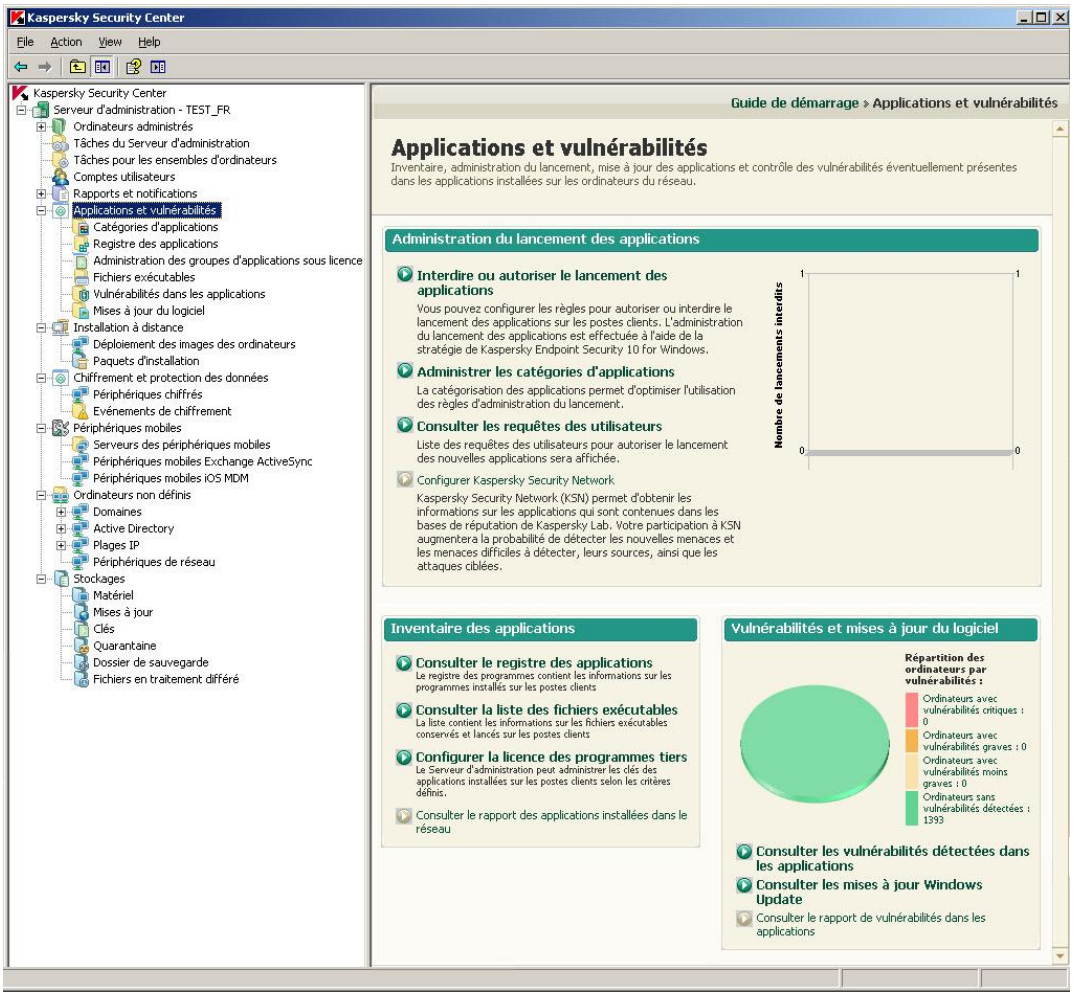

Illustration 3. Zone de travail

Le type de la zone de travail pour différents objets de l'arborescence de la console dépend du type des informations affichées. Il existe trois types de la zone de travail :

- ensemble de groupes d'administration ;
- liste des objets d'administration ;
- ensemble de barres d'informations.

Si une partie des éléments qui sont inclus dans l'objet de l'arborescence de la console n'est pas affichée dans l'arborescence de la console, la zone de travail est partagée sur les onglets. Chaque onglet correspond à un certain élément de l'objet de l'arborescence de la console (cf. ill. ci-après).

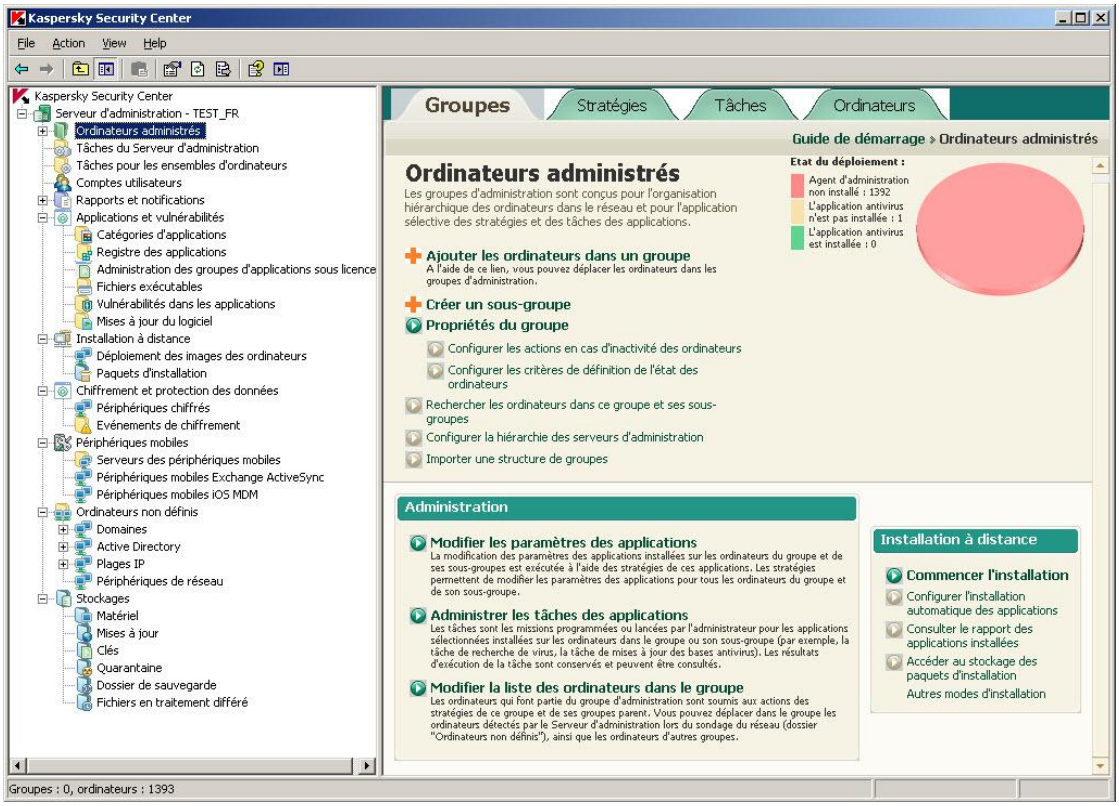

Illustration 4. Zone de travail partagée sur onglets

DANS CETTE SECTION

ENSEMBLE DE GROUPES D'ADMINISTRATION

La zone de travail représentée par l'ensemble de *groupe d'administration*, les tâches d'administration sont divisées en groupes. Chaque groupe d'administration contient l'ensemble de liens dont chaque lien correspond à la tâche d'administration définie (cf. ill. ci-après).

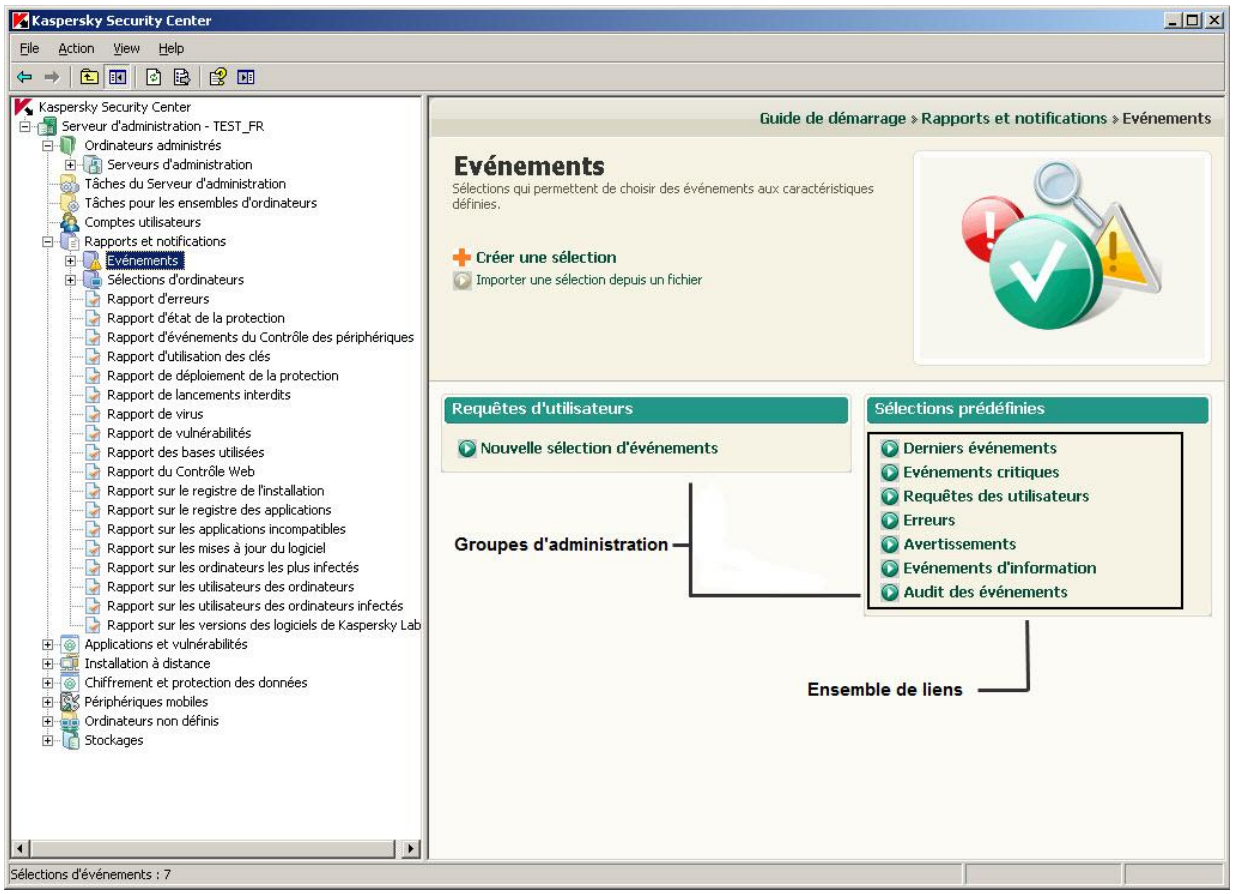

Illustration 5. Zone de travail présentée par l'ensemble de groupes d'administration

LISTE DES OBJETS D'ADMINISTRATION

La zone de travail présentée par la liste des objets d'administration reprend quatre zones (cf. ill. ci-après) :

- Groupe d'administration de la liste des objets.
- Liste des objets.
- Groupe de travail avec l'objet sélectionné (peut être absent).

- Groupe du filtrage de données (peut être absent).

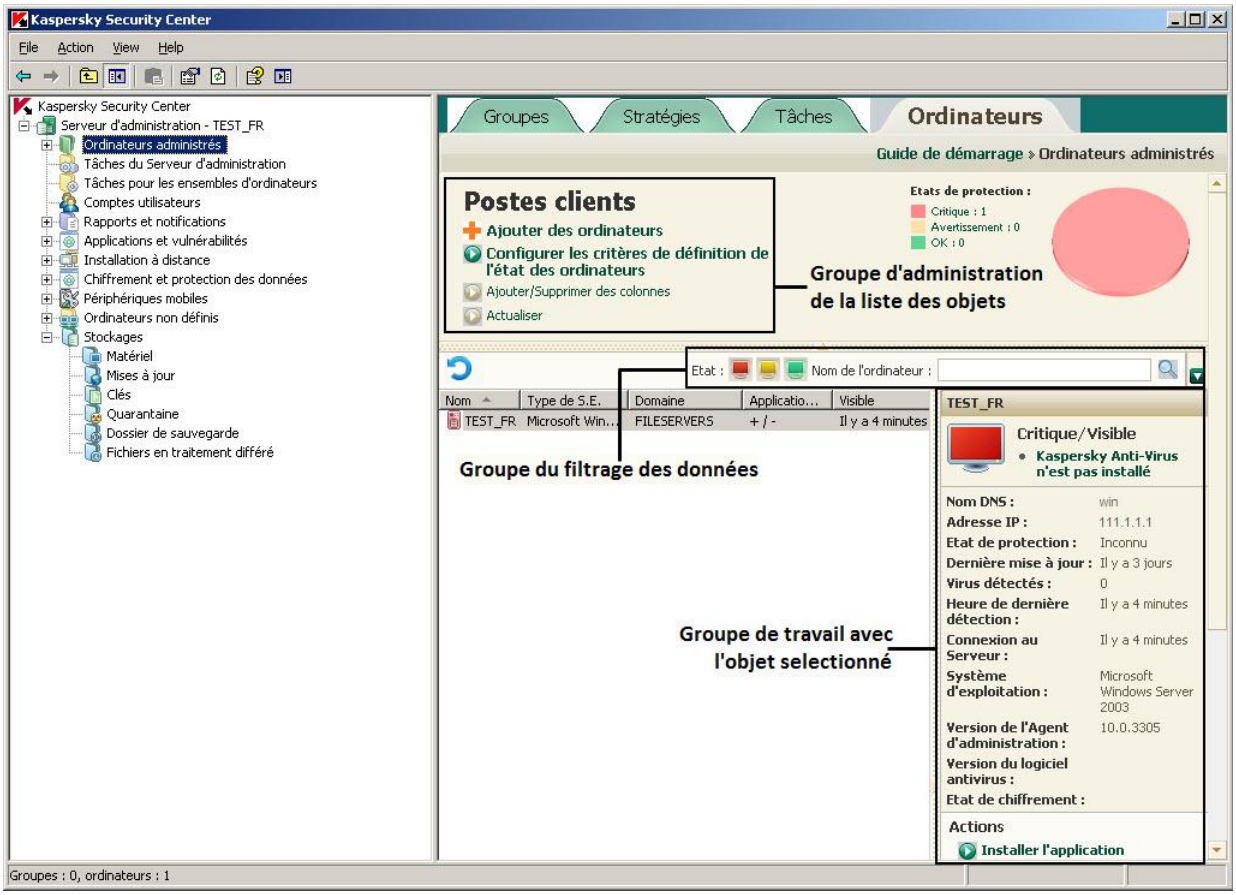

Illustration 6. Zone d'informations présentée par la liste des objets d'administration

Le groupe d'administration des objets contient l'en-tête de la liste et l'ensemble des liens dont chacune entre eux correspond à une certaine tâche d'administration de la liste.

La liste des objets est présentée sous forme du tableau. L'ensemble de colonne peut être modifié à l'aide du menu contextuel.

Le groupe de travail avec l'objet sélectionné contient les informations détaillées sur l'objet et l'ensemble des liens à exécuter les tâches principales d'administration de l'objet.

Le groupe du filtrage des données permet de créer les requêtes d'objets depuis la liste (cf. section "Groupe du filtrage de données" à la page 30).

ENSEMBLE DE GROUPES D'INFORMATIONS

Les données à caractère informatif sont affichées dans la zone de travail comme des *barres d'informations* sans éléments d'administration (cf. ill. ci-après).

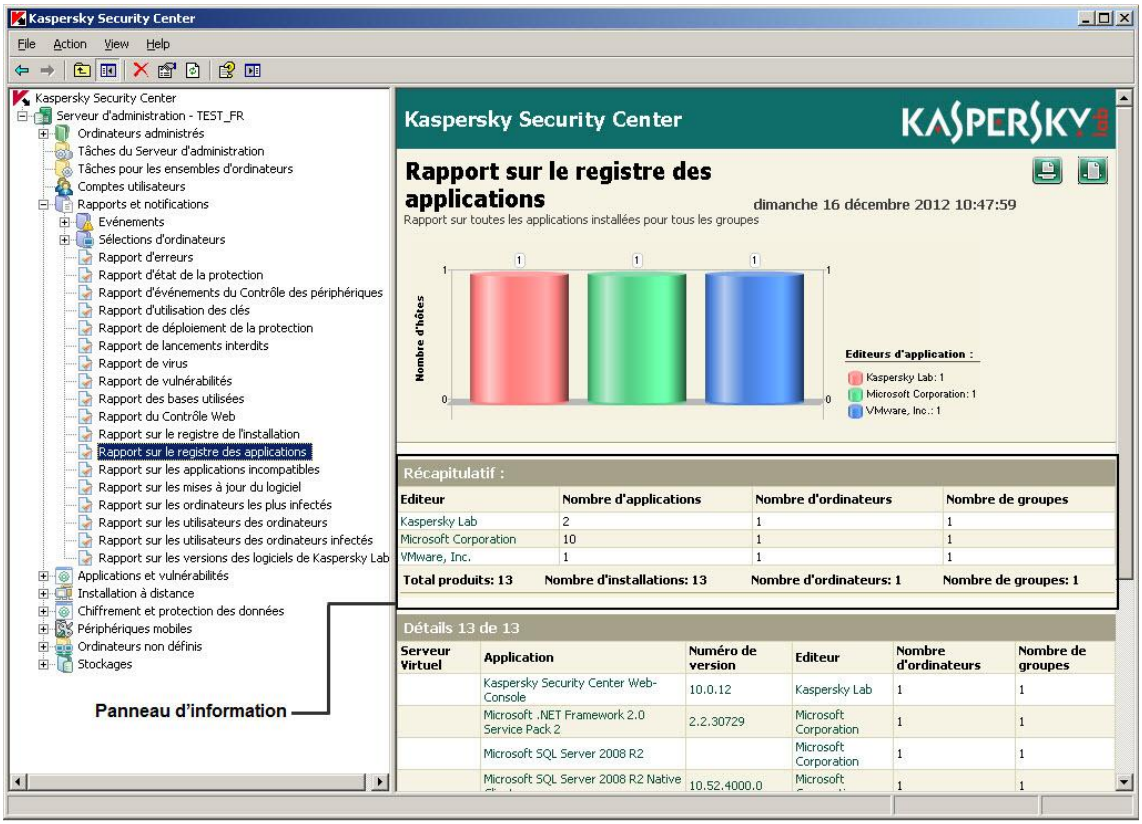

Illustration 7. Zone de travail présentée par l'ensemble de barres d'informations

Les barres d'informations peuvent être présentées sur plusieurs pages (cf. ill. ci-après).

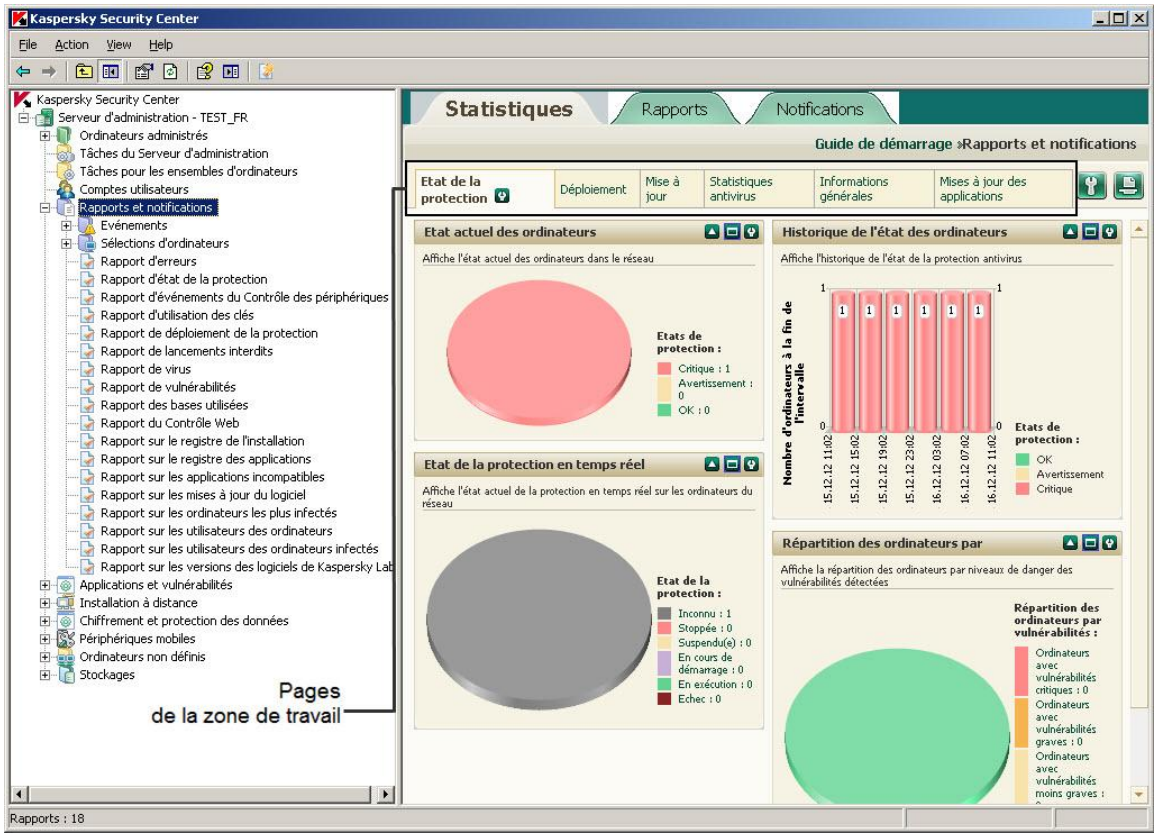

Illustration 8. Zone de travail partagée sur pages

GROUPE DU FILTRAGE DE DONNEES

Le *Groupe de filtrage de données* (ci -après *groupe de filtrage*) se trouve dans les zones de travail et dans les sections des fenêtre des dialogue qui contiennent les listes des objets suivants :

- ordinateurs ;
- applications ;
- événements ;
- vulnérabilités ;
- fichiers exécutables.

Le groupe du filtrage peut activer les éléments suivants d'administration (cf. ill. ci-après) :

- barre de recherche ;
- paramètres de choix ;

- boutons.

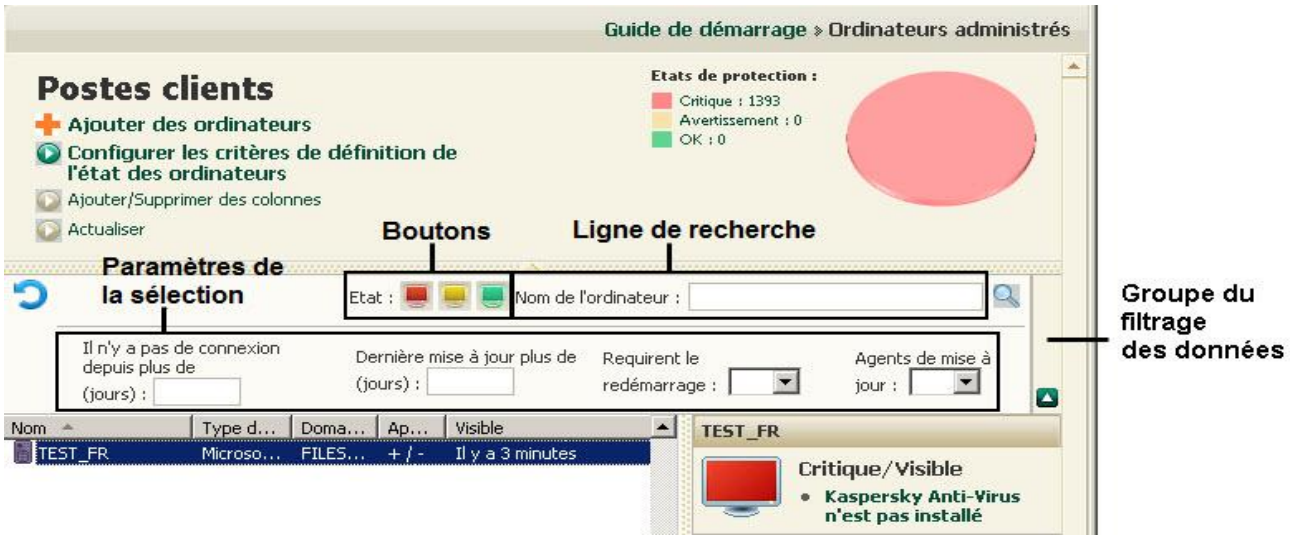

Illustration 9. Groupe de filtrage des données dans la zone de travail

Le groupe de filtrage est aussi présenté dans les fenêtres de dialogue, dans les sections contenant les listes.

Barre de recherche

Pour utiliser la ligne de recherche, il faut saisir le texte recherché dans le champ de saisie.

Pour décrire le texte recherché, les expressions régulières sont admises :

- *. Remplace n'importe quelle ligne d'une longueur de 0 ou plus de caractères.

Exemple :

Pour décrire les mots Serveur ou de serveur, il est possible d'utiliser la ligne Serveur*.

> Le symbole * ne peut pas être utilisé en tant que premier caractère dans la description du texte.

- ?. Remplace un n'importe quel caractère.

Exemple :

Pour décrire les mots Fenêtre ou Fenêtres, il est possible d'utiliser la ligne Fenêtr?.

> Le symbole ? ne peut pas être utilisé en tant que premier caractère dans la description du texte.

- [<intervalle>]. Remplace n'importe quel symbole de la plage indiquée ou de la multitude.

Exemple :

Pour décrire tout chiffre, il est possible d'utiliser la ligne [0–9].

Pour décrire un des symboles a, b, c, d, e, f, il est possible d'utiliser la ligne [abcdef].

Dans le groupe de filtrage de la liste des événements, la recherche de texte complet selon les colonnes **Evénement** et **Description** est accessible.

Pour décrire le texte recherché, il est admis d'utiliser les expressions régulières suivantes lors de la recherche de texte complet :

- Espace. Signifie la présence d'au moins un mot parmi les mots séparer par des espaces.

Exemple :

Pour décrire la phrase contenant le mot **Secondaire** ou **Virtuel**, il est possible d'utiliser la ligne **Secondaire Virtuel**.

- **+**. Avant le mot signifie la présence obligatoire du mot dans le texte.

Exemple :

Pour décrire la phrase contenant le mot **Secondaire**, et le mot **Virtuel**, il est possible d'utiliser la ligne **+Secondaire+Virtuel**.

- **-**. Avant le mot signifie l'absence obligatoire du mot dans le texte.

Exemple :

Pour décrire la phrase avec le mot **Secondaire** et sans le mot **Virtuel**, il est possible d'utiliser la ligne **+Secondaire-Virtuel**.

- **"<fragment du texte>"**. Le fragment du texte entre guillemets doit être entièrement présent dans le texte.

Exemple :

Pour décrire la phrase contenant le groupe de mots **Serveur secondaire**, il est possible d'utiliser la ligne **"Serveur secondaire"**.

Paramètres de choix

Pour utiliser les paramètres de la sélection, il faut indiquer la valeur à l'aide d'un des moyens suivants :

- saisir la valeur à la main ;
- sélectionner la valeur de la liste déroulante ;
- cocher (décocher) la case.

Boutons

Les boutons du groupe du filtrage représente des icônes de couleur sur le fond foncé.

En cliquant sur le bouton, le fond de l'icône devient clair. Si vous recliquez sur le bouton, le fond de l'icône redevient foncé.

Les règles du filtrage sont :

- L'élément de la liste avec la valeur indiquée de l'attribut est considéré comme sélectionné si le groupe du filtrage indique l'icône avec la valeur indiquée de l'attribut et cette icône est sur le fond foncé.

Exemple :

 – la requête sera composée d'ordinateurs avec état *Critique*.

 – la requête sera composée d'ordinateurs avec état *Avertissement*.

 – la requête sera composée d'ordinateurs avec état *OK*.

- L'élément de la liste avec la valeur indiquée de l'attribut est considéré comme non sélectionné si le groupe du filtrage indique l'icône avec la valeur indiquée de l'attribut et cette icône est sur le fond clair.

Exemple :

– la requête ne sera pas composée d'ordinateurs avec état *Critique*.

– la requête ne sera pas composée d'ordinateurs avec état *Avertissement*.

– la requête ne sera pas composée d'ordinateurs avec état *OK*.

- La requête contient tous les éléments de la liste si les icônes de toutes les valeurs des attributs sont affichées sur le fond clair (par exemple,) ou sur le fond foncé (par exemple,).

Les valeurs des attributs correspondent aux états des ordinateurs (ou des périphériques de réseau) et aux degrés d'importance des événements. La liste des états des ordinateurs, des périphériques de réseau et des degrés d'importance des événements, ainsi que les icônes correspondants est présentée dans l'annexe.

Travail avec le groupe du filtrage

Lors du travail avec le groupe du filtrage, vous pouvez former les sélections des données et annuler le filtrage, ainsi qu'activer le type élargi du groupe avec les paramètres complémentaires du filtrage :

- Composition de la sélection :
  - Lors de l'utilisation des boutons du groupe du filtrage, la sélection de la liste est composée automatiquement après avoir cliqué sur le bouton.
  - Lors de l'utilisation des paramètres de ligne et des paramètres de choix pour composer la requête, il faut cliquez sur le bouton en haut à droite du groupe du filtrage.
  - Lors de l'utilisation des boutons en combinaison avec les paramètres de ligne ou de choix pour former la requête, il faut cliquer sur le bouton en haut à droite du groupe du filtrage.
- Annulation du filtrage :

Pour annuler le filtrage, il faut cliquer sur le bouton . Le bouton apparaît à gauche du bouton après la première utilisation du groupe de filtrage pour former la requête.

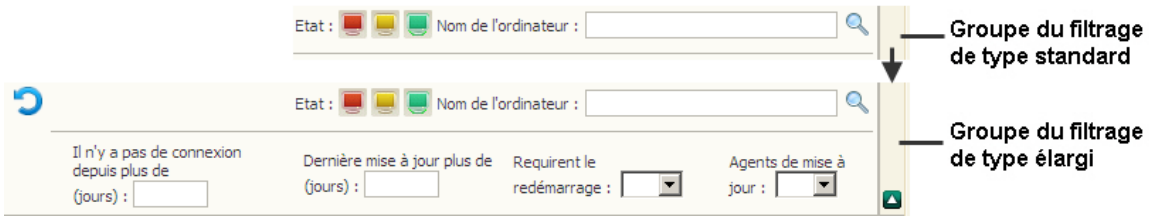

Illustration 10. Groupe du filtrage avec le type élargi de présentation

- Utilisation de type standard et élargi du groupe du filtrage :
  - Si le bouton existe dans la partie droite du groupe du filtrage, ce groupe possède un type standard et élargi de présentation (cf. ill. ci-dessus). Le type élargi de présentation possède les champs de saisie des valeurs des paramètres complémentaires du filtrage.
  - Le groupe du filtrage de type élargi peut être déployé à l'aide du bouton . Pour revenir au type standard du groupe du filtrage, il faut cliquer sur le bouton .

MENU CONTEXTUEL

Dans l'arborescence de la console Kaspersky Security Center, chaque objet possède le menu contextuel. Outre les commandes standards du menu contextuel de la console MMC, on retrouve les commandes qui permettent de réaliser les opérations sur cet objet. La liste des objets et des commandes supplémentaires du menu contextuel qui peuvent être exécutées est reprise dans l'application.

Dans la zone de travail chaque élément de l'objet sélectionné dans l'arborescence possède également un menu contextuel dont les commandes permettent la réalisation d'opérations sur les éléments sélectionnés. Les principaux types d'éléments et les commandes supplémentaires associées figurent dans l'application.

CONFIGURATION DE L'INTERFACE

Kaspersky Security Center permet de configurer l'interface de la Console d'administration.

Pour modifier les paramètres de l'interface déjà installés, procédez comme suit :

1. Dans l'arborescence de la console, passez à l'entrée du Serveur d'administration.
2. Dans le menu **Vue**, sélectionnez l'option **Configuration de l'interface**.
3. Dans la fenêtre ouverte **Configuration de l'interface** (cf. ill. ci-après), configurez l'affichage des éléments de l'interface à l'aide des cases suivantes :

- **Afficher l'administration système**

  Si la case est cochée, le dossier **Installation à distance** affiche le sous-dossier **Déploiement des images des ordinateurs** et le dossier **Stockages** affiche le sous-dossier **Matériel**.

Celle-ci est décochée par défaut.

- **Afficher le chiffrement et la protection des données**

  Si la case est cochée, l'arborescence de la console affiche le dossier **Chiffrement et protection des données** et la fonction de chiffrement des données sur les périphériques connectés au réseau devient accessible.

  Celle-ci est décochée par défaut.

- **Afficher les modules de contrôle des applications et des périphériques**

  Si la case est cochée, la fenêtre des propriétés de la stratégie Kaspersky Endpoint Security 10 for Windows affiche la section **Contrôle du bureau** et la fonctionnalité de contrôle des applications et des périphériques devient accessible.

  Celle-ci est décochée par défaut.

- **Afficher l'administration des périphériques mobiles**

  Si la case est cochée, l'arborescence de la console affiche le dossier **Périphériques mobiles**, et la fonction d'administration des périphériques mobiles via le Serveur d'administration devient accessible.

  Celle-ci est décochée par défaut.

- **Afficher les Serveurs d'administration secondaires**

  Si la case est cochée, l'arborescence de la console affiche les entrées des Serveurs d'administration secondaires et virtuels dans les groupes d'administration. Avec cela, la fonction liée avec les Serveurs d'administration secondaires et virtuels (par exemple, la création de la tâche d'installation à distance des applications sur les Serveurs d'administration secondaires) est accessible.

  Celle-ci est décochée par défaut.

- **Afficher les sections avec les paramètres de sécurité**

  Si la case est cochée, la section **Sécurité** s'affichera dans les fenêtres des propriétés du Serveur d'administration, des groupes d'administration et d'autres objets. Ceci permettra de fournir aux utilisateurs et aux groupes d'utilisateurs les droits de travail avec les objets, autres que les valeurs par défaut.

  Celle-ci est décochée par défaut.

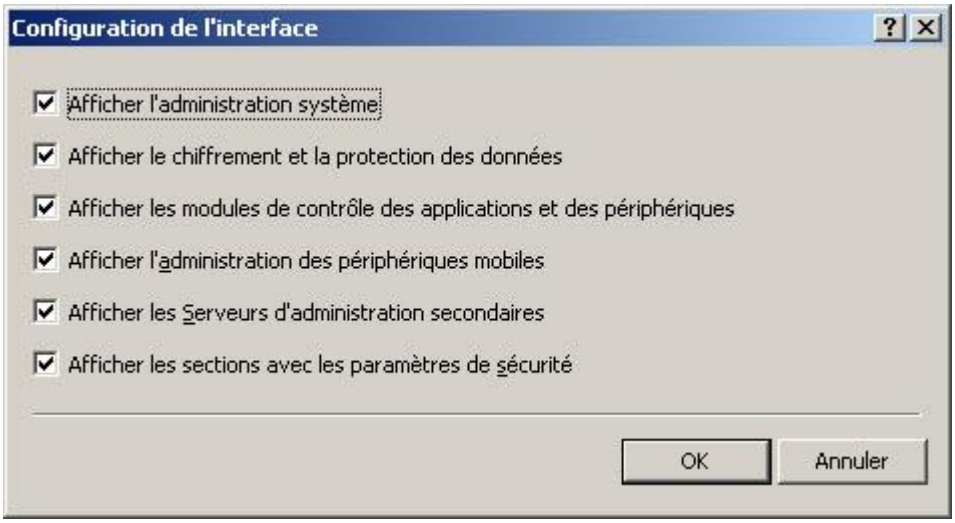

*Illustration 11. Fenêtre **Configuration de l'interface***

LICENCE DE L'APPLICATION

Cette section présente les notions principales relatives à l'activation de l'application. Elle explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

DANS CETTE SECTION

A PROPOS DU CONTRAT DE LICENCE

Le Contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.

Vous êtes réputé avoir accepté les conditions du Contrat de licence lorsque vous décidez d'installer l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application ou ne pas utiliser l'application.

A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application limité dans le temps et octroyé dans le cadre du Contrat de licence. La licence est associée à un code d'activation unique de votre copie de Kaspersky Security Center.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs périphériques.

  Le nombre d'appareils sur lequel vous pouvez utiliser l'application est défini par les termes du Contrat de licence.

- Contacter le Support Technique de Kaspersky Lab.

- Accès aux divers services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence.

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Il existe les types de licence suivants :

- *Evaluation :* une licence gratuite conçue pour découvrir l'application.

  En général, la durée de validité d'une licence d'évaluation est brève. Une fois que la licence expirée, Kaspersky Security Center continue son fonctionnement en mode de fonctionnalité partiellement limitée.

- *Commerciale :* licence payante octroyée à l'achat de l'application. Plusieurs options de licence de Kaspersky Security Center sont prévues.

  A l'expiration de la durée de validité de la licence commerciale, l'application continue son fonctionnement en mode de fonctionnalité partiellement limitée (cf. section "A propos des restrictions de la fonctionnalité de base" à la page 39). Pour pouvoir continuer à utiliser toutes les fonctions de Kaspersky Security Center, il faut renouveler la licence commerciale.

Il est conseillé de renouveler la licence avant son expiration afin de garantir la protection maximale de l'ordinateur contre toutes les menaces.

OPTIONS DE LICENCE DE KASPERSKY SECURITY CENTER

Dans Kaspersky Security Center, la licence peut être diffusée sur des groupes différents de fonctionnalité.

Fonctionnalité de base de la Console d'administration

Les fonctions suivantes sont disponibles :

- création des Serveurs d'administration virtuels pour administrer le réseau des offices à distance et des entreprises clientes ;
- formation d'une hiérarchie des groupes d'administration pour administrer l'ensemble de périphériques comme un tout unique ;
- contrôle d'état de sécurité antivirus de l'entreprise ;
- installation à distance des applications ;
- consultation de la liste des images des systèmes d'exploitation accessibles à l'installation à distance ;
- configuration centralisée des paramètres des applications installées sur les postes clients ;
- consultation et modification des groupes existants des applications sous licence ;
- réception des statistiques et des rapports sur le fonctionnement des applications, ainsi que la réception des notifications sur les événements critiques ;
- administration du processus de chiffrement et de protection des données ;
- consultation et modification manuelle de la liste du matériel détecté suite au sondage du réseau ;
- travail centralisé avec les fichiers placés en quarantaine ou dans le dossier de sauvegarde, et avec les fichiers dont le traitement est différé.

L'application Kaspersky Security Center avec la prise en charge de la fonctionnalité de base de la Console d'administration est livrée dans la suite logicielle de Kaspersky Lab conçue pour la protection du réseau de l'entreprise. Il peut également être téléchargé depuis le site de Kaspersky Lab (http://www.kaspersky.fr).

Le Serveur d'administration virtuel est une unité d'administration pour la fonctionnalité de base de l'application. Il est possible de créer jusqu'à 10 Serveurs d'administration virtuels.

Avant l'activation de l'application ou à l'expiration de la durée de validité de la licence commerciale, Kaspersky Security Center fonctionne en mode de fonctionnalité de base de la Console d'administration (cf. section "A propos des restrictions de la fonctionnalité de base" à la page 39).

Fonctionnalité de Kaspersky Security Center, Service Provider Edition (ci-après – SPE)

La fonctionnalité de la version SPE de l'application double la fonctionnalité de base de la Console d'administration, mais il est possible de créer plus de 10 Serveur d'administration virtuels.

La version SPE de l'application est livrée sous les conditions particulières aux partenaires de Kaspersky Lab. Pour plus d'informations sur le programme de partenariat, visitez le site Internet de Kaspersky Lab, à la page http://www.kaspersky.fr.

Fonctionnalité Administration système

Les fonctions suivantes sont disponibles :

- installation à distance des systèmes d'exploitation ;
- installation à distance des mises à jour du logiciel, recherche et correction des vulnérabilités ;
- administration d'accès des périphériques dans le réseau de l'entreprise (NAC) ;
- inventaire du matériel ;
- administration des groupes des applications sous licence ;
- connexion à distance aux postes clients.

Le poste client dans le groupe "Ordinateurs administrés" est une unité d'administration pour la fonctionnalité de l'Administration système.

Fonctionnalité Gestion des périphériques mobiles

La fonctionnalité de Gestion des périphériques mobiles est conçu pour administrer les périphériques mobiles Exchange ActiveSync et iOS MDM.

Pour les périphériques mobiles Exchange ActiveSync, les fonctions suivantes sont disponibles :

- création et modification des profils d'administration des périphériques mobiles, attribution des profils aux boîtes aux lettres des utilisateurs ;
- configuration des paramètres de fonctionnement du périphérique mobile (synchronisation du courrier, mot de passe de l'utilisateur, chiffrement des données, connexion des disques amovibles) ;
- installation des certificats sur les périphériques mobiles.

Pour les périphériques mobiles iOS MDM, les fonctions suivantes sont disponibles :

- création et modification des profils de configuration, installation des profils de configuration sur les périphériques mobiles ;
- installation des applications sur le périphérique mobile via App Store ou à l'aide des fichiers-manifestes(.plist) ;
- possibilité de bloquer le périphérique mobile, de remettre à zéro le mot de passe du périphérique et de supprimer toutes les données sur le périphérique mobile.

L'exécution des commandes prévues par les protocoles correspondants est aussi accessible dans le cadre de fonctionnalité Gestion des périphériques mobiles.

Le périphérique mobile est une unité d'administration de la fonctionnalité de Gestion des périphériques mobiles. Le périphérique mobile est considéré comme périphérique administré quand il est connecté au Serveur des périphériques mobiles.

A PROPOS DES RESTRICTIONS DE LA FONCTIONNALITE DE BASE

Avant l'activation de l'application ou à l'expiration de la licence commerciale, Kaspersky Security Center fonctionne en mode de fonctionnalité de base de la Console d'administration. La description des restrictions imposées sur le fonctionnement de l'application dans ce mode est reprise ci-après.

Gestion des périphériques mobiles

Il est impossible de créer un nouveau profil et de le désigner au périphérique mobile (iOS MDM) ou à la boîte aux lettres (Exchange ActiveSync). La modification des profils existants et leur désignation aux boîtes aux lettres est toujours disponible.

Administration des applications

Il est impossible de lancer les tâches d'installation et de suppression des mises à jour. Toutes les tâches lancées avant l'expiration de la licence sont exécutées jusqu'à la fin mais les dernières mises à jour ne sont pas installées. Par exemple, si avant l'expiration de la licence, la tâche d'installation des mises à jour critiques a été lancée, les mises à jour critiques trouvées avant l'expiration de la licence seront installées uniquement.

Le lancement et la modification des tâches de synchronisation, de recherche de vulnérabilités et de mise à jour de la base des vulnérabilités sont toujours disponibles. Les restrictions ne s'imposent pas aussi sur la consultation, la recherche et le classement des enregistrements dans la liste des vulnérabilités et des mises à jour.

Installation à distance des systèmes d'exploitation et des applications

Il est impossible de lancer les tâches de prise et d'installation de l'image du système d'exploitation. Les tâches lancées avant l'expiration de la licence sont exécutées jusqu'à la fin.

Administration d'accès dans le réseau

L'agent NAC et NAC sont permutés en mode "Désactivé" sans la possibilité d'activation.

Inventaire du matériel

La collecte des informations sur les nouveaux périphériques n'est pas disponible à l'aide de NAC et du Serveur des périphériques mobiles. Avec cela, les informations sur les ordinateurs et les périphériques connectés s'actualisent.

Les notifications sur la modification de la configuration des périphériques ne fonctionnent pas.

La liste du matériel est disponible à la consultation et à la modification manuelle.

Administration des groupes des applications sous licence

Il est impossible d'ajouter une nouvelle clé.

Les notifications sur les dépassements des restrictions sur l'utilisation des clés ne sont pas envoyées.

Connexion à distance aux postes clients

La connexion à distance aux postes clients n'est pas disponible.

Sécurité antivirus

L'Antivirus utilise les bases installées avant l'expiration de la licence.

A PROPOS DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale pour Kaspersky Security Center. Le code d'activation est une suite unique de 20 caractères alphanumériques au format XXXXX-XXXXX-XXXXX-XXXXX.

Pour activer l'application à l'aide du code d'activation, il faut se connecter au serveurs d'activation de Kaspersky Lab via Internet. Si la connexion aux serveurs d'activation et l'accès à Internet sont absents, l'activation de l'application est exécutée à l'aide du fichier clé (cf. section "A propos du fichier clé" à la page 40).

Le décompte de la durée de validité de la licence débute à partir du jour où l'application a été activée. Si vous avez acheté une licence autorisant l'utilisation de Kaspersky Security Center sur plusieurs appareils, le décompte de la durée de validité débute à partir du jour de la première utilisation du code d'activation.

En cas de perte ou de suppression accidentelle du code d'activation après l'activation de l'application, contactez le Support Technique de Kaspersky Lab pour le récupérer.

A PROPOS DU FICHIER CLE

Le *fichier clé est un* fichier de type xxxxxxx.key.

Le fichier clé est utilisé pour activer l'application. Le fichier clé contient toutes les informations nécessaires pour l'activation. Lors du processus d'activation à l'aide du fichier clé, la connexion au serveurs d'activation et l'accès à Internet ne sont pas requis.

Pour obtenir le fichier clé ou pour le restaurer après une suppression accidentelle vous pouvez envoyer une demande au Support Technique (cf. section "Contacter le Support Technique" à la page 160).

Le fichier clé contient les informations suivantes :

- La clé est une séquence unique de chiffres et de lettres. La clé peut être utilisée, par exemple, pour obtenir l'assistance technique de Kaspersky Lab.
- Les restrictions sur l'utilisation de l'application. Jusqu'à trois restrictions peuvent être indiquées dans le fichier clé de Kaspersky Security Center : nombre de Serveurs d'administration virtuels, nombre d'ordinateurs administrés et nombre de périphériques mobiles administrés. Le type de restriction est défini par la licence actuelle (cf. section "Options de licence de Kaspersky Security Center" à la page 37).
- La date de création du fichier clé est la date de création du fichier clé sur le serveur d'activation.
- La durée de validité de la licence est la durée prévue d'utilisation de l'application dans le Contrat de licence, calculée à partir de la date de la première activation de l'application à l'aide de ce fichier clé (par exemple, 1 an).

  La licence expire à la fin de la validité du fichier clé à l'aide duquel l'application a été activée.

- Le délai de validité du fichier clé est le délai défini à compter de la date de création du fichier clé. La durée de validité du fichier clé peut être de plusieurs années. L'activation de l'application à l'aide de ce fichier de clé est possible uniquement avant l'expiration de ce délai.

  Le délai de validité du fichier clé est automatiquement considéré comme expiré à partir de l'expiration de la licence d'utilisation de l'application activée à l'aide de ce fichier clé.

A PROPOS DES DONNEES

En acceptant les conditions du Contrat de licence, vous acceptez de transmettre automatiquement les informations sur les volumes de contrôle des fichiers traités (MD5), les informations pour définir la réputation de l'URL, ainsi que les données sur la protection contre le courrier indésirable. Vous acceptez aussi la collecte et la transfert des informations (depuis les postes clients sous Kaspersky Security Center) en provenance des moyens logiciels et des codes de retour obtenus après l'installation de ces moyens logiciels. Les informations transmises depuis les postes clients seront utilisées pour éliminer les problèmes dans le logiciel ou pour modifier sa fonctionnalité.

Toutes les informations obtenues ne contiennent aucunes données personnelles ou autres informations confidentielles. Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Pour plus d'informations sur la présentation des données, visitez notre site Internet http://support.kaspersky.com/fr et dans le Règlement sur Kaspersky Security Network livré avec l'application.

ASSISTANT DE CONFIGURATION INITIALE

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale de Kaspersky Security Center.

L'application Kaspersky Security Center offre la possibilité de configurer uniquement un ensemble minimum de paramètres indispensables à l'établissement d'un système d'administration centralisée de la protection. Il s'agit de l'Assistant de configuration initiale. Pendant le fonctionnement de l'Assistant, les modifications suivantes dans l'application sont :

- Ajout des clés ou des codes à diffuser automatiquement sur les ordinateurs dans les groupes d'administration.
- Configuration de l'interaction avec Kaspersky Security Network (KSN). KSN permet de recevoir les informations sur les applications installées sur les ordinateurs administrés. Ces informations se trouvent dans les bases de réputation de Kaspersky Lab. Si vous avez autorisé l'utilisation de KSN, l'Assistant active le service KSN Proxy qui assure l'interaction entre KSN et les postes clients.
- Composition des paramètres de diffusion des notifications par courrier électronique sur les événements survenus pendant l'utilisation du Serveur d'administration et des applications administrées (afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les ordinateurs le Messenger doit être lancé).
- Configuration des paramètres des mises à jour et de correction des vulnérabilités des applications installées sur les postes clients.
- Pour le niveau supérieur de la hiérarchie des ordinateurs administrés, les stratégies de protection des postes de travail et des serveurs, ainsi que les tâches de recherche de virus, de récupération des mises à jour et de copie de sauvegarde des données se composent.

> L'Assistant de configuration initiale crée les stratégies de protection uniquement pour les applications pour lesquelles ces stratégies ne sont pas encore présentées dans le dossier **Ordinateurs administrés**. L'Assistant de configuration initiale ne crée pas les tâches si les tâches avec de tels noms ont déjà été formées pour le niveau supérieur de la hiérarchie des ordinateurs administrés.

L'invitation à lancer l'Assistant de configuration initiale est affichée lors de la première connexion au Serveur d'administration après son installation. L'Assistant de configuration initiale peut être lancé à la main à l'aide du menu contextuel de l'entrée **Serveur d'administration <Nom de l'ordinateur>**.

VOIR EGALEMENT

Interaction du Serveur d'administration avec le service KSN Proxy.....57

NOTIONS PRINCIPALES

Cette section contient les définitions détaillées des notions principales, concernant Kaspersky Security Center.

DANS CETTE SECTION

SERVEUR D'ADMINISTRATION

Les modules de Kaspersky Security Center permettent de réaliser l'administration centralisée des applications de Kaspersky Lab installées sur les postes clients.

Les ordinateurs, sur lesquels le module Serveur d'administration est installé, s'appellent les *Serveurs d'administration* (ci-après aussi *Serveurs*).

Le Serveur d'administration s'installe sur l'ordinateur en qualité de service avec la sélection d'attributs suivante :

- sous le nom "Serveur d'administration de Kaspersky Security Center" ;
- avec lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte **Système local** ou le compte utilisateur selon la sélection effectuée lors de l'installation du Serveur d'administration.

Le Serveur d'administration exécute les fonctions suivantes :

- sauvegarde de la structure des groupes d'administration ;
- sauvegarde des informations sur la configuration des postes clients ;
- gestion des stockages des distributifs des applications ;
- installation à distance des applications sur les périphériques clients et suppression des applications ;
- mise à jour des bases et des modules des applications de Kaspersky Lab ;
- administration des stratégies et des tâches sur les postes clients ;
- sauvegarde des informations sur les événements survenus sur les périphériques clients ;
- formation des rapports sur le fonctionnement des applications de Kaspersky Lab ;

- extension des clés sur les périphériques clients, sauvegarde des informations sur les licences ;
- envoi des notifications sur l'exécution en cours de la tâche (par exemple, des virus détectés sur le poste client).

HIERARCHIE DES SERVEURS D'ADMINISTRATION

Les Serveurs d'administration peuvent développer une hiérarchie du type "serveur principal – serveur secondaire". Chaque Serveur d'administration peut avoir plusieurs Serveurs d'administration secondaires (ci-après *Serveurs secondaires*) aux différents niveaux d'hiérarchie. Le niveau d'intégration des Serveurs secondaires n'est pas limité. De plus, les postes clients de tous les Serveurs secondaires feront partie des groupes d'administration du Serveur principal. De cette façon, les participants du réseau informatique indépendants peuvent être administrés par différents Serveurs d'administration qui, à leur tour, sont administrés par le Serveur principal.

Le cas particulier des Serveurs d'administration secondaires : les *Serveurs d'administration virtuels* (cf. section "Serveur d'administration virtuel" à la page 43).

La hiérarchie des Serveurs d'administration peut être utilisée pour remplir les objectifs suivants :

- Limiter la charge sur le Serveur d'administration (par rapport à un Serveur installé sur le réseau).
- Diminuer le trafic sur le réseau et simplifier le travail sur les bureaux distants. Il n'est pas nécessaire d'établir de connexion entre le Serveur principal et tous les ordinateurs du réseau qui peuvent se trouver par exemple dans d'autres régions. Il suffit d'installer dans chaque segment du réseau un Serveur d'administration secondaire, de répartir les ordinateurs dans les groupes d'administration des Serveurs secondaires et fournir aux Serveurs secondaires une connexion au Serveur principal par des canaux de liaisons rapides.
- La répartition des responsabilités entre les administrateurs de la sécurité antivirus. En outre, toutes les possibilités d'administration centralisée et de surveillance de la sécurité antivirus du réseau de l'entreprise seront maintenues.
- L'utilisation de Kaspersky Security Center par les prestataires de services. Il suffit au prestataire de services d'installer Kaspersky Security Center et Kaspersky Security Center Web-Console. Pour gérer un grand nombre de postes clients des entreprises différentes, le prestataire de services peut inclure dans une hiérarchie des Serveurs d'administration les Serveurs d'administration virtuels.

Chaque ordinateur inclus dans la hiérarchie du groupe d'administration peut être connecté à un seul Serveur d'administration. Il vous faut vérifier la connexion des ordinateurs aux Serveurs d'administration. Pour ce faire, vous pouvez utiliser la fonction de recherche d'ordinateurs selon les attributs de réseau dans les groupes d'administration des différents Serveurs.

SERVEUR D'ADMINISTRATION VIRTUEL

Serveur d'administration virtuel (ci-après *Serveur virtuel*) – le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection antivirus du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport au Serveur d'administration physique, possède des restrictions suivantes :

- Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie du Serveur d'administration principal.
- Le Serveur d'administration virtuel utilise pour le travail les bases de données du Serveur d'administration principal : les tâches de copie de sauvegarde et de restauration de données, les tâches d'analyse et de réception des mises à jour ne sont pas prises en charge sur le Serveur virtuel. Ces tâches se résolvent dans le cadre du Serveur d'administration principal.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge pour le Serveur virtuel.

De plus, le Serveur d'administration virtuel possède des restrictions suivantes :

- Dans la fenêtre des propriétés du Serveur virtuel, l'ensemble de sections est limité.
- Pour une installation à distance des applications de Kaspersky Lab sur les postes clients fonctionnant sous l'administration du Serveur virtuel, il faut que l'Agent d'administration soit installé sur un des postes clients pour la connexion au Serveur virtuel. Lors de la première connexion au Serveur virtuel, cet ordinateur est automatiquement désigné en tant qu'agent de mises à jour et exécute le rôle de la passerelle des connexions des postes clients avec le Serveur virtuel.
- Le Serveur virtuel peut sonder le réseau uniquement par les agents de mises à jour.
- Pour redémarrer le Serveur virtuel la productivité duquel a été perturbée, Kaspersky Security Center redémarre le Serveur d'administration principal et tous les Serveurs virtuels.

L'administrateur du Serveur virtuel possède tous les privilèges dans le cadre de ce Serveur virtuel.

SERVEUR DES PERIPHERIQUES MOBILES

Le *Serveur des périphériques mobiles* est un module de Kaspersky Security Center qui offre l'accès aux périphériques mobiles et permet de les administrer via Console d'administration. Le Serveur des périphériques mobiles exécute la collecte des informations sur les périphériques mobiles, ainsi que l'enregistrement de leurs profils.

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. Ce Serveur des périphériques mobiles est utilisé pour administrer les périphériques mobiles qui prennent en charge le service Apple Push Notifications (APNs).

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.

AGENT D'ADMINISTRATION. GROUPE D'ADMINISTRATION

L'interaction entre le Serveur d'administration et les postes clients s'opère via le module *Agent d'administration* de l'application Kaspersky Security Center. L'Agent d'administration doit être installé sur tous les postes clients où l'administration des applications de Kaspersky Lab se réalise à l'aide de Kaspersky Security Center.

L'Agent d'administration exécute les fonctions suivantes :

- affiche les informations sur l'état actuel des applications ;
- envoie et reçoit les commandes d'administration ;
- synchronise les informations de configuration ;

- envoi au Serveur d'administration des informations sur les événements survenus sur les postes clients ;
- assure le fonctionnement de l'*agent de mises à jour*.

L'Agent d'administration s'installe sur l'ordinateur en tant que service avec la sélection d'attributs suivante :

- sous le nom "Agent d'administration de Kaspersky Security Center" ;
- avec le lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte **Système local**.

Le plug-in pour le fonctionnement avec Cisco® 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. Les paramètres de collaboration avec Cisco NAC sont indiqués dans la fenêtre des propriétés du Serveur d'administration.

En collaboration avec Cisco NAC, le Serveur d'administration joue le rôle d'un serveur standard des stratégies (Posture Validation Server), que l'administrateur peut utiliser pour autoriser ou interdire l'accès à un ordinateur du réseau (en fonction des conditions de la protection antivirus).

L'ordinateur, le serveur ou le poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab s'appelleront le *client du Serveur d'administration* (ci-après *poste client* ou *ordinateur*).

La multitude des ordinateurs du réseau de l'entreprise peut être divisée en groupes, qui créent une hiérarchie de la structure. De tels groupes s'appellent les *groupes d'administration*. La hiérarchie des groupes d'administration est affichée dans l'arborescence de la console dans la section du Serveur d'administration.

Groupe d'administration (ci-après groupe) : c'est l'ensemble des postes clients, réunis selon un critère dans le but d'administrer les ordinateurs en tant que groupe unique. Pour tous les postes clients dans le groupe, les éléments suivants sont installés :

- les paramètres uniques de fonctionnement des applications, à l'aide *des stratégies de groupe* ;
- un mode unique de fonctionnement des applications, grâce à la création de *tâches de groupe* avec l'ensemble établi des paramètres (par exemple : création et installation du *paquet d'installation* unique, mise à jour des bases et des modules d'applications, analyse de l'ordinateur à la demande et protection en temps réel).

Le poste client peut être inclus dans un seul groupe d'administration.

Vous pouvez créer une hiérarchie des Serveurs et des groupes de n'importe quel degré de complexité. Les Serveurs d'administration secondaires et virtuels, les groupes et les postes clients peuvent se trouver à un niveau de la hiérarchie.

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Les ordinateurs, sur lesquels le module *Console d'administration* est installé, s'appellent les *postes administrateurs*. A partir de ces ordinateurs, les administrateurs peuvent administrer à distance de manière centralisée les applications de Kaspersky Lab installées sur les postes clients.

Après avoir installé la Console d'administration sur l'ordinateur, dans le menu **Démarrer** → **Applications** → **Kaspersky Security Center**, l'icône de son lancement s'affiche.

Aucune restriction n'est imposée sur le nombre de postes administrateurs. Depuis chaque poste administrateur, il est possible d'administrer les groupes d'administration de plusieurs Serveurs d'administration dans le réseau. Le poste administrateur peut être connecté au Serveur d'administration (physique et virtuel) de n'importe quel niveau d'hiérarchie.

Le poste administrateur peut être inclus dans le groupe d'administration en tant que poste client.

Dans le cadre des groupes d'administration de n'importe quel Serveur d'administration, le même ordinateur peut être simultanément client du Serveur d'administration, Serveur d'administration et poste de l'administrateur.

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

L'administration des applications de Kaspersky Lab via la Console d'administration s'exécute à l'aide du module spécial : le *plug-in d'administration de l'application*. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Security Center.

Le plug-in d'administration de l'application s'installe sur le poste administrateur. A l'aide du plug-in d'administration de l'application, il est possible d'exécuter les actions suivantes dans la Console d'administration :

- créer et modifier les stratégies et les paramètres de l'application, ainsi que les paramètres des tâches de cette application ;
- obtenir les informations sur les tâches de l'application, sur les événements dans son fonctionnement, et sur les statistiques de fonctionnement de l'application obtenues depuis les postes clients.

STRATEGIES, PARAMETRES DE L'APPLICATION ET TACHES

L'action concrète, exécutée par l'application de Kaspersky Lab, porte le nom *la tâche*. Selon les fonctions exécutées, les tâches sont divisées par *types*.

L'ensemble des paramètres de fonctionnement de l'application lors de son exécution correspond à une tâche. L'ensemble des paramètres de fonctionnement de l'application, unique pour tous les types de ses tâches, compose les paramètres de l'application. Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches, constituent les paramètres de la tâche.

La description détaillée des types de tâches pour chaque application de Kaspersky Lab est présentée dans les manuels.

Nous appellerons *paramètres locaux de l'application* les paramètres de l'application qui sont définis pour le poste client particulier par l'interface locale, ou à distance par la Console d'administration.

La configuration centralisée des paramètres de fonctionnement des applications installées sur les postes clients s'opère à l'aide de la définition de stratégies.

La *Stratégie* est un ensemble de paramètres de fonctionnement de l'application. Cet ensemble est défini pour le groupe d'administration. La stratégie ne définit pas tous les paramètres de l'application.

Plusieurs stratégies avec les valeurs différentes des paramètres peuvent être définies pour une application, mais une seule stratégie pour l'application peut être active.

Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre pour l'application peut être créée dans chaque groupe.

Les paramètres de l'application sont définis par les paramètres des stratégies et des tâches.

Les sous-groupes et les Serveurs d'administration secondaires héritent des tâches de groupe des niveaux plus élevés de la hiérarchie. La tâche, définie pour le groupe, sera exécutée non seulement sur les postes clients inclus dans ce groupe, mais aussi sur les postes clients inclus dans les sous-groupes et dans les Serveurs d'administration secondaires aux niveaux suivants de la hiérarchie.

Chaque paramètre, présenté dans la stratégie, a pour attribut le "cadenas" :  . Le "cadenas" affiche, s'il est interdit de modifier le paramètre dans les stratégies du niveau intégré de la hiérarchie (pour les groupes intégrés et pour les Serveurs d'administration secondaires). Il en est de même pour les paramètres des tâches et les paramètres locaux de l'application. Si dans la stratégie, le "cadenas" est placé pour le paramètre, il sera impossible de prédéfinir sa valeur (cf. section "Corrélation de stratégie et des paramètres locaux de l'application" à la page 47).

Si dans la fenêtre des propriétés de la stratégie héritée vous décochez la case **Hériter des paramètres de la stratégie de niveau supérieur** située dans le groupe **Héritage des paramètres** de la section **Général**, l'action du "cadenas" pour cette stratégie sera annulée.

Il y a la possibilité d'activer la stratégie qui n'est pas active, selon l'événement. Cela permet, par exemple, d'installer des paramètres plus stricts de la protection antivirus dans les périodes de l'épidémie de virus.

Vous pouvez aussi former la stratégie pour les utilisateurs autonomes.

La création et la configuration des tâches pour les objets administrées par un Serveur d'administration s'effectuent de manière centralisée. Les tâches des types suivants peuvent être définies :

- *la tâche de groupe* : tâche qui définit les paramètres de fonctionnement de l'application installés sur les ordinateurs et inclus dans le groupe d'administration ;
- *la tâche locale* : tâche pour un ordinateur individuel ;
- *la tâche pour la sélection d'ordinateurs* : tâche pour la sélection aléatoire d'ordinateurs, qu'ils soient ou non compris dans le groupe d'administration ;
- *la tâche du Serveur d'administration* : la tâche, qui est définie directement pour le Serveur d'administration.

Une tâche de groupe peut être définie pour un groupe, même si l'application de Kaspersky Lab n'est pas installée sur tous les postes clients du groupe. Dans ce cas, la tâche de groupe s'exécute uniquement pour les ordinateurs sur lesquels l'application indiquée est installée.

Les tâches créées pour le poste client d'une manière locale sont exécutées uniquement pour cet ordinateur. Lors de la synchronisation du poste client avec le Serveur d'administration, les tâches locales seront ajoutées à la liste des tâches formées pour le poste client.

Puisque les paramètres de fonctionnement de l'application sont définis par la stratégie, les paramètres qui ne sont pas interdits peuvent être redéfinis, ainsi que les paramètres qui peuvent être installés uniquement pour l'exemplaire concret de la tâche. Par exemple, pour la tâche d'analyse du disque, il s'agit du nom du disque et des masques des fichiers analysés.

La tâche peut être lancée automatiquement (selon la planification) ou manuellement. Les résultats de l'exécution de la tâche sont enregistrés sur le Serveur d'administration et de manière locale. L'administrateur peut recevoir des notifications sur l'exécution de telle ou telle tâche, ainsi que parcourir les rapports détaillés.

Les informations sur les stratégies, les paramètres de l'application, les paramètres des tâches pour les sélections d'ordinateurs et les tâches de groupe sont enregistrées sur le Serveur et diffusées sur les postes clients lors de la synchronisation. Avec cela, le Serveur d'administration enregistre les informations sur les modifications locales autorisées par la stratégie et réalisées sur les postes clients. En outre, la liste des applications qui fonctionnent sur le client est actualisée, ainsi que leur état et la liste des tâches formées.

CORRELATION DE LA STRATEGIE ET DES PARAMETRES LOCAUX DE L'APPLICATION

A l'aide des stratégies, les mêmes valeurs des paramètres de fonctionnement de l'application peuvent être installées pour tous les ordinateurs inclus dans le groupe.

Vous pouvez redéfinir les valeurs des paramètres définies par la stratégie pour les ordinateurs individuels dans le groupe à l'aide des paramètres locaux de l'application. Avec cela, vous pouvez établir les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie (le paramètre n'est pas fermé par le "cadenas").

La valeur du paramètre, utilisée par l'application sur le poste client (cf. ill. ci-dessous), est définie par la présence du "cadenas" dans le paramètre de la stratégie :

- Si la modification du paramètre est interdite, la même valeur est utilisée sur tous les postes clients : définie par la stratégie.

- Si ce n'est pas interdit, l'application n'utilise alors pas la valeur qui est indiquée dans la stratégie sur chaque poste client, mais la valeur locale du paramètre. Cela dit, la valeur du paramètre peut être modifiée par les paramètres locaux de l'application.

Illustration 12. Stratégie et paramètres locaux de l'application

De cette façon, lorsque la tâche est en exécution sur un poste client, l'application utilise les paramètres définis selon deux manières différentes :

- par les paramètres de la tâche et les paramètres locaux de l'application, si l'interdiction de modifier le paramètre n'était pas établie dans la stratégie ;
- par la stratégie du groupe, si l'interdiction de modifier le paramètre était établie dans la stratégie.

Les paramètres locaux de l'application sont modifiés après la première utilisation de la stratégie conformément aux paramètres de la stratégie.

ADMINISTRATION DES SERVEURS D'ADMINISTRATION

Cette section contient les informations sur l'utilisation des Serveurs d'administration et sur la configuration des paramètres du Serveur d'administration.

DANS CETTE SECTION

CONNEXION AU SERVEUR D'ADMINISTRATION ET PERMUTATION ENTRE LES SERVEURS D'ADMINISTRATION

Lors du lancement, l'application Kaspersky Security Center tente de se connecter au Serveur d'administration. S'il existe plusieurs Serveurs d'administration sur votre réseau, l'application se connectera au Serveur utilisé lors d'une session précédente de Kaspersky Security Center.

Lors du premier démarrage de l'application après l'installation, une tentative de connexion au Serveur d'administration, indiqué lors de l'installation de Kaspersky Security Center, s'exécute.

Après la connexion au Serveur d'administration, la structure des dossiers de ce Serveur s'affiche dans l'arborescence de la console.

Si plusieurs Serveurs d'administration ont été ajoutés dans l'arborescence de la console, vous pouvez se déplacer entre eux.

Pour se connecter à un autre Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Se connecter au Serveur d'Administration**.
3. Dans la fenêtre ouverte **Paramètres de connexion** dans le champ **Adresse du serveur**, indiquez le nom du Serveur d'administration auquel vous voulez se connecter. En tant que le nom du Serveur d'administration, vous pouvez indiquer l'adresse IP ou le nom de l'ordinateur dans le réseau Windows. En cliquant sur le bouton **Avancé** dans la partie inférieure de la fenêtre, vous pouvez configurer les paramètres de connexion au Serveur d'administration (cf. ill. ci-après).

Pour vous connecter au Serveur d'administration à travers un port différent du port par défaut, indiquez, dans le champ **Adresse du serveur** la valeur au format <Nom du Serveur d'administration>:<Port>.

Les utilisateurs qui ne jouissent pas des privilèges de **Lecture** ne pourront pas accéder au Serveur d'administration.

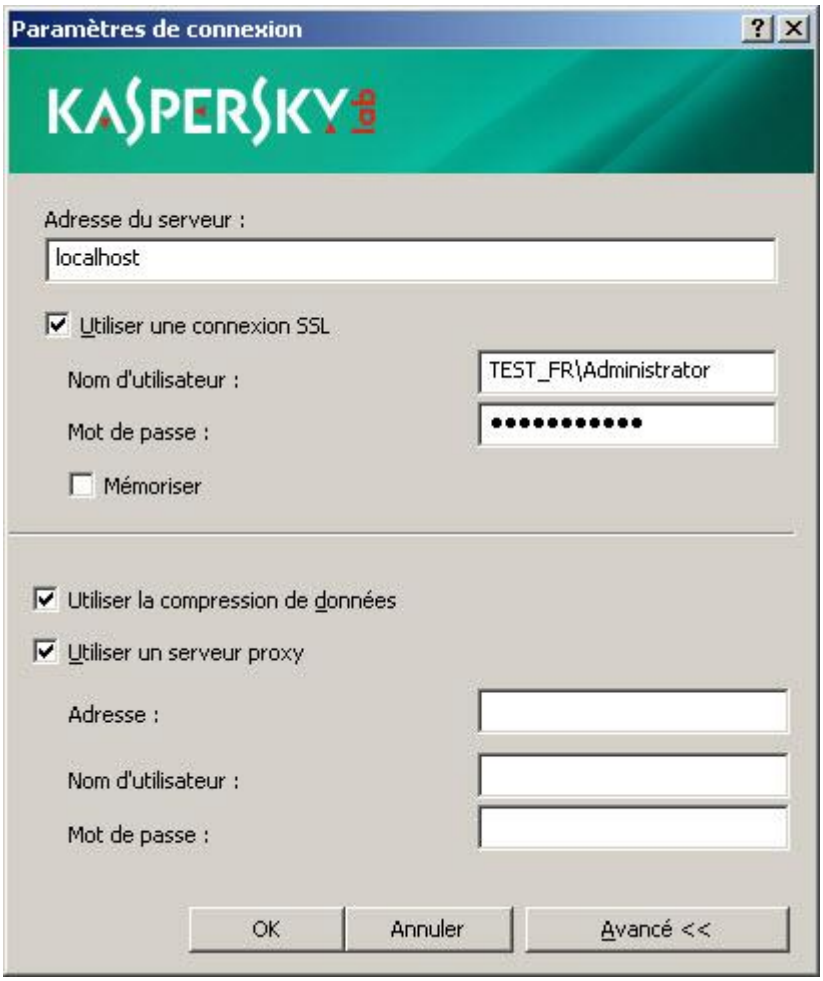

Illustration 13. Etablissement de la connexion au Serveur d'administration

4. Cliquez sur le bouton **OK** pour terminer la permutation entre les Serveurs.

Après la connexion au Serveur d'administration, la structure des dossiers de l'entrée correspondante est actualisée dans l'arborescence de la console.

PRIVILEGES D'ACCES AU SERVEUR D'ADMINISTRATION ET A SES OBJETS

Lors de l'installation de Kaspersky Security Center, les groupes d'utilisateurs **KLAdmins** et **KLOperators** sont automatiquement formés. Ces groupes possèdent des privilèges de connexion au Serveur d'administration et de fonctionnement avec ses objets.

Selon le compte utilisateur sous lequel l'installation de Kaspersky Security Center se déroule, les groupes **KLAdmins** et **KLOperators** sont créés de la manière suivante :

- Si l'installation se déroule sous le compte utilisateur, appartenant au domaine, alors les groupes sont créés dans le domaine, incluant le Serveur d'administration, et sur le Serveur d'administration.

- Si l'installation se déroule sous le compte du système, les groupes sont créés uniquement sur le Serveur d'administration.

La consultation des groupes **KLAdmins** et **KLOperators** et l'insertion des modifications nécessaires dans les privilèges d'utilisateurs des groupes **KLAdmins** et **KLOperators** peut être réalisée à l'aide des outils standards d'administration du système d'exploitation.

Tous les privilèges sont accordés au groupe **KLAdmins** et au groupe **KLOperators** : les privilèges sur **Lecture** et **Exécution**. L'ensemble des droits présentés dans le groupe **KLAdmins** n'est pas disponible à la modification.

Les utilisateurs du groupe **KLAdmins** portent le nom : *les administrateurs de Kaspersky Security Center*, les utilisateurs du groupe **KLOperators** – *les opérateurs de Kaspersky Security Center*.

Outre les utilisateurs du groupe **KLAdmins**, les privilèges d'administrateur de Kaspersky Security Center sont accordés aux administrateurs locaux des ordinateurs sur lesquels le Serveur d'administration est installé.

Il est possible d'exclure les administrateurs locaux de la liste des utilisateurs qui possèdent les privilèges d'administrateur de Kaspersky Security Center.

Toutes les opérations lancées par les administrateurs de Kaspersky Security Center sont exécutées avec les privilèges du compte du Serveur d'administration.

Pour chaque Serveur d'administration dans le réseau, un propre groupe **KLAdmins** peut être formé. Ce groupe possédera des privilèges uniquement dans le cadre du travail avec ce Serveur.

Si les ordinateurs appartiennent au même domaine et font partie des groupes d'administration de Serveurs différents, l'administrateur est l'administrateur de Kaspersky Security Center dans le cadre de tous ces groupes d'administration. Le groupe **KLAdmins** est unique pour ces groupes d'administration et est créé lors de l'installation du premier Serveur d'administration. Les opérations lancées par l'administrateur Kaspersky Security Center sont exécutées avec les privilèges du compte du Serveur d'administration pour lequel elles ont été lancées.

Après l'installation de l'application, l'administrateur Kaspersky Security Center peut procédez comme suit :

- Modifier les privilèges accordés aux groupes **KLOperators** ;

- Définir les privilèges d'accès aux fonctions de l'application Kaspersky Security Center aux autres groupes d'utilisateurs et aux utilisateurs particuliers enregistrés sur le poste d'administrateur ;

- Définir les privilèges d'accès des utilisateurs au travail dans chaque groupe d'administration.

L'administrateur de Kaspersky Security Center peut établir les privilèges d'accès à chaque groupe d'administration ou aux autres objets du Serveur d'administration dans la section **Sécurité** de la fenêtre des propriétés de l'objet sélectionné.

Vous pouvez surveiller les actions de l'utilisateur à l'aide des enregistrements sur les événements survenu pendant le fonctionnement du Serveur d'administration. Les enregistrements sur les événements s'affichent dans l'arborescence de la console dans le dossier **Evénements** dans le sous-dossier **Audit des événements**. Ces événements possèdent le degré d'importance **Message d'information**, les types d'événement commencent par le mot **Audit**.

CONDITIONS DE CONNEXION AU SERVEUR D'ADMINISTRATION VIA INTERNET

Si le Serveur d'administration est un serveur à distance, c'est-à-dire il se trouve en dehors du réseau d'entreprise, les postes clients se connectent à lui via Internet. Pour la connexion des postes clients au Serveur d'administration via Internet, il est nécessaire d'exécuter les conditions suivantes :

- Le Serveur d'administration à distance doit posséder l'adresse IP externe, et sur cette adresse les ports entrants 13000 et 14000 doivent être ouverts.
- L'installation de l'Agent d'administration est préalablement requise sur les postes clients.
- Lors de l'installation de l'Agent d'administration sur les postes clients, l'adresse IP externe du Serveur d'administration à distance doit être indiquée. Si pour l'installation, le paquet d'installation est utilisé, alors l'adresse IP doit être indiquée manuellement dans les propriétés du paquet d'installation dans la section **Paramètres**.
- Pour administrer les applications et les tâches du poste client à l'aide du Serveur d'administration à distance, il faut cocher la case **Maintenir la connexion au Serveur d'administration** dans la fenêtre des propriétés de cet ordinateur dans la section **Général**. Après avoir coché la case, il faut attendre la synchronisation avec le poste client distant. La connexion permanente avec le Serveur d'administration peut prendre en charge pas plus de 100 postes clients en même temps.

Pour accélérer l'exécution des tâches reçues depuis le Serveur d'administration à distance, vous pouvez ouvrir sur les postes clients le port 15000. Dans ce cas pour lancer une tâche, le Serveur d'administration envoie un paquet spécial à l'Agent d'administration par le port 15000 sans attendre la synchronisation avec le poste client.

CONNEXION SECURISEE AU SERVEUR D'ADMINISTRATION

L'échange des informations entre les postes clients et le Serveur d'administration, ainsi que la connexion de la Console d'administration au Serveur d'administration peuvent être exécutées en utilisant le protocole SSL (Secure Socket Layer). Le protocole SSL permet d'identifier les parties, qui coopèrent lors de la connexion, de chiffrer les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérants et le chiffrement des données par clés ouvertes sont à la base du protocole SSL.

DANS CETTE SECTION

CERTIFICAT DU SERVEUR D'ADMINISTRATION

L'authentification du Serveur d'administration lors de la connexion de la Console d'administration et de l'échange des informations avec les postes clients s'effectue selon le *certificat du Serveur d'Administration*. Le certificat est utilisé pour l'authentification lors de l'établissement de la connexion entre les Serveurs d'administration principaux et secondaires.

Le certificat du Serveur d'administration est automatiquement créé en cours de l'installation du module Serveur d'administration et sauvegardé dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Le certificat du Serveur d'administration n'est créé qu'une seule fois, à l'installation du Serveur d'administration. Dans le cas où le certificat du Serveur d'administration serait perdu, il est nécessaire pour le restaurer de réinstaller le composant du serveur d'administration et de restaurer les données.

AUTHENTIFICATION DU SERVEUR D'ADMINISTRATION LORS DE L'UTILISATION DE L'ORDINATEUR

Lors de la première connexion du poste client au Serveur d'administration, l'Agent d'administration sur le poste client reçoit une copie du certificat du Serveur d'administration et le sauvegarde localement.

Lors de l'installation locale de l'Agent d'administration sur le poste client, le certificat du Serveur d'administration peut être sélectionné à la main.

Selon la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée au cours des connexions ultérieures.

Par la suite, lors de chaque connexion du poste client au Serveur d'administration, l'Agent d'administration demandera le certificat du Serveur d'administration et le comparera avec sa copie locale. S'ils ne concordent pas, l'accès du Serveur d'administration au poste client sera interdit.

AUTHENTIFICATION DU SERVEUR LORS DE LA CONNEXION DE LA CONSOLE D'ADMINISTRATION

Lors de la première connexion au Serveur d'administration, la Console d'administration demande le certificat du Serveur d'administration et sauvegarde sa copie localement sur le poste administrateur. Selon la copie reçue du certificat, au cours des connexions suivantes de la Console d'administration au Serveur d'administration, l'identification du Serveur d'administration sera exécutée.

Si le certificat du Serveur d'administration ne concorde pas avec la copie du certificat sauvegardée sur le poste administrateur, la Console d'administration affiche une demande afin de pouvoir confirmer la connexion au Serveur d'administration portant le nom attribué et d'obtenir un nouveau certificat. Après la connexion, la Console d'administration sauvegardera la copie du nouveau certificat du Serveur d'administration. Elle sera utilisée ultérieurement pour identifier le Serveur.

SE DECONNECTER DU SERVEUR D'ADMINISTRATION

Pour se déconnecter du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.
2. Sélectionnez l'option **Se déconnecter du Serveur d'administration** dans le menu contextuel de l'entrée.

AJOUT D'UN SERVEUR D'ADMINISTRATION A L'ARBORESCENCE DE LA CONSOLE

Pour ajouter un Serveur d'administration à l'arborescence de la console, procédez comme suit :

1. Dans la fenêtre principale de l'application Kaspersky Security Center, sélectionnez l'entrée **Kaspersky Security Center** dans l'arborescence de la console.
2. Dans le menu contextuel, sélectionnez l'option **Créer** → **Serveur d'administration**.

Une entrée appelée **Serveur d'administration - <nom de l'ordinateur> (Non connecté)** apparaîtra dans l'arborescence de console. Utilisez cette entrée pour la connecter à n'importe quel Serveur installé sur votre réseau des Serveurs d'administration.

SUPPRESSION D'UN SERVEUR D'ADMINISTRATION DE L'ARBORESCENCE DE CONSOLE

Pour supprimer un Serveur d'administration de l'arborescence de la console, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration à supprimer.
2. Sélectionnez l'option **Supprimer** dans le menu contextuel de l'entrée.

CHANGEMENT DU COMPTE DU SERVICE DU SERVEUR D'ADMINISTRATION. UTILITAIRE KLSRVSWCH

S'il vous faut modifier le compte du service du Serveur d'administration, défini lors de l'installation de l'application Kaspersky Security Center, vous pouvez utiliser l'utilitaire de changement du compte du service du Serveur d'administration klsrvswch.

Lors de l'installation de Kaspersky Security Center, l'utilitaire est automatiquement copiée dans le dossier d'installation de l'application.

Le nombre de lancements de l'utilitaire est illimité.

Pour modifier le compte du service du Serveur d'administration, procédez comme suit :

1. Lancez l'utilitaire klsrvswch depuis le dossier d'installation Kaspersky Security Center.

   Finalement, l'Assistant de changement du compte du service du Serveur d'administration se lance. Suivez les instructions de l'Assistant.

2. La fenêtre **Compte du service du Serveur d'administration** permet de sélectionner une de deux options de définition du compte :

   - **Compte du système local**. Le service du Serveur d'administration se lance 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 service du Serveur d'administration.

   - **Compte d'utilisateur**. Le service du Serveur d'administration se lance sous le compte d'utilisateur inclus dans le domaine. Dans ce cas, le Serveur d'administration initie toutes les opérations avec les privilèges de ce compte.

     Pour sélectionner l'utilisateur dont le compte sera utilisé pour lancer le service du Serveur d'administration, procédez comme suit :

     1. Cliquez sur le bouton **Rechercher** et sélectionnez l'utilisateur dans la fenêtre ouverte **Sélection : "Utilisateur"**.

        Fermez la fenêtre **Sélection : "Utilisateur"** et cliquez sur le bouton **Suivant**.

     2. La fenêtre **Mot de passe du compte** permet de saisir le mot de passe pour le compte de l'utilisateur sélectionné, s'il le faut.

Une fois l'Assistant terminé, le compte du Serveur d'administration se change.

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.

AFFICHAGE ET MODIFICATION DES PARAMETRES DU SERVEUR D'ADMINISTRATION

Vous pouvez configurer les paramètres du Serveur d'administration dans la fenêtre des propriétés du Serveur d'administration.

- *Pour ouvrir la fenêtre Propriété : Serveur d'administration,*

  dans le menu contextuel de l'entrée du Serveur d'administration dans l'arborescence de la console, sélectionnez l'option **Propriété**.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES GENERAUX DU SERVEUR D'ADMINISTRATION

Vous pouvez configurer les paramètres généraux du Serveur d'administration dans les sections **Général**, **Paramètres** et **Sécurité** de la fenêtre des propriétés du Serveur d'administration.

La présence ou l'absence de la section **Sécurité** est définie par les paramètres d'interface de l'utilisateur. Pour inclure l'affichage de cette section, il faut passer dans le menu **Vue** → **Configuration de l'interface** et dans la fenêtre ouverte **Configuration de l'interface**, cocher la case **Afficher les sections avec les paramètres de sécurité**.

CONFIGURATION DES PARAMETRES DU TRAITEMENT DES EVENEMENTS

Vous pouvez consulter la liste des événements survenus lors du fonctionnement de l'application et configurer le traitement des événements dans la section **Evénements** de la fenêtre des propriétés du Serveur d'administration.

Chaque événement possède une caractéristique qui reflète son niveau d'importance. Les événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

CONTROLE DE L'EMERGENCE D'EPIDEMIES DE VIRUS

Kaspersky Security Center vous permet de réagir opportunément à l'apparition des menaces des épidémies de virus. L'évaluation de l'épidémie de virus se réalise par le contrôle de l'activité de virus sur les postes clients.

Vous pouvez configurer les règles d'évaluation d'une épidémie de virus et les actions à exécuter si elle apparaît dans la section **Attaque de virus** de la fenêtre des propriétés du Serveur d'administration.

L'ordre de notification sur l'événement *Attaque de virus* peut être défini dans la section **Evénements** de la fenêtre des propriétés du Serveur d'administration (cf. section "Configuration des paramètres du traitement des événements" à la page 55), dans la fenêtre des propriétés de l'événement *Attaque de virus*.

L'événement *Attaque de virus* se forme à l'origine des événements *Virus détecté* pendant le fonctionnement des applications antivirus. Par conséquent, pour pouvoir identifier une épidémie de virus, les informations sur les événements *Virus détecté* doivent être enregistrées sur le Serveur d'administration.

Les paramètres d'enregistrement des informations sur les événements *Virus détecté* se définissent dans les stratégies des applications antivirus.

Sous le titre *Virus détecté*, les informations en provenance des postes clients du Serveur d'administration principal sont prises en compte. Les informations depuis les Serveurs d'administration ne sont pas prises en compte. Pour chaque Serveur d'administration secondaire, les paramètres de l'événement *Attaque de virus* doivent être configurés individuellement.

RESTRICTION DU TRAFIC

Pour diminuer le trafic dans le réseau, il est possible de limiter la vitesse de transfert des données sur le Serveur d'administration depuis les plages IP ou les intervalles IP en particulier.

Vous pouvez créer et configurer les règles de restriction du trafic dans la section **Trafic** de la fenêtre des propriétés du Serveur d'administration.

CONFIGURATION DE LA COLLABORATION AVEC LE SYSTEME CISCO NETWORK ADMISSION CONTROL (NAC)

Vous pouvez établir les correspondances entre les conditions de protection antivirus des postes clients et les états de sécurité du système Cisco Network Admission Control (NAC).

Pour établir ces correspondances, il faut former les conditions selon lesquelles les postes clients se verront affecter les états de sécurité du système Cisco Network Admission Control (NAC) : *Healthy*, *Checkup*, *Quarantine* ou *Infected*.

Vous pouvez configurer les correspondances entre les états Cisco NAC et les conditions de protection antivirus des postes clients dans la section **Cisco NAC** de la fenêtre des propriétés du Serveur d'administration.

La section **Cisco NAC** s'affiche dans la fenêtre des propriétés du Serveur d'administration si, lors de l'installation de l'application conjointement avec le Serveur d'administration, le module Serveur de stratégies de Kaspersky Lab pour Cisco NAC a été installé (cf. *Manuel d'implantation de Kaspersky Security Center*). Dans le cas contraire, la section **Cisco NAC** ne s'affiche pas dans la fenêtre des propriétés du Serveur d'administration.

INTERACTION DU SERVEUR D'ADMINISTRATION AVEC LE SERVICE KSN PROXY

KSN Proxy est un service assurant l'interaction entre l'infrastructure de Kaspersky Security Network et les postes clients sous l'administration du Serveur d'administration.

L'utilisation de KSN Proxy vous offre les possibilités suivantes :

- Les postes clients peuvent exécuter les demandes à KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès direct à Internet.
- KSN Proxy met en cache les données traitées, en diminuant la charge sur le canal dans le réseau externe et en augmentant l'obtention des informations demandées par le poste client.

Vous pouvez configurer les paramètres de KSN Proxy dans la section **Serveur proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

TRAVAIL AVEC LES UTILISATEURS INTERNES

Les comptes des *utilisateurs internes* sont utilisés pour travailler avec les Serveurs d'administration virtuels. Sous le nom du compte de l'utilisateur interne, l'administrateur du Serveur virtuel permet de lancer Kaspersky Security Center Web-Console pour consulter les informations sur l'état de la protection antivirus du réseau. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieure 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.

Vous pouvez configurer les paramètres des comptes des utilisateurs internes dans la section **Utilisateurs internes** de la fenêtre de propriétés du Serveur d'administration.

La section **Utilisateurs internes** s'affiche dans la fenêtre des propriétés du Serveur d'administration uniquement si le Serveur d'administration est un Serveur virtuel ou s'il contient les Serveurs d'administration virtuels.

ADMINISTRATION DES GROUPES D'ADMINISTRATION

Cette section contient les informations sur le travail avec les groupes d'administration.

Vous pouvez exécuter les actions suivantes avec les groupes d'administration :

- ajouter au groupe d'administration le nombre quelconque des groupes imbriqués de tous les niveaux d'hiérarchie ;
- ajouter au groupe d'administration des postes clients ;
- modifier la hiérarchie des groupes d'administration en déplaçant des postes clients individuels ou des groupes entiers dans d'autres groupes ;
- supprimer d'un groupe d'administration les sous-groupes et les postes clients ;
- ajouter au groupes d'administration des Serveurs d'administration virtuels et secondaires ;
- déplacer les postes clients des groupes d'administration d'un Serveur vers les groupes d'administration d'un autre Serveur ;
- définir les applications de Kaspersky Lab qui seront installées automatiquement sur les postes clients ajoutés au groupe.

DANS CETTE SECTION

CREATION DES GROUPES D'ADMINISTRATION

La hiérarchie des groupes d'administration se forme dans la fenêtre principale de l'application Kaspersky Security Center dans le dossier **Ordinateurs administrés**. Les groupes d'administration s'affichent sous forme de dossiers dans l'arborescence de la console (cf. ill. ci-après).

Juste après l'installation de Kaspersky Security Center, le groupe **Ordinateurs administrés** contient uniquement le dossier vide **Serveurs d'administration**.

La présence ou l'absence du dossier **Serveurs d'administration** dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur. Pour inclure l'affichage de ce dossier, il faut passer dans le menu **Vue** → **Configuration de l'interface** et dans la fenêtre ouverte **Configuration de l'interface**, cocher la case **Afficher les serveurs d'administration secondaires**.

Lors de la création d'une hiérarchie de groupes d'administration, des postes clients, des machines virtuelles et des sous-groupes peuvent être ajoutés au dossier **Ordinateurs administrés**. Le dossier **Serveurs d'administration** permet d'ajouter des Serveurs d'administration secondaires.

Chaque groupe créé, tel que le groupe **Ordinateurs administrés**, contient d'abord uniquement le dossier vide **Serveurs d'administration** pour le fonctionnement avec les Serveurs d'administration secondaires de ce groupe. Les informations sur les stratégies, les tâches de ce groupe, ainsi que les périphériques compris dans ce groupe s'affichent sur les onglets correspondants dans la zone de travail de ce groupe.

Illustration 14. Consultation des hiérarchies des groupes d'administration

Pour créer un groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le nœud **Ordinateurs administrés**.
2. Si vous voulez créer un sous-groupe du groupe d'administration existant, dans le dossier **Ordinateurs administrés**, sélectionnez le sous-dossier correspondant au groupe auquel le nouveau groupe d'administration doit appartenir.

   Si vous créez un nouveau groupe d'administration de niveau supérieur de la hiérarchie, vous pouvez ignorer cette étape.
3. Lancez le processus de création du groupe d'administration par l'un des moyens suivants :
   - à l'aide de la commande du menu contextuel **Créer** → **Groupe** ;
   - à l'aide du lien **Créer un sous-groupe** situé dans la zone de travail de la fenêtre principale de l'application sous l'onglet **Groupes**.
4. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom du groupe et cliquez sur le bouton **OK**.

L'arborescence de la console affichera un nouveau dossier de groupe d'administration avec le nom saisi.

DEPLACEMENT DES GROUPES D'ADMINISTRATION

Vous pouvez déplacer les groupes d'administration à l'intérieur de la hiérarchie des groupes.

Le groupe d'administration est déplacé avec tous les sous-groupes, les Serveurs d'administration secondaires, les postes clients, les stratégies et les tâches de groupe. Tous les paramètres correspondant à sa nouvelle position dans la hiérarchie des groupes d'administration lui seront appliqués.

Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie. Si dans le dossier dans lequel vous déplacez le groupe d'administration, un groupe avec un tel nom existe déjà, le nom du groupe doit être modifié avec le déplacement. Si vous n'avez pas modifié préalablement le nom du groupe déplacé, le suffixe **_<numéro d'ordre>**, par exemple : **(1)**, **(2)**, sera automatiquement ajouté à son nom lors du déplacement.

Vous ne pouvez pas renommer le groupe **Ordinateurs administrés**, car il s'agit d'un élément incorporé à la Console d'administration.

Pour déplacer le groupe dans un autre dossier de l'arborescence de la console, procédez comme suit :

1. Sélectionnez le groupe déplacé dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - Déplacez le groupe à l'aide du menu contextuel :
     1. Sélectionnez l'option **Couper** dans le menu contextuel du groupe.
     2. Sélectionnez l'option **Insérer** dans le menu contextuel du groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
   - Déplacez le groupe à l'aide du menu principal de l'application :
     a. Sélectionnez l'option du menu principal **Action** → **Couper**.
     b. Sélectionnez dans l'arborescence de la console le groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
     c. Sélectionnez l'option du menu principal **Action** → **Insérer**.
   - Déplacez le groupe dans un autre groupe dans l'arborescence de la console à l'aide de la souris.

SUPPRESSION DES GROUPES D'ADMINISTRATION

Vous pouvez supprimer le groupe d'administration s'il ne contient pas des Serveurs d'administration secondaires, des groupes imbriqués et des postes clients, et si aucune tâche ou stratégie n'a été créée pour lui.

Avant la suppression du groupe d'administration, il faut supprimer de ce groupe les Serveurs d'administration secondaires, les groupes imbriqués et les postes clients.

Pour supprimer un groupe, procédez comme suite :

1. Sélectionnez le groupe d'administration dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - Sélectionnez l'option **Supprimer** dans le menu contextuel du groupe.
   - Sélectionnez l'option **Action** → **Supprimer** dans le menu principal de l'application.
   - cliquez sur le bouton **DEL**.

CREATION AUTOMATIQUE DE STRUCTURE DES GROUPES D'ADMINISTRATION

Kaspersky Security Center permet de former automatiquement une structure des groupes d'administration à l'aide de l'Assistant de création de la structure des groupes.

L'Assistant crée la structure des groupes d'administration sur la base des données suivantes :

- structure des domaines et des groupes du réseau Windows ;
- structure des groupes Active Directory ;
- contenu du fichier texte créé par l'administrateur à la main.

Lors de la composition du fichier texte, il faut respecter les règles suivantes :

- Le nom de chaque nouveau groupe doit commencer par une nouvelle ligne ; séparateur – traduction de la ligne. Les lignes vides sont ignorées.

Exemple :

Office 1

Office 2

Office 3

Trois groupes d'hiérarchie du premier niveau seront formés dans le groupe de destination.

- Il faut indiquer le nom du groupe placé par une barre oblique (/).

Exemple :

Office 1/Subdivision 1/Section 1/Groupe 1

Quatre sous-groupes placés l'un dans l'autre seront formés dans le groupe de destination.

- Pour former quelques groupes placés du même niveau d'hiérarchie, il faut indiquer "le chemin complet vers le groupe".

Exemple :

Office 1/Subdivision 1/Section 1

Office 1/Subdivision 2/Section 1

Office 1/Subdivision 3/Section 1

Office 1/Subdivision 4/Section 1

Dans le groupe de destination un groupe du premier niveau d'hiérarchie "Office 1" sera formé. Il sera composé de quatre groupes placés du même niveau d'hiérarchie "Subdivision 1", "Subdivision 2", "Subdivision 3", "Subdivision 4". Chaque groupe est composé d'un groupe "Section 1".

La création d'une structure de groupe à l'aide de l'Assistant ne viole pas l'intégrité du réseau : de nouveaux groupes sont ajoutés, mais ils ne remplacent pas les groupes existants. Le poste client ne peut pas être inclus une seconde fois dans le groupe d'administration, parce que, lors du déplacement du poste client dans le groupe d'administration, il est supprimé du groupe **Ordinateurs non définis**.

Si lors de la création d'une structure des groupes d'administration, le poste client pour des raisons quelconques n'a pas été inclus dans le groupe **Ordinateurs non définis** (éteint, déconnecté du réseau), il ne sera pas automatiquement déplacé dans le groupe d'administration. Vous pouvez ajouter les postes clients dans les groupes d'administration à la main après la fin du fonctionnement de l'Assistant.

Pour lancer la création automatique d'une structure des groupes d'administration, procédez comme suit :

1. Sélectionnez le dossier **Ordinateurs administrés** dans l'arborescence de la console.

2. Dans le menu contextuel du dossier **Ordinateurs administrés**, sélectionnez l'option **Toutes les tâches** → **Créer la structure du groupe**.

Finalement, l'Assistant de création d'une structure des groupes d'administration se lance. Suivez les instructions de l'Assistant.

INSTALLATION AUTOMATIQUE DES APPLICATIONS SUR LES ORDINATEURS DU GROUPE D'ADMINISTRATION

Vous pouvez définir les fichiers d'installation à utiliser pour l'installation automatique à distance des applications Kaspersky Lab sur les nouveaux clients qui viennent d'être intégrés au groupe.

Afin de configurer l'installation automatique des applications sur les nouveaux périphériques dans le groupe d'administration, procédez comme suit :

1. Sélectionnez le groupe d'administration nécessaire dans l'arborescence de la console.

2. Ouvrez la fenêtre des propriétés de ce groupe d'administration.

3. Dans la section **Installation automatique**, sélectionnez les paquets d'installation qui doivent être installés sur des nouveaux périphériques en cochant les cases à côté des noms de paquets d'installation des applications nécessaires. Cliquez sur le bouton **OK**.

Les tâches de groupe sont créées. Elles seront lancées sur les postes clients juste après avoir été ajoutées au groupe d'administration.

Si plusieurs paquets d'installation d'une seule application sont indiqués pour une installation automatique, la tâche d'installation sera uniquement créée pour la dernière version de l'application.

ADMINISTRATION A DISTANCE DES APPLICATIONS

Cette section contient les informations sur l'administration à distance des applications Kaspersky Lab installées sur les postes clients à l'aide des stratégies, des tâches et de la configuration des paramètres locaux des applications.

DANS CETTE SECTION

ADMINISTRATION DES STRATEGIES

La configuration centralisée des paramètres des applications installées sur les postes clients s'opère à l'aide de la définition de stratégies.

Les stratégies formées pour les applications dans le groupe d'administration s'affichent dans la zone de travail sous l'onglet **Stratégies**. Une icône figure devant le nom de chaque stratégie et caractérise son état.

Après la suppression d'une stratégie ou la fin de ses effets, l'application continue à fonctionner selon les paramètres définis dans la stratégie. Par la suite, il est possible de modifier ces paramètres à la main.

L'application d'une stratégie se déroule de la manière suivante : si des tâches résidentes (tâches de protection en temps réel) sont exécutées sur le poste client, leur exécution est poursuivie avec les nouvelles valeurs des paramètres. Les tâches lancées périodiquement (analyse à la demande, mise à jour des bases de l'application) sont exécutées avec les valeurs non modifiées. Le nouveau lancement des tâches périodiques est exécuté avec les valeurs modifiées des paramètres.

Dans le cas d'utilisation de la structure hiérarchique des Serveurs d'administration, les Serveurs secondaires obtiennent les stratégies du Serveur d'administration principal et les diffusent vers les postes clients. Quand le mode d'héritage est activé, les paramètres de la stratégie peuvent être modifiés sur le Serveur d'administration principal. Après cela, les modifications apportées dans les paramètres d'une stratégie se diffusent sur les stratégies héritées des Serveurs d'administration secondaires.

En cas de perte de la connexion entre les Serveurs principal et secondaire, la stratégie sur le Serveur secondaire continue de fonctionner selon les paramètres précédents. Les paramètres modifiés dans la stratégie sur le Serveur d'administration principal sont propagés vers le Serveur secondaire une fois que la connexion a été rétablie.

Lorsque le mode d'héritage est désactivé, les paramètres de la stratégie peuvent être modifiés sur le Serveur secondaire indépendamment du Serveur principal.

En cas de déconnexion entre le Serveur d'administration et le poste client, la stratégie pour les utilisateurs autonomes (si elle a été définie) entre en vigueur sur le poste client, ou la stratégie continue de fonctionner selon les paramètres précédents jusqu'au rétablissement de la connexion.

Les résultats de la diffusion de la stratégie sur les Serveurs d'administration secondaires figurent dans la fenêtre des propriétés de la stratégie sur le Serveur d'administration principal.

Les résultats de diffusion de la stratégie sur les postes clients s'affichent dans la fenêtre des propriétés de la stratégie du Serveur d'administration auquel ils sont connectés.

DANS CETTE SECTION

CREATION D'UNE STRATEGIE

Pour créer une stratégie pour un groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une stratégie.
2. Dans la zone de travail du groupe, sélectionnez l'onglet **Stratégies** et lancez l'Assistant de création d'une stratégie à l'aide du lien **Créer une stratégie**.

Ceci permet de lancer l'Assistant de création d'une stratégie. Suivez les instructions de l'Assistant.

Il est possible de créer de nombreuses stratégies pour une application, mais une seule d'entre elles peut être celle active. Lors de la création d'une nouvelle stratégie effective, la stratégie active précédente devient inactive.

Lors de la création de la stratégie, il est possible de configurer un ensemble minimal des paramètres sans lesquels l'application ne fonctionnera pas. Tous les autres paramètres prendront les valeurs par défaut correspondantes à celles définies lors de l'installation locale de l'application. Vous pouvez modifier la stratégie après sa création.

Les paramètres des applications Kaspersky Lab, qui se modifient après l'application des stratégies, sont décrits en détails dans les documentations correspondantes.

Après la création de la stratégie, les paramètres verrouillés (le "cadenas" est placé) commencent à agir sur les postes clients quels que soient les paramètres définis auparavant pour l'application.

AFFICHAGE DES STRATEGIES HERITEES DANS LE GROUPE IMBRIQUE

Pour activer l'affichage des stratégies héritées pour le groupe d'administration imbriqué, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut afficher les stratégies héritées.
2. Sélectionnez l'onglet **Stratégies** pour le groupe sélectionné dans la zone de travail.
3. Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Vue** → **Stratégies héritées**.

Finalement, les stratégies héritées s'affichent dans la liste des stratégies avec l'icône  (icône claire). Lorsque le mode d'héritage des paramètres est activé, la modification des stratégies héritées n'est possible que dans les groupes où elles ont été créées. La modification de ces stratégies héritées n'est pas disponible dans le groupe qui hérite les stratégies.

ACTIVATION D'UNE STRATEGIE

- *Pour activer une stratégie pour le groupe sélectionné, procédez comme suit :*

1. Dans la zone de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie qui doit être active.
2. Pour activer une stratégie, exécutez une des actions suivantes :
   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Stratégie active**.
   - Dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général** et dans le groupe des paramètres **Etat de la stratégie**, sélectionnez l'option **Stratégie active**.

Finalement, la stratégie devient active pour le groupe d'administration sélectionné.

Tout changement de stratégie réalisé simultanément sur un grand nombre de clients augmente considérablement la charge du Serveur d'administration ainsi que le volume du trafic réseau.

ACTIVATION AUTOMATIQUE D'UNE STRATEGIE LORS D'UN EVENEMENT "ATTAQUE DE VIRUS"

- *Pour que la stratégie soit automatiquement activée lors d'un événement "Attaque de virus", procédez comme suit :*

1. Dans la fenêtre des propriétés du Serveur d'administration, ouvrez la section **Attaque de virus**.
2. Ouvrez la fenêtre **Activation des stratégies** à l'aide du lien **Configurer l'activation des stratégies suite à "Attaque de virus"** et ajouter la stratégie dans la liste sélectionnée des stratégies activées lors de la détection d'une activité virale.

Si vous désactivez la stratégie en fonction de l'événement *Attaque de virus*, vous ne pouvez rétablir la stratégie précédente que manuellement.

APPLICATION DES STRATEGIES POUR LES UTILISATEURS NOMADES

La stratégie pour les utilisateurs autonomes entre en vigueur sur l'ordinateur en cas de déconnexion du réseau d'entreprise.

- *Pour appliquer la stratégie sélectionnée pour les utilisateurs autonomes,*

dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général** et dans le groupe des paramètres **Etat de la stratégie**, sélectionnez l'option **Stratégie d'utilisateur autonome**.

Finalement, la stratégie commence à agir sur les ordinateurs dans le cas de leur déconnexion du réseau d'entreprise.

SUPPRESSION D'UNE STRATEGIE

Pour supprimer une stratégie, procédez comme suite :

1. Dans la zone de travail du groupe sous l'onglet **Stratégies**, sélectionnez la stratégie qui doit être supprimée.
2. Supprimez la stratégie à l'aide d'un des moyens suivants :
   - Sélectionnez l'option **Supprimer** dans le menu contextuel de la stratégie.
   - A l'aide du lien **Supprimer la stratégie**, situé dans la zone de travail, dans le groupe de travail avec la stratégie sélectionnée.

COPIE D'UNE STRATEGIE

Pour copier une stratégie, procédez comme suit :

1. Dans la zone de travail du groupe nécessaire, sélectionnez une stratégie sous l'onglet **Stratégies**.
2. Sélectionnez l'option **Copier** dans le menu contextuel de la stratégie.
3. Sélectionnez dans l'arborescence de la console le groupe à ajouter une stratégie.

   La stratégie peut être ajoutée dans le groupe depuis lequel elle a été copiée.
4. Dans le menu contextuel de la liste des stratégies pour le groupe sélectionné sous l'onglet **Stratégies**, sélectionnez l'option **Insérer**.

La stratégie est copiée avec tous les paramètres et elle est diffusée sur tous les ordinateurs du groupe où elle a été déplacée. Si vous insérez la stratégie dans le groupe depuis lequel elle a été copiée, le suffixe de type **(<numéro d'ordre>)**, par exemple : **(1)**, **(2)** s'ajoute automatiquement au nom de la stratégie.

Une stratégie active devient inactive lors de la copie. Le cas échéant, vous pouvez en faire une stratégie active.

EXPORTATION D'UNE STRATEGIE

Pour exporter une stratégie, procédez comme suit :

1. Exportez la stratégie à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Toutes les tâches** → **Exporter**.
   - A l'aide du lien **Exporter la stratégie dans le fichier** situé dans la zone de travail, dans le groupe de travail avec la stratégie sélectionnée.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier de la stratégie et le chemin d'accès pour son enregistrement. Cliquez sur **Enregistrer**.

IMPORTATION D'UNE STRATEGIE

Pour importer une stratégie, procédez comme suit :

1. Dans la zone de travail du groupe nécessaire sous l'onglet **Stratégies**, sélectionnez un des moyens suivants d'importation de la stratégie :
   - Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Toutes les tâches** → **Importer**.
   - A l'aide du lien **Importer la stratégie du fichier** dans le groupe d'administration de la liste des stratégies.

2. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la stratégie. Cliquez sur **Ouvrir**.

Finalement, la stratégie ajoutée s'affiche dans la liste des stratégies.

Si dans la liste sélectionnée des stratégies, une stratégie avec le nom, similaire à la stratégie importée, existe déjà, le suffixe de type **(<numéro d'ordre>)**, par exemple : **(1)**, **(2)** sera ajouté au nom de la stratégie importée.

CONVERSION DES STRATEGIES

Kaspersky Security Center peut convertir les stratégies des versions précédentes des applications Kaspersky Lab en stratégies des versions actuelles de ces applications.

La conversion est possible pour les stratégies des applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security 10 for Windows.

Pour convertir les stratégies, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les stratégies.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez le point **Toutes les tâches** → **Assistant de conversion des stratégies et des tâches**.

L'Assistant de conversion des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Finalement l'Assistant forme des nouvelles stratégies qui utilisent les paramètres des stratégies des versions précédentes des applications Kaspersky Lab.

GERER LES TACHES

Kaspersky Security Center gère le fonctionnement des applications installées sur les postes clients par la création et l'exécution des tâches. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases et des modules des applications, les autres actions avec les applications.

Les tâches sont scindées en types suivants :

- *Tâches de groupe*. Tâches exécutées sur les postes clients du groupe d'administration sélectionné.
- *Tâches du Serveur d'administration*. Tâches exécutées sur le Serveur d'administration.
- *Tâches pour les ensembles d'ordinateurs*. Tâches exécutées sur les ordinateurs sélectionnés peu importe leur inclusion dans les groupes d'administration.
- *Tâches locales*. Tâches exécutées sur un poste client particulier.

La création des tâches pour l'application est possible uniquement si le poste de travail de l'administrateur est doté du module externe d'administration de l'application.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches pour les ensembles d'ordinateurs et des tâches locales.

L'échange des informations sur les tâches entre l'application installée sur le poste client et la base d'informations de Kaspersky Security Center a lieu au moment de la connexion de l'Agent d'administration au Serveur d'administration.

Vous pouvez modifier les paramètres des tâches, suivre l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les tâches.

Les tâches ne sont lancées sur un poste client que lorsque l'application pour laquelle les tâches ont été créées est lancée. Si l'application est désactivée, toutes les tâches courantes sont annulées.

Les résultats de l'exécution des tâches sont enregistrés dans les journaux des événements Microsoft Windows et Kaspersky Security Center d'une manière centralisée sur le Serveur d'administration et d'une manière locale sur chaque poste client.

DANS CETTE SECTION

CREATION D'UNE TACHE DE GROUPE

Pour créer une tâche de groupe, procédez comme suit :

1. La zone de travail du groupe pour lequel la création d'une tâche est requise, sélectionnez l'onglet **Tâches**.
2. 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.

CREATION D'UNE TACHE POUR LE SERVEUR D'ADMINISTRATION

Le Serveur d'administration exécute les tâches suivantes :

- diffusion automatique des rapports ;
- téléchargement des mises à jour dans le stockage ;
- sauvegarde des données du Serveur d'administration ;
- synchronisation des mises à jour Windows Update ;
- création du paquet d'installation sur la base de l'image du système d'exploitation de l'ordinateur de référence.

Uniquement la tâche de diffusion automatique des rapports est disponible sur le Serveur d'administration virtuel, ainsi que la tâche de création du paquet d'installation sur la base de l'image du système d'exploitation de l'ordinateur de référence. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur virtuel. La copie de sauvegarde des données du Serveur virtuel s'effectue dans le cadre de la copie de sauvegarde des données du Serveur principal.

Pour créer une tâche du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Lancez le processus de création de la tâche par via l'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez l'option **Créer** → **Tâche**.
   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

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

Les tâches **Téléchargement des mises à jour dans le stockage**, **Synchronisation des mises à jour Windows Update** et **Sauvegarde des données du Serveur d'administration** peuvent exister dans un seul exemplaire. Si les tâches **Téléchargement des mises à jour dans le stockage**, **Sauvegarde des données du Serveur d'administration** et **Synchronisation des mises à jour Windows Update** ont déjà été créées pour le Serveur d'administration, elles ne s'affichent dans la fenêtre de sélection du type de tâche de l'Assistant de création d'une tâche.

CREATION D'UNE TACHE POUR UNE SELECTION D'ORDINATEURS

Kaspersky Security Center permet de créer une tâche pour un ensemble d'ordinateurs sélectionné d'une manière aléatoire. Les ordinateurs dans l'ensemble peuvent être inclus dans des différents groupes d'administration ou ne faire partie d'un aucun groupe d'administration. Kaspersky Security Center permet d'exécuter les tâches principales suivantes pour l'ensemble d'ordinateurs :

- installation à distance de l'application (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- message pour utilisateur (cf. section "Envoi du message aux utilisateurs des postes clients" à la page 81) ;
- modification du Serveur d'administration (cf. section "Modification du Serveur d'administration pour les postes clients" à la page 80) ;
- administration du poste client (cf. section "Démarrage, arrêt et redémarrage à distance des postes clients" à la page 81) ;
- vérification des mises à jour (cf. section "Analyse des mises à jour récupérées" à la page 144) ;

- diffusion du paquet d'installation (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- installation à distance de l'application sur les Serveurs d'administration secondaires (cf. *Manuel d'implantation de Kaspersky Security Center*) ;
- tâche de désinstallation à distance de l'application (cf. *Manuel d'implantation de Kaspersky Security Center*).

Pour créer une tâche pour un ensemble d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les ensembles d'ordinateurs**.
2. Lancez le processus de création de la tâche par via l'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches pour les sélections d'ordinateurs**, sélectionnez l'option **Créer** → **Tâche**.
   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

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

CREATION D'UNE TACHE LOCALE

Pour créer une tâche locale pour un poste client, procédez comme suit :

1. Dans la zone de travail incluant le poste client, sélectionnez l'onglet **Ordinateurs**.
2. Dans la liste des ordinateurs, sous l'onglet **Ordinateurs**, sélectionnez l'ordinateur pour lequel il faut créer une tâche locale.
3. Lancez le processus de création d'une tâche pour l'ordinateur sélectionné à l'aide d'un des moyens suivants :
   - A l'aide du lien **Création d'une tâche** dans le groupe de fonctionnement de l'ordinateur.
   - Depuis la fenêtre des propriétés de l'ordinateur :
     a. Dans le menu contextuel de l'ordinateur, sélectionnez l'option **Propriétés**.
     b. Dans la fenêtre ouverte des propriétés de l'ordinateur, sélectionnez la section **Tâches** et cliquez sur le bouton **Ajouter**.

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

Pour plus d'informations sur la création et la configuration des tâches locales, reportez-vous à la documentation des applications Kaspersky Lab correspondantes.

AFFICHAGE D'UNE TACHE DE GROUPE HERITEE DANS LA ZONE DE TRAVAIL DU GROUPE IMBRIQUE

pour activer l'affichage des tâches héritées du groupe imbriqué dans la zone de travail, procédez comme suit :

1. Sélectionnez dans la zone de travail du groupe imbriqué, l'onglet **Tâches**.
2. Dans le menu contextuel de la liste des tâches, sélectionnez l'option **Vue** → **Tâches héritées**.

Finalement, les tâches héritées s'affichent dans la liste des tâches avec l'icône  . Lorsque le mode d'héritage des paramètres est activé, la modification des tâches héritées n'est possible que dans les groupes où elles ont été créées. La modification des tâches héritées n'est pas disponible dans le groupe qui hérite les tâches.

ACTIVATION AUTOMATIQUE DES POSTES CLIENTS AVEC LE LANCEMENT DE LA TACHE

Kaspersky Security Center permet de configurer les paramètres des tâches pour que le système d'exploitation se démarre avant l'exécution de la tâche sur les postes clients éteints.

Pour configurer le démarrage automatique des postes clients avant le lancement de la tâche, procédez comme suit :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les postes clients à l'aide du lien **Avancé**.
3. Dans la fenêtre **Avancé** qui s'ouvre, cochez la case **Activer les ordinateurs avant le lancement de la tâche par la fonction Wake On LAN (min.)**. Ensuite, spécifiez le temps souhaité en minutes.

Le système d'exploitation démarrera automatiquement sur les postes clients éteints avant le lancement de la tâche pour la période indiquée.

Le démarrage automatique du système d'exploitation est accessible uniquement sur les ordinateurs qui supportent la fonction Wake On Lan.

ARRET AUTOMATIQUE DE L'ORDINATEUR APRES L'EXECUTION DE LA TACHE

Kaspersky Security Center permet de configurer les paramètres des tâches de telle manière pour qu'après son exécution les postes clients, sur lesquels elle est diffusée, soient automatiquement éteints.

Pour que les postes clients soient automatiquement éteints après l'exécution des tâches, procédez comme suit :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les postes clients à l'aide du lien **Avancé**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Avancé** qui s'ouvre, cochez la case **Eteindre l'ordinateur après l'exécution de la tâche**.

LIMITATION DE LA DUREE D'EXECUTION DE LA TACHE

Pour limiter la durée d'exécution de la tâche sur les postes clients, procédez comme suit :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre de configuration des actions avec les postes clients à l'aide du lien **Avancé**.
3. Dans la liste déroulante **Avancé**, cochez la case **&Stopper si la tâche prend plus de (min.)** et indiquez la durée en minutes.

Kaspersky Security Center arrêtera automatiquement l'exécution de la tâche si à l'issue du temps indiqué, l'exécution de la tâche ne se terminera pas sur le poste client.

EXPORTATION D'UNE TACHE

Vous pouvez exporter les tâches de groupe et les tâches pour les ensembles d'ordinateurs dans un fichier. Les tâches du Serveur d'administration et les tâches locales ne peuvent pas être exportées.

Pour exporter une tâche, procédez comme suit :

1. Exportez la tâche à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Toutes les tâches** → **Exporter**.
   - A l'aide du lien **Exporter la tâche dans un fichier** situé dans la zone de travail, dans le groupe de travail avec la stratégie sélectionnée.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier et le chemin d'accès pour l'enregistrement. Cliquez sur **Enregistrer**.

Les privilèges des utilisateurs locaux ne sont pas exportés.

IMPORTATION D'UNE TACHE

Vous pouvez importer les tâches de groupe et les tâches pour les ensembles d'ordinateurs. Les tâches du Serveur d'administration et les tâches locales ne peuvent pas être importées.

Pour importer une tâche, procédez comme suit :

1. Sélectionnez la liste des tâches dans laquelle il faut importer la tâche :
   - Si vous voulez importer la tâche dans la liste des tâches de groupe, sélectionnez l'onglet **Tâches** dans la zone de travail du groupe nécessaire.
   - Si vous voulez importer la tâche dans la liste des ensembles d'ordinateurs, sélectionnez le dossier **Tâches pour les ensembles d'ordinateurs** dans l'arborescence de la console.
2. Sélectionnez un des moyens suivants d'importation de la tâche :
   - Dans le menu contextuel de la liste des tâches, sélectionnez l'option **Toutes les tâches** → **Importer**.
   - A l'aide du lien **Importer la tâche du fichier** dans le groupe d'administration de la liste des tâches.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la tâche. Cliquez sur **Ouvrir**.

La tâche ajoutée s'affiche dans la liste des tâches.

Si dans la liste sélectionnée, une tâche avec le nom, similaire à la tâche, existe déjà, le suffixe de type **(<numéro d'ordre>)**, par exemple : **(1)**, **(2)** sera ajouté au nom de la tâche importée.

CONVERSION DES TACHES

Kaspersky Security Center permet de convertir les tâches des versions précédentes des applications Kaspersky Lab en tâches des versions actuelles des applications.

La conversion est possible pour les tâches des applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Endpoint Security 8 for Windows ;
- Kaspersky Endpoint Security 10 for Windows.

Pour convertir les tâches, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les tâches.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez le point **Toutes les tâches** → **Assistant de conversion des stratégies et des tâches**.

L'Assistant de conversion des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

L'Assistant forme des nouvelles tâches qui utilisent les paramètres des tâches des versions précédentes des applications.

DEMARRAGE ET ARRET MANUELS DES TACHES

Pour lancer ou arrêter manuellement une tâche, procédez comme suit :

1. Sélectionnez une tâche dans la liste des tâches.
2. Lancez ou arrêter la tâche à l'aide d'un des moyens suivants :
   - Cliquez sur le bouton **Démarrer** ou **Arrêter** dans le groupe du travail avec la tâche sélectionnée.
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Démarrer** ou **Arrêter**.
   - Dans la section **Général** de la fenêtre des propriétés de la tâche, cliquez sur le bouton **Démarrer** ou **Arrêter**.

SUSPENSION ET REPRISE MANUELLES D'UNE TACHE

Pour suspendre ou reprendre l'exécution de la tâche lancée, procédez comme suit :

1. Sélectionnez une tâche dans la liste des tâches.
2. Suspendez ou reprenez l'exécution de la tâche à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Suspendre** ou **Reprendre**.
   - Dans la section **Général** de la fenêtre des propriétés de la tâche, cliquez sur le bouton **Suspendre** ou **Reprendre**.

SUIVI ET AFFICHAGE DES COMPTES-RENDUS D'ACTIVITE DES TACHES

Pour surveiller l'exécution des tâches,

sélectionnez la section **Général** de la fenêtre des propriétés des tâches.

Le milieu de la fenêtre de la section **Général** contient les informations sur l'état actuel de la tâche.

AFFICHAGE DE L'HISTORIQUE DES TACHES ENTREPOSE SUR LE SERVEUR D'ADMINISTRATION

Kaspersky Security Center permet de consulter les résultats de l'exécution des tâches de groupe, des tâches pour les ensembles d'ordinateurs et des tâches du Serveur d'administration. La consultation des résultats de l'exécution des tâches locales n'est pas disponible.

- *Pour consulter les résultats de l'exécution de la tâche,*

  sélectionnez la section **Général** de la fenêtre des propriétés de la tâche et à l'aide du lien **Résultats**, ouvrez la fenêtre **Résultats de la tâche**.

CONFIGURATION DU FILTRE D'INFORMATIONS SUR LES RESULTATS D'EXECUTION DE LA TACHE

Kaspersky Security Center permet de filtrer les informations sur les résultats de l'exécution des tâches de groupe, des tâches pour les ensembles d'ordinateurs et des tâches du Serveur d'administration. Le filtrage n'est pas disponible pour les tâches locales.

- *pour configurer le filtrage pour les informations sur les résultats de l'exécution de la tâche, procédez comme suit :*

  1. Sélectionnez la section **Général** de la fenêtre des propriétés de la tâche et à l'aide du lien **Résultats**, ouvrez la fenêtre **Résultats de la tâche**.

     Le tableau dans la partie supérieure de la fenêtre contient la liste de tous les postes clients pour lesquels la tâche a été désignée.

     Le tableau de la partie inférieure de la fenêtre contient les résultats de l'exécution des tâches sur le poste client sélectionné.

  2. Dans la fenêtre **Résultats de la tâche** dans le tableau qui vous intéresse, sélectionnez l'option **Filtre** du menu contextuel.

  3. Dans la fenêtre **Appliquer le filtre** qui s'ouvre, configurez les paramètres du filtre dans les sections de la fenêtre **Evénements**, **Ordinateurs** et **Heure**. Cliquez sur le bouton **OK**.

  Après cela, les informations qui vérifient les paramètres indiqués dans le filtre seront affichées dans la fenêtre **Résultats de la tâche**.

CONSULTATION ET MODIFICATION DES PARAMETRES LOCAUX DE L'APPLICATION

Le système d'administration Kaspersky Security Center permet d'administrer à distance les paramètres locaux des applications sur les postes clients via la Console d'administration.

Les *Paramètres locaux des applications* sont les paramètres de l'application individuels pour chaque poste client. A l'aide de Kaspersky Security Center, vous pouvez installer les paramètres locaux des applications pour les postes clients inclus dans le groupe d'administration.

Les descriptions détaillées des paramètres des applications Kaspersky Lab sont présentées dans les documentations respectives.

Pour consulter ou modifier les paramètres locaux de l'application, procédez comme suit :

1. Dans la zone de travail du groupe dans lequel se trouve le poste client nécessaire, sélectionnez l'onglet **Ordinateurs**.

2. Dans la fenêtre des propriétés du poste client dans la section **Applications**, sélectionnez l'application nécessaire.

3. Ouvrez la fenêtre des propriétés de l'application en double cliquant sur le nom de l'application ou à l'aide du bouton **Propriétés**.

La fenêtre des paramètres locaux de l'application sélectionnée s'ouvre. Il est possible de consulter et de modifier ces paramètres.

Vous pouvez modifier les valeurs des paramètres dont la modification n'est pas interdite par la stratégie de groupe (le paramètre n'est pas verrouillé dans la stratégie).

ADMINISTRATION DES POSTES CLIENTS

Cette section contient les informations sur l'utilisation des postes clients.

DANS CETTE SECTION

CONNEXION DES POSTES CLIENTS AU SERVEUR D'ADMINISTRATION

La connexion du poste client eu Serveur d'administration se réalise par l'Agent d'administration installé sur le poste client.

Lors de la connexion du poste client au Serveur d'administration, les opérations suivantes sont exécutées :

- Synchronisation automatique des données :
  - la synchronisation de la liste des applications installées sur le poste client ;
  - la synchronisation des stratégies, des paramètres des applications, des tâches et des paramètres des tâches.
- La réception par le Serveur des informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.
- La transmission sur le Serveur des informations sur les événements qui doivent être traités.

La synchronisation automatique des données s'effectue périodiquement, en fonction des paramètres de l'Agent d'administration (par exemple, une fois toutes les 15 minutes). Vous pouvez définir manuellement l'intervalle entre les connexions.

Les informations sur un événement sont envoyées sur le Serveur d'administration tout de suite après que l'événement a eu lieu.

Kaspersky Security Center permet de configurer la connexion du poste client au Serveur d'administration de telle manière pour que la connexion ne se termine pas à la fin d'exécution des opérations. Une connexion permanente est nécessaire si le contrôle d'état des applications est requis, et que le Serveur d'administration ne peut pas initier la connexion au poste client (par exemple, la connexion est protégée par un pare-feu, il est interdit d'ouvrir des ports sur le poste client, l'adresse IP du poste client est inconnue). La section **Général** de la fenêtre des propriétés du poste client permet de réaliser la connexion permanente du poste client avec le Serveur d'administration.

Il recommandé d'établir une connexion permanente avec les postes clients les plus importants, car le nombre total de connexions simultanées prises en charge par le Serveur d'administration est limité (plusieurs centaines).

Lors de la synchronisation manuelle, le mode auxiliaire de connexion est utilisé. Le Serveur d'administration initie la connexion dans ce mode. Avant la connexion sur le poste client, l'ouverture du port UDP est requise. Le Serveur d'administration envoie une demande de connexion sur le port UDP du poste client. En réponse, l'analyse du certificat du Serveur d'administration est exécutée. Si le certificat du Serveur coïncide avec la copie du certificat sur le poste client, la connexion est exécutée.

Le lancement manuel du processus de synchronisation est aussi utilisé pour recevoir les informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.

CONNEXION MANUELLE DU POSTE CLIENT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLMOVER

S'il vous faut connecter le poste client au Serveur d'administration à la main, vous pouvez utiliser l'utilitaire klmover sur le poste client.

Lors de l'installation de l'Agent d'administration sur le poste client, l'utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

- *Pour connecter le poste client au Serveur d'administration à la main à l'aide de l'utilitaire klmover,*

  lancez l'utilitaire klmover sur le poste client depuis la ligne de commande.

Lors du lancement depuis la ligne de commande, l'utilitaire klmover exécute les actions suivantes selon les clés utilisées :

- connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués ;
- enregistre les résultats de l'opération dans le fichier journal des événements, ou les afficher à l'écran.

Syntaxe de l'utilitaire :

```
klmover [-logfile <nomFichier>] [-address <adresse serveur>] [-pn <numéro du port>]
[-ps < numéro du port SSL>] [-nossl] [-cert <chemin du fichier certificat>] [-
silent][-dupfix]
```

Description des paramètres :

- -logfile <nom du fichier> : enregistre les résultats de l'exécution dans le fichier journal.

  Par défaut, les informations sont conservées dans le fichier stdout. Si la clé n'est pas utilisée, les résultats et les messages d'erreur sont affichés à l'écran.

- -address <adresse du serveur> : adresse du Serveur d'administration pour la connexion.

  L'adresse peut être une adresse IP, un nom NetBIOS ou DNS de l'ordinateur.

- -pn <numéro du port> : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration.

  Le numéro de port par défaut est 14000.

- -ps <numéro du port SSL> : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL.

  Le numéro de port par défaut est 13000.

- -nossl : utilise une connexion non sécurisée au Serveur d'administration.

  Si aucune clé n'est utilisée, la connexion de l'Agent d'administration au Serveur est établie à l'aide du protocole sécurisé SSL.

- -cert <chemin complet du fichier certificat> : utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.

  Si aucun modificateur n'est utilisé, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.

- -silent : exécute l'utilitaire en mode non interactif.

  Cette clé est utile, par exemple, pour exécuter l'outil à partir du script d'ouverture de session de l'utilisateur.

- -dupfix : clé utilisée en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

VERIFICATION DE LA CONNEXION DU POSTE CLIENT AVEC LE SERVEUR D'ADMINISTRATION

Kaspersky Security Center permet d'analyser les connexions du poste client avec le Serveur d'administration automatiquement ou à la main.

L'analyse automatique de la connexion s'effectue sur le Serveur d'administration. L'analyse manuelle de la connexion s'effectue sur le poste client.

DANS CETTE SECTION

VERIFICATION AUTOMATIQUE DE LA CONNEXION DU POSTE CLIENT AVEC LE SERVEUR D'ADMINISTRATION

Pour lancer l'analyse automatique de la connexion du poste client avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont le poste client fait partie.
2. Dans la zone de travail du groupe d'administration sous l'onglet **Ordinateurs**, sélectionnez le poste client.
3. Dans le menu contextuel du poste client, sélectionnez l'option **Analyser la connexion**.

La fenêtre, qui contient l'information sur l'accessibilité de l'ordinateur, s'ouvre.

VERIFICATION MANUELLE DE LA CONNEXION DU POSTE CLIENT AVEC LE SERVEUR D'ADMINISTRATION. UTILITAIRE KLNAGCHK

Vous pouvez vérifier la connexion et recevoir les informations détaillées sur les paramètres de connexion du poste client au Serveur d'administration à l'aide de l'utilitaire klnagchk.

Lors de l'installation de l'Agent d'administration sur le poste client, l'utilitaire klnagchk est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

Lors du lancement depuis la ligne de commande, l'utilitaire klnagchk exécute les actions suivantes selon les clés utilisées :

- Renvoie à l'écran ou enregistre dans un fichier les valeurs des paramètres de connexion de l'Agent d'administration installé sur le poste client, utilisés afin de se connecter au Serveur d'administration.
- Enregistre dans le fichier de journal les statistiques de l'Agent d'administration (à partir de son dernier démarrage) et les résultats de l'exécution de l'utilitaire, ou affiche les informations sur l'écran.
- Tente de connecter l'Agent d'administration au Serveur d'administration.

  Si la connexion n'a pas pu être établie, l'utilitaire envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état du poste.

Pour vérifier la connexion du poste client au Serveur d'administration à l'aide de l'utilitaire klnagchk,

lancez l'utilitaire klnagchk sur le poste client depuis la ligne de commande.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nomFichier>] [-sp] [-savecert <chemin du fichier certificat>] [-restart]
```

Description des paramètres :

- -logfile <nom du fichier> : enregistre les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur, ainsi que les résultats de l'exécution.

  Par défaut, les informations sont conservées dans le fichier stdout. Si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur sont affichés à l'écran.
- -sp : affiche le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy.

  Ce paramètre est utilisé si la connexion au Serveur d'administration est effectuée via un serveur proxy.
- -savecert <nom du fichier> : enregistre le certificat utilisé pour accéder au Serveur d'administration dans le fichier spécifié.
- -restart : redémarre l'Agent d'administration après exécution de l'utilitaire.

IDENTIFICATION DES POSTES CLIENTS SUR LE SERVEUR D'ADMINISTRATION

L'identification des postes clients est réalisée sur la base de leurs noms. Le nom d'un poste client est unique parmi tous les noms d'ordinateurs connectés au Serveur d'administration.

Le nom du poste client est transmis au Serveur d'administration, soit lors du sondage du réseau Windows et de la détection d'un nouvel ordinateur dans ce réseau, soit lors de la première connexion de l'Agent d'administration, installé sur le poste client, au Serveur d'administration. Par défaut, le nom concorde avec le nom du réseau Windows (nom NetBIOS). Si un poste client est déjà enregistré avec ce nom sur le Serveur d'administration, alors un numéro d'ordre sera ajouté à la fin du nom du nouveau poste client, par exemple : **<Nom>-1**, **<Nom>-2**. Sous ce nom, le poste client sera inclus dans le groupe d'administration.

AJOUT D'ORDINATEURS A UN GROUPE D'ADMINISTRATION

Pour inclure un ou plusieurs ordinateurs dans un groupe d'administration sélectionné, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le nœud **Ordinateurs administrés**.
2. Dans le dossier **Ordinateurs administrés** sélectionnez le sous-dossier qui correspond au groupe dans lequel les postes clients seront inclus.

   Si vous voulez activer les postes clients dans le groupe **Ordinateurs administrés**, cette étape peut être ignorée.
3. Dans la zone de travail du groupe d'administration sélectionné sous l'onglet **Ordinateurs**, lancez le processus d'inclusion des postes clients dans le groupe à l'aide d'un des moyens suivants :

   - Ajoutez les ordinateurs dans le groupe à l'aide du lien **Ajouter des ordinateurs** dans le groupe d'administration de la liste des ordinateurs.
   - Dans le menu contextuel de la liste des ordinateurs, sélectionnez l'option **Créer Ordinateur**.

   L'Assistant d'ajout des postes clients démarrera. Suivez ses instructions et définissez le mode d'ajout des postes clients au groupe et composez la liste des ordinateurs appartenant au groupe.

   Si vous formez la liste des ordinateurs à la main, vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant qu'adresse de l'ordinateur. Il est possible d'ajouter manuellement à la liste des ordinateurs uniquement les ordinateurs dont les informations ont été insérées dans la base de données du Serveur d'administration lors de la connexion de l'ordinateur ou lors du sondage du réseau.

   Pour importer la liste des ordinateurs depuis le fichier, il faut indiquer le fichier au format TXT avec la liste des adresses des ordinateurs ajoutés. Chaque adresse doit figurer sur une ligne séparée.

Après la fin de l'Assistant, les postes clients sélectionnés sont inclus dans les groupes d'administration et s'affichent dans la liste des ordinateurs sous les noms établis pour eux par le Serveur d'administration.

Il est possible d'ajouter le poste client dans le groupe d'administration sélectionné, en le déplaçant à l'aide de la souris depuis le dossier **Ordinateurs non définis** dans le dossier du groupe d'administration.

MODIFICATION DU SERVEUR D'ADMINISTRATION POUR LES POSTES CLIENTS

Vous pouvez modifier le Serveur d'administration, sous lequel les postes clients se trouvent, par un autre Serveur à l'aide de la tâche **Modification du Serveur d'administration**.

Pour modifier le Serveur d'administration, dans lequel se trouvent les postes clients, par un autre Serveur, procédez comme suit :

1. Connectez-vous au Serveur d'administration, qui gère les postes clients.
2. Créez une tâche de modification du Serveur d'administration à l'aide d'un des moyens :

   - S'il faut modifier le Serveur d'administration pour les ordinateurs qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page 68).
   - S'il faut modifier le Serveur d'administration pour les ordinateurs qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page 69).

   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 d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Modification du Serveur d'administration**.

3. Lancez la tâche créée.

Après la fin de la tâche, les postes clients, pour lesquels elle a été créée, passent sous l'administration du Serveur d'administration indiqué dans les paramètres de la tâche.

Si le Serveur d'administration prend en charge la fonctionnalité de chiffrement et de protection des données, lors de la création de la tâche **Modification du Serveur d'administration**, un avertissement s'affiche. Cet avertissement signale que lors de la présence des données chiffrés sur les ordinateurs après le passage des ordinateurs sous l'administration d'un autre serveur, les utilisateurs auront l'accès uniquement aux données chiffrées dont ils travaillaient auparavant. Dans les autres cas, l'accès aux données chiffrées ne sera pas octroyé. La description détaillée des scénarios dont l'accès aux données chiffrées ne sera pas offert est décrite dans le Manuel de l'administrateur de Kaspersky Endpoint Security 10f or Windows.

DEMARRAGE, ARRET ET REDEMARRAGE A DISTANCE DES POSTES CLIENTS

Kaspersky Security Center permet d'administrer à distance les postes clients : les allumer, éteindre, redémarrer.

Pour administrer à distance les postes clients, procédez comme suit :

1. Connectez-vous au Serveur d'administration, qui gère les postes clients.

2. Créez une tâche d'administration du poste client via l'un des moyens suivants :

   - S'il faut allumer, éteindre ou redémarrer les ordinateurs qui font partie du groupe d'administration sélectionné, créer une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page 68).

   - S'il faut allumer, éteindre ou redémarrer les ordinateurs qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page 69).

   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 d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Administration du poste client**.

3. Lancez la tâche créée.

Après la fin du fonctionnement de la tâche, la commande sélectionnée (démarrage, arrêt, redémarrage) sera exécutée sur les postes clients sélectionnés.

ENVOI DU MESSAGE AUX UTILISATEURS DES POSTES CLIENTS

Pour envoyer un message aux utilisateurs des postes clients, procédez comme suit :

1. Connectez-vous au Serveur d'administration, qui gère les postes clients.

2. Créez une tâche d'envoi du message aux utilisateurs des postes clients via l'un des moyens suivants :

   - S'il faut envoyer un message aux utilisateurs des postes clients qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page 68).

- S'il faut envoyer un message aux utilisateurs des postes clients qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page 69).

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 d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Message pour l'utilisateur**.

3. Lancez la tâche créée.

A la fin du fonctionnement de la tâche, le message créé sera envoyé aux utilisateurs des postes clients sélectionnés.

DIAGNOSTIC A DISTANCE DES POSTES CLIENTS. UTILITAIRE DE DIAGNOSTIC A DISTANCE KASPERSKY SECURITY CENTER

L'utilitaire de diagnostic à distance Kaspersky Security Center (ci-après : utilitaire de diagnostic à distance) est conçue pour exécuter à distance des opérations suivantes sur les postes clients :

- activation et désactivation du traçage, modification du niveau de traçage, téléchargement du fichier de traçage ;
- téléchargement des paramètres des applications ;
- téléchargement des journaux des événements ;
- lancement du diagnostic et téléchargement des résultats du diagnostic ;
- lancement et arrêt des applications.

L'utilitaire de diagnostic à distance s'installe automatiquement sur l'ordinateur conjointement avec la Console d'administration.

DANS CETTE SECTION

CONNEXION DE L'UTILITAIRE DE DIAGNOSTIC A DISTANCE AU POSTE CLIENT

Pour connecter l'utilitaire de diagnostic à distance au poste client, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez n'importe quel groupe d'administration.
2. Dans la zone de travail sous l'onglet **Ordinateurs** dans le menu contextuel de n'importe quel poste client, sélectionnez l'option **Outils externes** → **Diagnostic à distance**.

   La fenêtre principale de l'utilitaire de diagnostic à distance s'ouvre.
3. Dans le champ droit de la fenêtre principale de l'utilitaire de diagnostic à distance, définissez les moyens de connexion au poste client :
   - **Accès à l'aide des outils du réseau Microsoft Windows**.
   - **Accès à l'aide des outils du Serveur d'administration**.
4. Si dans le premier champ de la fenêtre principale de l'utilitaire, vous avez sélectionné l'option **Accès à l'aide des outils du réseau Microsoft Windows**, procédez comme suit :
   - Dans le champ **Ordinateur**, indiquez l'adresse de l'ordinateur à se connecter.

     L'adresse de l'ordinateur peut être une adresse IP, un nom NetBIOS ou DNS.

     Par défaut, l'adresse de l'ordinateur est indiqué, dont l'utilitaire a été lancé depuis son menu contextuel.
   - Indiquez un compte pour se connecter à l'ordinateur :
     - **Se connecter au nom de l'utilisateur en cours** (sélectionné par défaut). Connexion sous compte utilisateur actuel.
     - **Utiliser, lors de la connexion, le nom d'utilisateur et le mot de passe fournis**. Connexion sous compte indiqué. Indiquez **Nom d'utilisateur** et **Mot de passe** du compte nécessaire.

   La connexion au poste client est possible uniquement sou le compte d'administrateur local du poste client.
5. Si dans le premier champ, vous avez sélectionné **Accès à l'aide des outils du Serveur d'administration**, procédez comme suit :
   - Dans le champ **Serveur d'administration**, indiquez l'adresse du Serveur d'administration depuis lequel il faut se connecter au poste client.

     L'adresse du Serveur peut être une adresse IP, un nom NetBIOS ou DNS.

     Par défaut l'adresse du Serveur, depuis lequel l'utilitaire a été lancé, est indiquée.
   - S'il faut, cochez les cases **Utiliser SSL**, **Compresser le trafic** et **Le poste appartient au Serveur d'administration secondaire**.

     Si la case **Le poste appartient au Serveur d'administration secondaire** est cochée, le champ **Serveur secondaire** permet de sélectionner le Serveur d'administration secondaire sous l'administration duquel le poste client se trouve, en cliquant sur le bouton **Parcourir**.
6. Pour se connecter au poste client, cliquez sur le bouton **Entrer**.

La fenêtre de diagnostic à distance du poste client s'ouvre (cf. ill. ci-après). La partie gauche de la fenêtre reprend les liens pour exécuter les opérations de diagnostic des postes clients. La partie droite de la fenêtre reprend l'arborescence des objets du poste client avec lesquels l'utilitaire peut fonctionner. La partie inférieure de la fenêtre affiche le processus d'exécution des opérations de l'utilitaire.

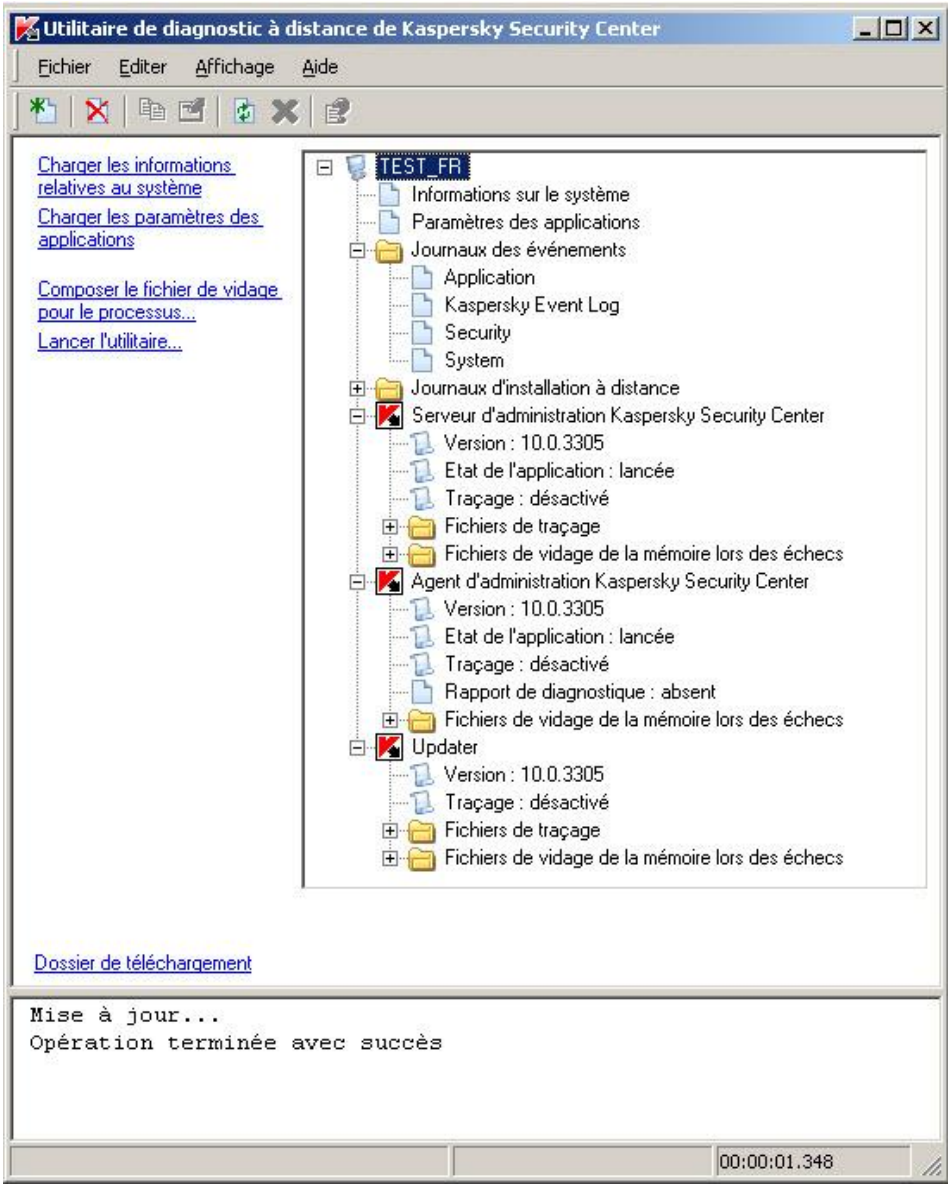

Illustration 15. Utilitaire de diagnostic à distance. Fenêtre de diagnostic à distance du poste client

L'utilitaire de diagnostic à distance sauvegarde les fichiers téléchargés des postes clients sur le bureau de l'ordinateur, depuis lequel il était lancé.

ACTIVATION ET DESACTIVATION DU TRAÇAGE, TELECHARGEMENT DU FICHIER DE TRAÇAGE

Pour activer le traçage, télécharger le fichier de traçage ou désactiver le traçage, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'ordinateur nécessaire.
2. Dans l'arborescence des objets du poste client, sélectionnez l'application pour laquelle il faut froncer le traçage, et activez le traçage à l'aide du lien **Activer le traçage** dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance.

   Activation et désactivation du traçage des applications avec l'autodéfense sont possibles uniquement lors de la connexion au poste client via les outils du Serveur d'administration.

   Dans certains cas, pour activer le traçage de l'application antivirus, il faut redémarrer cette application et sa tâche.
3. L'entrée de l'application pour laquelle le traçage a été activé, dans le dossier **Fichiers de traçage**, sélectionnez le fichier nécessaire et téléchargez-le à l'aide du lien **Télécharger le fichier**. Pour les fichiers de grande taille, il existe une possibilité de télécharger uniquement les dernières parties du traçage.

   Vous pouvez supprimer le fichier de traçage sélectionné. La suppression du fichier de traçage est possible après la désactivation du traçage.
4. Désactivez le traçage pour l'application sélectionnée à l'aide du lien **Désactiver le traçage**.

TELECHARGEMENT DES PARAMETRES DES APPLICATIONS

Pour télécharger les paramètres des applications, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'ordinateur nécessaire.
2. Dans l'arborescence des objets de la fenêtre de diagnostic à distance de l'ordinateur, sélectionnez l'entrée supérieure avec le nom de l'ordinateur et sélectionnez l'action nécessaire dans la partie gauche de la fenêtre :

   - **Charger les informations relatives au système**.
   - **Charger les paramètres des applications**.
   - **Composer le fichier de vidage pour le processus**.

     Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'application sélectionnée pour laquelle il faut former le fichier de vidage de la mémoire.
   - **Lancer l'utilitaire**.

     Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'utilitaire sélectionné et les paramètres de son lancement.

     L'utilitaire sélectionné sera téléchargé et lancé sur le poste client.

TELECHARGEMENT DES JOURNAUX DES EVENEMENTS

Pour télécharger les journaux des événements, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'ordinateur nécessaire.
2. Dans le dossier **Journaux des événements** de l'arborescence des objets de l'ordinateur, sélectionnez le journal nécessaire et téléchargez-le à l'aide du lien **Charger le journal des événements** dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance.

LANCEMENT DU DIAGNOSTIC ET TELECHARGEMENT DE SES RESULTATS

Pour lancer le diagnostic pour l'application et télécharger ses résultats, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'ordinateur nécessaire.
2. Dans l'arborescence des objets du poste client, sélectionnez l'application nécessaire et lancez le diagnostic à l'aide du lien **Poser le diagnostic**.

   Dans l'entrée de l'application sélectionnée, le rapport de diagnostic apparaîtra dans l'arborescence des objets.
3. Sélectionnez le rapport formé de diagnostic dans l'arborescence des objets et téléchargez-le à l'aide du lien **Télécharger le fichier**.

LANCEMENT, ARRET OU RELANCEMENT DES APPLICATIONS

Le lancement, relancement et arrêt des applications sont possibles uniquement à la connexion au poste client par les outils du Serveur d'administration.

Pour lancer, arrêter ou relancer l'application, procédez comme suit :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous au poste client nécessaire.
2. Dans l'arborescence des objets du poste client, sélectionnez l'application nécessaire et sélectionnez l'action dans la partie gauche de la fenêtre :
   - **Arrêter l'application**.
   - **Relancer l'application**.
   - **Exécuter l'application**.

   Selon l'action sélectionnée, l'application sera lancée, arrêtée ou relancée.

UTILISATION DES RAPPORTS, DES STATISTIQUES ET DES NOTIFICATIONS

Cette section reprend les informations sur l'utilisation des rapports, des statistiques et des sélections d'événements et de postes clients dans Kaspersky Security Center, ainsi que sur la configuration des notifications du Serveur d'administration.

DANS CETTE SECTION

UTILISATION DES RAPPORTS

Les rapports dans Kaspersky Security Center contiennent les informations sur l'état du système de protection. Les rapports se forment à partir des informations enregistrées sur le Serveur d'administration. Vous pouvez créer les rapports pour les objets suivants :

- pour une sélection de postes clients ;
- pour les ordinateurs appartenant à un groupe d'administration déterminé ;
- pour un ensemble de postes clients issus de divers groupes d'administration ;
- pour tous les ordinateurs dans le réseau (accessible pour le rapport de déploiement).

L'application propose un ensemble de modèles de rapport standard. Il est possible également de composer des modèles personnalisés des rapports. Les rapports s'affichent dans la fenêtre principale de l'application, dans le dossier de l'arborescence de la console **Rapports et notifications**.

DANS CETTE SECTION

CREER LE NOUVEAU RAPPORT

Pour créer un rapport,

sélectionnez dans l'arborescence de la console le dossier **Rapports et notifications** et exécutez une des actions suivantes :

- Dans le menu contextuel du dossier **Rapports et notifications**, sélectionnez l'option **Créer** → **Rapport**.
- Dans la zone de travail du dossier **Rapports et notifications** sous l'onglet **Rapport**, lancez le processus de création du rapport à l'aide du lien **Créer un modèle de rapport**.

L'Assistant de création d'un modèle de rapport se lance. Suivez les instructions de l'Assistant.

A la fin du fonctionnement de l'Assistant, le modèle formée du rapport sera ajouté dans le dossier **Rapports et notifications** de l'arborescence de la console. Ce modèle peut être utilisé pour créer et afficher des rapports.

GENERATION ET AFFICHAGE DE RAPPORTS

Pour former et consulter le rapport, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
2. Sélectionnez le modèle de rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.

   La zone de travail affiche le rapport formé selon le modèle sélectionné.

Le rapport affiche les données suivantes :

- le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur la création d'un rapport créée pour un groupe de périphériques ;
- diagramme illustrant les données générales du rapport ;
- tableau récapitulatif avec les données illustrant les indices calculés ;
- tableau avec les données détaillées.

ENREGISTREMENT DU RAPPORT

Afin de sauvegarder un rapport formé, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
2. Sélectionnez le modèle de rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.
3. Dans le menu contextuel du modèle de rapport sélectionné, sélectionnez l'option **Enregistrer**.

L'Assistant d'enregistrement du rapport se lance. Suivez les instructions de l'Assistant.

Après la fin de fonctionnement de l'Assistant, le dossier avec le fichier du rapport enregistré s'ouvre.

CREATION D'UNE TACHE DE DIFFUSION DU RAPPORT

La diffusion des rapports dans l'application Kaspersky Security Center s'effectue à l'aide de la tâche d'envoi du rapport. Les rapports peuvent être diffusés par courrier électronique ou enregistrés dans le dossier sélectionné, par exemple, dans le dossier partagé sur le Serveur d'administration ou sur l'ordinateur local.

Pour créer une tâche d'envoi d'un rapport, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
2. Sélectionnez le modèle de rapport, qui vous intéresse, dans l'arborescence de la console ou dans la zone de travail sous l'onglet **Rapports**.
3. Dans le menu contextuel du modèle de rapport, sélectionnez l'option **Envoi des rapports**.

L'Assistant de création de la tâche d'envoi du rapport sélectionné se lance. Suivez les instructions de l'Assistant.

Pour créer une tâche de diffusion de plusieurs rapports, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Lancez le processus de création de la tâche par via l'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez l'option **Créer** → **Tâche**.
   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

Finalement, l'Assistant de création d'une tâche du Serveur d'administration se lance. Suivez les instructions de l'Assistant. Dans la fenêtre de l'Assistant **Type de tâche**, sélectionnez le type de tâche **Envoi du rapport**.

La tâche d'envoi du rapport créée s'affiche dans le dossier de l'arborescence de la console **Tâches du Serveur d'administration**.

La tâche d'envoi du rapport est créée automatiquement dans le cas, si les paramètres du courrier électronique ont été spécifiés lors de l'installation de Kaspersky Security Center.

TRAVAILLER AVEC LES DONNEES STATISTIQUES

Les données statistiques sur l'état du système de protection s'affichent dans la zone de travail du dossier **Rapports et notifications** sous l'onglet **Statistiques**. L'onglet **Statistiques** contient plusieurs pages dont chaque page contient les barres d'informations affichant les données statistiques. Les données statistiques sont présentées dans les barres d'informations sous forme de tableaux ou de diagrammes camemberts ou colonnes. Les données dans les barres d'informations sont actualisées lors du fonctionnement de l'application et reflètent l'état actuel du système de protection antivirus.

Vous pouvez modifier le nombre et le contenu des pages sous l'onglet **Statistiques**, le nombre de barres d'informations sur chaque page, ainsi que le mode d'affichage des données dans les barres d'informations.

Pour modifier les paramètres d'affichage des données statistiques et pour imprimer les données, les boutons suivants sont utilisés :

-  – situé en haut à droite de l'onglet **Statistiques**. La configuration du contenu de l'onglet **Statistiques** : ajout, suppression des pages des statistiques, leur emplacement.
-  – situé à droite du nom de la page. La configuration des paramètres de la page des statistiques.

-  – situé à droite du nom du volet d'informations. La configuration des paramètres de la barre d'informations.
-  – situé à droite du nom du volet d'informations. Le roulement de la barre d'informations.
-  – situé à droite du nom du volet d'informations. Le déploiement de la barre d'informations.
-  – situé en haut à droite de l'onglet **Statistiques**. L'impression de la page affichée des statistiques.

CONFIGURATION DES PARAMETRES DE NOTIFICATIONS

Kaspersky Security Center offre la possibilité de configurer les paramètres de notification de l'administrateur pour les événements survenus sur les postes clients et de sélectionner le mode de notification :

- courrier électronique ;
- SMS ;
- fichier exécutable.

Pour configurer les paramètres de notifications sur les événements survenus sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez la fenêtre des propriétés du dossier **Rapports et notifications** à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Rapports et notifications**, sélectionnez l'option **Propriétés**.
   - Dans la zone de travail du dossier **Rapports et notifications** sous l'onglet **Notifications**, ouvrez la fenêtre à l'aide du lien **Modifier les paramètres d'envoi des notifications**.
2. Dans la section **Notification** de la fenêtre des propriétés du dossier **Rapports et notifications**, configurez les paramètres de notifications pour les événements.

Les paramètres configurés de notification sont diffusés sur tous les événements survenus sur les postes clients.

Vous pouvez configurer les paramètres de notification pour l'événement dans la fenêtre des propriétés de cet événement. L'accès rapide aux paramètres d'événements s'effectue à l'aide des liens **Modifier les paramètres des événements de Kaspersky Endpoint Security** et **Modifier les paramètres des événements du Serveur d'administration**.

VOIR EGALEMENT

Configuration des paramètres du traitement des événements 55

SELECTIONS D'EVENEMENTS

Les informations sur les événements survenus pendant le fonctionnement de Kaspersky Security Center et sur les applications administrés sont enregistrées dans le journal système Microsoft Windows et dans le journal des événements Kaspersky Security Center. Vous pouvez consulter les informations du journal des événements Kaspersky Security Center dans le dossier de l'arborescence de la console **Rapports et notifications** dans le sous-dossier **Evénements**.

Les informations dans le dossier **Evénements** sont présentées sous forme des sélections dont chaque sélection inclut les événements qui répondent aux conditions particulières. Une fois que l'application a été installée, le dossier contient diverses sélections standards. Vous pouvez créer des sélections complémentaires d'événements, ainsi qu'exporter les informations sur les événements dans un fichier.

DANS CETTE SECTION

CONSULTATION D'UNE REQUETE D'EVENEMENTS

Pour consulter une sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Ouvrez une sélection d'événements par l'un des moyens suivants :
   - Ouvrez le dossier **Evénements** et sélectionnez le dossier avec la sélection d'événements nécessaire.
   - Dans la zone de travail du dossier **Evénements** à l'aide du lien correspondant au nom de la sélection d'événements nécessaires.

La zone de travail reprend la liste des événements du type sélectionné enregistrés sur le Serveur d'administration.

Vous pouvez trier les informations dans la liste des événements en ordre croissant ou décroissant à partir de n'importe quel paramètre.

CONFIGURATION D'UNE REQUETE D'EVENEMENTS

Pour configurer la sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Ouvrez la fenêtre de la sélection d'événements nécessaire dans le dossier **Evénements**.
3. Ouvrez la fenêtre des propriétés de la sélection à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la sélection, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Propriété de la sélection** dans le groupe d'administration de la sélection d'événements.

   Dans la fenêtre ouverte des propriétés de la sélection d'événements, vous pouvez configurer les paramètres de la sélection.

CREATION D'UNE REQUETE D'EVENEMENTS

Pour créer une sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Lancez le processus de création d'une sélection d'événements via l'un des moyens suivants :
   - Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Nouvelle requête**.
   - A l'aide du lien **Créer une sélection** dans la zone de travail du dossier **Evénements**.
3. Dans la fenêtre ouverte **Nouvelle sélection d'événements**, indiquez le nom de la sélection créée et cliquez sur le bouton **OK**.

Finalement, dans l'arborescence de la console dans le dossier **Evénements** un nouveau dossier avec le nom, que vous avez indiqué, sera créé.

Par défaut, la sélection d'événements créée contient tous les événements enregistrés sur le Serveur d'administration. Pour que la sélection d'événements affiche uniquement les événements qui vous intéressent, il faut configurer les paramètres de sélection.

EXPORTATION D'UNE SELECTION DANS LE FICHIER TEXTE

Pour exporter la sélection d'événements dans un fichier texte, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Ouvrez la fenêtre de la sélection d'ordinateurs nécessaire dans le dossier **Evénements**.
3. Lancez le processus d'exportation d'une sélection d'événements via l'un des moyens suivants :
   - Dans le menu contextuel d'une requête d'événements, sélectionnez l'option **Toutes les tâches** → **Exporter**.
   - A l'aide du lien **Exporter les événements dans un fichier** dans le groupe d'administration de la sélection d'événements.

Finalement, l'Assistant d'exportation des événements se lancera. Suivez les instructions de l'Assistant.

SUPPRESSION DES EVENEMENTS DEPUIS LA SELECTION

Pour supprimer un événement, procédez comme suite :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Evénements**.
2. Ouvrez la fenêtre de la sélection d'ordinateurs nécessaire dans le dossier **Evénements**.
3. Sélectionnez les événements à supprimer à l'aide de la souris et des touches **Shift** ou **Ctrl**.
4. Supprimez les événements sélectionnés via l'un des moyens suivants :
   - Dans le menu contextuel du n'importe quel événement parmi les événements sélectionnés, sélectionnez l'option **Supprimer**.

     Lors de la sélection de l'option du menu contextuel **Supprimer tout**, tous les événements affichés, peu importe les événements que vous avez sélectionnés pour supprimer, seront supprimés de la sélection.
   - A l'aide du lien **Supprimer l'événement** si un événement a été sélectionné, ou à l'aide du lien **Supprimer les événements** si plusieurs événements ont été sélectionnés dans le groupe de travail avec les événements sélectionnés.

Finalement, les événements sélectionnés seront supprimés du dossier **Evénements**.

SELECTION D'ORDINATEURS

Les informations relatives à l'état des postes clients sont reprises dans un dossier de l'arborescence de la console **Rapports et notifications** dans le sous-dossier **Sélections d'ordinateurs**.

Les informations dans le dossier **Sélections d'ordinateurs** sont présentées sous forme d'un ensemble de sélections avec chaque sélection affichant les informations sur les ordinateurs qui répondent aux conditions particulières. Une fois que l'application a été installée, le dossier contient diverses sélections standards. Vous pouvez créer les sélections d'ordinateurs complémentaires, exporter les paramètres des sélections dans un fichier, ainsi que créer les sélections avec les paramètres importés du fichier.

DANS CETTE SECTION

AFFICHAGE D'UNE SELECTION D'ORDINATEURS

Pour afficher une sélection d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Ouvrez une sélection d'ordinateurs à l'aide d'un des modes suivants :
   - Ouvrez le dossier **Sélections d'ordinateurs** et sélectionnez le dossier avec la sélection d'ordinateur nécessaire.
   - Dans la zone de travail du dossier **Sélections d'ordinateurs** à l'aide du lien correspondant au nom de la sélection d'ordinateurs nécessaire.

Finalement, la zone de travail présentera la liste des ordinateurs qui répondent aux paramètres de la sélection.

Vous pouvez trier les informations dans la liste des ordinateurs en ordre croissant ou décroissant à partir de n'importe quel paramètre.

CONFIGURATION D'UNE SELECTION D'ORDINATEURS

Pour configurer la sélection d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Ouvrez la fenêtre de la sélection d'ordinateurs nécessaire dans le dossier **Sélections d'ordinateurs**.

3. Ouvrez la fenêtre des propriétés de la sélection à l'aide d'un des moyens suivants :

   - Dans le menu contextuel de la sélection, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Propriété de la sélection** dans le groupe d'administration de la sélection d'ordinateurs.

Dans la fenêtre ouverte des propriétés de la sélection d'ordinateurs, vous pouvez configurer ses paramètres.

CREATION D'UNE SELECTION D'ORDINATEURS

Pour créer une sélection d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Lancez le processus de création d'une sélection d'ordinateurs via l'un des moyens suivants :

   - Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Nouvelle requête**.
   - A l'aide du lien **Créer une sélection** dans la zone de travail du dossier **Sélections d'ordinateurs**.

3. Dans la fenêtre ouverte **Nouvelle sélection d'ordinateurs**, indiquez le nom de la sélection créée et cliquez sur le bouton **OK**.

Finalement, dans l'arborescence de la console dans le dossier **Sélections d'ordinateurs** un nouveau dossier avec le nom, que vous avez indiqué, sera créé.

Par défaut, la sélection créée d'ordinateurs contient tous les ordinateurs inclus dans les groupes d'administration du Serveur sous l'administration duquel la sélection a été créée. Pour que la sélection d'événements affiche uniquement les ordinateurs qui vous intéressent, il faut configurer les paramètres de sélection.

EXPORTATION DES PARAMETRES DE LA SELECTION D'ORDINATEURS DANS UN FICHIER

Pour exporter les paramètres de la sélection d'ordinateurs dans le fichier texte, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Ouvrez la fenêtre de la sélection d'ordinateurs nécessaire dans le dossier **Sélections d'ordinateurs**.
3. Dans le menu contextuel d'une requête d'ordinateurs, sélectionnez l'option **Toutes les tâches** → **Exporter les paramètres**.
4. Dans la fenêtre ouverte **Enregistrer sous**, définissez le nom du fichier d'exportation des paramètres de la sélection, sélectionnez le dossier à enregistrer ce fichier et cliquez sur le bouton **Enregistrer**.

Les paramètres de la sélection d'ordinateurs seront enregistrés dans le fichier indiqué.

CREATION D'UNE SELECTION D'ORDINATEURS SELON LES PARAMETRES IMPORTES

Créer une sélection d'ordinateurs selon les paramètres importés :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Créer une sélection d'ordinateurs selon les paramètres, importés depuis le fichier, à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du dossier, sélectionnez l'option **Toutes les tâches** → **Importer**.
   - A l'aide du lien **Importer une sélection depuis un fichier** dans le groupe d'administration du dossier.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer les paramètres de la sélection. Cliquez sur **Ouvrir**.

Finalement, le dossier **Sélections d'ordinateurs** affiche la sélection **Nouvelle sélection** dont les paramètres ont été importés depuis le fichier indiqué.

Si dans le dossier **Sélections d'ordinateurs** une sélection avec le nom **Nouvelle sélection** existe déjà, le suffixe de type **(<numéro d'ordre>)**, par exemple : **(1)**, **(2)** sera ajouté au nom de la sélection créée.

SUPPRESSION DES ORDINATEURS DEPUIS LES GROUPES D'ADMINISTRATION DANS LA SELECTION

Lors du travail avec la sélection d'ordinateurs, vous pouvez supprimer les ordinateurs depuis les groupes d'administration sans travailler avec les groupes d'administration depuis lesquels il faut supprimer les ordinateurs.

Pour supprimer les ordinateurs depuis les groupes d'administration, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Sélections d'ordinateurs**.
2. Ouvrez la fenêtre de la sélection d'ordinateurs nécessaire dans le dossier **Sélections d'ordinateurs**.
3. Sélectionnez les ordinateurs à supprimer à l'aide des boutons **Shift** ou **Ctrl**.
4. Supprimez les ordinateurs sélectionnés depuis les groupes d'administration à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du n'importe quel ordinateur parmi les ordinateurs sélectionnés, sélectionnez l'option **Supprimer**.
   - A l'aide du lien **Supprimer du groupe** dans le groupe de travail avec les ordinateurs sélectionnés.

Finalement, les ordinateurs sélectionnés seront supprimés depuis les groupes d'administration dont ils faisaient partie.

ORDINATEURS NON DEFINIS

Cette section reprend les informations sur l'utilisation des ordinateurs du réseau de l'entreprise, non inclus dans les groupes d'administration.

Les informations relatives aux ordinateurs du réseau de l'entreprise qui n'appartiennent pas à un groupe d'administration figurent dans le dossier **Ordinateurs non définis**. Le dossier **Ordinateurs non définis** contient trois sous-dossiers : **Domaines**, **Plages IP** et Active Directory.

Dans le dossier **Ordinateurs non définis** du Serveur d'administration virtuel, le dossier **Plages IP** est absent. Les postes clients, trouvés lors du sondage des plages IP sur le Serveur virtuel, s'affichent dans le dossier **Domaines**.

Le dossier **Domaines** contient la hiérarchie des dossiers, qui affichent la structure des domaines et des groupes de fonctionnement du réseau Windows de l'entreprise, non inclus dans les groupes d'administration. Chaque sous-dossier parmi les sous-dossiers du dossier **Domaines** du niveau final contient la liste des ordinateurs du domaine ou du groupe de fonctionnement. Lors de l'inclusion de l'ordinateur dans n'importe quel groupe d'administration, les informations sur ces ordinateurs se suppriment du dossier **Domaines**. Lors de l'exclusion de l'ordinateur du groupe d'administration, les informations sur cet ordinateur apparaissent à nouveau dans le dossier **Domaines**, dans le sous-dossier du domaine ou dans le groupe de fonctionnement incluant l'ordinateur.

La représentation des ordinateurs dans le dossier **Active Directory** repose sur la structure des groupes Active Directory.

La représentation des ordinateurs dans le dossier **Plages IP** repose sur la structure des plages IP créés sur le réseau d'entreprise. Vous pouvez modifier la structure du dossier **Plages IP**, en créant des nouvelles plages IP et en modifiant les plages IP existantes.

DANS CETTE SECTION

SONDAGE DU RESEAU

Le Serveur d'administration obtient les informations relatives à la structure du réseau et aux ordinateurs qui en font partie lors des sélections fréquentes adressées au réseau Windows, aux sous-réseaux IP ou Active Directory créés dans le réseau informatique de l'entreprise. Le contenu du dossier **Ordinateurs non définis** est actualisé sur la base du résultat de ces sélections.

Le Serveur d'administration peut réaliser les types de sondage du réseau suivants :

- **Sondage du réseau Windows**. Il existe deux types de sondage du réseau Windows : rapide et complet. Lors du sondage rapide, seules les informations relatives à la liste des noms NetBIOS des ordinateurs de tous les domaines et des groupes de travail du réseau sont récoltées. Durant le sondage complet, les informations suivantes sont demandées depuis chaque poste client : nom du système d'exploitation, adresse IP, nom DNS, nom NetBIOS.

- **Sondage des plages IP**. Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP et rassemble toutes les informations sur les ordinateurs appartenant aux plages IP.

- **Sondage des groupes Active Directory**. Les données du Serveur d'administration permettent d'enregistrer des informations relatives à la structure des groupes Active Directory, ainsi qu'aux noms DNS des ordinateurs du groupe Active Directory.

Sur la base des informations obtenues et des données sur la structure du réseau de l'entreprise, Kaspersky Security Center actualise le contenu des dossiers **Ordinateurs non définis** et **Ordinateurs administrés**. Si dans le réseau de l'entreprise le déplacement automatique des ordinateurs dans les groupes d'administration est configuré, les ordinateurs détectés dans le réseau sont inclus dans les groupes d'administration.

DANS CETTE SECTION

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONDAGE DU RESEAU WINDOWS

Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Domaines**.

2. La fenêtre **Propriétés : Domaines** s'ouvre à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du dossier, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Modifier les paramètres du sondage** dans le groupe d'administration du dossier.

   Finalement, la fenêtre **Propriétés : Domaines** s'ouvre. Cette fenêtre permet de modifier les paramètres du sondage du réseau Windows.

Vous pouvez aussi modifier les paramètres du sondage du réseau Windows dans la zone de travail du dossier **Ordinateurs non définis** à l'aide du lien **Modifier les paramètres du sondage** dans le groupe **Sondage du réseau Windows**.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage du réseau Windows sont effectués dans la fenêtre des propriétés de l'agent de mise à jour, dans la section **Sondage du réseau**.

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONDAGE DES GROUPES ACTIVE DIRECTORY

Pour modifier les paramètres de sondage des groupes Active Directory, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Active Directory**.

2. La fenêtre **Propriétés : Active Directory** s'ouvre à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du dossier, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Modifier les paramètres du sondage** dans le groupe d'administration du dossier.

   La fenêtre **Propriétés : Active Directory** s'ouvre. Cette fenêtre permet de modifier les paramètres du sondage des groupes Active Directory.

Vous pouvez aussi modifier les paramètres du sondage des groupes Active Directory dans la zone de travail du dossier **Ordinateurs non définis** à l'aide du lien **Modifier les paramètres du sondage** dans le groupe **Sondage Active Directory**.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage des groupes Active Directory sont effectués dans la fenêtre des propriétés de l'agent de mise à jour, dans la section **Sondage du réseau**.

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONDAGE DES PLAGES IP

Pour modifier les paramètres du sondage des plages IP, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le dossier **Plages IP**.
2. La fenêtre **Propriétés : Plages IP** s'ouvre à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du dossier, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres du sondage** dans le groupe d'administration du dossier.

   La fenêtre **Propriétés : Plages IP** s'ouvre. Cette fenêtre permet de modifier les paramètres du sondage des plages IP.

Vous pouvez aussi modifier les paramètres du sondage des plages IP dans la zone de travail du dossier **Ordinateurs non définis** à l'aide du lien **Modifier les paramètres du sondage** dans le groupe **Sondage des plages IP**.

Sur le Serveur d'administration virtuel l'affichage et la modification des paramètres du sondage des plages IP sont effectués dans la fenêtre des propriétés de l'agent de mise à jour, dans la section **Sondage du réseau**. Les postes clients, trouvés suite au sondage des plages IP, s'affichent dans le dossier **Domaines** du Serveur virtuel.

TRAVAIL AVEC LES DOMAINES WINDOWS. AFFICHAGE ET MODIFICATION DES PARAMETRES DU DOMAINE

Pour modifier les paramètres du domaine, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Domaines**.
2. Sélectionnez le domaine et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du domaine, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Afficher les propriétés du groupe**.

   La fenêtre **Propriété : <Nom du domaine>** s'ouvre. Cette fenêtre permet de configurer les paramètres du domaine sélectionné.

TRAVAIL AVEC LES PLAGES IP

Vous pouvez configurer les paramètres des plages IP existantes, ainsi que créer les nouvelles plages IP.

DANS CETTE SECTION

CREATION DE LA PLAGE IP

Pour créer une plage IP, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Plages IP**.
2. Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Plage IP**.
3. Dans la fenêtre ouverte **Nouvelle plage IP**, configurez les paramètres de la plage IP créée.

La plage IP créée apparaîtra dans le dossier **Plages IP**.

AFFICHAGE ET MODIFICATION DES PARAMETRES DE PLAGE IP

Pour modifier les paramètres de la plage IP, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Plages IP**.
2. Sélectionnez la plage IP et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la plage IP, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Afficher les propriétés du groupe**.

La fenêtre **Propriétés : <Nom de la plage IP>** s'ouvre. Cette fenêtre permet de configurer les paramètres de la plage IP sélectionnée.

TRAVAIL AVEC LES GROUPES ACTIVE DIRECTORY. AFFICHAGE ET MODIFICATION DES PARAMETRES DU GROUPE

Pour modifier les paramètres du groupe Active Directory, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs non définis**, sélectionnez le sous-dossier **Active Directory**.
2. Sélectionnez le groupe Active Directory et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
   - Dans le menu contextuel du groupe, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Afficher les propriétés du groupe**.

La fenêtre **Propriété : <Nom du groupe Active Directory>** s'ouvre. Cette fenêtre permet de configurer les paramètres du groupe Active Directory sélectionné.

TRAVAIL AVEC LA LISTE GLOBALE DES UTILISATEURS

Suite au sondage du réseau, les données sur les utilisateurs détectés dans le réseau sont transmises sur le Serveur d'administration. Le dossier **Comptes utilisateurs** de l'arborescence de la console permet de consulter les données sur les utilisateurs.

Les commandes suivantes sont disponibles dans le menu contextuel du compte utilisateur :

- **Envoyer le message par courrier électronique**. La fenêtre **Message à l'utilisateur** s'ouvre. A l'aide de cette commande, il est possible d'envoyer le message électronique à l'utilisateur. Le lien pour télécharger le paquet des applications mobiles peut être ajouté dans un tel message.
- **Envoyer le message SMS**. La fenêtre **Texte SMS** s'ouvre. Cette commande permet d'envoyer un message SMS à l'utilisateur. Le lien pour télécharger le paquet des applications mobiles (cf. section "Installation de l'application sur le périphérique mobile à l'aide du paquet des applications mobiles" à la page 129) peut être ajouté dans un tel message.
- **Installer le certificat**. La fenêtre **Désignation du certificat** s'ouvre. Cette commande permet d'installer le certificat sur le périphérique mobile de l'utilisateur.
- **Installer le profil iOS MDM**. La fenêtre **Installation du profil iOS MDM** s'ouvre. Cette commande permet d'installer le profil iOS MDM sur le périphérique mobile de l'utilisateur. Cette fonctionnalité est disponible uniquement pour les périphériques mobiles iOS MDM.
- **Exporter la liste**. La fenêtre **Exporter la liste** s'ouvre. Cette fenêtre permet d'enregistrer la liste des utilisateurs dans le fichier.
- **Propriétés**. Ouvre la fenêtre des propriétés du compte qui permet de consulter les informations sur l'utilisateur.

CREATION DES REGLES DE DEPLACEMENT AUTOMATIQUE DES ORDINATEURS DANS UN GROUPE D'ADMINISTRATION

Vous pouvez configurer le déplacement automatique des ordinateurs, détectés lors du sondage du réseau de l'entreprise, dans les groupes d'administration.

Pour configurer la règle de déplacement automatique des ordinateurs dans un groupe d'administration,

ouvrez la fenêtre des propriétés du dossier **Ordinateurs non définis** à l'aide d'un des moyens suivants :

- Dans le menu contextuel du dossier, sélectionnez l'option **Propriétés**.
- A l'aide du lien **Configurer les règles du déplacement des ordinateurs vers le groupe d'administration** dans la zone de travail du dossier.

Finalement, la fenêtre **Propriétés : Ordinateurs non définis** s'ouvre. Configurez la règle de déplacement automatique des ordinateurs dans un groupe d'administration dans la section **Déplacement des ordinateurs**.

UTILISATION DU MODE DYNAMIQUE VDI SUR LES POSTES CLIENTS

Kaspersky Security Center prend en charge la possibilité d'activation du mode dynamique Virtual Desktop Infrastructure (VDI). Si le mode VDI est activé sur le poste client, cet ordinateur ne sera pas affiché dans la liste des postes clients connectés lors de l'arrêt du poste client, et les données sur celui-ci seront supprimées de la base. Cette possibilité sera utile lors de l'utilisation d'un grand nombre de machines virtuelles dans le réseau de l'entreprise. Lors de l'arrêt de la machine virtuelle ou lors de son retour dans l'état enregistré, cette machine virtuelle ne sera pas affichée dans la liste des ordinateurs connectés au Serveur d'administration. Les données sur les ordinateurs arrêtés sont actualisées à l'expiration du temps d'attente constitué de trois périodes et demi de synchronisation de l'Agent d'administration plus 25 minutes.

DANS CETTE SECTION

ACTIVATION DU MODE DYNAMIQUE VDI DANS LES PROPRIETES DU PAQUET D'INSTALLATION DE L'AGENT D'ADMINISTRATION

Pour activer le mode dynamique VDI, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : Agent d'administration de Kaspersky Security Center** s'ouvre.
3. Dans la fenêtre **Propriétés : Agent d'administration de Kaspersky Security Center**, sélectionnez la section **Avancé**.
4. Dans la section **Avancé**, cochez la case **Activer le mode dynamique pour VDI**.

Le poste client sur lequel l'Agent d'administration s'installe sera une partie de Virtual Desktop Infrastructure.

RECHERCHE D'ORDINATEURS QUI FONT PARTIE DE VDI

Pour rechercher les ordinateurs qui font partie de VDI, procédez comme suit :

1. Dans la zone de travail du dossier **Ordinateurs non définis** à l'aide du lien **Rechercher les ordinateurs non définis**, ouvrez la fenêtre **Recherche**.
2. Dans la fenêtre **Recherche** sous l'onglet **Machines virtuelles** dans la liste déroulante **Membre d'une Virtual Desktop Infrastructure**, sélectionnez l'option **Oui**.
3. Cliquez sur le bouton **Rechercher**.

La recherche d'ordinateurs membres de Virtual Desktop Infrastructure sera exécutée.

DEPLACEMENT DANS LE GROUPE D'ADMINISTRATION DES ORDINATEURS QUI FONT PARTIE DE VDI

Pour déplacer les ordinateurs qui font partie de VDI dans le groupe d'administration, procédez comme suit :

1. Dans la zone de travail du dossier **Ordinateurs non définis** à l'aide du lien **Configurer les règles de déplacement des ordinateurs vers le groupe d'administration**, ouvrez la fenêtre des propriétés du dossier **Ordinateurs non définis**.
2. Dans la fenêtre des propriétés du dossier **Ordinateurs non définis** dans la section **Déplacement des ordinateurs**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouvelle règle** s'ouvre.
3. Dans la fenêtre **Nouvelle règle**, sélectionnez la section **Machines virtuelles**.
4. Dans la liste déroulante **Membre d'une Virtual Desktop Infrastructure**, sélectionnez l'option **Oui**.

La règle de déplacement des ordinateurs dans le groupe d'administration sera créée.

ADMINISTRATION DES APPLICATIONS SUR LES POSTES CLIENTS

Kaspersky Security Center permet d'administrer les applications de Kaspersky Lab et d'autres éditeurs installées sur les postes clients.

L'administrateur peut exécuter les actions suivantes :

- créer les catégories des applications sur la base des critères définis ;
- administrer les catégories des applications à l'aide des règles spécialement créées ;
- administrer le lancement des applications sur les postes clients ;
- exécuter l'inventaire et suivre le registre du logiciel installé sur les postes clients ;
- corriger les vulnérabilités du logiciel installé sur les postes clients ;
- installer les mises à jour Windows Update et d'autres éditeurs de logiciels sur les postes clients ;
- surveiller l'utilisation des clés pour les groupes des applications sous licence.

DANS CETTE SECTION

GROUPES DES APPLICATIONS

Cette section décrit l'utilisation des groupes des applications installées sur les postes clients.

Création des catégories d'applications

Kaspersky Security Center permet de créer les catégories des applications installées sur les postes clients.

Il est possible de créer les catégories à l'aide des moyens suivants :

- L'administrateur indique le dossier dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur indique l'ordinateur dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur définit les critères selon lesquels les applications se trouvent dans la catégorie sélectionnée.

Quand une catégorie des applications est créée, l'administrateur peut définir les règles pour cette catégorie des applications. Les règles définissent le comportement des applications qui sont incluses dans la catégorie indiquée. Par exemple, il est possible d'interdire ou d'autoriser le lancement des applications qui font partie de la catégorie.

Administration du lancement des applications sur les postes clients

Kaspersky Security Center permet de gérer le lancement des applications sur les postes clients en mode "Tout ce qui n'est pas autorisé est interdit" (pour plus d'informations, cf. Manuel de l'administrateur pour l'application Kaspersky Endpoint Security 10 for Windows). Le mode "Tout ce qui n'est pas autorisé est interdit" signifie que le lancement uniquement des applications, qui font partie des catégories indiquées, sera autorisé sur les postes clients sélectionnés. L'administrateur peut consulter les résultats de l'analyse statique des règles de lancement des applications sur les postes clients pour chaque utilisateur.

Inventaire du logiciel installé sur les postes clients

Kaspersky Security Center permet d'exécuter l'inventaire du logiciel sur les postes clients. L'Agent d'administration collecte les informations sur toutes les applications installées sur les postes clients. Les informations obtenues suite à l'inventaire s'affichent dans la zone de travail du dossier **Registre des applications**. L'administrateur peut consulter les informations détaillées sur chaque application, y compris la version et l'éditeur.

Administration des groupes des applications sous licence

Kaspersky Security Center permet de créer les groupes des applications sous licence. Le groupe des applications sous licence inclut les applications qui répondent aux critères définis par l'administrateur. L'administrateur peut indiquer les critères suivants pour les groupes des applications sous licence :

- nom de l'application ;
- version de l'application ;
- éditeur ;
- repère de l'application.

Les applications qui correspondent à un ou plusieurs critères sont placées automatiquement dans le groupe. Pour créer un groupe des applications sous licence, au moins un critère d'inclusion des applications dans ce groupe doit être défini.

Chaque groupe des applications sous licence possède sa clé. La clé du groupe des applications sous licence définit le nombre admissible des installations pour les applications qui font partie du groupe. Si le nombre d'installations dépasse la restriction définie dans la clé, l'événement d'informations s'enregistre sur le Serveur d'administration. L'administrateur peut indiquer la date de fin de validité de la clé. Lorsque cette date survient, l'événement d'information est enregistré sur le Serveur d'administration.

Consultation des informations sur les fichiers exécutables

Kaspersky Security Center collecte toutes les informations sur les fichiers exécutables qui ont été lancés sur les postes clients dès le moment d'installation du système d'exploitation sur ceux-ci. Les informations collectées sur les fichiers exécutables s'affichent dans la fenêtre principale de l'application, dans la zone de travail du dossier **Fichiers exécutables**.

DANS CETTE SECTION

CREATION DES CATEGORIES D'APPLICATIONS

Pour créer une catégorie d'applications, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Catégories des applications**.

2. Le lien **Créer une catégorie** permet de lancer l'Assistant de création de la catégorie d'utilisateur.

3. Sélectionnez le type de la catégorie d'utilisateur dans la fenêtre de l'Assistant :

   - **Catégorie complétée à la main**. Dans ce cas, vous pouvez définir manuellement les critères selon lesquels les fichiers exécutables feront partie de la catégorie créée.

   - **Catégorie complétée automatiquement**. Dans ce cas, vous pouvez indiquer le dossier dont les fichiers exécutables seront automatiquement placés dans la catégorie créée.

   - **Catégorie incluant les fichiers exécutables depuis les ordinateurs sélectionnés**. Dans ce cas, vous pouvez indiquer l'ordinateur. Les fichiers exécutables détectés sur l'ordinateur seront automatiquement placés dans la catégorie.

4. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la catégorie d'utilisateur des applications est créée. Il est possible de consulter les catégories créées dans le dossier **Catégories des applications**.

CONFIGURATION D'ADMINISTRATION DU LANCEMENT DES APPLICATIONS SUR LES POSTES CLIENTS

Pour configurer la gestion du lancement des applications sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Catégories des applications**.

2. Dans la zone de travail du dossier **Catégories des applications**, créez une catégorie des application (cf. section “Création des catégories des applications” à la page 104) dont vous voulez gérer le lancement.

3. Dans le dossier **Ordinateurs administrés** sous l'onglet **Stratégie** à l'aide du lien **Créer une stratégie de Kaspersky Endpoint Security**, lancez l'Assistant de création de la stratégie pour l'application Kaspersky Endpoint Security 10 for Windows et suivez les consignes de l'Assistant.

   Si une telle stratégie déjà existe, cette étape peut être ignorée. L'administration du lancement des applications dans la catégorie indiquée peut être configurée dans les paramètres de cette stratégie. La stratégie créée s'affiche dans le dossier **Ordinateurs administrés** sous l'onglet **Stratégies**.

4. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés** pour l'application Kaspersky Endpoint Security10 for Windows.

   La fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows s'ouvre.

5. Dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows dans la section **Contrôle du lancement des applications**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

6. Dans la fenêtre **Règle de contrôle du lancement des applications** dans la liste déroulante **Catégorie**, sélectionnez la catégorie des applications pour laquelle la règle du lancement sera diffusée. Configurez les paramètres de la règle du lancement pour la catégorie sélectionnée des applications.

   Pour plus de détails sur les règles de contrôle du lancement des applications, cf. Manuel de l'administrateur de Kaspersky Endpoint Security 10 for Windows.

7. Cliquez sur le bouton **OK**.

Le lancement des applications sur les postes clients qui font partie de la catégorie indiquée sera exécuté conformément à la règle créée. La règle créée s'affichent dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 10 for Windows dans la section **Contrôle du lancement des applications**.

CONSULTATION DES RESULTATS DE L'ANALYSE STATIQUE DES REGLES DE LANCEMENT DES FICHIERS EXECUTABLES

Pour consulter les informations sur le lancement des fichiers exécutables interdits par l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Ordinateurs administrés**, sélectionnez l'onglet **Stratégies**.
2. Dans le menu contextuel **Stratégies de protection**, choisissez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie de protection s'ouvre.

3. Dans la fenêtre des propriétés, sélectionnez la section **Contrôle du lancement des applications** et cliquez sur le bouton **Analyse statique**.

   La fenêtre **Analyse de la liste des privilèges d'accès** s'ouvre.

4. La partie gauche de la fenêtre **Analyse de la liste des privilèges d'accès** affiche la liste des utilisateurs composée sur la base des données Active Directory.
5. Sélectionnez l'utilisateur dans la liste.

   La partie droite de la fenêtre affichera les catégories des applications désignées à cet utilisateur.

6. Pour consulter les fichiers exécutables dont le lancement est interdit par l'utilisateur, cliquez sur le bouton **Consulter les fichiers** dans la fenêtre **Analyse de la liste des privilèges d'accès**.

   La fenêtre s'ouvre. Cette fenêtre affiche la liste des fichiers exécutables dont le lancement est interdit par l'utilisateur.

7. Pour consulter la liste de fichiers exécutables qui font partie d'une catégorie,, sélectionnez la catégorie des applications et cliquez sur le bouton **Consulter les fichiers de la catégorie**.

La fenêtre s'ouvre. Cette fenêtre affiche la liste des fichiers exécutables qui font partie de la catégorie des applications.

CONSULTATION DU REGISTRE DES APPLICATIONS

Pour consulter le registre des applications installées sur les postes clients,

dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le sous-dossier **Registre des applications**.

La zone de travail du dossier **Registre des applications** affiche la liste des applications détectées sur les postes clients par l'Agent d'administration installés sur ces postes.

La fonctionnalité du recueil d'information sur les applications installées est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

- *Pour consulter les propriétés de l'application sélectionnée,*

  dans le menu contextuel de l'application, sélectionnez l'option **Propriétés.**

  La fenêtre qui affiche les informations générales sur l'application et les informations sur les fichiers exécutables de l'application, ainsi que la liste des ordinateurs avec l'application installée s'ouvrira.

Pour consulter les applications qui satisfont les critères définis, vous pouvez utiliser les champs de filtrage dans la zone de travail du dossier **Registre des applications**.

Les informations relatives aux applications sur les postes clients connectés aux Serveurs d'administration secondaires et virtuels sont également rassemblées et enregistrées dans le registre des applications du Serveur d'administration principal. Vous pouvez consulter ces informations à l'aide du rapport de registre des applications, en incluant dans le rapport les données de la part des Serveurs d'administration virtuels et secondaires.

- *Pour inclure dans le rapport les informations depuis les Serveurs d'administration secondaires, procédez comme suit :*

  1. Dans le dossier **Rapports et notifications**, sélectionnez **Rapport sur les versions des logiciels de Kaspersky Lab**.

  2. Dans le menu contextuel du rapport, sélectionnez l'option **Propriétés**.

     La fenêtre **Propriétés : Rapport sur les versions des logiciels de Kaspersky Lab** s'ouvrira.

  3. Dans la section **Hiérarchie des Serveurs d'administration**, cochez la case **Utiliser les données à partir des Serveurs d'administration secondaires et virtuels**.

CREATION DES GROUPES DES APPLICATIONS DE LICENCE

- *Pour créer un groupe des applications sous licence, procédez comme suit :*

  1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Administration des groupes des applications sous licence**.

  2. A l'aide du lien **Ajouter le groupe des applications sous licence**, lancez **Assistant d'ajout du groupe des applications sous licence**.

  3. Suivez les instructions de l'Assistant.

  Suite au fonctionnement de l'Assistant, le groupe des applications sous licence est créé. Ce groupe s'affiche dans le dossier **Administration des groupes des applications sous licence**.

ADMINISTRATION DES CLES POUR LES GROUPES DES APPLICATIONS SOUS LICENCE

- *Pour créer une clé pour le groupe des applications sous licence, procédez comme suit :*

  1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Administration des groupes des applications sous licence**.

  2. Dans la zone de travail du dossier **Administration des groupes des applications sous licence** à l'aide du lien **Administrer les clés des applications sous licence**, ouvrez la fenêtre **Administration des clés des applications sous licence**.

  3. Dans la fenêtre **Administration des clés des applications sous licence**, cliquez sur le bouton **Ajouter**.

     Le fenêtre **Clé** s'ouvre.

4. Dans la fenêtre **Clé**, indiquez les paramètres de la clé et les restrictions que cette clé impose sur le groupe des applications sous licence.

   - **Nom**. Le nom de la clé.
   - **Commentaires**. Les remarques de la clé sélectionnée.
   - **Limite**. Le nombre de postes clients sur lesquels l'application, utilisant cette clé, peut être installée.
   - **Date d'expiration**. La date d'expiration de validité de la clé.

Les clés créées s'affichent dans le dossier **Administration des clés des applications sous licence**.

Pour appliquer une clé au groupe des applications sous licence, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Administration des groupes des applications sous licence**.
2. Dans le dossier **Administration des groupes des applications sous licence**, sélectionnez le groupe des applications sous licence auquel vous voulez appliquer la clé.
3. Dans le menu contextuel du groupe des applications sous licence, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du groupe de licence s'ouvre.
4. Dans la fenêtre des propriétés du groupe des applications sous licence dans la section **Clés**, sélectionnez l'option **Contrôler la violation des restrictions de licence définie**.
5. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la clé** s'ouvre.
6. Dans la fenêtre **Sélection de la clé**, sélectionnez la clé que vous voulez appliquer au groupe des applications sous licence.
7. Cliquez sur le bouton **OK**.

Les restrictions pour le groupe des applications sous licence indiquées dans la clé seront diffusées sur le groupe sélectionné des applications sous licence.

CONSULTATION DES INFORMATIONS SUR LES FICHIERS EXECUTABLES

Pour consulter la liste de tous les fichiers exécutables détectés sur les postes clients,

Dans l'arborescence de la console du dossier **Rapports et notifications**, sélectionnez le joint **Fichiers exécutables**.

La zone de travail du dossier **Fichiers exécutables** affiche la liste des fichiers exécutables qui ont été lancés sur les postes clients dès le moment d'installation du système d'exploitation ou qui ont été détectés pendant le fonctionnement de la tâche d'inventaire de Kaspersky Endpoint Security 10 for Windows.

Pour consulter les données sur les fichiers exécutables qui satisfont les critères définis, vous pouvez utiliser le filtrage.

Pour consulter les propriétés du fichier exécutable,

dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.

La fenêtre qui contient les informations sur le fichier exécutable s'ouvre, ainsi que la liste des postes clients sur lesquels le fichier exécutable est présent.

VULNERABILITES DANS LES APPLICATIONS

Kaspersky Security Center permet de trouver et de corriger les vulnérabilités dans les applications installées sur les postes clients.

La recherche de vulnérabilités est exécutée à l'aide de la tâche **Recherche de vulnérabilités et de mises à jour des applications**. L'Agent d'administration collecte les informations sur toutes les applications installées sur les postes clients, et en cas de vulnérabilités détectées, il transmet les informations sur celles-ci au Serveur d'administration.

Après l'exécution de la tâche, vous pouvez consulter le rapport sur les vulnérabilités dans les applications, ainsi que les informations sur chaque vulnérabilité détectée et sur la mise à jour à installer pour fermer cette vulnérabilité.

Il est possible de corriger les vulnérabilités détectées dans les applications à l'aide de la tâche de groupe **Installation des mises à jour des applications et correction des vulnérabilités**.

La fonctionnalité du recueil d'information sur les vulnérabilités dans les applications est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

DANS CETTE SECTION

CONSULTATION DES INFORMATIONS RELATIVES AUX VULNERABILITES DANS LES APPLICATIONS

- *Pour consulter la liste des vulnérabilités détectées sur les postes clients,*

  dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Vulnérabilités dans les applications**.

  La zone de travail du dossier affiche la liste des vulnérabilités dans les applications détectées sur les postes clients par l'Agent d'administration installé sur ces postes.

- *Pour obtenir les informations sur la vulnérabilité sélectionnée,*

  dans le menu contextuel de la vulnérabilité, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la vulnérabilité s'ouvre. Cette fenêtre affiche les informations suivantes :

- l'application contenant la vulnérabilité ;
- la liste des ordinateurs avec la vulnérabilité détectée ;
- les informations sur la correction de la vulnérabilité.

- *Pour consulter le rapport sur toutes les vulnérabilités détectées,*

  dans le dossier **Vulnérabilités dans les applications**, utilisez le lien **Consulter le rapport de vulnérabilités dans les applications**.

  Le rapport sur les vulnérabilités dans les applications installées sur les postes clients sera créé. Le rapport peut être consulté dans le dossier **Rapports et notifications**.

La fonctionnalité du recueil d'information sur les vulnérabilités dans les applications est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

RECHERCHE DE VULNERABILITES DANS LES APPLICATIONS

Si vous avez exécuté la configuration de l'application à l'aide de l'Assistant de configuration initiale, la tâche de recherche de vulnérabilités est créée automatiquement. Il est possible de consulter la tâche dans le dossier **Ordinateurs administrés** sous l'onglet **Tâches**.

- *Pour créer une tâche de recherche de vulnérabilités dans les applications installées sur les postes clients, procédez comme suit :*

  1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Vulnérabilités dans les applications**.

  2. A l'aide du lien **Configurer la recherche de vulnérabilités** dans la zone de travail, lancez l'Assistant de création de la tâche de recherche de vulnérabilités et de mises à jour requises.

     La fenêtre de l'Assistant de création de la tâche s'ouvre.

  3. Suivez les instructions de l'Assistant.

  Une fois l'Assistant terminé, la tâche **Recherche de vulnérabilités et de mises à jour des applications** est créée. Cette tâche s'affiche dans la liste des tâches dans le dossier **Ordinateurs administrés** sous l'onglet **Tâches**.

FERMETURE DE VULNERABILITES DANS LES APPLICATIONS

Si dans l'Assistant de configuration initiale dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Rechercher et installer les mises à jour des applications**, la tâche **Installation des mises à jour des applications et correction des vulnérabilités** est créée automatiquement. La tâche s'affiche dans le dossier **Ordinateurs administrés** sous l'onglet **Tâches**.

- *Pour créer une tâche de correction des vulnérabilités à l'aide des mises à jour disponibles pour les applications, procédez comme suit :*

  1. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs administrés** sous l'onglet **Tâches**.

  2. Le lien **Création d'une tâche** permet de lancer l'Assistant de création d'une tâche.

  3. Dans la fenêtre de l'Assistant **Sélection du type de tâche**, indiquez le type de tâche **Installation des mises à jour des applications et correction des vulnérabilités**.

  4. Suivez les instructions de l'Assistant.

  Une fois l'Assistant terminé, la tâche **Installation des mises à jour des application et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Ordinateurs administrés** sous l'onglet **Tâche**.

MISES A JOUR DU LOGICIEL

Kaspersky Security Center permet d'administrer les mises à jour du logiciel installé sur les postes clients et de corriger les vulnérabilités dans les applications de Microsoft et d'autres éditeurs de logiciels à l'aide de l'installation des mises à jour nécessaires.

Kaspersky Security Center permet d'exécuter la recherche de mises à jour à l'aide de la tâche de recherche de mises à jour et télécharge les mises à jour dans le stockage des mises à jour. Après la fin de la recherche de mises à jour, l'application offre à l'administrateur les informations sur les mises à jour disponibles et sur les vulnérabilités dans les applications qui peuvent être fermées à l'aide de ces mises à jour.

Les informations sur les mises à jour Microsoft Windows disponibles sont transmises en provenance du centre des mises à jour Windows. Le Serveur d'administration peut être utilisé dans le rôle du serveur Windows Update (WSUS). Pour utiliser le Serveur d'administration dans le rôle du serveur Windows Update, il faut configurer la synchronisation des mises à jour avec le centre des mises à jour Windows. Après la configuration de la synchronisation des données avec le centre des mises à jour Windows, le Serveur d'administration, avec une fréquence définie, fournit les mises à jour aux services Windows Update sur les postes clients.

Il est aussi possible d'administrer les mises à jour du logiciel à l'aide de la stratégie de l'Agent d'administration. Pour ce faire, il faut créer la stratégie de l'Agent d'administration et de configurer les paramètres des mises à jour du logiciel dans les fenêtres correspondantes de l'Assistant de création de la stratégie.

L'administrateur peut consulter la liste des mises à jour disponibles dans le dossier **Mises à jour du logiciel** qui fait partie du dossier **Applications et vulnérabilités**. Ce dossier contient la liste des mises à jour obtenues par le Serveur d'administration des applications de Microsoft et d'autres éditeurs de logiciels qui peuvent être diffusées sur les postes clients. Après la consultation des informations sur les mises à jour disponibles, l'administrateur peut exécuter l'installation des mises à jour sur les postes clients.

Avant l'installation des mises à jour sur tous les postes clients, il est possible d'exécuter l'installation de contrôle pour s'assurer que les mises à jour installées ne provoquent pas d'erreurs pendant le fonctionnement des applications sur les postes clients.

DANS CETTE SECTION

CONSULTATION DES INFORMATIONS SUR LES MISES A JOUR DISPONIBLES

- *Pour consulter la liste des mises à jour disponibles pour les applications installées sur les postes clients,*

  dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Mises à jour du logiciel**.

  Dans la zone de travail du dossier, vous pouvez consulter la liste des mises à jour existantes pour les applications installées sur les postes clients.

- *Pour consulter les propriétés de la mise à jour,*

  dans la zone de travail du dossier **Mises à jour du logiciel** dans le menu contextuel de la mise à jour, sélectionnez l'option **Propriétés.**

Les informations suivantes sont accessibles à la consultation dans la fenêtre des propriétés de la mise à jour :

- la liste des postes clients pour lesquels la mise à jour est conçue (*ordinateurs ciblés*) ;
- les vulnérabilités dans les applications que cette mise à jour ferme.

SYNCHRONISATION DES MISES A JOUR WINDOWS UPDATE AVEC LE SERVEUR D'ADMINISTRATION

Si dans l'Assistant de configuration initiale dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Utiliser le Serveur d'administration dans le rôle du serveur WSUS**, la tâche de synchronisation des mises à jour Windows Update est automatiquement créée. Il est possible de lancer la tâche dans le dossier **Tâches du Serveur d'administration**. La fonctionnalité de mise à jour du logiciel est disponible uniquement après une fin réussie de la tâche **Synchronisation des mises à jour Windows Update**.

Pour créer la tâche de synchronisation des mises à jour Windows Update avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. A l'aide du lien **Configurer la synchronisation des mises à jour Windows Update**, lancez l'Assistant de création de la tâche d'obtention des données depuis le centre des mises à jour Windows.
3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche **Synchronisation des mises à jour Windows Update** est créée. Cette tâche s'affiche dans le dossier **Tâches du Serveur d'administration**.

La tâche de synchronisation des mises à jour Windows Update peut être aussi créée dans le dossier **Tâches du Serveur d'administration** à l'aide du lien **Créer une tâche**.

INSTALLATION DES MISES A JOUR SUR LES POSTES CLIENTS

Si dans l'Assistant de configuration initiale dans la fenêtre **Paramètres d'administration des mises à jour**, vous avez sélectionné l'option **Rechercher et installer les mises à jour des applications**, la tâche **Installation des mises à jour des applications et correction des vulnérabilités** est créée automatiquement. Il est possible d'arrêter ou de lancer la tâche dans le dossier **Ordinateurs administrés** sous l'onglet **Tâches**.

Si dans l'Assistant de configuration initiale vous avez sélectionné l'option **Rechercher les mises à jour requises pour l'installation**, vous pouvez installer les mises à jour du logiciel sur les postes clients à l'aide de la tâche **Installation des mises à jour des applications et correction des vulnérabilités**.

Pour créer une tâche d'installation des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Applications et vulnérabilités**, sélectionnez le sous-dossier **Mises à jour du logiciel**.
2. Dans le dossier **Mises à jour du logiciel,** ouvrez le menu contextuel de la mise à jour et sélectionnez l'option **Installer la mise à jour→ Nouvelle tâche** ou utilisez le lien **Installer la mise à jour** dans le groupe de fonctionnement avec les mises à jour sélectionnées.

   L'Assistant de création de la tâche d'installation des mises à jour et de correction des vulnérabilités s'ouvre.
3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche **Installation des mises à jour des application et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Ordinateurs administrés** sous l'onglet **Tâche**.

Dans les paramètres de la tâche d'installation des mises à jour, vous pouvez configurer l'installation de contrôle des mises à jour.

Pour configurer l'installation de contrôle des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Ordinateurs administrés** sous l'onglet **Tâches**, sélectionnez la tâche **Installation des mises à jour des applications et correction des vulnérabilités**.

2. Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de la tâche **Installation des mises à jour des applications et correction des vulnérabilités** s'ouvre.

3. Dans la fenêtre des propriétés de la tâche dans la section **Installation de contrôle**, sélectionnez une des options disponibles de l'installation de contrôle :

   - **Ne pas analyser**. Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

   - **Exécuter l'analyse sur les ordinateurs indiqués**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur certains ordinateurs. Cliquez sur le bouton **Ajouter** et sélectionnez les ordinateurs qui requièrent l'exécution de l'installation de contrôle des mises à jour.

   - **Exécuter l'analyse sur les ordinateurs dans le groupe indiqué**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le groupe d'ordinateurs. Dans le champ **Définissez le groupe test**, indiquez le groupe d'ordinateurs à exécuter l'installation de contrôle.

   - **Exécuter l'analyse sur le pourcentage indiqué des ordinateurs**. Sélectionnez cette option si vous voulez exécuter l'analyse des mises à jour sur une partie des ordinateurs ciblés. Dans le champ **Pourcentage des ordinateurs test du nombre total des ordinateurs ciblés**, indiquez le pourcentage des ordinateurs qui requièrent l'exécution de l'installation de contrôle des mises à jour.

4. Lors de la sélection de toutes les options sauf la première dans le champ **Temps pour prendre la décision sur la suite d'installation**, indiquez le nombre d'heures à passer après l'installation de contrôle des mises à jour avant le début d'installation des mises à jour sur tous les ordinateurs ciblés.

CONFIGURATION DES MISES A JOUR DES APPLICATIONS DANS LA STRATEGIE DE L'AGENT D'ADMINISTRATION

Pour configurer les mises à jour Windows Update pour les postes clients dans la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le champ **Ordinateurs administrés** sous l'onglet **Stratégies** à l'aide du lien **Créer une stratégie**, lancez l'Assistant de création d'une stratégie.

2. Dans la fenêtre de l'Assistant **Sélection de l'application pour créer une stratégie de groupe**, indiquez en tant qu'application **Agent d'administration** Kaspersky Security Center.

3. Dans la fenêtre de l'Assistant **Mises à jour et vulnérabilités dans les applications**, cochez la case **Utiliser le Serveur d'administration dans le rôle du serveur WSUS** si vous voulez utiliser le Serveur d'administration en tant que serveur des mises à jour.

   Dans ce cas, les mises à jour seront téléchargées sur le Serveur d'administration et elles seront installées sur les postes clients à l'aide de l'Agent d'administration. Si la case est décochée, le Serveur d'administration n'est pas utilisé pour télécharger et pour installer les mises à jour Windows.

4. Dans la fenêtre de l'Assistant **Mises à jour et vulnérabilités dans les applications** dans le groupe **Mode de recherche des mises à jour Windows Update**, sélectionnez une des options :

   - **En ligne**. Le Serveur d'administration à l'aide de l'Agent d'administration initie la demande de l'agent de mise à jour Windows sur le poste client à la source des mises à jour : Windows Update Servers ou WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'agent de mise à jour Windows.

   - **Autonome**. Lors du mode autonome, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations en provenance de l'agent de mise à jour Windows sur les mises à jour obtenues lors de la dernières synchronisation de l'agent de mise à jour Windows avec la source de mise à jour. Si la synchronisation de l'agent de mise à jour Windows avec la source de mise à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration vieillissent.

   - **Désactivé**. Le Serveur d'administration ne collecte pas les informations sur les mises à jour.

La stratégie créée s'affiche dans le dossier **Ordinateurs administrés** sous l'onglet **Stratégies**.

Si la stratégie de l'Agent d'administration est déjà créée, procédez comme suit :

1. Dans le dossier **Ordinateurs administrés** sous l'onglet **Stratégies**, sélectionnez la stratégie de l'Agent d'administration.

2. Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**. La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

3. Dans la fenêtre des propriétés de la stratégie de l'Agent d'administration, exécutez la configuration de la mise à jour Windows Update dans la section **Mises à jour et vulnérabilités dans les applications**.

INSTALLATION A DISTANCE DES SYSTEMES D'EXPLOITATION ET DES APPLICATIONS

Kaspersky Security Center permet de créer les images des systèmes d'exploitation et de les déployer sur les postes clients par le réseau, ainsi que d'exécuter l'installation à distance des applications de Kaspersky Lab et d'autres éditeurs de logiciels

Prise des images des systèmes d'exploitation

Kaspersky Security Center permet d'exécuter la prise des images des systèmes d'exploitation des ordinateurs ciblés et de livrer ces images sur le Serveur d'administration. Finalement, les images reçues des systèmes d'exploitation sont conservées sur le Serveur d'administration dans le dossier partagé. La prise et la création de l'image du système d'exploitation de l'ordinateur d'étalon est exécutée à l'aide de la tâche de création du paquet d'installation (cf. section “Création des paquets d'installation des applications” à la page 119).

Pour créer les images du système d'exploitation, le paquet d'outils Windows Automated Installation Kit (WAIK) doit être installé sur le Serveur d'administration.

La fonctionnalité de prise de l'image du système d'exploitation a des particularités suivantes :

- Il est interdit de prendre l'image du système d'exploitation de l'ordinateur sur lequel le Serveur d'administration est installé.
- Pendant la prise de l'image du système d'exploitation, la remise à zéro des paramètres de l'ordinateur de référence est effectuée par l'utilitaire sysprep.exe. En case de nécessité de restaurer les paramètres de l'ordinateur de référence, il faut cocher la case **Enregistrer la copie de sauvegarde de l'ordinateur** dans l'Assistant de création de l'image du système d'exploitation.
- Durant la prise de l'image, le redémarrage de l'ordinateur de référence est exécuté.

Déploiement des images des systèmes d'exploitation sur les nouveaux ordinateurs

L'administrateur peut utiliser les images reçues pour le déploiement sur les nouveaux ordinateurs dans le réseau sur lesquels le système d'exploitation n'a pas encore été installé. Pour ce but, la technologie Preboot eXecution Environment (PXE) est utilisée. L'administrateur désigne l'ordinateur dans le réseau qui sera utilisé en tant que serveur PXE. Cet ordinateur doit répondre aux exigences suivantes :

- L'Agent d'administration doit être installé sur l'ordinateur.
- Le serveur DHCP ne doit pas fonctionner sur l'ordinateur parce que le serveurs PXE utilise les mêmes ports que DHCP.
- Le segment du réseau qui fait partie de l'ordinateur ne doit pas avoir d'autres serveurs PXE.

Pour déployer le système d'exploitation, il faut que le poste client possède la carte réseau, l'ordinateur soit connecté au réseau, et l'option d'installation Network boot soit sélectionnée pendant le démarrage de l'ordinateur dans l'environnement BIOS.

Le déploiement du système d'exploitation est exécuté dans la séquence suivante :

1. Le serveur PXE établit la connexion avec le nouveau poste client lors du démarrage du poste client.
2. Le poste client est inclus dans l'environnement Windows Preinstallation Environment (WinPE).

   Pour inclure le poste client dans l'environnement WinPE, la configuration de la composition des pilotes pour l'environnement WinPE peut être requise.

3. Le poste client est enregistré sur le Serveur d'administration.

4. L'administrateur désigne au poste client le paquet d'installation avec l'image du système d'exploitation.

   L'administrateur peut ajouter les pilotes nécessaires dans le paquet d'installation avec l'image du système d'exploitation et indiquer les fichiers de configuration avec les paramètres du système d'exploitation (le fichier des réponses) qui doivent être appliqués pendant l'installation.

5. Le déploiement du système d'exploitation est exécuté sur le poste client.

L'administrateur peut manuellement indiquer les adresses MAC des postes clients non connectés et désigner à ceux-ci le paquet d'installation avec l'image du système d'exploitation. Quand les postes clients indiqués se connectent au serveur PXE, l'installation du système d'exploitation est automatiquement exécutée sur ces ordinateurs.

Déploiement des images des systèmes d'exploitation sur les ordinateurs avec le système d'exploitation déjà installé

Le déploiement des images du système d'exploitation sur les postes clients qui possèdent déjà le système d'exploitation de travail est exécuté à l'aide de la tâche d'installation à distance pour les ensembles d'ordinateurs.

Installation des applications de Kaspersky Lab et d'autres éditeurs de logiciels

L'administrateur peut créer les paquets d'installation de toutes les applications, y compris les applications indiquées par l'utilisateur, et installer ces applications sur les postes clients à l'aide de la tâche d'installation à distance.

DANS CETTE SECTION

CREATION DES IMAGES DES SYSTEMES D'EXPLOITATION

La création des images des systèmes d'exploitation est exécutée à l'aide de la tâche de prise d'image du système d'exploitation de l'ordinateur de référence.

Pour créer la tâche de prise d'image du système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. A l'aide du lien **Créer un paquet d'installation**, lancez l'Assistant de création du paquet d'installation.

3. Dans la fenêtre de l'Assistant **Sélection du type de paquet d'installation**, cliquez sur le bouton **Créer le paquet d'installation avec l'image du S.E. de l'ordinateur de référence**.

4. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche du Serveur d'administration **Prise de l'image du S.E. à partir de l'ordinateur de référence** est créée. Il est possible de consulter la tâche dans le dossier **Tâches du Serveur d'administration**.

Suite à l'exécution de la tâche **Prise de l'image du S.E. à partir de l'ordinateur de référence**, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer le système d'exploitation sur les postes clients à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance. Il est possible de consulter le paquet d'installation dans le dossier **Paquets d'installation**.

AJOUT DES PILOTES POUR L'ENVIRONNEMENT DE PREINSTALLATION WINDOWS (WINPE)

Pour ajouter les pilotes pour l'environnement WinPE, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le sous-dossier **Déploiement des images des ordinateurs**.

2. Dans la zone de travail du dossier **Déploiement des images des ordinateurs** à l'aide du lien **Configurer la composition des pilotes pour l'environnement de préinstallation Windows (WinPE)**, ouvrez la fenêtre **Pilotes pour l'environnement de préinstallation Windows**.

3. Dans la fenêtre **Pilotes pour l'environnement de préinstallation Windows**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout du pilote** s'ouvre.

4. Dans la fenêtre **Ajout du pilote**, indiquez le nom du pilote et le chemin d'accès au paquet d'installation du pilote. Le chemin d'accès au paquet d'installation peut être indiqué lorsque vous cliquez sur le bouton **Sélectionner** dans la fenêtre **Ajout du pilote**.

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

   Le pilote sera ajouté dans le stockage du Serveur d'administration. Le pilote ajouté dans le stockage s'affiche dans la fenêtre **Sélection du pilote**.

6. Cliquez sur le bouton **OK** dans la fenêtre **Sélection du pilote**.

Le pilote sera ajouté dans l'environnement de préinstallation Windows (WinPE).

AJOUT DES PILOTES DANS LE PAQUET D'INSTALLATION AVEC L'IMAGE DU SYSTEME D'EXPLOITATION

Pour ajouter des pilotes dans le paquet d'installation avec l'image du système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. Dans le menu contextuel du paquet d'installation avec l'image du système d'exploitation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Pilotes complémentaires**.

4. Dans le section **Pilotes complémentaires**, cliquez sur le bouton **Ajouter**.

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

5. Dans la fenêtre **Sélection du pilote**, sélectionnez les pilotes que vous voulez ajouter dans le paquet d'installation avec l'image du système d'exploitation.

   Les nouveaux pilotes peuvent être ajoutés dans le stockage du Serveur d'administration, en cliquant sur le bouton **Ajouter** dans la fenêtre **Sélection du pilote**.

6. Cliquez sur le bouton **OK**.

Les pilotes ajoutés s'affichent dans la section **Pilotes complémentaires** dans la fenêtre des propriétés du paquet d'installation avec l'image du système d'exploitation.

CONFIGURATION DES PARAMETRES DE L'UTILITAIRE SYSPREP.EXE

Pour configurer la paramètres de l'utilitaire sysprep.exe, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. Dans le menu contextuel du paquet d'installation avec l'image du système d'exploitation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Paramètres sysprep.exe**.

4. Dans la section **Paramètres sysprep.exe**, indiquez le fichier de configuration qui sera utilisé lors du déploiement du système d'exploitation sur le poste client :

   - **Utiliser le fichier de configuration par défaut**. Sélectionnez cette option pour utiliser le fichier-réponse créé par défaut pendant la prise de l'image du système d'exploitation.

   - **Définir le fichier de configuration**. Sélectionnez cette option pour utiliser votre propre fichier-réponse.

5. Cliquez sur le bouton **Appliquer** pour que les modifications apportées entrent en vigueur.

DEPLOIEMENT DES SYSTEMES D'EXPLOITATION SUR LES NOUVEAUX ORDINATEURS DANS LE RESEAU

Pour déployer le système d'exploitation sur les nouveaux ordinateurs qui ne possèdent pas encore de système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le sous-dossier **Déploiement des images des ordinateurs**.

2. Dans le dossier **Déploiement des images des ordinateurs** à l'aide du lien **Administrer la liste des serveurs PXE dans le réseau**, ouvrez la fenêtre **Propriétés** : **Déploiement des images des ordinateurs** sur la section **Serveurs PXE**.

3. Dans la section **Serveurs PXE**, cliquez sur le bouton **Ajouter** et dans la fenêtre ouverte **Serveurs PXE**, sélectionnez l'ordinateur qui sera utilisé en tant que serveur PXE.

   L'ordinateur ajouté s'affichera dans la section Serveurs PXE.

4. Dans la section **Serveurs PXE** sélectionnez le serveur PXE et cliquez sur le bouton **Propriétés**.

5. Dans la fenêtre des propriétés du serveur PXE sélectionné dans la section **Paramètres de connexion au serveur PXE**, exécutez la configuration des paramètres de connexion du Serveur d'administration au serveur PXE.

6. Exécutez le démarrage du poste client sur lequel vous voulez déployer le système d'exploitation.

7. Dans l'environnement BIOS du poste client, sélectionnez l'option d'installation Network boot.

   Le poste client se connecte au serveur PXE et s'affiche dans la zone de travail du dossier **Déploiement des images des ordinateurs**.

8. Dans le groupe **Actions** à l'aide du lien **Désigner le paquet d'installation**, sélectionnez le paquet d'installation qui sera utilisé pour installer le système d'exploitation sur l'ordinateur sélectionné.

   Après l'ajout de l'ordinateur et la désignation du paquet d'installation pour celui-ci, le déploiement du système d'exploitation sur cet ordinateur commence automatiquement.

9. Pour annuler le déploiement du système d'exploitation sur le poste client, utilisez le lien **Annuler l'installation des images du S.E.** dans le groupe **Actions**.

Pour ajouter les ordinateurs par l'adresse MAC,

- à l'aide du lien **Ajouter l'adresse MAC de l'ordinateur cible** dans le dossier **Déploiement des images des ordinateurs**, ouvrez la fenêtre **Nouvel ordinateur ciblé** et indiquez l'adresse MAC de l'ordinateur que vous voulez ajouter.

- à l'aide du lien **Importer les adresses MAC des ordinateurs ciblés à partir du fichier** dans le dossier **Déploiement des images des ordinateurs**, sélectionnez le fichier qui contient la liste des adresses MAC de tous les ordinateurs sur lesquels vous voulez déployer le système d'exploitation.

DEPLOIEMENT DES SYSTEMES D'EXPLOITATION SUR LES POSTES CLIENTS

Pour exécuter le déploiement du système d'exploitation sur les postes clients avec le système d'exploitation déjà installé, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance** à l'aide du lien **Exécuter l'Assistant d'installation à distance**, lancez l'Assistant d'installation à distance.

2. Dans la fenêtre de l'Assistant **Sélection du paquet d'installation**, indiquez le paquet d'installation avec l'image du système d'exploitation.

3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche d'installation à distance du système d'exploitation sur les postes clients est créée. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches pour les ensembles d'ordinateurs**.

CREATION DES PAQUETS D'INSTALLATION DES APPLICATIONS

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

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. A l'aide du lien **Créer un paquet d'installation**, lancez l'Assistant de création du paquet d'installation.

3. Dans la fenêtre de l'Assistant **Sélection du type de paquet d'installation**, cliquez sur un des boutons :

   - **Générer le paquet d'installation pour l'application de Kaspersky Lab**. Sélectionnez cette option si vous voulez créer un paquet d'installation pour l'application de Kaspersky Lab.

   - **Générer le paquet d'installation pour l'application indiquée par l'utilisateur**. Sélectionnez cette option si vous voulez créer un paquet d'installation pour l'application demandée par l'utilisateur.

   - **Créer le paquet d'installation avec l'image du S.E. de l'ordinateur de référence**. Sélectionnez cette option si vous voulez créer un paquet d'installation avec l'image du système d'exploitation de l'ordinateur de référence.

     Une fois l'Assistant terminé, la tâche du Serveur d'administration **Prise de l'image du S.E. à partir de l'ordinateur de référence** est créée. Suite à l'exécution de cette tâche, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer l'image du système d'exploitation à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance.

4. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, le paquet d'installation est créé. Ce paquet peut être utilisé pour installer l'application sur les postes clients. Il est possible de consulter le paquet d'installation dans le dossier **Paquets d'installation**.

Pour plus d'informations sur l'utilisation des paquets d'installation, cf. *Manuel d'implantation de Kaspersky Security Center*.

INSTALLATION DES APPLICATIONS SUR LES POSTES CLIENTS

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

1. Dans l'arborescence de la console dans le dossier **Installation à distance** à l'aide du lien **Exécuter l'Assistant d'installation à distance**, lancez l'Assistant d'installation à distance.

2. Dans la fenêtre de l'Assistant **Sélection du paquet d'installation**, indiquez le paquet d'installation de l'application que vous voulez installer.

3. Suivez les instructions de l'Assistant.

Une fois l'Assistant terminé, la tâche d'installation à distance de l'application sur les postes clients est créée. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches pour les ensembles d'ordinateurs**.

GESTION DES PERIPHERIQUES MOBILES

Cette section décrit l'administration des périphériques mobiles connectés au Serveur d'administration. Les informations sur la connexion des périphériques mobiles sont décrites dans le Manuel d'implantation de Kaspersky Security Center.

DANS CETTE SECTION

ADMINISTRATION DES PERIPHERIQUES MOBILES VIA LES OUTILS EXCHANGE ACTIVESYNC

Il est possible d'administrer les périphériques mobiles connectés Exchange ActiveSync dans la fenêtre des propriétés du Serveur des périphériques mobiles Exchange ActiveSync qui s'affiche dans le sous-dossier **Serveurs des périphériques mobiles** dans le dossier **Périphériques mobiles** de l'arborescence de la console.

L'administrateur peut exécuter les actions suivantes avec les périphériques mobiles Exchange ActiveSync :

- Créer les profils d'administration des périphériques mobiles Exchange ActiveSync et les ajouter aux boîtes aux lettres des utilisateurs.

  Le *Profil d'administration des périphériques mobiles Exchange ActiveSync* est une stratégie ActiveSync utilisée sur le serveur Microsoft Exchange pour administrer les périphériques mobiles Exchange ActiveSync. Il est possible de désigner la propriété "profil par défaut" au profil d'administration des périphériques mobiles Exchange ActiveSync. Un tel profil est automatiquement attribué aux nouvelles boîtes aux lettres dont le profil a été supprimé. Il est impossible de supprimer le profil par défaut. Pour supprimer le profil par défaut actuel, il faut désigner la propriété "profil par défaut" à un autre profil.

  La boîte aux lettres peut être sous l'administration d'un seul profil d'administration uniquement.

- Configurer les paramètres suivants du périphérique mobile :

  - synchronisation du courrier ;
  - utilisation des applications ;
  - mot de passe de l'utilisateur ;
  - chiffrement des données ;
  - connexion des supports amovibles.

  Selon le type de système d'exploitation sous l'administration duquel le périphérique mobile connecté Exchange ActiveSync se trouve, l'ensemble des paramètres d'administration de ce périphérique peut se différer.

- Installer les certificats sur le périphérique mobile Exchange ActiveSync.

Les informations sur la connexion des périphériques mobiles Exchange ActiveSync au Serveur des périphériques mobiles Exchange ActiveSync sont décrites dans le Manuel d'implantation de Kaspersky Security Center.

CONSULTATION DES INFORMATIONS SUR LES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Afin de voir les informations sur le périphérique mobile Exchange ActiveSync, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Périphériques mobiles Exchange ActiveSync**.

   La zone de travail du dossier affiche les périphériques mobiles connectés au Serveur des périphériques mobiles Exchange ActiveSync.

2. Dans le menu contextuel du périphérique mobile, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du périphérique mobile s'ouvre.

Les informations sur le périphérique mobile connecté Exchange ActiveSync s'affichent dans la fenêtre des propriétés du périphérique mobile dans la section **Général**.

MODIFICATION DU PROFIL D'ADMINISTRATION DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Pour modifier le 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 sous-dossier **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, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés du serveur des périphériques mobiles** s'ouvre.

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

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

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

6. Dans la fenêtre **Profils des paramètres**, sélectionnez le profil et cliquez sur le bouton **Propriétés**.

   Ouvrez la fenêtre des propriétés du profil.

7. Exécutez la modification du profil dans la fenêtre des propriétés du profil.

8. Cliquez sur le bouton **OK** afin d'enregistrer les modifications introduites.

Les modifications des paramètres du profil seront enregistrées.

INSTALLATION DES CERTIFICATS SUR LES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Pour installer le certificat sur le périphérique mobile Exchange ActiveSync, procédez comme suit :

1. Sélectionnez le dossier **Comptes utilisateurs** dans l'arborescence de la console.

2. Dans la zone de travail du dossier **Comptes utilisateurs**, sélectionnez le compte utilisateur dont vous voulez installer le certificat sur le périphérique mobile.

3. Dans le groupe des paramètres **Actions** à l'aide du lien **Installer le certificat sur les périphériques mobiles de l'utilisateur**, ouvrez la fenêtre **Désignation du certificat**.

4. Dans la fenêtre **Désignation du certificat** dans le groupe des paramètres **Type de certificat**, sélectionnez le type de certificat. Les types de certificats suivants sont disponibles :

   - **Certificat général**. Sélectionnez cette option pour envoyer le certificat général de Kaspersky Security Center à l'utilisateur. Le certificat général est utiliser pour vérifier l'authenticité du Serveur d'administration par le client.

   - **Certificat postal**. Sélectionnez cette option pour envoyer le certificat postal à l'utilisateur. Le certificat postal est utilisé pour la connexion du client de messagerie au serveur et pour le chargement des messages.

   - **Certificat pour VPN**. Sélectionnez cette option pour envoyer le certificat pour VPN à l'utilisateur. Le certificat pour VPN permet d'établir la connexion VPN avec la réseau de l'entreprise.

   Pour une authentification réussie, il faut ajouter le certificat du Serveur d'administration utilisé pour la signature des certificats clients comme le certificat de confiance sur le serveur Microsoft Exchange. Chemin d'accès au certificat :

   %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klsrvmdm.cer.

5. Dans le groupe des paramètres **Mode de notification de l'utilisateur**, configurez les paramètres suivants :

   - **A l'aide de SMS**. Cochez la case pour envoyer à l'utilisateur une notification SMS sur le fait que le certificat est installé sur son périphérique. 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 pour obtenir l'accès au certificat.

   - **Par courrier électronique**. Cochez la case pour envoyer à l'utilisateur une notification par courrier électronique sur le fait que le certificat est installé sur son périphérique.

   - Dans le champ **Objet**, indiquez l'objet du message.

6. Dans le champ **Texte du message**, saisissez le message pour l'utilisateur. Si vous voulez que l'utilisateur confirme son identité à l'aide du mot de passe, dans la liste déroulante à côté du champ **Texte du message**, saisissez l'option **Mot de passe à usage unique** et saisissez le mot de passe de l'utilisateur pour obtenir l'accès au certificat.

7. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le mode d'authentification de l'utilisateur. L'authentification est nécessaire pour confirmer l'identité de l'utilisateur lors de l'obtention du certificat.

   - **Authentification de domaine**. Si cette option a été sélectionnée, l'utilisateur indique le nom de l'utilisateur et le mot de passe d'accès au domaine.

   - **Mot de passe à usage unique**. Si cette option a été sélectionnée, l'utilisateur saisit le mot de passe à usage unique. Ce mode d'authentification doit être utilisé si l'utilisateur du périphérique n'est pas dans le domaine.

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

Le certificat sera installé sur le périphérique mobile de l'utilisateur.

Si vous souhaitez indiquer votre certificat personnel, procédez comme suit :

1. Dans la fenêtre **Désignation du certificat**, cochez la case **Définir le certificat personnel**.

2. Dans la liste déroulante à côté de la case **Définir le certificat personnel**, sélectionnez une des deux options d'installation du certificat :

   - **Certificat (.cer, .pem)**. Dans ce cas, il est possible d'indiquer la partie publique ou privée du certificat :

     1. Cliquez sur le bouton **Sélectionner** à côté du champ **Partie privée du certificat**. Indiquez la partie privée du certificat au format PKCS#8 (*.prk).

     2. Cliquez sur le bouton **Sélectionner** à côté du champ **Partie publique du certificat**. Indiquez la partie publique du certificat au format PEM (*.cer).

   - **Certificat au format PKSC12**. Dans ce cas, il est possible d'indiquer un fichier au format PKSC12.

     1. Cliquez sur le bouton **Sélectionner** à côté du champ Certificat PKSC12. Indiquez le fichier du certificat au format p12 ou pfx.

     2. Dans le champ **Mot de passe du certificat**, saisissez le mot de passe du certificat indiqué.

Le certificat personnel doit répondre aux exigences suivantes :

- Clé RSA générée : 1024 bit.
- Délai de validité de la clé : un an.
- Extensions : restrictions principales : n'est pas CA ; utilisation de la clé : signature numérique, chiffrement ; key_id est généré et authority_key_id est ajouté.
- Les données remplies de l'utilisateur : organizationName, organizationalUnitName, commonName, emailAddress.
- Signé par le certificat serveur du Serveur d'administration.

SUPPRESSION DES INFORMATIONS DEPUIS LE PERIPHERIQUE MOBILE EXCHANGE ACTIVESYNC

Afin de supprimer les informations depuis le périphérique mobile Exchange ActiveSync, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Périphériques mobiles Exchange ActiveSync**.

   La zone de travail du dossier affiche les périphériques mobiles connectés au Serveur des périphériques mobiles Exchange ActiveSync.

2. Dans le menu contextuel du périphérique mobile, sélectionnez l'option **Purger le périphérique**.

Suite à l'exécution de cette commande, toutes les données du périphérique mobile sélectionné Exchange ActiveSync sont supprimées.

Pour annuler la purge du périphérique mobile Exchange ActiveSync,

dans le menu contextuel du périphérique, sélectionnez l'option **Annulation de la purge du périphérique**.

SUPPRESSION DU PERIPHERIQUE MOBILE EXCHANGE ACTIVESYNC

Pour supprimer le périphérique mobile Exchange ActiveSync de la liste des périphériques, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Périphériques mobiles Exchange ActiveSync**.

   La zone de travail du dossier affiche les périphériques mobiles connectés au Serveur des périphériques mobiles Exchange ActiveSync.

2. Dans le menu contextuel du périphérique mobile, sélectionnez l'option **Supprimer le périphérique**.

Suite à cette commande, le périphérique mobile Exchange ActiveSync ne sera plus affiché dans la liste des périphériques mobiles connectés Exchange ActiveSync.

ADMINISTRATION DES PERIPHERIQUES MOBILES IOS MDM

Il est possible d'administrer les périphériques mobiles iOS MDM dans la Console d'administration dans le dossier **Périphériques mobiles** à l'aide des moyens suivants :

- via le menu contextuel du périphérique mobile dans le dossier **Périphériques mobiles iOS MDM** ;
- dans la fenêtre des propriétés du Serveurs des périphériques mobiles iOS MDM dans le dossier **Serveurs des périphériques mobiles**.

L'administrateur peut exécuter les actions suivantes avec les périphériques mobiles iOS MDM :

- Ajouter et modifier les profils de configuration pour les périphériques iOS MDM. Le *Profil de configuration* contient les paramètres et les restrictions pour le périphérique mobile.

  L'installation des profils de configuration sur les périphériques mobiles iOS MDM est décrite dans le Manuel d'implantation de Kaspersky Security Center.

- Installer les profils provisioning sur le périphérique mobile iOS MDM. Le *Profil provisioning* est un profil utilisé pour administrer les applications non diffusées via App Store. Le profil provisioning contient les informations sur la licence et il est lié à l'application concrète.

  L'installation des profils provisioning sur les périphériques mobiles iOS MDM est décrite dans le Manuel d'implantation de Kaspersky Security Center.

- Installer les applications sur le périphérique mobile iOS MDM via App Store ou à l'aide des fichiers-manifestes (.plist). Le *Fichier-manifeste* contient la description de l'application pour le périphérique mobile iOS MDM et le lien à l'aide duquel il est possible de télécharger cette application. Avant d'installer l'application sur le périphérique mobile iOS MDM, l'application doit être ajoutée sur le Serveur des périphériques mobiles iOS MDM (cf. section “Ajout de l'application administrée sur le Serveur des périphériques mobiles iOS MDM” à la page 127).
- Bloquer le périphérique mobile iOS MDM.
- Réinitialiser le mot de passe du périphérique mobile iOS MDM.
- Supprimer toutes les données depuis le périphérique mobile iOS MDM.

Une notification PUSH est envoyée à tous les périphériques mobiles connectés iOS MDM toutes les 24 heures. Si le périphérique ne répond pas pendant 30 jours, un tel périphérique est automatiquement marqué comme inactif et il ne peut plus se connecter au Serveur d'administration, jusqu'à ce que l'administrateur n'enlève pas le marquage **Inactif** dans le menu contextuel du périphérique mobile iOS MDM.

Les informations sur l'installation du Serveur des périphériques mobiles iOS MDM sont décrites dans le Manuel d'implantation de Kaspersky Security Center.

CONFIGURATION DE LA CONNEXION DES PERIPHERIQUES MOBILES AU SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour configurer les paramètres de connexion des périphériques mobiles iOS MDM au Serveur des périphériques mobiles iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Serveurs des périphériques mobiles**.
2. Dans le 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 le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Paramètres**.
5. Dans la section **Paramètres**, cochez la case **Période de mise à jour des informations sur les périphériques** et indiquez (en heures) la fréquence de mise à jour des informations sur les périphériques mobiles iOS MDM. La valeur par défaut est de 24 heures.
6. Dans le groupe des paramètres **Ports de connexion**, configurez 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.
7. Cliquez sur le bouton **OK**.

ADMINISTRATION DU PERIPHERIQUE MOBILE IOS MDM A L'AIDE DES COMMANDES DU MENU CONTEXTUEL

Pour administrer le périphérique mobile iOS MDM à l'aide des commandes du menu contextuel, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Périphériques mobiles iOS MDM**.
2. Dans la zone de travail du dossier **Périphériques mobiles iOS MDM**, sélectionnez le périphérique mobile iOS MDM.
3. Dans le menu contextuel du périphérique, sélectionnez la commande pour le périphérique mobile iOS MDM ou utilisez le lien analogue dans le menu **Actions**.

   Les commandes suivantes sont disponibles :
   - **Verrouiller le périphérique**. L'activation forcée de Lock Screen sur le périphérique mobile iOS MDM.
   - **Réinitialiser le mot de passe du périphérique**. Supprime le mot de passe du périphérique mobile iOS MDM.

- **Purger le périphérique**. Supprime toutes les informations depuis le périphérique mobile iOS MDM. Les paramètres du périphérique reviennent aux valeurs par défaut.
- **Installer le profil sur le périphérique**. Installe le profil de configuration sur le périphérique mobile iOS MDM.
- **Supprimer le profil du périphérique**. Supprime le profil de configuration sélectionné depuis le périphérique mobile iOS MDM.
- **Installer le profil provisioning sur le périphérique**. Installe le profil provisioning sur le périphérique mobile iOS MDM.
- **Supprimer le profil provisioning du périphérique**. Supprime le profil provisioning depuis le périphérique mobile iOS MDM.
- **Installer l'application sur le périphérique**. Installe l'application sur le périphérique mobile iOS MDM.
- **Saisir le code redemption de l'application**. Active le code redemption saisi si cela est nécessaire pour continuer l'installation de l'application sur le périphérique mobile iOS MDM.
- **Supprimer l'application depuis le périphérique**. Supprime l'application administrée via profil MDM depuis le périphérique mobile iOS MDM.
- **Configurer les paramètres d'itinérance pour le périphérique**. Permet de configurer les paramètres d'itinérance vocale et d'itinérance des données pour le périphérique mobile iOS MDM. Ces paramètres peuvent être modifiés par l'utilisateur du périphérique mobile iOS MDM.
- **Supprimer la commande depuis la file d'attente**. Supprime la commande depuis la file d'attente pour le périphérique mobile sélectionné iOS MDM.
- **Marquer le périphérique comme inactif**. Coche la case **Inactif** dans la base de données pour le périphérique mobile iOS MDM, après quoi, toutes les tentatives de connexion au Serveur d'administration sont rejetées.
- **Enlever le marquage "inactif" du périphérique**. Décoche la case **Inactif** dans la base de données pour le périphérique mobile iOS MDM, après quoi, le périphérique peut se connecter de nouveau au Serveur des périphériques mobiles iOS MDM.
- **Supprimer**. Supprime l'enregistrement sur le périphérique mobile iOS MDM depuis la base de données, après quoi, toutes les tentatives de connexion de ce périphérique au Serveur des périphériques mobiles iOS MDM sont rejetées.

La commande sélectionnée est ajoutée dans la file d'attente des commandes pour le périphérique mobile iOS MDM.

MODIFICATION DES PROFILS DE CONFIGURATION

Pour modifier le profil de configuration, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Serveurs des périphériques mobiles**.
2. Dans le 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 le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez l'option **Profils**.
5. Dans la section **Profils**, cliquez sur le bouton **Modifier**.

   Lancez l'application iPhone Configuration Utility. Si l'application n'est pas installée, elle doit être installée sur l'ordinateur avec la Console d'administration installée.
6. Exécutez la modification du profil de configuration dans l'application iPhone Configuration Utility.

AJOUT DE L'APPLICATION ADMINISTREE SUR LE SERVEUR DES PERIPHERIQUES MOBILES IOS MDM

Pour ajouter l'application administrée 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 sous-dossier **Serveurs des périphériques mobiles**.
2. Dans le 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 le menu contextuel du Serveur des périphériques mobiles iOS MDM, sélectionnez la section **Ordinateurs administrés**.
5. Dans le section **Ordinateurs administrés**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout de l'application** s'ouvre.
6. Dans la fenêtre **Ajout de l'application** dans le champ **Nom de l'application**, indiquez le nom de l'application ajoutée.
7. Dans le champ **Apple ID ou lien vers l'application**, indiquez Apple ID de l'application ajoutée ou le lien selon lequel il est possible de télécharger l'application.
8. Cochez la case **Supprimer l'application lors de la suppression du profil** si vous voulez supprimer l'application après la suppression du profil MDM depuis le périphérique mobile IOS MDM.
9. Cochez la case **Interdire la création des copies de sauvegarde des données de l'application** si vous voulez interdire la copie de sauvegarde des données de l'application à l'aide des outils iTunes.
10. Cliquez sur le bouton **OK**.

L'application ajoutée s'affiche dans la section **Applications administrées** de la fenêtre des propriétés du Serveur des périphériques mobiles iOS MDM.

INSTALLATION DE L'APPLICATION ADMINISTREE SUR LE PERIPHERIQUE MOBILE IOS MDM

Pour installer l'application administrée sur le périphérique mobile iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Périphériques mobiles**, sélectionnez le sous-dossier **Périphériques mobiles iOS MDM**.
2. Dans la zone de travail du dossier **Périphériques mobiles iOS MDM**, sélectionnez le périphérique mobile iOS MDM.
3. Dans le menu contextuel du périphérique mobile iOS MDM, sélectionnez la commande **Installer l'application sur le périphérique** ou utilisez la commande analogue dans le menu **Action**.

   La fenêtre **Sélection de l'application** s'ouvre.
4. Dans la fenêtre **Sélection de l'application**, sélectionnez l'application que vous voulez installer.

   Il est possible d'installer sur le périphérique mobile iOS MDM uniquement les applications ajoutées sur le Serveur des périphériques mobiles iOS MDM (cf. section “Ajout de l'application administrée sur le Serveur des périphériques mobiles iOS MDM” à la page 127).

La commande d'installation de l'application sera ajoutée dans la file d'attente des commandes pour le périphérique mobile iOS MDM. Si vous voulez supprimer la commande depuis la file d'attente, sélectionnez la commande **Supprimer la commande depuis la file d'attente** dans le menu contextuel du périphérique mobile iOS MDM.

CONFIGURATION DES PARAMETRES D'ITINERANCE SUR LE PERIPHERIQUE MOBILE IOS MDM

Pour configurer les paramètres d'itinérance pour le périphérique mobile iOS MDM, procédez comme suit :

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

2. Dans la zone de travail du dossier **Périphériques mobiles iOS MDM**, sélectionnez le périphérique mobile iOS MDM.

3. Sélectionnez la commande **Configurer les paramètres d'itinérance pour le périphérique** dans le menu contextuel du périphérique mobile iOS MDM.

   La fenêtre **Paramètres d'itinérance** s'ouvre.

4. Dans la fenêtre **Paramètres d'itinérance**, configurez les paramètres suivants :

   - **Activer l'itinérance vocale**. Cochez la case pour activer l'itinérance vocale sur le périphérique mobile iOS MDM. Si l'itinérance vocale est activée, l'utilisateur du périphérique mobile iOS MDM peut téléphoner et répondre au téléphone dans l'itinérance.

   - **Activer l'itinérance des données**. Cochez la case pour activer l'itinérance des données sur le périphérique mobile. Si l'itinérance des données est activée, l'utilisateur du périphérique mobile iOS MDM peut utiliser Internet dans l'itinérance.

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

CREATION DU PAQUET DES APPLICATIONS MOBILES

Pour créer un paquet des applications mobiles, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **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**, cliquez sur le bouton **Nouveau**.

   L'Assistant de création du paquet des applications mobiles se lancera.

4. Dans la fenêtre de l'Assistant **Paramètres**, cochez la case **Créer un coffre-fort avec l'application sélectionnée**.

   Les règles de la stratégie de sécurité peuvent être appliquées aux applications placées dans le coffre-fort. Les règles pour l'application peuvent être configurées dans la fenêtre des propriétés de la stratégie de l'application Kaspersky Endpoint Security 10 pour les périphériques mobiles dans la section **Coffres-forts**.

La paquet créé des applications mobiles s'affiche dans la fenêtre **Administration des paquets des applications mobiles**.

INSTALLATION DE L'APPLICATION SUR LE PERIPHERIQUE MOBILE A L'AIDE DU PAQUET DES APPLICATIONS MOBILES

Pour Installer l'application sur le périphérique mobile à l'aide du paquet des applications mobiles, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Installation à distance**, sélectionnez le sous-dossier **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**, sélectionnez le paquet de l'application mobile que vous voulez installer sur le périphérique mobile.

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

   Le lien pour télécharger l'application mobile 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.

L'utilisateur du périphérique mobile exécute indépendamment l'installation de l'application sur le périphérique mobile.

CHIFFREMENT ET PROTECTION DES DONNEES

Le chiffrement des données diminue les risques de la fuite non préméditée des informations dans le cas de vol/perte de l'ordinateur portable, du support amovible ou du disque dur, ou lors de l'accès aux données des utilisateurs non autorisés et des applications.

La fonction de chiffrement est assurée par l'application Kaspersky Endpoint Security 10 for Windows. Kaspersky Endpoint Security 10 for Windows permet de chiffrer les fichiers enregistrés dur les disques locaux de l'ordinateur et sur les supports amovibles, ainsi que les supports amovibles et les disques durs entièrement.

La configuration des règles de chiffrement est exécutée à l'aide de Kaspersky Security Center via la définition de stratégies. Le chiffrement et le déchiffrement selon les règles définies sont exécutés lors de l'application de la stratégie.

La disponibilité de la fonctionnalité de chiffrement est définie par les paramètres de l'interface d'utilisateur (cf. section “Configuration de l'interface” à la page 34).

L'administrateur peut exécuter les actions suivantes :

- configurer et exécuter le chiffrement et le déchiffrement des fichiers sur les disques locaux de l'ordinateur ;
- configurer et exécuter le chiffrement des fichiers sur les supports amovibles ;
- former les règles d'accès des applications aux fichiers chiffrés ;
- créer et transmettre à l'utilisateur le fichier clé d'accès aux fichiers chiffrés si l'ordinateur de l'utilisateur a des restrictions de la fonctionnalité de chiffrement des fichiers ;
- configurer et exécuter le chiffrement des disques durs ;
- administrer l'accès des utilisateurs aux disques durs chiffrés et aux supports amovibles (administrer les comptes de l'agent d'authentification, former et transmettre aux utilisateurs les groupes de réponse sur la demande de restauration du nom et du mot de passe du compte et les clés d'accès aux périphériques chiffrés) ;
- consulter les états de chiffrement et les rapports sur le chiffrement des fichiers.

Ces opérations sont exécutées à l'aide des outils de l'application Kaspersky Endpoint Security 10 for Windows. Les instructions détaillées sur l'exécution des opérations et la description des particularités de fonctionnalité de chiffrement sont décrites dans le *Manuel de l'administrateur de Kaspersky Endpoint Security 10 for Windows*.

DANS CETTE SECTION

CONSULTATION DE LA LISTE DES PERIPHERIQUES CHIFFRES

Pour consulter la liste des périphériques dont les informations ont été chiffrées, procédez comme suit :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console du Serveur d'administration.
2. Passez à la liste des périphériques chiffrés à l'aide d'un des moyens suivants :
   - A l'aide du lien **Accéder à la liste des périphériques chiffrés** dans le groupe **Administration des périphériques chiffrés**.
   - Dans l'arborescence de la console sélectionnez, sélectionnez le sous-dossier **Périphériques chiffrés**.

Finalement, la zone de travail reprend les informations sur les périphériques présents dans le réseau sur lesquels il y a des fichiers chiffrés et les informations sur les périphériques chiffrés au niveau des disques. Après avoir déchiffré les informations sur le périphérique, le périphérique sera automatiquement supprimé de la liste.

Vous pouvez trier les informations dans la liste des périphériques en ordre croissant ou décroissant à partir de n'importe quel paramètre.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface d'utilisateur (cf. section “Configuration de l'interface” à la page 34).

CONSULTATION DE LA LISTE DES EVENEMENTS DE CHIFFREMENT

Pendant l'exécution des tâches de chiffrement et de déchiffrement des données sur les postes clients, Kaspersky Endpoint Security 10 for Windows envoie dans Kaspersky Security Center les informations sur les événements survenus des types suivants :

- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause de l'insuffisance d'espace sur le disque ;
- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause des problèmes avec la licence ;
- il est impossible de chiffrer/déchiffrer le fichier ou créer l'archive chiffrée à cause de l'absence des privilèges d'accès ;
- l'accès au fichier chiffré est interdit à l'application ;
- les erreurs inconnues.

Pour consulter la liste des événements survenus lors du chiffrement des données sur les postes clients, procédez comme suit :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console du Serveur d'administration.
2. Passez à la liste des événements survenus lors du chiffrement à l'aide d'un des moyens suivants :
   - A l'aide du lien **Accéder à la liste des erreurs** dans le groupe d'administration **Erreur de chiffrement des données**.
   - Dans l'arborescence de la console sélectionnez, sélectionnez le sous-dossier **Evénements du chiffrement**.

Finalement, la zone de travail reprend les informations sur les problèmes survenus lors du chiffrement des données sur les postes clients.

Vous pouvez exécuter les actions suivantes avec la liste des événements de chiffrement :

- trier les enregistrements dans l'ordre croissant ou décroissant des données dans n'importe quelle colonne ;
- exécuter la recherche rapide selon les enregistrements (selon la coïncidence de texte avec la sous-ligne dans n'importe quel champ de la liste) ;
- exporter la liste formée des événements dans le fichier texte.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface d'utilisateur (cf. section “Configuration de l'interface” à la page 34).

EXPORTATION DE LA LISTE DES EVENEMENTS DE CHIFFREMENT DANS LE FICHIER TEXTE

Pour exporter la liste des événements de chiffrement dans un fichier texte, procédez comme suit :

1. Formez la liste des événements de chiffrement (cf. section “Consultation de la liste des événements de chiffrement” à la page 131).
2. Dans le menu contextuel de la liste des événements, sélectionnez l'option **Exporter la liste**.

   La fenêtre **Exporter la liste** s'ouvre.
3. Dans la fenêtre **Exporter la liste**, indiquez le nom du fichier texte avec la liste des événements, sélectionnez le dossier dans lequel la liste sera enregistrée et cliquez sur le bouton **Enregistrer**.

   La liste des événements de chiffrement sera enregistrée dans le fichier indiqué.

FORMATION ET CONSULTATION DES RAPPORTS SUR LE CHIFFREMENT

L'administrateur peut former les rapports suivants :

- le rapport sur le chiffrement des périphériques qui contient les informations sur l'état de chiffrement des périphériques pour tous les groupes des ordinateurs ;
- le rapport sur les privilèges d'accès aux périphériques chiffrés qui contient les informations sur l'état des comptes utilisateurs qui possèdent l'accès aux périphériques chiffrés ;
- le rapport sur les erreurs de chiffrement qui contient les erreurs survenues lors de l'exécution des tâches de chiffrement et de déchiffrement des données sur les postes clients ;
- le rapport sur l'état de chiffrement des ordinateurs qui contient les informations sur la conformité de l'état de chiffrement des ordinateurs à la stratégie de chiffrement ;
- le rapport sur le blocage d'accès aux fichiers qui contient les informations sur le blocage d'accès des applications aux fichiers chiffrés.

Pour consulter le rapport sur le chiffrement des périphériques, procédez comme suit :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - A l'aide du lien **Consulter le rapport sur le chiffrement des périphériques**, lancez l'Assistant de création du modèle du rapport.
   - Sélectionnez le sous-dossier **Périphériques chiffrés**, puis à l'aide du lien **Consulter le rapport sur le chiffrement des périphériques**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Un nouveau rapport apparaît dans le dossier **Rapports et notifications** de l'arborescence de la console. Le processus de formation du rapport est lancé. Le rapport s'affichera dans la zone de travail de la console.

Pour consulter le rapport sur les privilèges d'accès aux périphériques chiffrés, procédez comme suit :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - A l'aide du lien **Consulter le rapport sur les privilèges d'accès aux périphériques chiffrés** dans le groupe **Administration des périphériques chiffrés**, lancez l'Assistant de création du modèle du rapport.
   - Sélectionnez le sous-dossier **Périphériques chiffrés**, puis à l'aide du lien **Consulter le rapport sur les privilèges d'accès aux périphériques chiffrés**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Un nouveau rapport apparaît dans le dossier **Rapports et notifications** de l'arborescence de la console. Le processus de formation du rapport est lancé. Le rapport s'affichera dans la zone de travail de la console.

Pour consulter le rapport sur les erreurs de chiffrement, procédez comme suit :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - A l'aide du lien **Consulter le rapport sur les erreurs de chiffrement** dans le groupe d'administration **Erreur de chiffrement des données**, lancez l'Assistant de création du modèle du rapport.
   - Sélectionnez le sous-dossier **Périphériques chiffrés**, puis à l'aide du lien **Consulter le rapport sur les erreurs de chiffrement**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

Un nouveau rapport apparaît dans le dossier **Rapports et notifications** de l'arborescence de la console. Le processus de formation du rapport est lancé. Le rapport s'affichera dans la zone de travail de la console.

Pour consulter le rapport sur l'état de chiffrement des ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**.
2. Exécutez une des actions suivantes :
   - En cliquant sur le bouton droit de la souris, faites appeler le menu contextuel du dossier **Rapports et notifications**, sélectionnez l'option **Créer** → **Modèle du rapport** et lancez l'Assistant de création du modèle du rapport.
   - Le lien **Créer un modèle du rapport** permet de lancer l'Assistant de création du modèle du rapport.

3. Suivez les indices de l'Assistant de création du modèle du rapport. Dans la fenêtre **Sélection du type de modèle de rapport** dans la section **Autre**, sélectionnez l'option **Rapport d'état de chiffrement des ordinateurs**.

   Après la fin de fonctionnement de l'Assistant de création du modèle du rapport, un nouveau modèle du rapport apparaîtra dans le dossier **Rapports et notifications** de l'arborescence de la console.

4. Dans le dossier **Rapports et notifications**, sélectionnez le modèle du rapport créé sur les étapes précédentes de l'instruction.

Le processus de formation du rapport est lancé. Le rapport s'affichera dans la zone de travail de la Console d'administration.

Les informations sur la conformité des états de chiffrement des ordinateurs et des supports amovibles à la stratégie de chiffrement sont aussi à consulter dans les panneaux d'information sous l'onglet **Statistiques** du dossier **Rapports et notifications** (cf. section "**Travailler avec les données statistiques**" à la page 89).

Pour consulter le rapport sur le blocage d'accès aux fichiers, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**.

2. Exécutez une des actions suivantes :

   - En cliquant sur le bouton droit de la souris, faites appeler le menu contextuel du dossier **Rapports et notifications**, sélectionnez l'option **Créer** → **Modèle du rapport** et lancez l'Assistant de création du modèle du rapport.

   - Le lien **Créer un modèle du rapport** permet de lancer l'Assistant de création du modèle du rapport.

3. Suivez les indices de l'Assistant de création du modèle du rapport. Dans la fenêtre **Sélection du type de modèle de rapport** dans la section **Autre**, sélectionnez l'option **Rapport sur le blocage d'accès aux fichiers**.

   Après la fin de fonctionnement de l'Assistant de création du modèle du rapport, un nouveau modèle du rapport apparaîtra dans le dossier **Rapports et notifications** de l'arborescence de la console.

4. Dans le dossier **Rapports et notifications**, sélectionnez le modèle du rapport créé sur les étapes précédentes de l'instruction.

Le processus de formation du rapport est lancé. Le rapport s'affichera dans la zone de travail de la Console d'administration.

ADMINISTRATION D'ACCES DES PERIPHERIQUES DANS LE RESEAU DE L'ENTREPRISE (NAC)

Kaspersky Security Center permet de 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. Les agents NAC sont installés sur les postes clients avec l'Agent d'administration.

Dans chaque segment tapageur du réseau, deux agents NAC sont utilisés : principal et de réserve. L'agent principal NAC est utilisé pour une application permanente des stratégies d'accès dans le réseau. Lors de la désactivation de l'ordinateur sur lequel l'agent principal NAC fonctionne, l'agent de réserve NAC assume ses fonctions, en assurant le fonctionnement continu NAC dans le réseau de l'entreprise. Le déploiement et la répartition des rôles des agents NAC peut être exécuté manuellement et automatiquement.

Avant de créer les règles de restriction d'accès des périphériques dans le réseau et la liste "blanche" des périphériques, l'administrateur doit créer les éléments du réseau. Les *Eléments du réseau* est un groupe des périphériques formé sur la base des critères définis par l'administrateur.

L'administrateur peut indiquer les critères suivants d'ajout des périphériques dans un élément du réseau :

- attributs réseau (adresse IP, adresse MAC) ;
- fabricant du périphérique ;
- affiliation du périphérique dans le domaine ;
- état de protection du périphérique ;
- présence sur le périphérique des mises à jour critiques non installés des applications et des mise à jour de sécurité.

Quand l'élément du réseau est créé, l'administrateur peut créer pour lui les règles de restriction d'accès ou l'ajouter dans la liste "blanche".

L'administrateur peut créer les règles suivantes de restriction d'accès dans le réseau :

- La règle qui bloque l'accès dans le réseau pour tous les périphériques qui sont inclus dans l'élément du réseau.
- La règle conformément à laquelle la demande d'accès dans le réseau, en provenance de tout périphérique de l'élément du réseau, est retransmise vers le portail d'autorisation. Le *Portail d'autorisation* est un service Internet qui assure l'accès dans le réseau aux périphériques d'hôte. L'administrateur crée les comptes et les transmet aux utilisateurs des périphériques d'hôte.
- La règle qui autorise aux périphériques qui font partie de l'élément du réseau l'accès uniquement aux adresses réseau indiqués.

L'administrateur peut sélectionner l'élément du réseau et de l'ajouter dans la liste "blanche". Les périphériques de la liste "blanche" ont l'accès complet dans le réseau de l'entreprise.

DANS CETTE SECTION

PASSAGE AUX PARAMETRES NAC DANS LES PROPRIETES DE L'AGENT D'ADMINISTRATION

Pour accéder à la configuration des paramètres NAC dans les propriétés de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs administrés**.
2. Dans le dossier **Ordinateurs administrés** sous l'onglet **Ordinateurs**, sélectionnez le poste client avec l'Agent d'administration installé.
3. Dans le menu contextuel du poste client, choisissez l'option **Propriétés**.

   La fenêtre des propriétés du poste client s'ouvre.
4. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.
5. Dans la section **Applications**, sélectionnez l'Agent d'administration et cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de l'application Agent d'administration de Kaspersky Security Center** s'ouvre.
6. Dans la fenêtre **Propriétés de l'application Agent d'administration de Kaspersky Security Center**, sélectionnez la section **Administration de l'accès au réseau (NAC)** et exécutez la configuration des paramètres NAC.

SELECTION DU MODE DE FONCTIONNEMENT DE L'AGENT NAC

Pour sélectionner le mode de fonctionnement de l'agent NAC, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136), sélectionnez la section **Administration de l'accès au réseau (NAC)**.
2. Dans la section jointe **Paramètres** dans le groupe des paramètres **Mode de fonctionnement de l'agent NAC**, sélectionnez le mode de fonctionnement de l'agent NAC :

   - **Désactivé**. Sélectionnez cette option pour désactiver l'agent NAC.

- **Principal**. Sélectionnez cette option pour utiliser l'agent NAC en tant que agent principal. L'agent principal NAC assure l'application continue des règles de restriction d'accès dans le segment du réseau.

- **De réserve**. Sélectionnez cette option pour utiliser l'agent NAC en tant que agent de réserve. Dans le cas d'inactivité de l'agent NAC principal, il est permuté sur l'agent de réserve.

3. Dans le groupe des paramètres **Mode de fonctionnement NAC**, sélectionnez le mode de fonctionnement NAC :

   - **Désactivé**. Sélectionnez cette option si vous ne voulez pas appliquer les règles de restriction d'accès dans le segment du réseau dans lequel l'agent NAC fonctionne.

   - **Normal**. Sélectionnez cette option pour que les règles créées de restriction d'accès entrent en vigueur immédiatement dans le segment du réseau dans lequel l'agent NAC fonctionne.

   - **Simulation**. Sélectionnez cette option pour que les règles créées de restriction d'accès fonctionnent en mode de test. Dans ce cas, les règles ne s'appliquent pas. Cependant, l'enregistrement des événements d'application des règles dans le journal a lieu.

CREATION DES ELEMENTS DU RESEAU

Pour créer l'élément du réseau, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Eléments du réseau**.

2. Dans la liste déroulante **Ajouter**, sélectionnez le type des périphériques que vous voulez ajouter dans un élément du réseau (par exemple, les ordinateurs).

   La fenêtre **Création d'un élément du réseau** s'ouvre.

3. Dans la fenêtre **Création d'un élément du réseau**, saisissez le nom de l'élément créé du réseau.

   Dans la liste déroulante **Ajouter**, sélectionnez les critères d'inclusion des périphériques réseau dans l'élément créé du réseau :

   - **Par les attributs réseau**. Lors de la sélection de cette option, l'ordinateur ou les ordinateurs peuvent être ajoutés dans l'élément du réseau selon l'adresse IP, l'adresse MAC, la plage IP ou le masque du sous-réseau.

   - **Selon l'éditeur**. Lors de la sélection de cette option, il est possible d'ajouter les ordinateurs dans l'élément du réseau selon l'éditeur.

   - **Par l'appartenance à un domaine**. Lors de la sélection cette option, il est possible d'ajouter les ordinateurs dans l'élément du réseau sur la base de leur appartenance à un domaine quelconque. Il est possible d'utiliser l'affiliation dans le domaine comme le critère qui autorise l'accès dans le réseau de l'entreprise.

   - **Selon l'état de l'ordinateur**. Lors de la sélection de cette option, il est possible d'indiquer l'état de protection de l'ordinateur, par exemple "Critique". Pour les ordinateurs avec un tel état, il est possible de créer les règles qui limitent l'accès dans le réseau.

   - **Selon le logiciel**. Lors de la sélection de cette option, il est possible d'ajouter les ordinateurs dans l'élément du réseau selon le type du système d'exploitation, l'état du navigateur et la présence des mises à jour.

   Les critères ajoutés s'affichent dans le champ **Critères** dont l'objet réseau doit satisfaire.

4. Cliquez sur le bouton **OK**.

Les éléments créés du réseau s'affichent dans la fenêtre des propriétés de la stratégie de l'Agent d'administration Kaspersky Security Center dans la section jointe **Eléments du réseau**.

CREATION DES REGLES DE RESTRICTION D'ACCES DANS LE RESEAU

Pour créer une règle de restriction d'accès dans le réseau, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Règles d'accès**.

2. Dans la section **Règles d'accès**, sélectionnez la section jointe **Restrictions d'accès** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Propriétés de la règle de limitation d'accès** s'ouvre.

3. Dans la fenêtre **Propriétés de la règle de limitation d'accès**, saisissez le nom pour la règle créée.

4. Dans la fenêtre **Propriétés de la règle de limitation d'accès**, cliquez sur le bouton **Ajouter** pour sélectionner l'élément du réseau sur lequel la règle se propagera. Il est possible d'ajouter plusieurs éléments du réseau dans une règle.

   La fenêtre **Ajout des éléments du réseau** s'ouvre.

5. Dans la fenêtre **Ajout des éléments du réseau**, sélectionnez l'élément du réseau et cliquez sur le bouton **OK**.

   L'élément sélectionné du réseau s'affichera dans la fenêtre **Propriétés de la règle de limitation d'accès**.

6. Dans la fenêtre **Propriétés de la règle de limitation d'accès** dans le groupe des paramètres **Limiter l'accès au réseau**, sélectionnez une des options suivantes :

   - **Interdire l'accès au réseau**. Lors de la sélection de cette option, l'accès au réseau est interdit à tous les périphériques de l'élément du réseau.

   - **Rediriger vers le portail d'autorisation**. Lors de la sélection de cette option, la redirection de la demande est exécutée en provenance du périphérique qui fait partie de l'élément du réseau sur le serveur d'autorisation.

   - **Autoriser l'accès uniquement aux adresses indiquées**. Lors de la sélection de cette option, indiquez dans le champ de saisie **Adresses disponibles** les adresses accessibles aux périphériques qui font partie de l'élément du réseau.

7. Cliquez sur le bouton **OK**.

La règle créée s'affiche dans la section jointe **Restrictions d'accès**.

CREATION DE LA LISTE "BLANCHE"

Pour créer la liste "blanche" des périphériques, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Règles d'accès**.

2. Dans la section **Règles d'accès**, sélectionnez la section jointe **Liste blanche** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout des éléments du réseau** s'ouvre.

3. Dans la fenêtre **Ajout des éléments du réseau**, sélectionnez l'élément du réseau que vous voulez ajouter dans la liste "blanche".

4. Cliquez sur le bouton **OK**.

Les éléments du réseau ajoutés dans la liste "blanche" s'affichent dans la section jointe **Liste blanche**. Les périphériques de la liste "blanche" ont l'accès complet dans le réseau de l'entreprise.

CREATION DE LA LISTE DES ADRESSES RESEAU AUTORISEES

Pour créer la liste des adresses réseau autorisées, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Adresses des services réseau**.

2. Dans la section **Adresses des services réseau** dans la liste déroulante à droite du bouton **Ajouter**, sélectionnez le type d'adresse réseau :

   - **Adresses réseau autorisées**. Sélectionnez cette option pour ajouter les adresses autorisées pour les périphériques d'hôte.

     La fenêtre **Adresses réseau autorisées** s'ouvre. Cette fenêtre permet d'ajouter les adresses des services réseau selon l'adresse IP, l'adresse MAC, la plage IP et le masque du sous-réseau.

   - **Portail d'autorisation**. Sélectionnez cette option pour ajouter l'adresse du portail d'autorisation sur laquelle les demandes en provenance des périphériques d'hôtes seront redirigées.

     La fenêtre **Portail d'autorisation** s'ouvre. Cette fenêtre permet d'indiquer l'adresse du serveur sur laquelle les demandes en provenance des périphériques réseau seront redirigées.

Les adresses réseau ajoutées s'affichent dans la section **Adresses des services réseau**.

CREATION DES COMPTES POUR L'UTILISATION SUR LE PORTAIL D'AUTORISATION

Pour créer un compte pour l'utilisation sur le portail d'autorisation, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Page d'autorisation**.

2. Dans la section **Page d'autorisation**, sélectionnez la section jointe **Comptes**.

3. Dans le section **Comptes**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout d'un compte** s'ouvre.

4. Dans la fenêtre **Ajout d'un compte**, configurez les paramètres du compte.

5. Si vous voulez interdire l'accès au réseau pour ce compte, cochez la case **Interdire le compte**.

6. Cliquez sur le bouton **OK**.

Les comptes créés s'affichent dans la section **Compte** jointe à la section **Page d'autorisation**.

CONFIGURATION DE L'ASPECT DE LA PAGE D'AUTORISATION

Pour configurer l'aspect de la page d'autorisation, procédez comme suit :

1. Dans la fenêtre **Paramètres de l'application Agent d'administration Kaspersky Security Center** (cf. section "**Passages aux paramètres NAC dans les propriétés de l'Agent d'administration**" à la page 136) dans la section **Administration de l'accès au réseau (NAC)**, sélectionnez la section jointe **Page d'autorisation**.

2. Dans la section **Page d'autorisation**, sélectionnez la section jointe **Aspect**.

3. Dans le groupe des paramètres **Logo**, sélectionnez le logo qui sera utilisé sur la page d'autorisation :

   - **Par défaut**. Sélectionnez cette option si vous voulez utiliser le logo de Kaspersky Lab sur la page d'autorisation.

   - **D'utilisateur** Sélectionnez cette option si vous voulez utiliser logo personnel. En cliquant sur le bouton **Sélectionner**, il est possible d'indiquer le chemin d'accès au fichier du logo. Le logo doit posséder les mêmes paramètres que le logo utilisé par défaut.

4. Dans le groupe des paramètres **Page d'autorisation**, sélectionnez la page d'autorisation vers laquelle les demandes d'obtention d'accès dans le réseau de l'entreprise seront redirigées.

   - **Par défaut**. Sélectionnez cette option si vous voulez utiliser la page par défaut sur le portail d'autorisation. Pour modifier la page par défaut, cliquez sur le bouton **Enregistrer dans le fichier** et enregistrez la page d'autorisation dans le fichier pour la modification.

   - **D'utilisateur**. Sélectionnez cette option si vous voulez utiliser la page d'autorisation modifiée de Kaspersky Lab ou votre page d'autorisation personnelle. Cliquez sur le bouton **Sélectionner** et indiquez le chemin d'accès au fichier de la page d'autorisation.

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

CONFIGURATION DES PARAMETRES NAC DANS LA STRATEGIE DE L'AGENT D'ADMINISTRATION

Pour configurer les paramètres NAC dans la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Ordinateurs administrés**, passez sous l'onglet **Stratégies**.

2. Passez à la configuration des paramètres NAC à l'aide d'un des moyens suivants :

   - A l'aide du lien **Modifier les paramètres de la stratégie** dans le menu **Actions**, ouvrez la fenêtre des propriétés de la stratégie de l'Agent d'administration Kaspersky Security Center et sélectionnez la section **Administration de l'accès au réseau (NAC)**.

   - Utilisez les liens dans les groupe des paramètres **Administration de l'accès au réseau (NAC)** dans le menu **Actions**.

INVENTAIRE DU MATERIEL DETECTE DANS LE RESEAU

Kaspersky Security Center collecte les informations sur le matériel détecté suite au sondage du réseau. Tout matériel connecté au réseau de l'entreprise est soumis à l'inventaire. A chaque sondage du réseau, les informations sur le matériel sont mises à jour. La liste du matériel détecté peut contenir les types suivants des périphériques :

- ordinateurs ;
- périphériques mobiles ;
- périphériques réseau ;
- périphériques virtuels ;
- modules d'ordinateur ;
- périphérie d'ordinateur ;
- périphériques connectés ;
- téléphonie VoIP ;
- stockages réseau.

Le matériel détecté durant le sondage du réseau s'affiche dans le dossier **Stockages** placé dans le dossier **Matériel** de l'arborescence de la console.

L'administrateur peut manuellement ajouter les nouveaux périphériques à la liste du matériel ou modifier les informations sur le matériel déjà présent dans le réseau. Il est possible de consulter et de modifier les informations détaillées sur les périphériques dans les propriétés du périphérique.

L'administrateur peut attribuer l'indice "Matériel corporatif" aux périphériques détectés. Cet indice peut être manuellement attribué dans les propriétés du périphérique ou définir les critères pour son attribution automatique. Dans ce cas, l'indice "Matériel corporatif" est attribué selon le type de périphérique. A l'aide de l'indice "Matériel corporatif", il est possible d'autoriser ou d'interdire la connexion du matériel au réseau.

Kaspersky Security Center permet d'exécuter l'amortissement du matériel. Pour ce faire, il faut cocher la case **Le périphérique est retiré du service** dans les propriétés du périphérique. Un tel périphérique ne s'affiche pas dans la liste du matériel.

DANS CETTE SECTION

AJOUT D'INFORMATIONS SUR LES NOUVEAUX PERIPHERIQUES

Pour ajouter les informations sur les nouveaux périphériques dans le réseau, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Matériel**.
2. Dans la zone de travail du dossier **Matériel** à l'aide du lien **Ajouter le périphérique**, ouvrez la fenêtre **Nouveau périphérique**.

   La fenêtre **Nouveau périphérique** s'ouvre.
3. Dans la fenêtre **Nouveau périphérique** dans la liste déroulante **Type**, sélectionnez le type de périphérique que vous voulez ajouter.
4. Cliquez sur le bouton **OK**.

   La fenêtre des propriétés du périphérique dans la section **Général** s'ouvre.
5. Dans la section **Général**, remplissez les champs de saisie par les données sur le périphérique. Les paramètres suivants sont disponibles dans la section **Général** :

   - **Périphérique corporatif**. Cochez la case si vous voulez attribuer l'indice "Corporatif" au périphérique. Selon cet indice, il est possible d'exécuter la recherche de périphériques dans le dossier **Matériel**.
   - **Le périphérique est retiré du service**. Cochez la case si vous ne voulez pas afficher le périphérique dans la liste des périphériques dans le dossier **Matériel**.
6. Cliquez sur le bouton **Appliquer**.

Le nouveau périphérique s'affiche dans la zone de travail du dossier **Matériel**.

CONFIGURATION DES CRITERES DE DEFINITION DES PERIPHERIQUES CORPORATIFS

Pour configurer les critères de définition des périphériques corporatifs, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Matériel**.
2. Dans la zone de travail du dossier **Matériel** à l'aide du lien **Configurer les critères de définition des périphériques corporatifs**, ouvrez la fenêtre des propriétés du matériel.
3. Dans la fenêtre des propriétés du matériel dans la section **Périphériques corporatifs**, sélectionnez le mode d'attribution de l'indice "Corporatif" :

   - **Etablir manuellement la caractéristique "Corporatif" pour le périphérique**. L'indice "Périphérique corporatif" est désigné au périphérique manuellement dans la fenêtre des propriétés du périphérique dans la section **Général**.
   - **Etablir automatiquement la caractéristique "Corporatif" pour le périphérique**. Dans le groupe des paramètres **Selon le type de périphérique**, indiquez les types des périphériques auxquels l'application va automatiquement attribuer l'indice "Corporatif".
4. Cliquez sur le bouton **Appliquer**.

MISE A JOUR DES BASES ET DES MODULES D'APPLICATION

Cette section décrit le téléchargement et la diffusion des mises à jour des bases et des modules d'application à l'aide de Kaspersky Security Center.

Pour maintenir le système de protection, il faut opportunément actualiser les bases et les modules des applications Kaspersky Lab administrés à l'aide de Kaspersky Security Center.

Pour actualiser les bases et les modules des applications Kaspersky Lab administrés à l'aide de Kaspersky Security Center, la tâche du Serveur d'administration **Téléchargement des mises à jour dans le stockage** est utilisée. Suite à son exécution, les bases et les mises à jour des modules d'applications se téléchargent depuis la source des mises à jour.

La tâche **Téléchargement des mises à jour dans le stockage** n'est pas disponible sur les Serveurs d'administration virtuels. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur virtuel.

Vous pouvez configurer l'analyse des mises à jour reçues sur la productivité et sur la présence des erreurs avant l'installation sur les postes clients.

DANS CETTE SECTION

CREATION D'UNE TACHE DE TELECHARGEMENT DES MISES A JOUR DANS LE REFERENTIEL

La tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration est créée automatiquement lors du fonctionnement de l'Assistant de configuration initiale de Kaspersky Security Center. La tâche de téléchargement des mises à jour dans le stockage peut être créée dans un exemplaire unique. Par conséquent, vous pouvez créer une tâche de téléchargement des mises à jour dans le stockage uniquement si elle a été supprimée de la liste des tâches du Serveur d'administration.

Pour créer une tâche de téléchargement des mises à jour dans le stockage, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Lancez le processus de création de la tâche par via l'un des moyens suivants :
   - Dans le menu contextuel du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez l'option **Créer** → **Tâche**.
   - A l'aide du lien **Création d'une tâche** dans la zone de travail.

Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant. Dans la fenêtre de l'Assistant **Type de tâche**, sélectionnez le type de tâche **Téléchargement des mises à jour dans le stockage**.

Après la fin de fonctionnement de l'Assistant, la tâche créée **Téléchargement des mises à jour dans le stockage** apparaît dans la liste des tâches du Serveur d'administration.

Suite à l'exécution de la tâche **Téléchargement des mises à jour dans le stockage**, les mises à jour des bases et des modules des applications sont copiées depuis la source définie vers le dossier partagé.

Les mises à jour du dossier partagé sont diffusées sur les postes clients et les Serveurs d'administration secondaires.

Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

- Les Serveurs de mises à jour Kaspersky Lab sont les serveurs Kaspersky Lab où sont déposés les mises à jour de la base antivirus et des modules de programmes.
- Serveur d'administration principal.
- Le serveur FTP/HTTP ou le dossier de réseau des mises à jour – le serveur FTP, HTTP, le dossier local ou de réseau ajouté par l'utilisateur et contenant les mises à jour actuelles. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'ordinateur avec le Serveur d'administration installé.

  Pour actualiser le Serveur d'administration à partir du serveur FTP/HTTP ou à partir du dossier local, il faut copier sur ces ressources la structure valide des dossiers avec les mises à jour, qui coïncide avec la structure formée lors de l'utilisation des serveurs de mise à jour de Kaspersky Lab.

La sélection de la ressource dépend des paramètres de la tâche. L'option par défaut télécharge les mises à jour depuis les serveurs de mise à jour Kaspersky Lab par Internet.

CONFIGURATION DES PARAMETRES DE LA TACHE DE TELECHARGEMENT DES MISES A JOUR DANS LE STOCKAGE

Pour configurer les paramètres de la tâche de téléchargement des mises à jour dans le stockage, procédez comme suit :

1. Dans la zone de travail du dossier de l'arborescence de la console **Tâches du Serveur d'administration**, sélectionnez la tâche **Téléchargement des mises à jour dans le stockage** dans la liste des tâches.
2. Ouvrez la fenêtre des propriétés de la tâche à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres de la tâche** dans la zone de travail de la tâche sélectionnée.

   La fenêtre des propriétés de la tâche **Téléchargement des mises à jour dans le stockage** s'ouvre. Cette fenêtre permet de configurer les paramètres de téléchargement des mises à jour dans le stockage du Serveur d'administration.

ANALYSE DES MISES A JOUR RECUPEREES

Pour que Kaspersky Security Center analyse les mises à jour reçues avant des les diffuser sur les postes clients, procédez comme suit :

1. Dans la zone de travail du dossier **Tâches du Serveur d'administration** de l'arborescence de la console, sélectionnez la tâche **Téléchargement des mises à jour dans le stockage** dans la liste des tâches.
2. Ouvrez la fenêtre des propriétés de la tâche à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres de la tâche** dans la zone de travail de la tâche sélectionnée.

3. Dans la fenêtre ouverte des propriétés des tâches dans la section **Vérification des mises à jour**, cochez la case **Vérifier les mises à jour avant de les déployer** et sélectionnez la tâche de vérification des mises à jour à l'aide d'un des moyens suivants :

   - Cliquez sur le bouton **Sélectionner** pour sélectionner une tâche de vérification des mises à jour déjà créée.

   - Cliquez sur le bouton **Créer** pour créer une tâche de vérification des mises à jour.

     L'Assistant de création d'une tâche de vérification des mises à jour s'ouvre. Suivez les instructions de l'Assistant.

     Durant le processus de création de la tâche de vérification des mises à jour, il faut sélectionner un groupe d'administration dont la tâche sera exécutée sur les ordinateurs. Les ordinateurs de ce groupe sont appelés les *ordinateurs d'essai*.

   Pour les ordinateurs d'essai, il est recommandé d'utiliser des ordinateurs bien protégés avec la configuration logicielle la plus répandue dans le réseau de l'entreprise. La qualité de la vérification sera ainsi accrue, le risque de faux-positifs ainsi que la probabilité d'identifier des virus lors de la vérification seront réduits (en cas de détection de virus sur les ordinateurs d'essai, la tâche de vérification des mises à jour est considérée comme manquée).

4. Fermez la fenêtre des propriétés de la tâche de téléchargement des mises à jour dans le stockage, en cliquant sur le bouton **OK**.

Dans le cadre de l'exécution de la tâche de téléchargement des mises à jour dans le stockage, la tâche de vérification des mises à jour reçues sera exécutée. Le Serveur d'administration va copier les mises à jour depuis la source, va les placer dans un dossier temporaire et va lancer la tâche de vérification des mises à jour. Si l'exécution de cette tâche réussit, les mises à jour seront copiées depuis le dossier temporaire vers le dossier partagé du Serveur d'administration (<Dossier d'installation Kaspersky Security Center>\Share\Updates), puis seront diffusées vers les postes clients pour lesquels le Serveur d'administration est une source de mise à jour.

Si, à la fin de la tâche de vérification des mises à jour placées dans le dossier temporaire, les mises à jour sont considérées comme incorrectes ou si la tâche se solde sur une erreur, la copie des mises à jour dans le dossier partagé n'a pas lieu et la version précédente des mises à jour est conservée sur le Serveur d'administration. Les tâches dont la programmation est **Lors du téléchargement des mises à jour dans le stockage** ne sont pas lancées. Ces opérations sont réalisées à l'exécution suivante de la tâche de téléchargement des mises à jour dans le stockage si la vérification du nouvel ensemble des mises à jour réussit.

L'ensemble de mises à jour est considéré comme incorrect si sur au moins un ordinateur d'essai une des conditions suivantes est remplie :

- une erreur s'est produite pendant l'exécution de la tâche de mise à jour ;
- après l'application des mises à jour, l'état de la protection en temps réel de l'application antivirus est modifié ;
- un objet infecté a été identifié durant l'analyse à la demande ;
- une erreur de l'application de Kaspersky Lab s'est produite.

Si aucune des conditions citées n'est remplie sur aucun des ordinateurs d'essai, alors les mises à jour sont considérées comme correctes et la tâche de vérification des mises à jour a réussi.

CONFIGURATION DES STRATEGIES DE VERIFICATION ET DES TACHES AUXILIAIRES

Lors de la création d'une tâche de vérification des mises à jour, le Serveur d'administration crée des stratégies de vérification, ainsi que des tâches de groupe auxiliaires de mise à jour et d'analyse à la demande.

L'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande prend un certain temps. Ces tâches sont exécutées dans le cadre d'exécution de la tâche d'analyse de la mise à jour. La tâche d'analyse des mises à jour est exécutée dans le cadre d'exécution de la tâche de téléchargement des mises à jour dans le stockage. Le temps d'exécution de la tâche de téléchargement des mises à jour dans le stockage inclut le temps d'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande.

Vous pouvez modifier les paramètres des stratégies de vérification et des tâches auxiliaires.

Pour modifier les paramètres de la stratégie de vérification ou de la tâche auxiliaire, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe pour lequel la tâche d'analyse des mises à jour sera formée.
2. La zone de travail permet de sélectionner un des onglets suivants :
   - **Stratégies** si vous voulez modifier les paramètres de la stratégie de vérification ;
   - **Tâches** si vous voulez modifier les paramètres de la tâche auxiliaire.
3. Dans la zone de travail de l'onglet, sélectionnez la stratégie ou la tâche les paramètres de laquelle vous voulez modifier.
4. Ouvrez la fenêtre des propriétés de cette stratégie (tâche) à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la stratégie (tâche), sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres de la stratégie** (**Modifier les paramètres de la tâche**) dans le groupe de travail avec la stratégie (la tâche) sélectionnée.

Pour que l'analyse des mises à jour soit exécutée correctement, il faut suivre les restrictions suivantes sur la modification des paramètres des stratégies de vérification et des tâches auxiliaires :

- Dans les paramètres des tâches auxiliaires :
  - Enregistrer sur le Serveur d'administration tous les événements correspondant aux niveaux d'importance **Critique** et **Erreur**. Sur la base des événements de ce type, le Serveur d'administration analyse le fonctionnement des applications.
  - Utiliser le Serveur d'administration en tant que source des mises à jour.
  - Définir le type de programmation des tâches : **Mode manuel**.
- Dans les paramètres des stratégies de vérification :
  - Ne pas utiliser les technologies iChecker, iSwift et iStream d'accélération de l'analyse.
  - Sélectionner les actions sur les objets infectés : **Ne pas demander/Ignorer/Enregistrer l'information dans le rapport**.
- Dans les paramètres des stratégies de vérification et des tâches auxiliaires :

  Si le redémarrage de l'ordinateur est requis après l'installation des mises à jour des modules logiciels, il faut l'exécuter sans attendre. Si l'ordinateur n'est pas redémarré, il sera impossible de vérifier ce type de mise à jour. Pour certaines applications, l'installation de mises à jour qui requièrent un redémarrage peut être interdites ou réalisées uniquement après confirmation de l'utilisateur. Ces restrictions doivent être désactivées dans les paramètres des stratégies de vérification et des tâches auxiliaires.

AFFICHAGE DES MISES A JOUR RECUPEREES

- *Pour consulter la liste des mises à jour reçues,*

  dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Mises à jour**.

La zone de travail du dossier **Mises à jour** présente la liste des mises à jour enregistrées sur le Serveur d'administration.

DEPLOIEMENT DE MISES A JOUR AUTOMATIQUE

Kaspersky Security Center permet de diffuser et d'installer automatiquement les mises à jour sur les postes clients et sur les Serveurs d'administration secondaires.

DANS CETTE SECTION

DEPLOIEMENT DE MISES A JOUR VERS LES CLIENTS IMMEDIATEMENT APRES LE TELECHARGEMENT

- *Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les postes clients tout de suite après le téléchargement des mises à jour dans le stockage du Serveur d'administration, procédez comme suit :*

  1. Connectez-vous au Serveur d'administration, qui gère les postes clients.
  2. Créez une tâche de diffusion des mises à jour de cette application pour les postes clients sélectionnées via l'un des moyens suivants :
     - S'il faut diffuser les mises à jour sur les postes clients qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné (cf. section "Création d'une tâche de groupe" à la page 68).
     - S'il faut diffuser les mises à jour sur les postes clients qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page 69).

     Ceci permet de lancer l'Assistant de création de tâche. Suivez ses instructions, exécutant les conditions suivantes :

     a. Dans la fenêtre de l'Assistant **Type de tâche** dans l'entrée de l'application nécessaire, sélectionnez la tâche de diffusion des mises à jour.

        Le nom de la tâche de diffusion des mises à jour, qui s'affiche dans la fenêtre **Type de tâche**, dépende de l'application pour lequel la tâche a été créée. Pour plus d'informations sur les noms des tâches de mise à jour pour les applications sélectionnées de Kaspersky Lab, cf. Manuels pour ces applications.

     b. Dans la fenêtre de l'Assistant **Programmation** dans le champ **Programmation**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage**.

  La tâche créée de diffusion des mises à jour sera lancée pour les ordinateurs sélectionnés chaque fois lors du téléchargement des mises à jour dans le stockage du Serveur d'administration.

Si la tâche de diffusion des mises à jour de l'application nécessaire a déjà été créée pour les ordinateurs sélectionnés, pour une diffusion automatique des mises à jour sur les postes clients dans la fenêtre des propriétés de la tâche dans la section **Programmation**, il faut sélectionner l'option de lancement **Lors du téléchargement des mises à jour dans le stockage** dans le champ **Programmation pour**.

REDISTRIBUTION AUTOMATIQUE DES MISES A JOUR SUR LES SERVEURS D'ADMINISTRATION SECONDAIRES

Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les Serveurs d'administration secondaires tout de suite après le téléchargement des mises à jour dans le stockage du Serveur d'administration principal, procédez comme suit :

1. Dans l'arborescence de la console dans l'entrée du Serveur d'administration principal, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Dans la liste des tâches de la zone de travail, sélectionnez la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
3. Ouvrez la section **Paramètres** de la fenêtre des propriétés de la tâche sélectionnée via l'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres** dans le groupe d'utilisation de la tâche sélectionnée.
4. Dans la section **Paramètres** de la fenêtre de la tâche, ouvrez la fenêtre **Autres paramètres** à l'aide du lien **Personnaliser** dans la sous-section **Autres paramètres**.
5. Dans la fenêtre ouverte **Autres paramètres**, cochez la case **Forcer la mise à jour des serveurs secondaires**.

Dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Forcer la mise à jour des Serveurs secondaires**.

Immédiatement après la réception des mises à jour par le Serveur d'administration principal, des tâches de téléchargement des mises à jour par les Serveurs d'administration secondaires seront automatiquement lancées, indépendamment de la planification prévue dans la configuration de ces tâches.

INSTALLATION AUTOMATIQUE DES MISES A JOUR DES MODULES D'APPLICATION DES SERVEURS ET DES AGENTS D'ADMINISTRATION

Pour que les mises à jour des modules d'applications des Serveurs d'administration et des Agents d'administration s'installent automatiquement après leur téléchargement dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console dans l'entrée du Serveur d'administration principal, sélectionnez le dossier **Tâches du Serveur d'administration**.
2. Dans la liste des tâches dans la zone de travail, sélectionnez la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
3. Ouvrez la section **Paramètres** de la fenêtre des propriétés de la tâche sélectionnée via l'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres** dans le groupe d'utilisation de la tâche sélectionnée.

4. Dans la section **Paramètres** de la fenêtre de la tâche, ouvrez la fenêtre **Autres paramètres** à l'aide du lien **Personnaliser** dans la sous-section **Autres paramètres**.

5. Dans la fenêtre ouverte **Autres paramètres**, cochez les cases :

   - **Actualiser les modules des Serveurs d'administration**. Si la case est cochée, les mises à jour des modules du Serveur d'administration, quand elles sont récupérées, sont installées après la fin de la tâche de récupération des mises à jour par le Serveur d'administration. Si la case est décochée, les mises à jour pourront être installées manuellement seulement. Par défaut, la case est cochée.

   - **Actualiser les modules des Agents d'administration**. Si la case est cochée, les mises à jour des modules du Serveur d'administration, quand elles sont récupérées, sont installées après la fin de la tâche de récupération des mises à jour par le Serveur d'administration. Si la case est décochée, les mises à jour pourront être installées manuellement seulement. Par défaut, la case est cochée.

Après la réception des mises à jour par le Serveur d'administration principal, des tâches d'installation des mises à jour des modules logiciels sélectionnés seront automatiquement lancées.

FORMATION DE LA LISTE DES AGENTS DE MISE A JOUR ET CONFIGURATION DES PARAMETRES

Pour composer la liste des agents de mise à jour et les configurer pour la diffusion des mises à jour sur les ordinateurs dans le cadre du groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le nœud **Ordinateurs administrés**.

2. Dans le dossier **Ordinateurs administrés** sélectionnez le groupe d'administration pour lequel il est requis de former la liste des agents de mise à jour.

   Si vous voulez former la liste des agents de mise à jour pour le groupe **Ordinateurs administrés**, cette étape peut être ignorée.

3. Ouvrez la fenêtre des propriétés du groupe à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du groupe, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Configurer les agents de mises à jour pour le groupe**.

4. Dans la fenêtre des propriétés du groupe dans la section **Agents de mise à jour**, formez la liste des ordinateurs, qui exécuteront la fonction de l'agent de mise à jour dans le cadre du groupe d'administration, à l'aide des boutons **Ajouter** et **Supprimer**.

5. Pour chaque agent de mise à jour dans la liste, ouvrez la fenêtre de ses propriétés, en cliquant sur le bouton **Propriétés**, et configurez les paramètres de l'agent de mise à jour.

RECUPERATION DES MISES A JOUR PAR LES AGENTS DE MISES A JOUR

Kaspersky Security Center permet de livrer les mises à jour sur les postes clients des groupes d'administration non pas via le Serveur d'administration, mais via les agents de mises à jour de ces groupes.

Pour configurer la récupération des mises à jour pour le groupe via les agents de mises à jour, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le nœud **Ordinateurs administrés**.

2. Dans le dossier **Ordinateurs administrés**, sélectionnez le groupe nécessaire.

   Si vous avez sélectionné le groupe **Ordinateurs administrés**, cette étape peut être ignorée.

3. Ouvrez la fenêtre des propriétés du groupe à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du groupe, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Configurer les agents de mises à jour pour le groupe**.

4. Dans la fenêtre des propriétés du groupe dans la section **Agents de mise à jour**, sélectionnez l'agent de mise à jour via lequel les mises à jour seront livrées sur les postes clients.

5. En cliquant sur le bouton **Propriété**, ouvrez la fenêtre des propriétés de l'agent de mise à jour et sélectionnez la section **Source de mises à jour**.

6. Cochez la case **Utiliser la tâche de récupération des mises à jour** et sélectionnez la tâche de réception des mises à jour à l'aide d'un des moyens suivants :

   - Cliquez sur le bouton **Sélectionner** pour sélectionner une tâche déjà formée de récupération des mises à jour par l'agent de mises à jour.

   - Cliquez sur le bouton **Nouvelle tâche** pour créer une tâche de récupération des mises à jour par l'agent de mise à jour.

La tâche de récupération des mises à jour par l'agent de mise à jour est une tâche de l'Agent d'administration, le type de tâche – **Téléchargement des mises à jour dans le stockage**. La tâche de récupération des mises à jour par l'agent de mise à jour est une tâche locale : pour chaque ordinateur, exécutant le rôle de l'agent de mises à jour, la tâche doit être créée séparément.

TRAVAIL AVEC LES CLES DES APPLICATIONS

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés des applications administrées de Kaspersky Lab.

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

Lors de l'ajoute de la clé à l'aide de Kaspersky Security Center, les propriétés de la clé sont enregistrées sur le Serveur d'administration. Sur la base de ces informations, l'application forme le rapport sur l'utilisation des clés et notifie l'administrateur sur l'expiration de la validité des licences et sur l'excès des restrictions mises dans les propriétés des clés. Vous pouvez configurer les paramètres de notifications sur l'utilisation des clés dans la composition des paramètres du Serveur d'administration.

DANS CETTE SECTION

CONSULTATION DES INFORMATIONS SUR LES CLES UTILISEES

Pour consulter les informations sur les clés utilisées,

sélectionnez dans l'arborescence de la console dans le dossier **Stockages** le sous-dossier **Mises à jour**.

La zone de travail représentera la liste des clés utilisées sur les postes clients.

A côté de chaque clé, une icône, correspondant au type de son utilisation, s'affiche :

- - l'information sur la clé utilisée est reçue depuis le poste client connecté au Serveur d'administration. Le fichier de cette clé n'est pas enregistré sur le Serveur d'administration.
- – le fichier clé se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé est désactivée.
- – le fichier clé se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé est activée.

Vous pouvez consulter les informations sur les clés utilisées pour l'application sur le poste client, en ouvrant la fenêtre des propriétés des applications de la section **Applications** de la fenêtre des propriétés du poste client.

AJOUT DE LA CLE DANS LE STOCKAGE DU SERVEUR D'ADMINISTRATION

Pour ajouter une clé dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Clés**.
2. Lancez la tâche d'ajout de la clé à l'aide d'un des moyens suivants :
   - dans le menu contextuel de la liste des clés, sélectionnez l'option **Ajouter une clé** ;
   - à l'aide du lien **Ajouter une clé** dans le groupe d'administration de la liste des clés.

L'Assistant d'ajout d'une clé est lancé. Suivez les instructions de l'Assistant.

DIFFUSION DES CLES SUR LES POSTES CLIENTS

Kaspersky Security Center permet de diffuser la clé sur les postes clients à l'aide de la tâche de diffusion de la clé.

Afin de diffuser une clé sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Clés**.
2. Lancez la tâche de diffusion de la clé à l'aide d'un des moyens suivants :
   - dans le menu contextuel de la liste des clés, sélectionnez l'option **Diffuser la clé** ;
   - à l'aide du lien **Diffuser la clé sur les ordinateurs administrés** dans le groupe d'administration de la liste des clés.

L'Assistant de création de la tâche de diffusion de la clé est lancé. Suivez les instructions de l'Assistant.

Les tâches créées à l'aide de l'Assistant de création de la tâche de diffusion de la clé sont des tâches pour des sélections d'ordinateurs situées dans le dossier **Tâches pour les ensembles d'ordinateurs** de l'arborescence de console.

Vous pouvez aussi créer une tâche de groupe ou une tâche locale de diffusion de la clé à l'aide de l'Assistant de création de la tâche pour le groupe d'administration et pour le poste client.

DIFFUSION AUTOMATIQUE DE LA CLE

Kaspersky Security Center permet de diffuser automatiquement sur les postes clients les clés placées dans le stockage des clés sur le Serveur d'administration.

Afin de diffuser automatiquement une clé sur les postes clients, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console dans le dossier **Stockages** le dossier joint **Clés**.
2. Sélectionnez la clé que vous voulez diffuser.

3. Ouvrez la fenêtre des propriétés de la clé sélectionnée à l'aide d'un des moyens suivants :

   - dans le menu contextuel de la clé, sélectionnez l'option **Propriétés** ;
   - à l'aide du lien **Ouvrir la fenêtre des propriétés de la clé** dans le groupe de travail avec la clé sélectionnée.

4. Dans la fenêtre ouverte des propriétés de la clé, cochez la case **Clé diffusée automatiquement**. Fermez la fenêtre des propriétés de la clé.

La clé sera automatiquement diffusée sur les postes clients où l'application sans clé active est installée.

La diffusion de la clé est exécutée via les moyens de l'Agent d'administration. Avec cela les tâches auxiliaires de diffusion de la clé pour l'application ne se forment pas. La clé est ajoutée en tant que clé active.

Lors de la diffusion de la clé, la restriction de licence, mise dans les propriétés de la clé, est tenue en compte. Si la restriction est atteinte, la clé n'est pas diffusée sur le poste client.

CREATION ET CONSULTATION DU RAPPORT D'UTILISATION DES CLES

Pour créer un rapport d'utilisation des clés sur les postes clients,

dans l'arborescence de la console dans le dossier **Rapports et notifications**, sélectionnez le modèle du rapport **Rapport d'utilisation des clés** ou créez un nouveau modèle du rapport de type homonyme.

La zone de travail du rapport d'utilisation des clés affichera les informations sur les clés actives et complémentaires utilisées sur les postes clients. Le rapport contient aussi les informations sur les ordinateurs sur lesquels les clés sont utilisées, ainsi que les informations sur les restrictions définies dans les paramètres des clés.

STOCKAGES DES DONNEES

Cette section contient les informations sur les données enregistrées sur le Serveur d'administration et utilisées pour suivre les états des postes clients et leur service.

Les données, utilisées pour surveiller l'état des postes clients et leur service, s'affichent dans le dossier de l'arborescence de la console **Stockages**.

Le dossier **Stockages** contient les objets suivants :

- les mises à jour, reçues par le Serveur d'administration, qui se diffusent sur les postes clients (cf. section "Affichage des mises à jour reçues" à la page 147) ;
- la liste de l'inventaire détecté dans le réseau.
- les clés détectées sur les postes clients (cf. section "Travail avec les clés des applications" à la page 151) ;
- les fichiers placés par les applications antivirus dans les dossiers de quarantaine des postes client ;
- les fichiers placés dans les dossiers de sauvegarde des postes clients ;
- les fichiers pour lesquels les applications antivirus ont décidé d'une analyse ultérieure.

DANS CETTE SECTION

EXPORTATION DE LA LISTE DES OBJETS EN QUARANTAINE DANS LE FICHIER TEXTE

Vous pouvez exporter de la liste des objets en quarantaine dans le fichier texte.

Pour exporter de la liste des objets en quarantaine dans le fichier texte, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier du stockage nécessaire.
2. Dans le menu contextuel de la liste des objets du stockage, sélectionnez l'option **Exporter la liste**.

   La fenêtre **Exporter la liste** s'ouvre. Cette fenêtre permet d'indiquer le nom du fichier texte et l'adresse du dossier dans lequel il sera placé.

PAQUETS D'INSTALLATION

Kaspersky Security Center place dans les stockages de données les paquets d'installation des applications de Kaspersky Lab et des applications des éditeurs tiers.

Paquet d'installation représente l'ensemble de fichiers nécessaires pour installer l'application. Le paquet d'installation contient les paramètres du processus d'installation et de la configuration initiale de l'application installée.

Si vous voulez installer une application quelconque sur le poste client, il faut créer le paquet d'installation (cf. section “Création des paquets d'installation des applications” à la page 119) pour cette application ou utiliser le paquet d'installation déjà créé. La liste des paquets d'installation créés se trouvent dans le dossier de l'arborescence de la console **Installation à distance**, du sous-dossier **Paquets d'installation**.

Pour plus d'informations sur l'utilisation des paquets d'installation, cf. *Manuel d'implantation de Kaspersky Security Center*.

QUARANTAINE ET DOSSIER DE SAUVEGARDE

Les applications Kaspersky Lab installées sur les postes clients peuvent placer les fichiers en quarantaine ou dans le dossier de sauvegarde lors de l'analyse des ordinateurs.

Quarantaine est un stockage spécial qui contient les fichiers potentiellement infectés par les virus ou irréparables lors de la détection.

Dossier de sauvegarde est conçu pour enregistrer les copies de sauvegarde des fichiers qui ont été supprimés ou modifiés lors de la réparation.

Kaspersky Security Center forme une liste générale des fichiers placés en quarantaine ou dans le dossier de sauvegarde par les applications de Kaspersky Lab sur les postes clients. Les Agents d'administration des postes clients transmettent les informations sur les fichiers en quarantaine et dans les dossiers de sauvegarde sur le Serveur d'administration. Via la Console d'administration il est possible de consulter les propriétés des fichiers qui se trouvent dans les stockages sur les postes clients, lancer l'analyse antivirus des stockages et en supprimer les fichiers.

L'utilisation de la quarantaine et du dossier de sauvegarde est accessible à Windows Workstations et Kaspersky Anti-Virus for Windows Servers des versions 6.0 supérieures, et à Kaspersky Endpoint Security 10 for Windows.

Kaspersky Security Center ne copie pas les fichiers depuis les dossiers sur le Serveur d'administration. Tous les fichiers sont placés dans les stockages des postes clients. La restauration des fichiers s'exécute sur l'ordinateur avec l'application antivirus installée qui a placé le fichier dans le stockage.

DANS CETTE SECTION

ACTIVATION DE LA GESTION A DISTANCE DES FICHIERS DANS LES STOCKAGES

La gestion à distance des fichiers dans les stockages sur les postes clients est désactivée par défaut.

Pour activer la gestion à distance des fichiers dans les stockages sur les postes clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer la gestion à distance des fichiers dans les stockages.

2. Dans la zone de travail du groupe, ouvrez l'onglet **Stratégies**.

3. Sous l'onglet **Stratégies**, sélectionnez la stratégie de protection antivirus qui place les fichiers dans les stockages sur les postes clients.

4. Dans la fenêtre des propriétés de la stratégie dans le groupe **Informer le Serveur d'administration**, cochez les cases qui correspondent aux stockages pour lesquels vous voulez activer l'administration à distance.

L'emplacement du groupe **Informer le Serveur d'administration** dans la fenêtre des propriétés de la stratégie et les noms des cases dans le groupe sont individuels pour chaque application antivirus.

CONSULTATION DES PROPRIETES DU FICHIER PLACE DANS LE STOCKAGE

Pour consulter les propriétés du fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Dossier de sauvegarde**.

2. Dans la zone de travail du dossier **Quarantaine** (**Dossier de sauvegarde**) sélectionnez le fichier dont les paramètres requièrent la consultation.

3. Ouvrez la fenêtre des propriétés du fichier à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Ouvrir les propriétés de l'objet** dans le groupe de travail avec le fichier sélectionné.

SUPPRESSION DES FICHIERS DEPUIS LE STOCKAGE

Pour supprimer le fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Dossier de sauvegarde**.

2. Dans la zone de travail du dossier **Quarantaine** (**Dossier de sauvegarde**), sélectionnez les fichiers à supprimer à l'aide des touches **Shift** et **Ctrl**.

3. Supprimez les fichiers à l'aide d'un des moyens suivants :

   - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.

   - A l'aide du lien **Supprimer les objets** (**Supprimer l'objet** lors de la suppression d'un fichier) dans le groupe de travail avec les fichiers sélectionnés.

Finalement, les applications antivirus, qui ont placé les fichiers sélectionnés dans les stockages sur les postes clients, suppriment les fichiers de ces stockages.

RESTAURATION DES FICHIERS DEPUIS LE STOCKAGE

Pour restaurer le fichier depuis la quarantaine ou le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Dossier de sauvegarde**.

2. Dans la zone de travail du dossier **Quarantaine** (**Dossier de sauvegarde**), sélectionnez les fichiers à restaurer à l'aide des touches **Shift** et **Ctrl**.

3. Lancez le processus de restauration des fichiers à l'aide d'un des moyens suivants :

   - Sélectionnez l'option **Restaurer** dans le menu contextuel des fichiers.
   - A l'aide du lien **Restaurer** dans le groupe de travail avec les fichiers sélectionnés.

Finalement, les applications antivirus, qui ont placé les fichiers dans les stockages sur les postes clients, restaurent les fichiers dans les dossiers d'origine.

ENREGISTREMENT DU FICHIER DEPUIS LE STOCKAGE SUR LE DISQUE

Kaspersky Security Center permet d'enregistrer sur le disque les copies des fichiers placés par l'application antivirus en quarantaine ou dans le dossier de sauvegarde sur le poste client. Les fichiers sont copiés dans le dossier indiqué sur l'ordinateur avec Kaspersky Security Center installé.

Pour enregistrer une copie du fichier de la quarantaine ou du dossier de sauvegarde sur le disque, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Dossier de sauvegarde**.
2. Dans la zone de travail du dossier **Quarantaine** (**Dossier de sauvegarde**), sélectionnez le fichier à copier sur le disque.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :

   - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
   - A l'aide du lien **Enregistrer sur le disque** dans le groupe de travail avec le fichier sélectionné.

L'application antivirus qui avait stocké ce fichier en quarantaine sur le poste client sauvegardera la copie du fichier dans le dossier indiqué.

ANALYSE DES FICHIERS EN QUARANTAINE

Pour analyser les fichiers en quarantaine, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Quarantaine**.
2. Dans la zone de travail du dossier **Quarantaine**, sélectionnez les fichiers à analyser à l'aide des touches **Shift** et **Ctrl**.
3. Lancez le processus d'analyse des fichiers à l'aide d'un des modes suivants :

   - Dans le menu contextuel du fichier, sélectionnez l'option **Analyser les objets en quarantaine**.
   - A l'aide du lien **Analyser** dans le groupe de travail avec les fichiers sélectionnés.

Finalement, pour les applications antivirus, qui ont placé les fichiers en quarantaine, la tâche d'analyse à la demande sera lancée sur les postes clients sur lesquels les fichiers sélectionnés se trouvent en quarantaine.

FICHIERS AVEC EN TRAITEMENT DIFFERE

Les informations sur les fichiers en traitement différé, détectés sur les postes clients, se trouvent dans le dossier **Stockages**, dans le sous-dossier **Fichiers en traitement différé**.

Le traitement différé et la réparation des fichiers de l'application antivirus se réalisent à la demande ou après la réalisation d'un événement déterminé. Vous pouvez configurer les paramètres de réparation différée des fichiers.

REPARATION DU FICHIER AVEC EN TRAITEMENT DIFFERE

Pour lancer la réparation du fichier en traitement différé, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers en traitement différé**.
2. Dans la zone de travail du dossier **Fichiers en traitement différé**, sélectionnez le fichier à réparer.
3. Lancez le processus de réparation du fichier à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Réparer**.
   - A l'aide du lien **Réparer** dans le groupe de travail avec le fichier sélectionné.

   Cela entraîne la tentative de réparer le fichier.

Si le fichier est réparé, l'application antivirus, installée sur le poste client, le restaure dans le dossier d'origine. L'enregistrement sur le fichier est supprimé de la liste du dossier **Fichiers avec un traitement différé**. Si la réparation du fichier est impossible, l'application antivirus, installée sur le poste client, supprime le fichier depuis l'ordinateur. L'enregistrement sur le fichier est supprimé de la liste du dossier **Fichiers avec un traitement différé**.

ENREGISTREMENT DU FICHIER AVEC EN TRAITEMENT DIFFERE SUR LE DISQUE

Kaspersky Security Center permet d'enregistrer les copies des fichiers sur les postes clients en traitement différé sur le disque. Les fichiers sont copiés dans le dossier indiqué sur l'ordinateur avec Kaspersky Security Center installé.

Pour enregistrer une copie du fichier en traitement différé sur le disque, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers en traitement différé**.
2. Dans la zone de travail du dossier **Fichiers en traitement différé**, sélectionnez les fichiers à copier sur le disque.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
   - A l'aide du lien **Enregistrer sur le disque** dans le groupe de travail avec le fichier sélectionné.

Finalement, l'application antivirus du poste client, sur lequel le fichier sélectionné en traitement différé a été détecté, enregistre une copie du fichier dans le dossier indiqué.

SUPPRESSION DES FICHIERS DU DOSSIER "FICHIERS AVEC UN TRAITEMENT DIFFERE"

*Pour supprimer le fichier du dossier **Fichiers en traitement différé**, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le sous-dossier **Fichiers en traitement différé**.

2. Dans la zone de travail du dossier **Fichiers en traitement différé**, sélectionnez les fichiers à supprimer à l'aide des touches **Shift** et **Ctrl**.

3. Supprimez les fichiers à l'aide d'un des moyens suivants :

   - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.

   - A l'aide du lien **Supprimer les objets** (**Supprimer l'objet** lors de la suppression d'un fichier) dans le groupe de travail avec les fichiers sélectionnés.

Finalement, les applications antivirus, qui ont placé les fichiers sélectionnés dans les stockages sur les postes clients, suppriment les fichiers depuis ces stockages. Les enregistrements sur les fichiers sont supprimés de la liste dans le dossier **Fichiers en traitement différé**.

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 13), 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 service du 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 service du Support Technique, veuillez prendre connaissances des Règles d'octroi du Support Technique (http://support.kaspersky.com/support/details). Ceci permettra à nos experts de 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, il faudra indiquer le code d'activation ou le fichier clé (cf. section "A propos du fichier clé" à la page 40).

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 demande au 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

La personne qui gère les opérations du programme grâce à un système d'administration centralisé à distance de Kaspersky Security Center.

Agent d'administration

le 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 composant est un composant 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 d'authentification

L'interface qui permet de passer la procédure d'authentification pour accéder aux disques durs chiffrés et pour démarrer le système d'exploitation après le chiffrement du disque dur système.

Agent des mises a jour

L'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.

Attaque de virus

Les tentatives multiples d'infection d'un ordinateur par un virus.

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

Client du Serveur d'administration (poste client)

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

Cle active

La clé utilisée au moment actuel pour faire fonctionner l'application.

Cle complementaire

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

Console d'administration

Le 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.

G

GROUPE D'ADMINISTRATION

L'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.

GROUPE DES APPLICATIONS SOUS LICENCE

Le groupe des applications créé sur la base des critères définis par l'administrateur (par exemple, selon l'éditeur) pour lesquels le comptage des installations sur les postes clients a lieu.

K

KASPERSKY SECURITY NETWORK (KSN)

L'infrastructure des services en ligne et des services offrant l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab sur les menaces inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection, ainsi que diminue la possibilité des faux positifs.

L

LE SERVEUR DES PERIPHERIQUES MOBILES EXCHANGE ACTIVESYNC

Le 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

Le 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 DISPONIBLE

Le 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

L'ensemble de 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.

PROFIL

L'ensemble des paramètres de comportement des périphériques mobiles Exchange ActiveSync lors de la connexion au serveur Microsoft Exchange.

PROFIL DE CONFIGURATION

La 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 ce 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

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

PERIPHERIQUE MOBILE IOS MDM

Le 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 164).

R

RESTAURATION

Le déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il etait avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

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

SERVEUR DES PERIPHERIQUES MOBILES

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

SERVEUR D'ADMINISTRATION VIRTUEL

Le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport au Serveur d'administration physique, possède des restrictions suivantes :

Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie du Serveur d'administration principal.

Le Serveur d'administration virtuel utilise pour le travail les bases de données du Serveur d'administration principal : les tâches de copie de sauvegarde et de restauration de données, les tâches d'analyse et de réception des mises à jour ne sont pas prises en charge sur le Serveur virtuel. Ces tâches se résolvent dans le cadre du Serveur d'administration principal.

La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge pour le Serveur virtuel.

T

TACHE

Les 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

La tâche définie pour un groupe et exécutée sur tous les postes clients de ce groupe d'administration.

TACHE LOCALE

La tâche définie et exécutée sur un poste client particulier.

TACHE POUR UNE SELECTION D'ORDINATEURS

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

U

UTILISATEURS INTERNES

Les comptes des utilisateurs internes sont utilisés pour travailler avec les Serveurs d'administration virtuels. Sous le nom du compte de l'utilisateur interne, l'administrateur du Serveur virtuel permet de lancer Kaspersky Security Center Web-Console pour consulter les informations sur l'état de la protection antivirus du réseau. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieure 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.

V

VULNERABILITE

Le manque dans le système d'exploitation ou dans le programme qui peut être utilisé par les éditeurs de logiciels malveillant pour pénétrer dans le système ou dans le programme et pour nuire son intégrité. Un grand nombre de vulnérabilités dans le système fait en sorte que le fonctionnement du système soit fragile parce que les virus, installés dans le système, peuvent amener aux erreurs de fonctionnement du système et des programmes installés.

W

WINDOWS SERVER UPDATE SERVICES (WSUS)

L'application utilisée pour diffuser les mises à jour des applications Microsoft sur les ordinateurs des utilisateurs dans le réseau de l'entreprise.

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.

NOTIFICATIONS 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 и Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

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

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

Novell est une marque de Novell, Inc. déposée aux Etats-Unis et dans d'autres pays.

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

INDEX

M

N

P

R

S

T

U

V