Kaspersky Security Center 9.0

Manuel d'administrateur

VERSION DE L'APPLICATION : 9.0

Cher utilisateur,

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

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

Date d'édition : 21/09/11

http://www.kaspersky.fr
http://entreprise.kaspersky.fr

CONTENU

A PROPOS DE CE MANUEL

Ce manuel contient une description du rôle de Kaspersky Security Center 9.0 (ci-après – Kaspersky Security Center) et une description pas à pas de ses fonctions. Le document décrit aussi les notions et les fonctions principales de l'application Kaspersky Security Center.

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 complémentaires (à la page 11)

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

Kaspersky Security Center (à la page 13)

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

Administration des clés Kaspersky Security Center (à la page 18)

Cette section décrit les particularités du contrat de licence de l'application Kaspersky Security Center.

Interface de l'application (à la page 21)

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

Assistant de configuration initiale (à la page 34)

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

Notions principales (à la page 36)

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

Administration des Serveurs d'administration (à la page 43)

Cette section contient les informations sur le travail avec les Serveurs d'administration et sur la configuration des paramètres du Serveur d'administration.

Administration des groupes d'administration (à la page 52)

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

Administration à distance des applications (à la page 56)

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.

Administration des postes clients (à la page 69)

Cette section contient les informations sur le travail avec les postes clients.

Manipulation avec les rapports, les statistiques et les notifications (à la page 80)

Cette section reprend les informations sur le fonctionnement avec les rapports et les statistiques dans Kaspersky Security Center, ainsi que sur la configuration des notifications du Serveur d'administration.

Requêtes d'événements et d'ordinateurs (à la page 84)

Cette section reprend les informations sur le fonctionnement avec les extractions des événements dans le fonctionnement de Kaspersky Security Center et des applications administrées, ainsi que sur le fonctionnement avec les extractions des postes clients.

Ordinateurs non définis (à la page 90)

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

Applications et vulnérabilités (à la page 95)

Cette section décrit le travail avec les applications et les vulnérabilités que Kaspersky Security Center découvre sur les postes clients.

Mise à jour des bases et des modules d'application (à la page 98)

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 106)

Cette section décrit les possibilités de Kaspersky Security Center sur le travail avec les clés des applications administrées de Kaspersky Lab.

Stockages des données (à la page 109)

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 115)

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

Glossaire

La section reprend les termes utilisés dans ce document.

Kaspersky Lab (à la page 122)

Cette section reprend les informations sur Kaspersky Lab.

Informations sur le code tiers (à la page 123)

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 124)

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

Index

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

CONVENTIONS

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

Tableau 1. Conventions

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

SOURCES D'INFORMATIONS COMPLEMENTAIRES

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

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

Kaspersky Lab offre de nombreuses sources d'informations sur l'application. Vous pouvez choisir celle qui vous convient le mieux en fonction de l'urgence et de la gravité de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

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

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

Page sur le site Web de Kaspersky Lab

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

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

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

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

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

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

Système d'aide électronique

Une aide complète est livrée avec l'application.

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

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

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

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

Documentation

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

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

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

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

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

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

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

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

CONTACTER LE GROUPE DE REDACTION DE LA DOCUMENTATION POUR LES UTILISATEURS

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

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

KASPERSKY SECURITY CENTER

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

Le logiciel est proposé dans deux versions :

- Kaspersky Security Center 9.0 (ci-après – Kaspersky Security Center) est proposé gratuitement avec toutes les applications de Kaspersky Lab de la suite Kaspersky Open Space Security (version vendue en boîte). Il peut également être téléchargé depuis le site de Kaspersky Lab (http://www.kaspersky.fr).

- Kaspersky Security Center 9,0, Service Provider Edition (ci-après – Kaspersky Security Center SPE) est livré sous les conditions particulières aux partenaires de Kaspersky Lab. Pour plus d'informations, visitez le site Internet de Kaspersky Lab, à la page http://www.kaspersky.com/fr/partners.

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

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

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

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

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

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

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

- Former une hiérarchie de groupes d'administration qui assure une protection antivirus de l'entreprise. Les groupes d'administration permettent d'administrer la sélection d'ordinateurs comme un tout unique.

- Effectuer l'installation et la désinstallation à distance des applications de Kaspersky Lab.

- Effectuer à distance l'administration centralisée des applications de Kaspersky Lab.

- Recevoir et diffuser de façon centralisée sur les postes clients les mises à jour des bases et des modules des applications de Kaspersky Lab.

- Recevoir les notifications sur les événements critiques dans le fonctionnement des applications de Kaspersky Lab.

- Recevoir les statistiques et les rapports de fonctionnement des applications de Kaspersky Lab.

- Administrer les clés des applications installées de Kaspersky Lab.

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

- Travailler de façon centralisée avec les applications des éditeurs tiers, installées sur les postes clients.

DANS CETTE SECTION

NOUVEAUTES

Modifications apportées dans l'application Kaspersky Security Center 9.0 par rapport à la version Kaspersky Administration Kit 8.0 :

- La possibilité de créer les Serveurs d'administration virtuels a été réalisée.
- La fonction KSN Proxy a été ajoutée. Cette fonction assure l'interaction entre KSN et les postes clients.
- Le composant Kaspersky Security Center Web-Console a été ajouté dans l'application.
- La fonction du contrôle de fonctionnement des applications a été ajoutée.
- La fonction de la récolte centralisée des informations sur l'état de configuration matérielle sur les ordinateurs administrés a été ajoutée.
- La fonction du registre centralisé des applications a été élargie.
- La fonction du contrôle de vulnérabilités dans les applications sur les ordinateurs administrés a été ajoutée.
- La prise en charge Windows® Failover Clustering pour le Serveur d'administration a été ajoutée.
- La fonction de la mise à jour des descriptions des applications incompatibles lors de la création des paquets d'installation des applications antivirus a été ajoutée.
- La possibilité d'obtenir les notifications sur les nouvelles versions des applications corporatives de Kaspersky Lab et la possibilité d'obtenir les nouvelles versions dans le cadre de la tâche de mise à jour du Serveur d'administration a été ajoutée.
- L'ensemble de rapports et de panneaux d'informations a été élargi.
- Le mécanisme de désignation automatique des agents de mises à jour a été réalisé.
- La possibilité de sonder le réseau et d'installer à distance les applications à l'aide de l'Agent d'administration a été ajoutée.
- L'interface d'utilisateur de la Console d'administration a été retravaillée.
- La possibilité d'utiliser la passerelle des connexions a été ajoutée.
- L'installateur séparé pour la Console d'administration a été ajouté.
- La possibilité de recherche de texte d'informations par la Console d'administration a été réalisée.
- La fonction de l'identification des machines virtuelles a été réalisée. Il est possible de réaliser la recherche et d'établir les règles de déplacement des ordinateurs conformément aux paramètres de la machine virtuelle.
- Le support du mode dynamique pour Virtual Desktop Infrastructure (VDI) a été réalisé.
- Le composant Gestionnaire des connexions permettant d'installer les intervalles de temps du transfert de données depuis l'Agent d'administration vers le Serveur a été ajouté.

- La possibilité d'administrer l'interaction avec Microsoft® NAP dans la stratégie de l'Agent d'administration a été ajoutée.
- La possibilité de créer des comptes Kaspersky Security Center, qui ne sont pas des comptes des utilisateurs Windows, a été ajoutée.
- La possibilité d'exclusion des groupes d'administration sélectionnés depuis la zone d'action de la tâche a été ajoutée.
- L'installateur séparé (son distributif est exclu de la composition de l'application) pour installer Kaspersky Security Center System Health Validator a été créé.

CONFIGURATIONS MATERIELLES ET LOGICIELLES

Serveur d'administration et Kaspersky Security Center Web-Console

- Configuration logicielle :
  - Microsoft Data Access® Components (MDAC) de version 2.8 ou supérieure ou Microsoft Windows DAC 6.0.
  - Système de gestion des bases de données : Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, MySQL versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091 ou MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.
  - Microsoft Windows Server® 2003 et supérieur ; Microsoft Windows Server 2003 x64 et supérieur ; Microsoft Windows Server 2008 ; Microsoft Windows Server 2008 déployé en mode Server Core ; Microsoft Windows Server 2008 x64 avec Service Pack 1et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows Server 2008 R2 ; Microsoft Windows Server 2008 R2 déployé en mode Server Core ; Microsoft Windows XP Professional avec Service Pack 2 et supérieur ; Microsoft Windows XP Professional x64 et supérieur ; Microsoft Windows Vista® avec Service Pack 1 et supérieur, Microsoft Windows Vista x64 avec Service Pack 1et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows 7; Microsoft Windows 7 x64.
- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.
  - Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
    - Processeur avec 1.4 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.

Console d'administration Kaspersky

- Configuration logicielle :
  - Système d'exploitation Microsoft Windows.

    La version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration.
  - Microsoft Management Console version 2.0 et supérieure.
  - Lors du fonctionnement sous Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 ou Microsoft Windows Vista : la présence du navigateur installé Microsoft Internet Explorer® 7.0 ou suivant est requise.
  - L'utilisation sous Microsoft Windows 7 requiert Microsoft Internet Explorer 8.0 ou suivant.
- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.
  - Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
    - Processeur avec 1.4 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - 1 Go d'espace disque disponible.

Agent d'administration et agent de mises à jour

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

    La version du système d'exploitation pris en charge est définie selon les exigences des applications dont l'administration est accessible via Kaspersky Security Center.
- Configuration matérielle :
  - Pendant le fonctionnement sous le système d'exploitation Windows 32 bits :
    - Processeur avec 1 GHz ou plus ;
    - 512 Mo de mémoire vive ;
    - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.

- Pendant le fonctionnement sous le système d'exploitation Windows 64 bits :
  - Processeur avec 1.4 GHz ou plus ;
  - 512 Mo de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation Linux 32 bits :
  - Processeur avec 1 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation Linux 64 bits :
  - Processeur avec 1.4 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation Mac OS :
  - Processeur avec 1 GHz ou plus ;
  - 1 Go de mémoire vive ;
  - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.

ADMINISTRATION DES CLES KASPERSKY SECURITY CENTER

Cette section décrit les particularités du contrat de licence de l'application Kaspersky Security Center.

Dans le contexte de l'octroi de licences de Kaspersky Security Center, les notions suivantes sont définies :

- contrat de licence (cf. section "Présentation du contrat de licence" à la page 18) ;
- licence (cf. section "A propos des licences Kaspersky Security Center" à la page 18) ;
- clé (cf. section "A propos des clés" à la page 19) ;
- fichier clé (cf. section "A propos des fichiers clés" à la page 19) ;
- activation de l'application (à la page 20).

Ces notions sont liées d'une manière indissoluble et forment un schéma unique de l'octroi de licences.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un accord conclu entre une personne physique ou morale détenant une copie légale de l'application et Kaspersky Lab. Le contrat est repris dans chaque application de Kaspersky Lab. Il reprend des informations détaillées sur les droits et les restrictions d'utilisation de l'application.

Selon le contrat de licence, en achetant et en installant l'application de Kaspersky Lab, vous recevez le droit illimité sur la possession de sa copie.

A PROPOS DES LICENCES KASPERSKY SECURITY CENTER

Licence : le droit d'utilisation de l'application en toute intégrité et des services complémentaires liés à l'application. Ces services sont offerts par Kaspersky Lab et ses partenaires.

La licence de Kaspersky Security Center permet de créer des Serveurs d'administration virtuels. Les licences avec les restrictions suivantes sont prévues :

- La licence permettant de créer jusqu'à 50 Serveurs d'administration virtuels.
- La licence permettant de créer jusqu'à 100 Serveurs d'administration virtuels.

Chaque licence est caractérisée par la durée de validité et le type.

Durée de validité de la licence : est un intervalle de temps pendant lequel vous possédez l'accès aux fonctions de l'application et le droit d'utilisation des services complémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

Les *types suivants de licences* sont prévus :

- *Evaluation* : une licence gratuite conçue pour faire connaissance avec Kaspersky Security Center.

  La licence d'évaluation permet de créer des Serveurs d'administration virtuels. En utilisant la licence d'évaluation, vous ne pouvez pas contacter le service du Support Technique. A la fin de sa validité, il n'est plus possible de créer des Serveurs d'administration virtuels.

  La durée de validité de la licence d'évaluation ne peut pas être renouvelée. Il est impossible d'utiliser l'application selon la licence d'évaluation après l'utilisation de l'application selon la licence commerciale

- *Commerciale* : une licence payante offerte lors de l'achat de Kaspersky Security Center.

  La licence commerciale permet de créer des Serveurs d'administration virtuels et la possibilité de contacter le service du Support Technique. A la fin de validité de la licence commerciale, l'application Kaspersky Security Center pendant un intervalle de temps (15 jours) notifie sur l'expiration de la validité de la licence. Si vous ne renouvelez pas la durée de validité de la licence durant cette période, vous ne pourrez plus créer des Serveurs d'administration virtuels, ainsi que contacter le service du Support Technique.

A PROPOS DES CLES

Clé est une suite de caractères qui confirme le droit d'utilisation de l'application.

Clé active est une clé utilisée au moment actuel pour faire fonctionner l'application.

Clé complémentaire est une clé qui confirme le droit d'utilisation de l'application, non utilisée au moment actuel.

Pour confirmer la licence, vous pouvez ajouter deux clés. Dans ce cas, une clé sera active et l'autre sera complémentaire.

A PROPOS DES FICHIERS CLES

Fichier clé : un moyen technique permettant d'ajouter une clé, liée au fichier clé, dans le stockage des clés.

Le fichier clé est livré avec le logiciel si vous avez acheté ce dernier chez un revendeur de Kaspersky Lab. Il est envoyé par courrier électronique si vous avez acheté le logiciel en ligne.

Les informations suivantes sont reprises dans le fichier clé :

- Durée de validité de la licence.
- Type de licence (d'évaluation, commerciale).
- Restriction de licence (par exemple, le nombre d'ordinateurs qui peuvent utiliser cette licence).
- Délai périssable du fichier clé.

Délai périssable du fichier clé est une période, à l'expiration de laquelle le fichier clé devient inactif, et comme conséquence, la possibilité d'ajouter une clé, liée avec ce fichier clé, dans le stockage des clés se perd. Le délai périssable du fichier clé est considéré dès le moment de création du fichier clé.

ACTIVATION DE L'APPLICATION

Pour obtenir les possibilités d'utiliser les fonctions et les services complémentaires liés avec l'application, il est nécessaire d'activer l'application.

Pour activer l'application Kaspersky Security Center, procédez comme suit :

1. Achetez une licence.
2. Recevez le fichier clé ou le code d'activation prévu par les conditions de cette licence.
3. A l'aide du fichier clé ou du code d'activation, indiquez la clé, liée à la licence, en tant que clé active du Serveur d'administration principal à l'aide d'un des moyens suivants :
   - Ajoutez la clé à l'aide de l'Assistant de configuration initiale.
   - Ajoutez la clé dans le dossier **Stockages** du Serveur d'administration principal, dans le dossier joint **Clés**.
   - Dans la fenêtre des propriétés du Serveur principal, sélectionnez la section **Clés** et ajoutez la clé dans le groupe **Clé active**.
4. Redémarrez la Console d'administration.

RENOUVELLEMENT DE LA LICENCE

Lors de l'ajout des clés dans le stockage, une des clés devient active et l'autre - complémentaire.

A la fin de la durée de validité de la licence, indiquée dans le fichier de la clé active, vous pouvez utiliser la clé complémentaire pour renouveler la durée de validité de la licence.

Primordialement, la clé indiquée lors de l'activation de l'application devient la clé active.

La clé complémentaire devient automatiquement active à l'expiration de la licence.

Si le fichier clé, appliqué pour ajouter la clé active, se trouve dans la *liste noire des fichiers clés*, Kaspersky Security Center notifie sur la détection du fichier clé dans la liste noire et procède comme suit :

- En présence de la clé active, modifie son statut sur *active*.
- Lors de l'absence de la clé complémentaire, vous ne pouvez pas créer des Serveurs d'administration virtuels et de contacter le service du Support Technique.

La vérification de l'actualité du fichier clé se passe à chaque obtention des mises à jour pour le Serveur d'administration Kaspersky Security Center.

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 assure l'interface d'administration. Elle représente un outil autonome centralisé, intégré dans 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 DU PROGRAMME

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 assure la gestion des fenêtres et offre l'accès au système d'informations. Le point 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. L'ensemble de boutons dans la barre d'outils change selon la section actuelle ou pour le dossier de l'arborescence de la console.

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

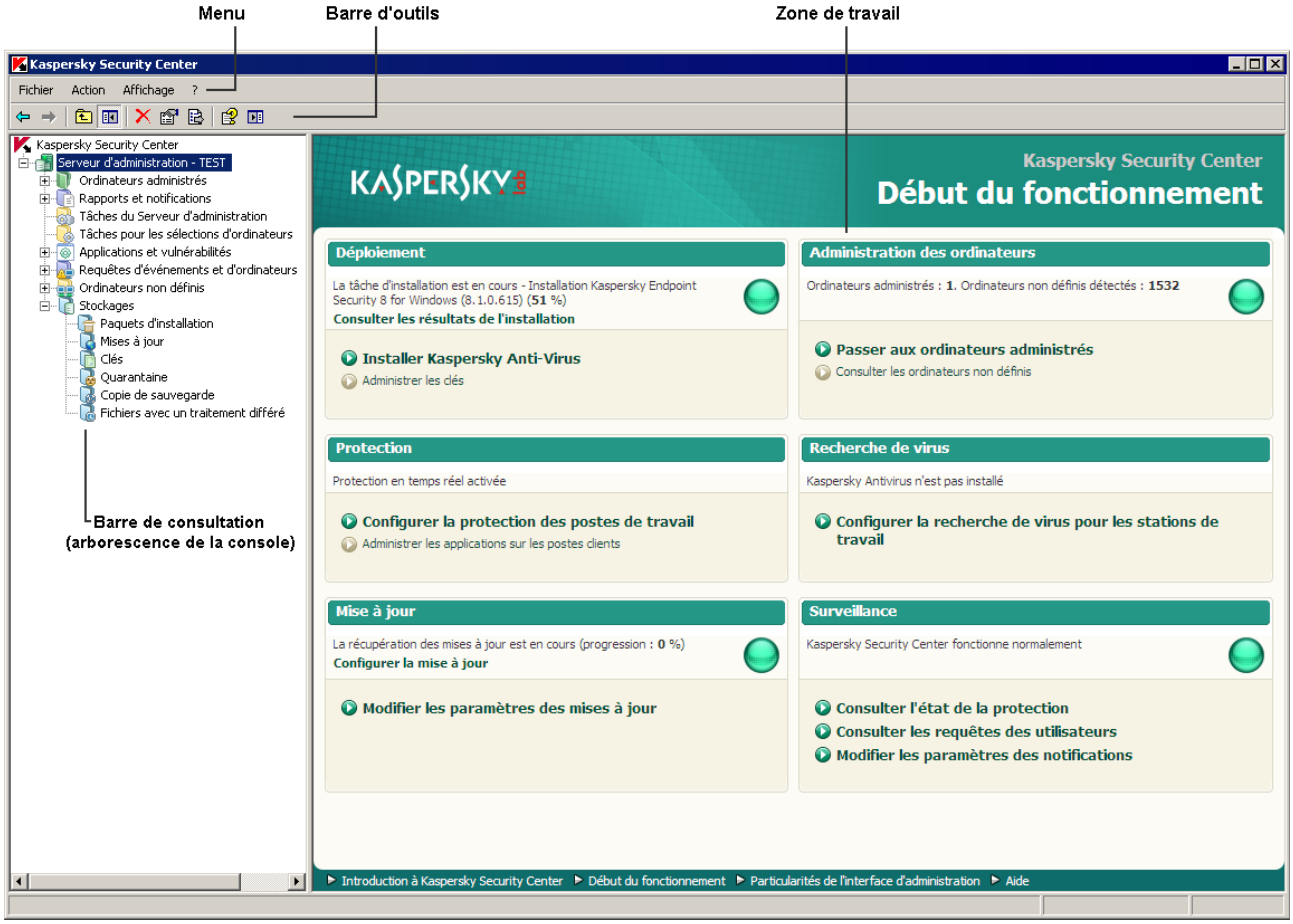


Illustration 1. Fenêtre principale de Kaspersky Security Center

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 **Extraction des événements et des ordinateurs**. 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**.
- **Rapports et notifications**.
- **Tâches du Serveur d'administration**.
- **Tâches pour les sélections d'ordinateurs**.
- **Requêtes d'événements et d'ordinateurs**.
- **Applications et vulnérabilités**.
- **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 **Rapports et notifications** de l'arborescence de la console contient l'ensemble des modèles pour former les rapports d'état du système de protection antivirus sur les postes clients des groupes d'administration.

Le dossier **Tâches du Serveur d'administration** contient l'ensemble de tâches, définies pour le Serveur d'administration. Il existe trois types de tâches du Serveur d'administration : l'envoi automatique des rapports, la sauvegarde des données et le téléchargement des mises à jour dans le stockage du Serveur d'administration.

Le dossier **Tâches pour les sélections d'ordinateurs** contient les tâches définies 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 **Requêtes d'événements et d'ordinateurs** inclut les sous-dossiers suivants :

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

Le dossier **Administration des applications** 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 Windows Update**. Contient la liste des mises à jour des applications Microsoft Windows reçues par le Serveur d'administration qui peuvent être déployées sur les postes client.

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 la zone 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 :

- **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.
- **Mises à jour**. Contient la liste des mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les postes client.
- **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 avec un traitement différé**. Contient la liste des fichiers pour lesquels les applications antivirus ont décidé le traitement ultérieur.

ZONE DE TRAVAIL

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.

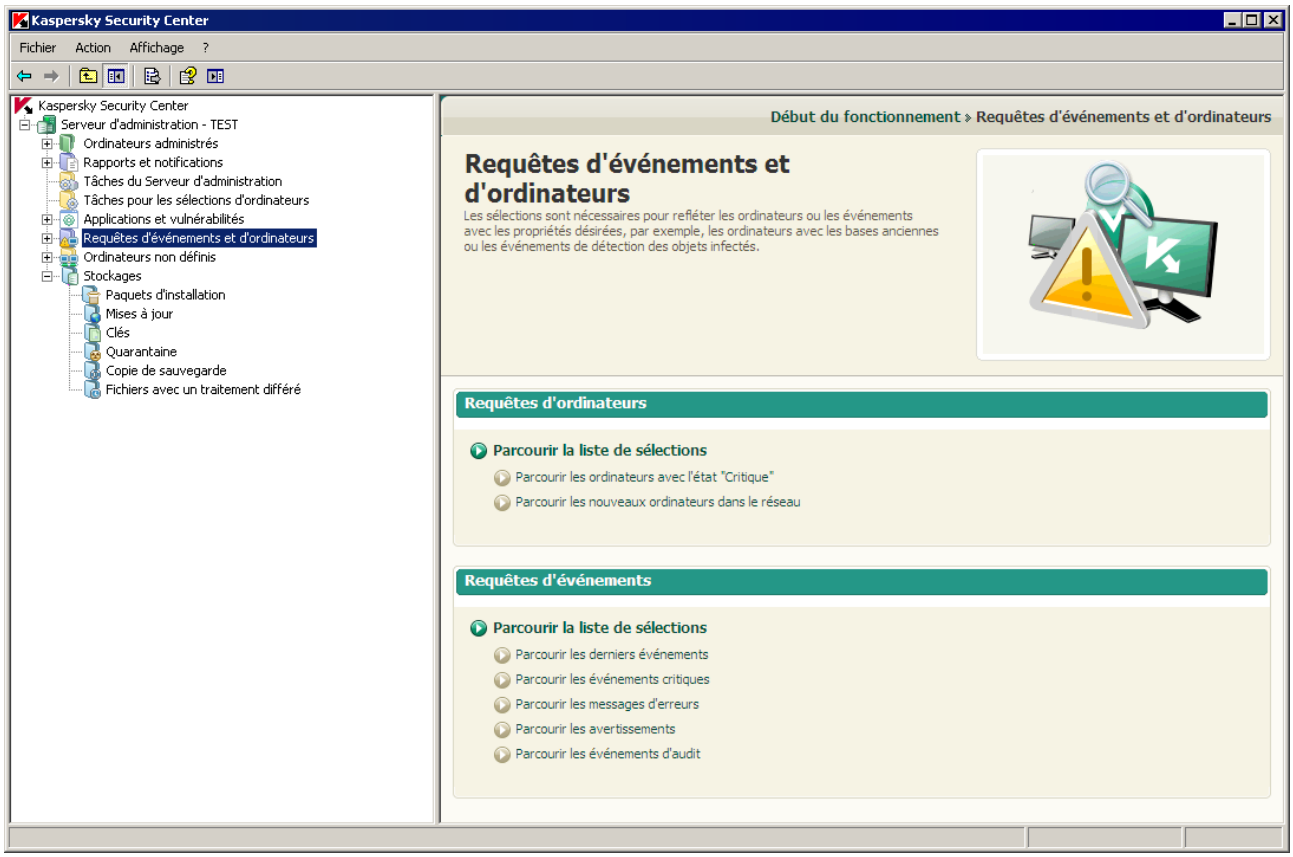


Illustration 3. Zone de travail

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 groupes d'informations.

Dans les cas, quand 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).

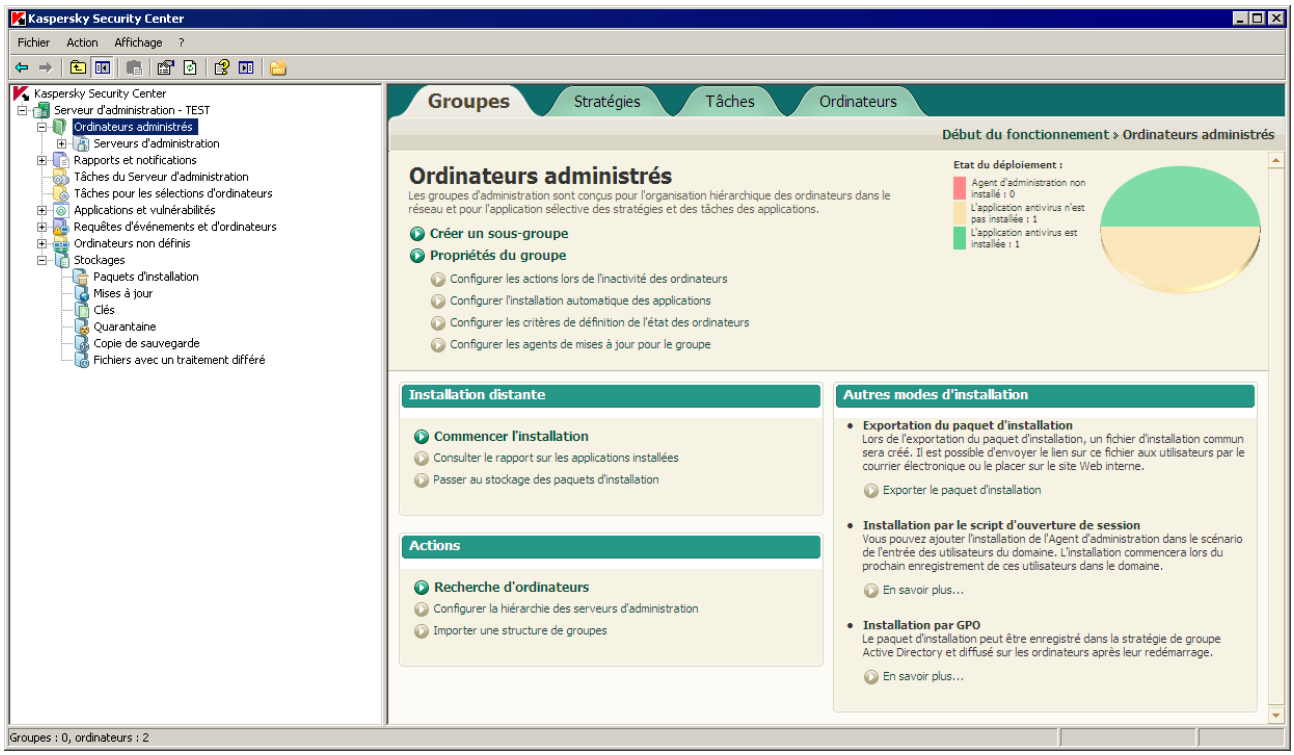


Illustration 4. Zone de travail partagée sur onglets

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).

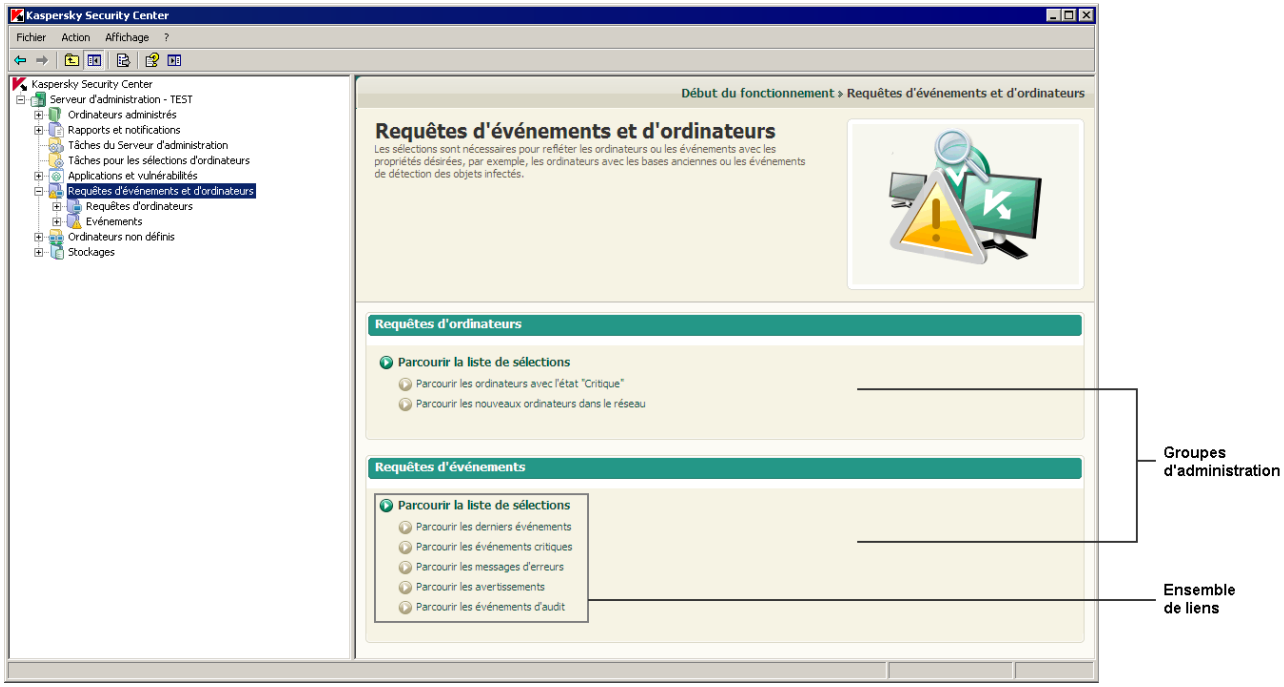


Illustration 5. Zone de travail présentée par l'ensemble de groupes d'administration

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).

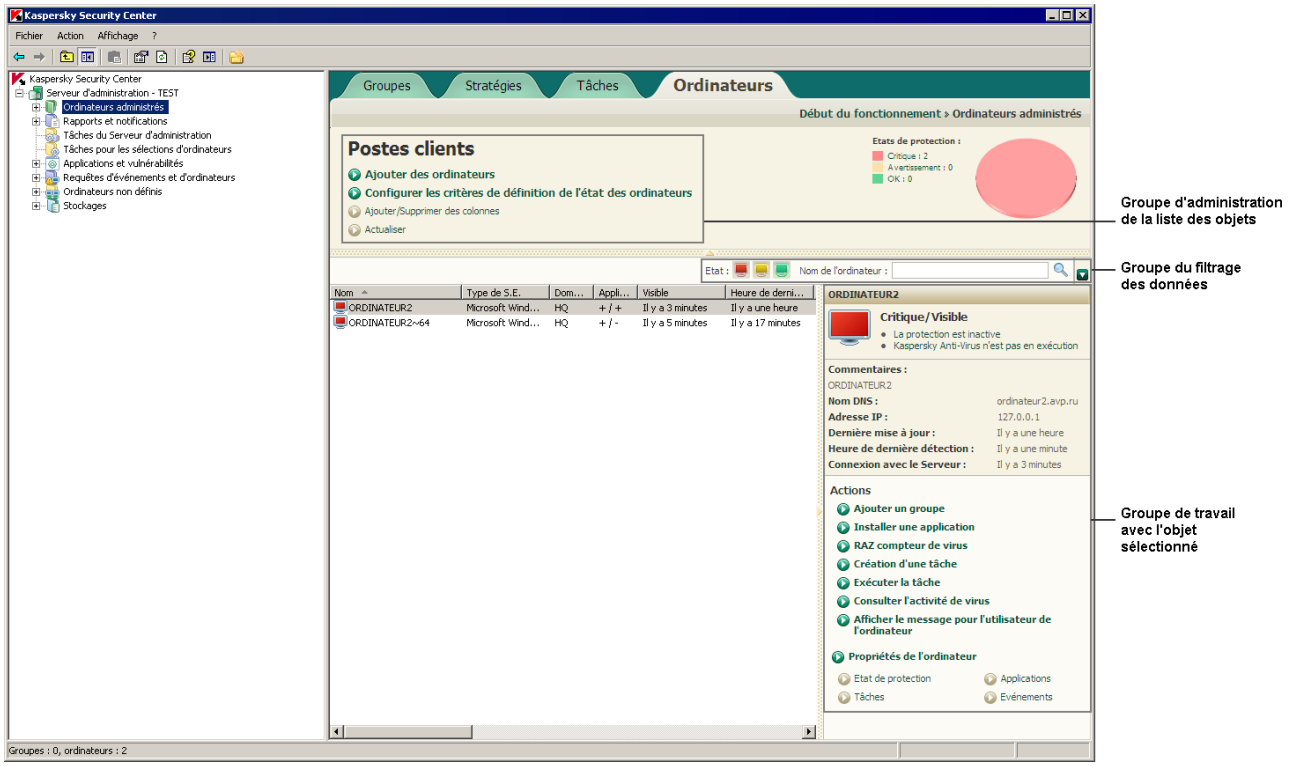


Illustration 6. Zone d'informations présentée par la liste des objets d'administration

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 *groupes d'informations* sans éléments d'administration (cf. ill. ci-après).

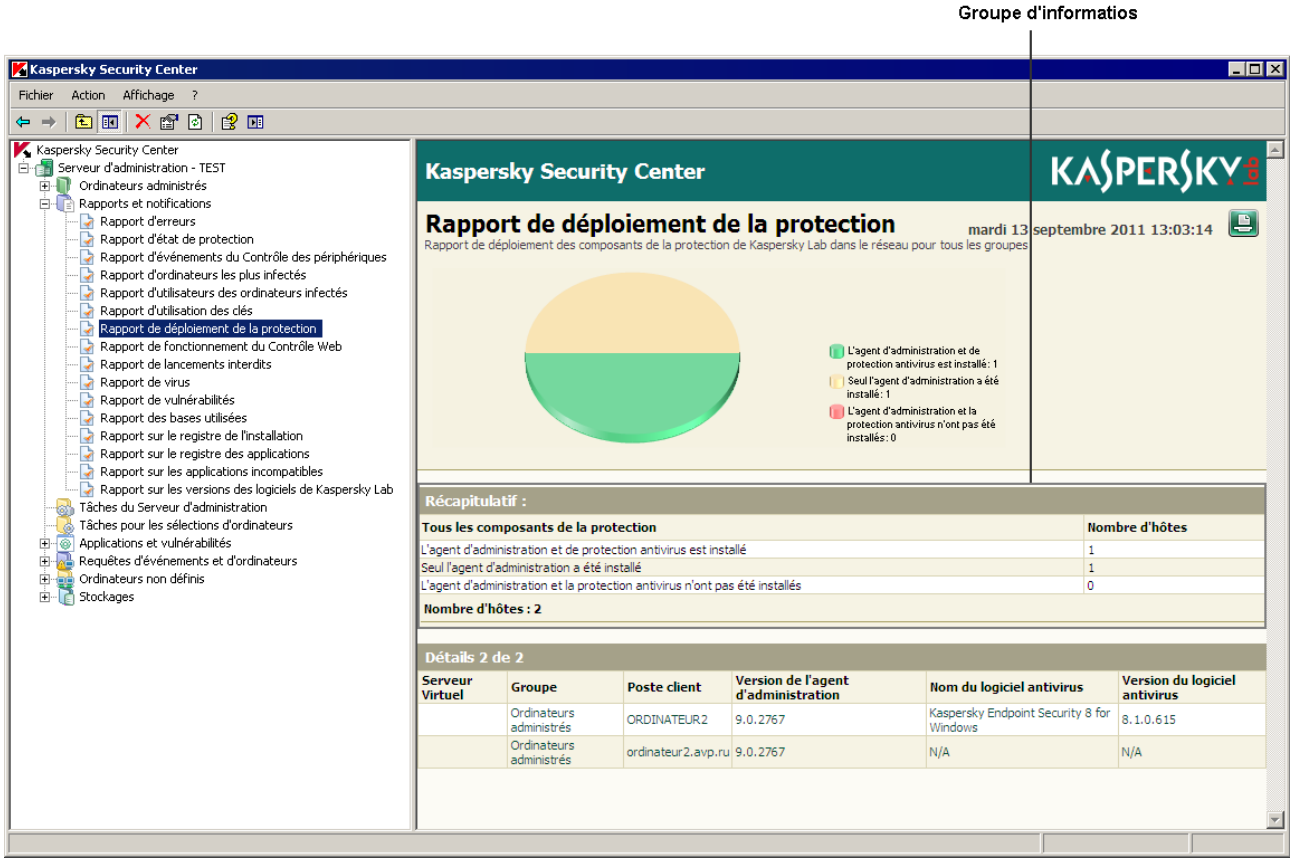


Illustration 7. Zone de travail présentée par l'ensemble de groupes d'informations

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

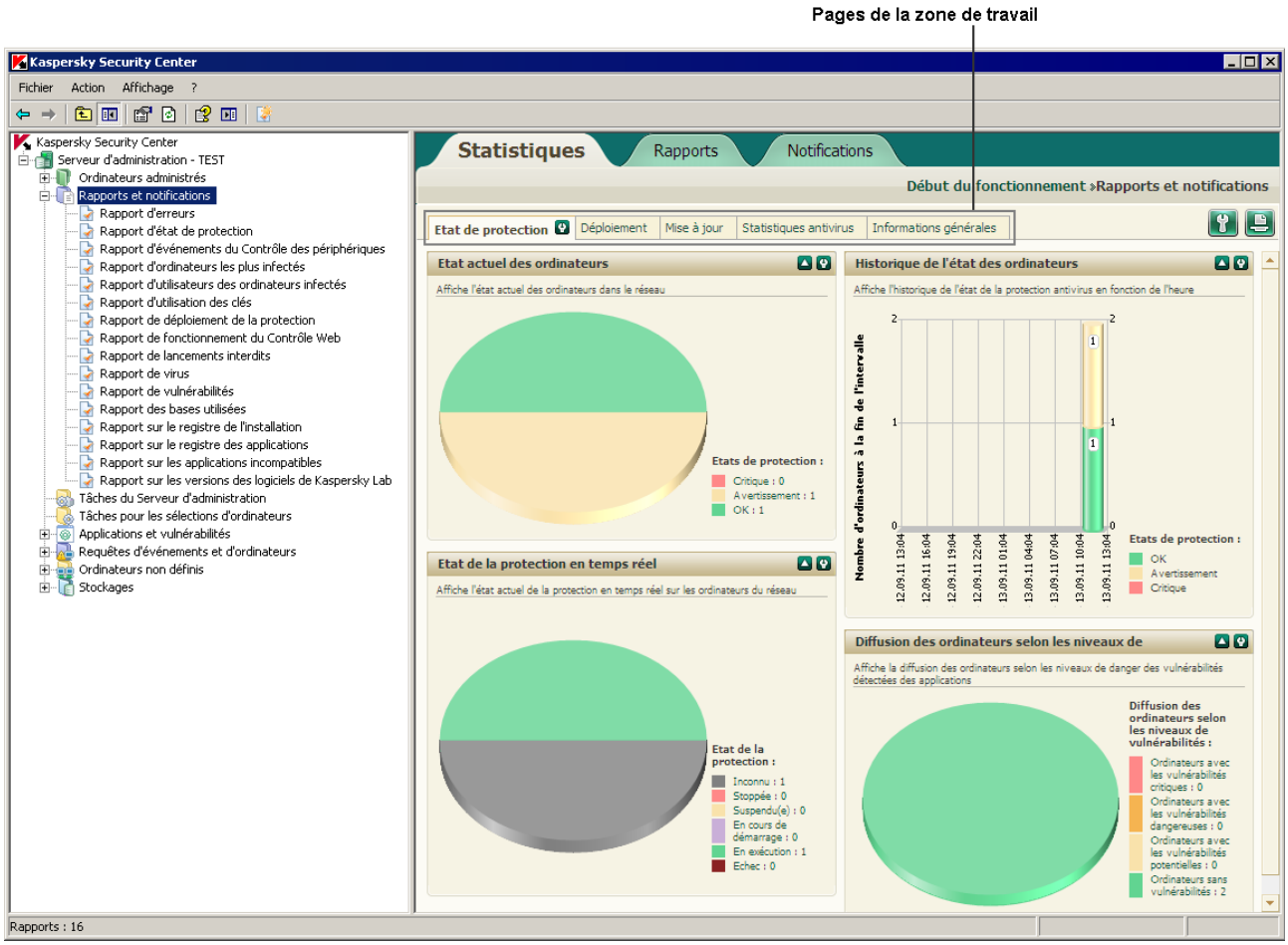


Illustration 8. Zone de travail partagée sur pages

GROUPE DU FILTRAGE DE DONNEES

Le *groupe du filtrage de données* (ci-après *groupe du filtrage*) est situé dans la zone de travail contenant la liste des ordinateurs, des applications ou des événements.

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

- paramètres de ligne ;
- paramètres de choix ;
- boutons.

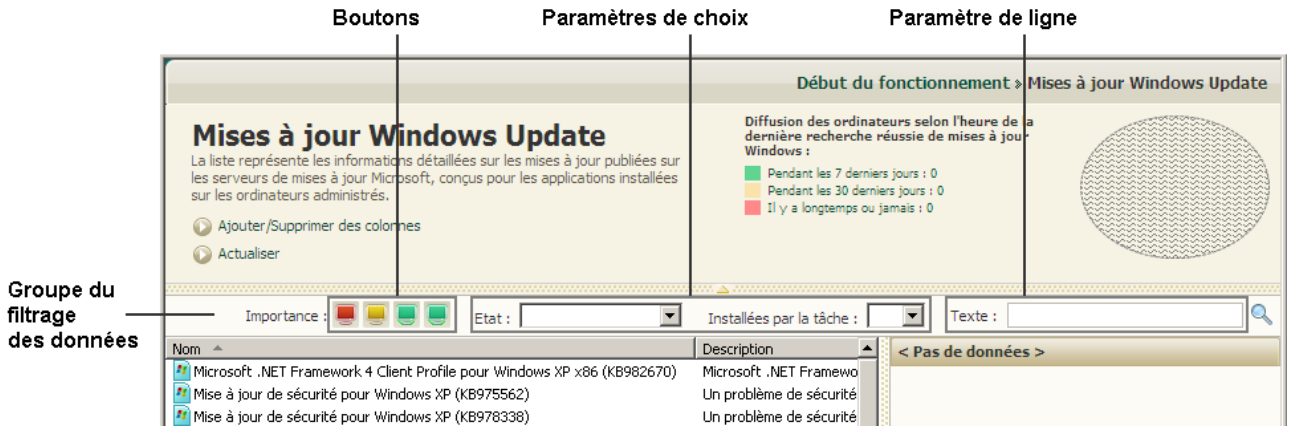


Illustration 9. Groupe du filtrage de données

Paramètres de ligne

Pour utiliser les paramètres de ligne du filtrage, il faut saisir le texte recherché dans le champ de saisie.

Pour décrire le texte recherché dans la requête d'événements dans le champ **Description d'événement**, les caractères suivants sont possibles :

- A l'intérieur d'un seul mot :
  - *****. Remplace n'importe quelle ligne d'une longueur de 0 ou plus de caractères.

Exemple :

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

  - **?**. Remplace un n'importe quel caractère.

Exemple :

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

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

- Pour lier plusieurs mots :
  - 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 choix, il faut sélectionner la valeur dans la liste déroulante.

Boutons

Le 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*.

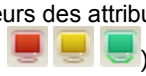
- L'élément de la liste avec la valeur indiquée de l'attribut est considéré comme non sélectionné si le groupe du filtrage indique l'icône avec la valeur indiquée de l'attribut et cette icône est sur le fond clair.

  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

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

- Composition de la requête :
  - Lors de l'utilisation des boutons du groupe du filtrage, la requête 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 situé à côté du bouton .

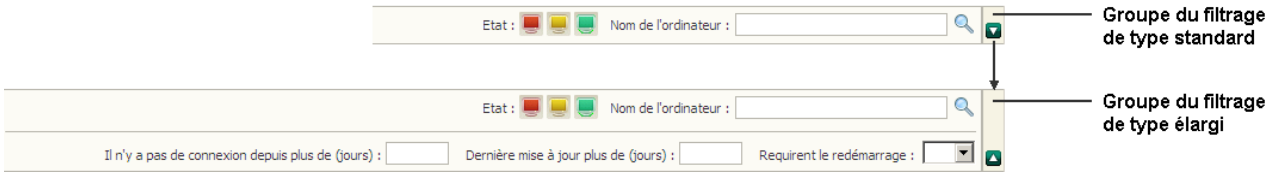


Illustration 10. Groupe du filtrage avec le type élargi de présentation

- 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 son propre 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 au nœud 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 les Serveurs d'administration secondaires**.

     Si la case est cochée, l'arborescence de la Console d'administration affichera 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) sera 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.

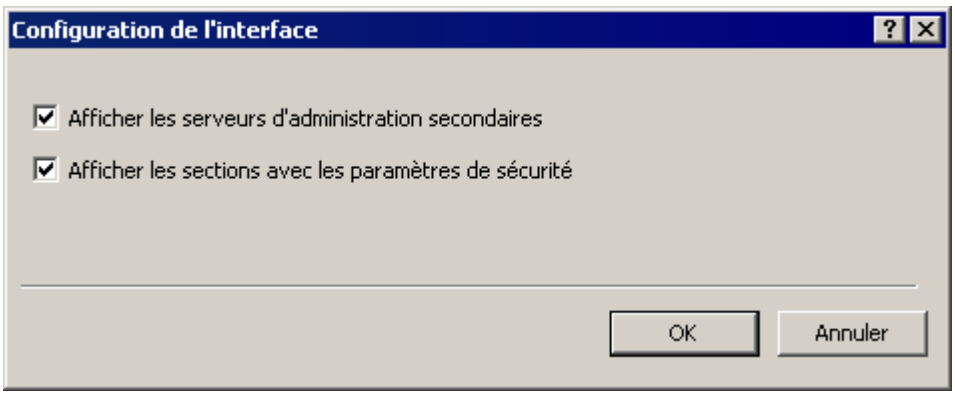


*Illustration 11. Fenêtre **Configuration de l'interface***

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 contre les virus. 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 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 et par NET SEND 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).

- 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 réserve 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 50

NOTIONS PRINCIPALES

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

DANS CETTE SECTION

SERVEUR D'ADMINISTRATION

Les composants 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 composant 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 de Kaspersky Administration Server ;
- 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 ;
- organisation des référentiels de distribution des applications de Kaspersky Lab ;
- installation à distance des applications de Kaspersky Lab sur les ordinateurs et leur désinstallation ;
- 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 postes clients ;

- formation des rapports sur le fonctionnement des applications de Kaspersky Lab ;
- extension des clés sur les postes 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 37).

La hiérarchie des Serveurs d'administration peut être utilisée pour les buts 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 fonctionnement avec des 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 avec le 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 Serveurs différents.

SERVEUR D'ADMINISTRATION VIRTUEL

Serveur d'administration virtuel (ci-après *Serveur virtuel*) – le composant 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.

Outre cela, 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.

AGENT D'ADMINISTRATION. GROUPE D'ADMINISTRATION

L'interaction entre le Serveur d'administration et les postes clients s'opère via le composant *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 une sélection d'attributs suivante :

- sous le nom de Kaspersky Network Agent ;
- avec 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 dans le cas où 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 certaine 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 points 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 composant *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 composant 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.

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 41).

Si dans la fenêtre des propriétés de la stratégie héritée vous décochez la case **Hériter des paramètres de la stratégie de niveau supérieur** dans la section **Activité et héritage**, 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 nomades.

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 programmation) 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 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.

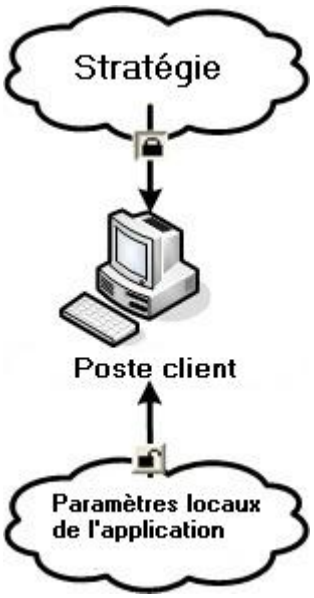


Illustration 12. Stratégie et paramètres locaux de l'application

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 le travail avec les 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 avec le Serveur d'administration, indiqué lors de l'installation de Kaspersky Security Center, s'exécute.

Après la connexion avec le 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>.

Si vous ne possédez aucun droit d'opérateur ou d'administrateur de Kaspersky Security Center pour le réseau choisi, l'accès au Serveur d'administration sera refusé.

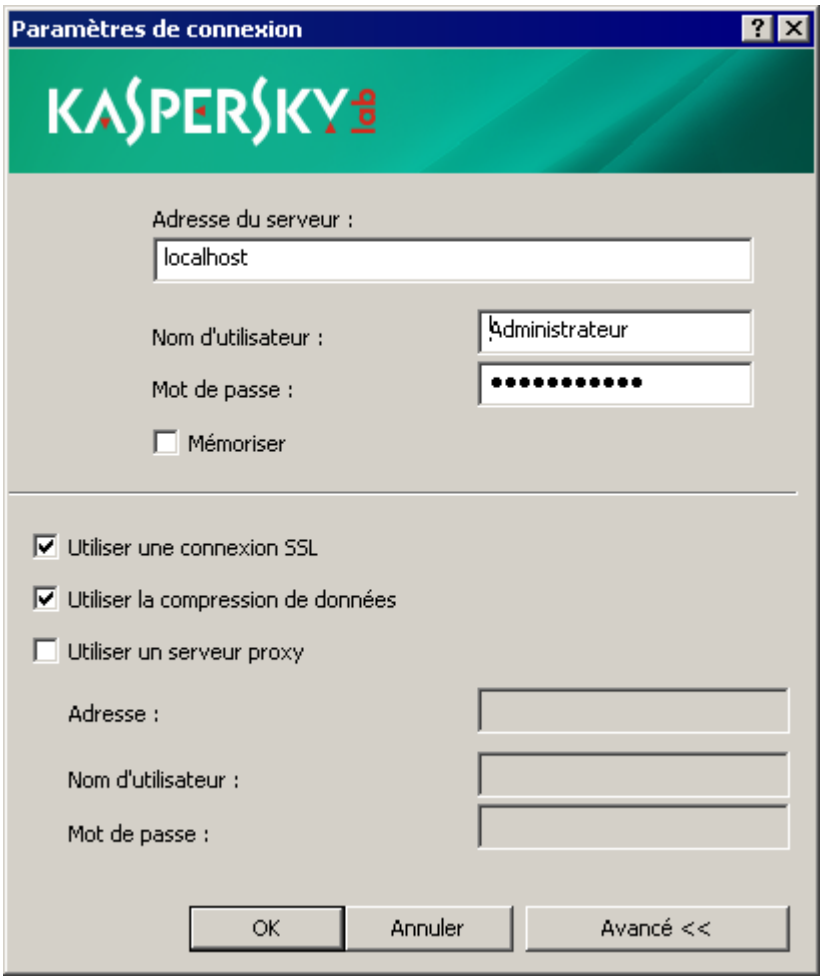


Illustration 13. Etablissement de la connexion au Serveur d'administration

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

Après la connexion avec le 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 passe, les groupes **KLAdmins** et **KLOperators** sont créés de la manière suivante :

- Si l'installation se passe 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 passe 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 dans 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 dossier joint **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 avec le 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 crypter les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérants et le cryptage 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 composant 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 Kaspersky Security Center, sélectionnez l'entrée **Kaspersky Security Center**.
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. Sélectionnez l'entrée correspondant au Serveur d'administration à supprimer dans l'arborescence de console.
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.

Suite au fonctionnement de l'Assistant, 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.

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 de l'épidémie de virus et les actions dans le cas de son apparition 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 49), dans la fenêtre des propriétés de l'événement **Attaque de virus**.

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

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

Sous le titre **Virus découvert**, 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 composant **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 KSN Proxy 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 dans le cas 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 des 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 des groupes d'administration, des postes clients et des sous-groupes peuvent être ajoutés au dossier **Ordinateurs administrés**. Le dossier **Serveurs d'administration** permet d'ajouter les 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 postes clients compris dans ce groupe s'affichent sur les onglets correspondants dans la zone de travail de ce groupe.

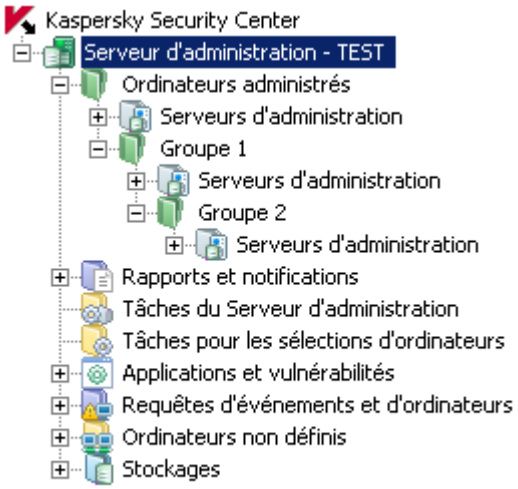


Illustration 14. Consultation des hiérarchies des groupes d'administration

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

1. Dans l'arborescence de la console, ouvrez le dossier **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 un nouveau groupe d'administration doit appartenir.

   Si vous créer un nouveau groupe d'administration du niveau supérieur de la hiérarchie, vous pouvez ignorer cette étape.
3. Lancez le processus de création du groupe d'administration par 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 ouverte **Nom de groupe**, saisissez le nom de groupe et cliquez sur le bouton **OK**.

Finalement, l'arborescence de la console affichera un nouveau dossier du groupe d'administration avec le nom défini.

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 2/Subdivision 2/Section 1

Office 3/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 se supprime 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.

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 passe d'une manière suivante : si des tâches résidentes (tâches de protection en temps réel) sont exécutées sur le poste client, elles sont poursuivies avec les nouvelles valeurs des paramètres sans interruption. Les tâches exécutées périodiquement (analyse à la demande, mise à jour des bases de l'application) continue l'exécution 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 nomades (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 **Avancé** 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.

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 nomades entre en vigueur sur l'ordinateur dans le cas de déconnexion du réseau d'entreprise.

Pour appliquer la stratégie sélectionnée pour les utilisateurs nomades,

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

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 sous l'onglet **Stratégies**, sélectionnez une stratégie.
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 **_1** 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 numérique **(1)** 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.

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**.

Finalement, 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 sélections d'ordinateurs*. Tâches exécutées sur les ordinateurs sélectionnés peu importe leur inclusion dans les groupes d'administration.
- *Tâches locales*. Tâches exécutées sur le 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 dans le cas où l'application pour laquelle les tâches ont été créées est en lancée. Si l'application est désactivée, toutes les tâches courantes sont annulées.

Les résultats d'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.

Si lors de la création de la tâche vous avez défini le nom de la tâche existante dans ce groupe des tâches, le suffixe **_1** sera automatiquement ajouté au nom d'une nouvelle tâche.

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.

Uniquement la tâche de diffusion automatique des rapports est disponible sur le Serveur virtuel. 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. Sélectionnez le dossier **Tâches du Serveur d'administration** dans l'arborescence de la console.
2. Lancez le processus de création de la tâche par 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** et **Sauvegarde des données du Serveur d'administration** peuvent exister qu'en un seul exemplaire. Si la tâche de téléchargement des mises à jour dans le stockage ou la tâche de sauvegarde des données du Serveur d'administration a déjà été créée pour le Serveur d'administration, alors elle ne s'affiche pas dans la fenêtre de sélection du type de tâche de l'Assistant de création d'une tâche.

CREATION D'UNE TACHE POUR LA 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 75).
- Modification du Serveur d'administration (cf. section "Modification du Serveur d'administration pour les postes clients" à la page 73).
- Administration du poste client (cf. section "Démarrage, arrêt et redémarrage à distance des postes clients" à la page 74).
- Vérification des mises à jour (cf. section "Analyse des mises à jour récupérées" à la page 99).
- 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 une sélection d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
2. Lancez le processus de création de la tâche par 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 avec 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 **Planification**.
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.

Finalement, le système d'exploitation se 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 **Planification**.
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 **Planification**.
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.

Finalement, 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 sélections 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**.

Finalement, la tâche ajoutée s'affiche dans la liste des tâches.

Si dans la liste sélectionnée, une tâche avec le nom, similaire à la tâche importée, existe déjà, le suffixe numérique **(1)** 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.

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**.

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

Finalement 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 d'exécution des tâches de groupe, des tâches pour les ensembles d'ordinateurs et des tâches du Serveur d'administration. La consultation des résultats d'exécution des tâches locales n'est pas disponible.

- *Pour consulter les résultats d'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 d'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 d'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 ouverte **Appliquer le filtre**, 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.

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 qui inclut 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 à l'aide du double click de la souris sur le nom de l'application ou à l'aide du bouton **Propriétés**.

Finalement, la fenêtre des paramètres locaux de l'application sélectionnée s'ouvrira. 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 le travail avec les 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 pour le poste client ;
  - la synchronisation des stratégies, des paramètres de l'application, 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 dans le cas, où le contrôle d'état des applications est requis, et que le Serveur d'administration ne peut pas initier la connexion avec le 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.

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>] 1 [-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**.

Finalement 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 d'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>] 1 [-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 dossier joint 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**.

   Finalement, l'Assistant d'ajout des postes clients sera démarré. Suivez ses instructions et définissez le mode d'ajout des postes clients au groupe et composez la liste des ordinateurs appartenant au groupe.

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 aussi possible d'ajouter dans le groupe d'administration sélectionné le poste client, détecté dans le réseau du Serveur d'administration, 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, sous lequel les postes clients se trouvent, 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 61).
   - 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 62).

   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.

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 par 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 61).
   - 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 62).

   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 par 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 61).
   - 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 62).

   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**.

   Finalement, la fenêtre principale de l'utilitaire de diagnostic à distance s'ouvrira.
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**.

Finalement, la fenêtre de diagnostic à distance du poste client s'ouvrira (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.

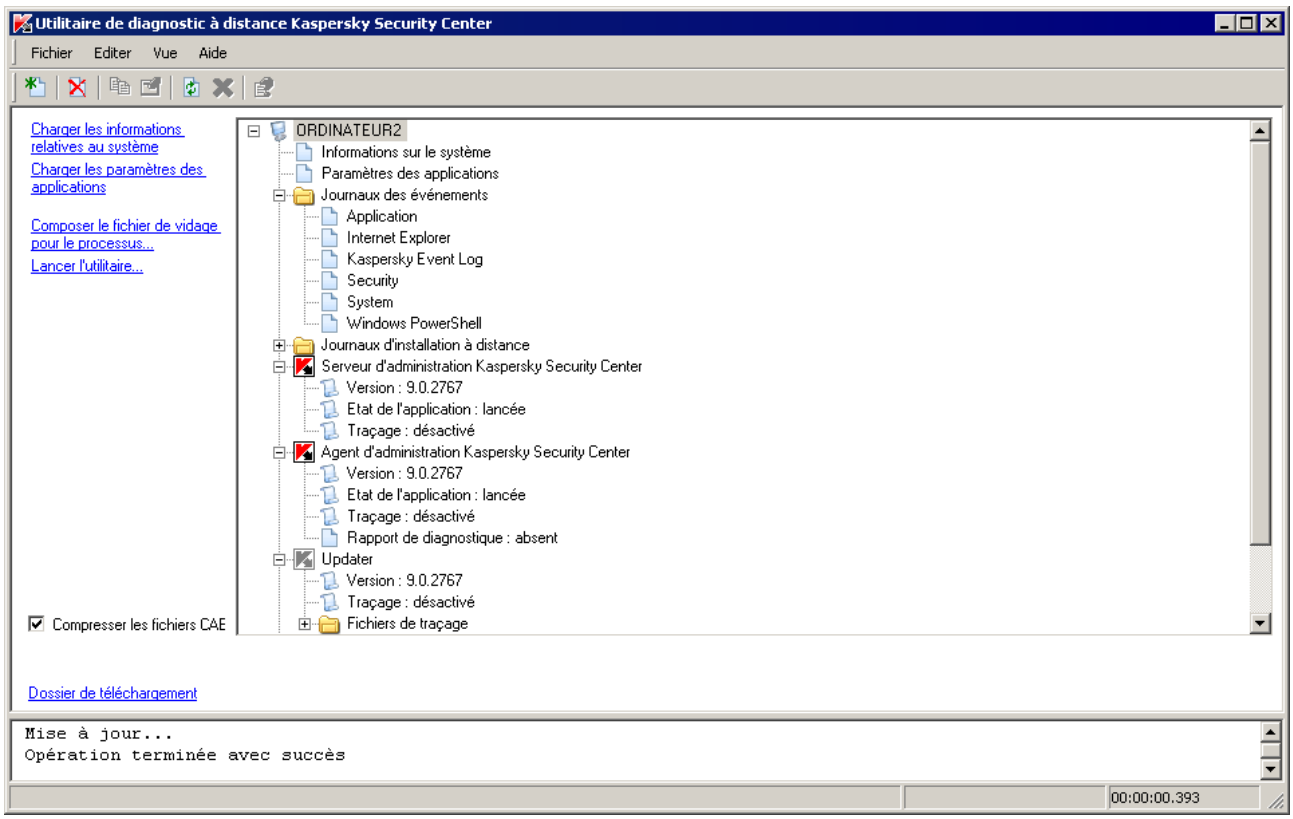


Illustration 15. Utilitaire de diagnostic à distance. Fenêtre de diagnostic à distance du poste client

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.

     Finalement, 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**.

   Finalement, 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.

MANIPULATION AVEC LES RAPPORTS, LES STATISTIQUES ET LES NOTIFICATIONS

Cette section reprend les informations sur le fonctionnement avec les rapports et les statistiques 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 antivirus. Les rapports se forment sur la base des informations enregistrées sur le Serveur d'administration. Vous pouvez créer les rapports pour les objets suivants :

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

L'application propose une sélection 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,

Dans l'arborescence de la console, sélectionnez 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**.

Finalement, l'Assistant de création d'un modèle du rapport se lancera. 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 du rapport qui vous intéresse dans l'arborescence de la console.

   Finalement, 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 d'ordinateurs ;
- diagramme illustrant les données générales du rapport ;
- tableau récapitulatif avec les données illustrant les indices calculés ;
- tableau avec les données détaillées.

SAUVEGARDE 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. Dans l'arborescence de la console, sélectionnez le modèle du rapport selon lequel le rapport nécessaire a été formé.
3. Dans le menu contextuel du modèle sélectionné du rapport, sélectionnez l'option **Enregistrer**.

Finalement, l'Assistant d'enregistrement du rapport se lancera. 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 de diffusion 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 de diffusion d'un rapport, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Rapports et notifications** sélectionnez une règle de ce rapport.
2. Dans le menu contextuel du modèle du rapport, sélectionnez l'option **Envoi des rapports**.

Finalement, l'Assistant de création de la tâche de diffusion 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 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 créée de diffusion du rapport s'affiche dans le dossier de l'arborescence de la console **Tâches du Serveur d'administration**.

La tâche de diffusion 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 antivirus 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 volets d'informations affichant les données statistiques. Les données statistiques sont présentées sur les volets d'informations sous forme de tableaux ou de diagrammes camemberts ou colonnes. Les données dans les volets 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 volets d'informations sur chaque page, ainsi que le mode d'affichage des données dans les volets 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 du volet d'informations.

-  – situé à droite du nom du volet d'informations. Le roulement du volet d'informations.
-  – situé à droite du nom du volet d'informations. Le déploiement du volet 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 une possibilité de configurer les paramètres de notification de l'administrateur sur les événements sur les postes clients et de sélectionner le mode de notification :

- Courrier électronique.
- NET SEND.
- Fichier exécutable.

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

1. 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 **Notifications** de la fenêtre des propriétés du dossier **Rapports et notifications**, configurez les paramètres des notifications sur les événements.

Finalement, les paramètres configurés de notification se diffusent 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 se réalise 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 49

EXTRACTION DES EVENEMENTS ET DES ORDINATEURS

Cette section reprend les informations sur le fonctionnement avec les extractions des événements dans le fonctionnement de Kaspersky Security Center et des applications administrées, ainsi que sur le fonctionnement avec les extractions des postes clients.

DANS CETTE SECTION

REQUETES D'ORDINATEURS

Les informations relatives à l'état des postes clients sont reprises dans un dossier de l'arborescence de la console : **Requêtes d'événements et d'ordinateurs** dans le dossier joint **Requêtes d'ordinateurs**.

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

DANS CETTE SECTION

AFFICHAGE D'UNE REQUETE D'ORDINATEURS

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

1. Dans l'arborescence de la console du dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.

2. Ouvrez une requête d'ordinateurs à l'aide d'un des modes suivants :

   - Ouvrez le dossier **Requêtes d'ordinateurs** et sélectionnez le dossier avec la requête d'ordinateur nécessaire.

   - Dans la zone de travail du dossier **Requêtes d'ordinateurs** dans le groupe **Requêtes prédéfinies** à l'aide du lien correspondant au nom de la requête d'ordinateurs nécessaire.

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

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 REQUETE D'ORDINATEURS

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

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.

2. Ouvrez la fenêtre de la requête d'ordinateurs nécessaire dans le dossier **Requêtes d'ordinateurs**.

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

   - Dans le menu contextuel de la requête, sélectionnez l'option **Propriétés**.

   - A l'aide du lien **Propriété de la requête** dans le groupe d'administration de la requête d'ordinateurs.

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

CREATION D'UNE REQUETE D'ORDINATEURS

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

1. Dans l'arborescence de la console du dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.

2. Lancez le processus de création d'une requête d'ordinateurs par un des moyens suivants :

   - Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Nouvelle requête**.

   - A l'aide du lien **Créer une requête** dans la zone de travail du dossier **Requêtes d'ordinateurs**.

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

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

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

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

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

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.
2. Ouvrez la fenêtre de la requête d'ordinateurs nécessaire dans le dossier **Requêtes 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 requête et le chemin d'enregistrement du fichier.

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

Créer une requête d'ordinateurs selon les paramètres importés :

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.
2. Créer une requête 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 requête 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 requête. Cliquez sur **Ouvrir**.

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

Si dans le dossier **Requêtes d'ordinateurs** une requête avec le nom **Nouvelle requête** existe déjà, le suffixe numérique **(1)** sera ajouté au nom de la requête créée.

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

Lors du travail avec la requête 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 dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Requêtes d'ordinateurs**.
2. Ouvrez la fenêtre de la requête d'ordinateurs nécessaire dans le dossier **Requêtes 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.

REQUETES D'EVENEMENTS

Les informations sur les événements dans 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 **Requêtes d'événements et d'ordinateurs** dans le dossier joint **Evénements**.

Les informations dans le dossier **Evénements** sont présentées sous forme des requêtes dont chaque requête inclut les événements qui répondent aux conditions particulières. Une fois que l'application a été installée, le dossier contient diverses requêtes standards. Vous pouvez créer des requêtes 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 requête d'événements, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Evénements**.

2. Ouvrez une requête d'événements à l'aide d'un des modes suivants :

   - Ouvrez le dossier **Evénements** et sélectionnez le dossier avec la requête d'événements nécessaire.

   - Dans la zone de travail du dossier **Evénements**, dans le groupe **Sélection prédéfinie**, à l'aide du lien correspondant au nom de la requête d'événements nécessaires.

Finalement, la zone de travail représentera la liste des événements de type sélectionné qui sont 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 requête d'événements, procédez comme suit :

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

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

CREATION D'UNE REQUETE D'EVENEMENTS

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

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Evénements**.
2. Lancez le processus de création d'une requête d'événements par un des moyens suivants :
   - Dans le menu contextuel du dossier, sélectionnez l'option **Créer** → **Nouvelle requête**.
   - A l'aide du lien **Créer une requête** dans la zone de travail du dossier **Evénements**.
3. Dans la fenêtre ouverte **Nouvelle requête d'événements**, indiquez le nom de la requête 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 requête d'événements créée contient tous les événements enregistrés sur le Serveur d'administration. Pour que la requête d'événements affiche uniquement les événements qui vous intéressent, il faut configurer les paramètres de requête.

EXPORTATION D'UNE REQUETE DANS LE FICHIER TEXTE

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

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Evénements**.
2. Ouvrez la fenêtre de la requête d'ordinateurs nécessaire dans le dossier **Evénements**.
3. Lancez le processus d'exportation d'une requête d'événements par 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 requête d'événements.

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

SUPPRESSION DES EVENEMENTS DEPUIS LA REQUETE

Pour supprimer un événement, procédez comme suite :

1. Dans l'arborescence de la console dans le dossier **Requêtes d'événements et d'ordinateurs**, sélectionnez le dossier joint **Evénements**.

2. Ouvrez la fenêtre de la requête 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 par 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 requête.

   - 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**.

ORDINATEURS NON DEFINIS

Cette section reprend les informations sur le travail avec les 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 dossier joint parmi les dossiers joints 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 dossier joint 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 requêtes 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 requêtes.

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 dossier joint **Domaines**.
2. La fenêtre **Propriétés : Domaines** s'ouvrira 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'ouvrira. 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 dossier joint **Active Directory**.
2. La fenêtre **Propriétés : Active Directory** s'ouvrira 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 : Active Directory** s'ouvrira. 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'ouvrira 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 : Plages IP** s'ouvrira. 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 dossier joint **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**.

   Finalement, la fenêtre **Propriété : <Nom du domaine>** s'ouvrira. 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 dossier joint **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.

Finalement, 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 dossier joint **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**.

Finalement, la fenêtre **Propriétés : <Nom de la plage IP>**s'ouvrira. 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 dossier joint **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**.

Finalement, la fenêtre **Propriété : <Nom du groupe Active Directory>** s'ouvrira. Cette fenêtre permet de configurer les paramètres du groupe Active Directory sélectionné.

CREATION DES REGLES DE DEPLACEMENT AUTOMATIQUE DES ORDINATEURS DANS LE 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 le déplacement automatique des ordinateurs dans le 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'ouvrira. Configurez la règle de déplacement automatique des ordinateurs dans le groupe d'administration dans la section **Déplacement des ordinateurs**.

APPLICATIONS ET VULNERABILITES

Cette section décrit le travail avec les applications et les vulnérabilités que Kaspersky Security Center découvre sur les postes clients.

Kaspersky Security Center permet de suivre le registre des applications et des fichiers exécutables sur les postes clients, consulter et installer les mises à jour Windows Update, ainsi que d'éliminer les vulnérabilités détectées sur les postes clients. Outre cela, Kaspersky Security Center permet de créer les catégories des applications selon les critères sélectionnés.

Les informations sur les applications, les fichiers exécutables, les mises à jour Windows Update et les vulnérabilités détectées sur les postes clients se trouvent dans le dossier de l'arborescence de la console **Applications et vulnérabilités**.

DANS CETTE SECTION

REGISTRE DES APPLICATIONS

Le dossier **Registre des applications** qui fait partie du dossier **Applications et vulnérabilités** contient la liste des applications que l'Agent d'administration a détectées sur les postes clients sur lesquels il est installé.

La fonctionnalité du recueil d'information sur les applications installées est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

En ouvrant la liste des propriétés de l'application, sélectionnées dans la zone de travail du dossier **Registre des applications**, vous pouvez recevoir des informations générales sur l'application et des informations sur les fichiers exécutables de l'application, ainsi que consulter la liste des ordinateurs sur lesquels l'application a été installée.

Pour consulter les données sur les applications qui satisfont les critères définis, vous pouvez utiliser le filtre, en sélectionnant l'option **Filtre** dans le menu contextuel de la liste 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.

FICHIERS EXECUTABLES

La dossier **Fichiers exécutables** qui fait partie du dossier **Applications et vulnérabilités** contient la liste des fichiers exécutables qui ont été lancés sur les postes clients ou ont été détectés pendant le processus de fonctionnement de la tâche d'inventaire de Kaspersky Endpoint Security.

En ouvrant la fenêtre des propriétés du fichier exécutable sélectionné dans la zone de travail du dossier **Fichiers exécutables**, vous pouvez recevoir les informations sur le fichier exécutable, ainsi que consulter la liste des ordinateurs sur lesquels il est présent.

Pour consulter les données sur les fichiers exécutables qui satisfont les critères définis, vous pouvez utiliser le filtre, en sélectionnant l'option **Filtre** dans le menu contextuel de la liste des fichiers exécutables.

MISES A JOUR WINDOWS UPDATE

Le dossier **Mises à jour Windows Update** qui fait partie du dossier **Applications et vulnérabilités** contient la liste des mises à jour, reçues par le Serveur d'administration, des applications Microsoft Windows qui peuvent être diffusées sur les postes clients.

En ouvrant la fenêtre des propriétés de la mise à jour sélectionnée dans la zone de travail du dossier **Mises à jour Windows Update**, vous pouvez consulter les informations sur la mise à jour, la liste des postes clients pour lesquels la mise à jour est conçue (*ordinateurs ciblés*), ainsi que les informations sur les vulnérabilités à éliminer dans les applications à l'aide de cette mise à jour.

Vous pouvez lancer l'installation à distance des mises à jour, sélectionnées dans la liste, sur les ordinateurs ciblés à l'aide d'un des moyens suivants :

- en sélectionnant l'option **Installer la mise à jour** dans le menu contextuel des mises à jour marquées ;
- à l'aide du lien **Installer la mise à jour** dans le groupe de travail avec les mises à jour marquées.

CATEGORIES DES APPLICATIONS. ADMINISTRATION DU LANCEMENT DES APPLICATIONS

Dans le dossier **Catégories des applications** qui fait partie du dossier **Applications et vulnérabilités**, vous pouvez créer les catégories des applications pour gérer le lancement de ces applications sur les postes clients avec Kaspersky Endpoint Security 8.0 for Windows installé.

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. Manuels de Kaspersky Endpoint Security 8.0 for Windows). La gestion du lancement des applications en mode "Tout ce qui n'est pas autorisé est interdit" signifie que le lancement uniquement des applications, qui font partie de la catégorie indiquée, sera autorisé sur les postes clients.

Vous pouvez créer la catégorie des applications par un des moyens suivants :

- en sélectionnant dans le menu contextuel du dossier **Catégories des applications** ou de la liste des catégories l'option **Créer** → **Catégorie** ;
- à l'aide du lien **Créer une catégorie** dans le groupe d'administration de la liste des catégories.

Finalement, l'Assistant de création de la catégorie d'utilisateur se lancera. Suivez les instructions de l'Assistant.

➧ *Pour configurer la gestion du lancement des applications sur les postes clients sélectionnés, procédez comme suit :*

1. Créez des catégories nécessaires des applications dans le dossier **Catégories des applications** dans l'arborescence de la console.

2. Créez une règle de contrôle du lancement des applications pour le groupe sélectionné des postes clients dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security 8.0 for Windows, dans la section **Contrôle du lancement des applications**. Testez les règles créées.

3. Activez les règles créées du contrôle du lancement des applications.

Pour plus d'informations sur les catégories des applications recommandées de créer, ainsi que sur la configuration de gestion du lancement des applications, cf. Manuels de Kaspersky Endpoint Security 8.0 for Windows.

VULNERABILITES DANS LES APPLICATIONS

Le dossier **Vulnérabilités dans les applications** qui fait partie du dossier **Applications et vulnérabilités** contient la liste des vulnérabilités dans les applications que l'Agent d'administration a détectées sur les postes clients sur lesquels il est installé.

La fonctionnalité du recueil d'information sur les vulnérabilités dans les applications est prise en charge uniquement pour les systèmes d'exploitation Microsoft Windows.

En ouvrant la fenêtre des propriétés de l'application sélectionnée dans le dossier **Vulnérabilités dans les applications**, vous pouvez recevoir les informations générales sur la vulnérabilité, sur l'application dans laquelle la vulnérabilité a été détectée, consulter la liste des ordinateurs sur lesquels la vulnérabilité a été détectée, ainsi que les informations sur la fermeture de la vulnérabilité.

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 antivirus, 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 dans le cas 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. Sélectionnez le dossier **Tâches du Serveur d'administration** dans l'arborescence de la console.
2. Lancez le processus de création de la tâche par 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.

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 le groupe de fonctionnement avec la tâche sélectionnée.

Finalement, la fenêtre des propriétés de la tâche **Téléchargement des mises à jour dans le stockage** s'ouvrira. 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 le groupe de fonctionnement avec 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 déjà formée de vérification des mises à jour.

   - Cliquez sur le bouton **Créer** pour créer une tâche de vérification des mises à jour.

     Finalement, l'Assistant de création des tâches de vérification des mises à jour s'ouvrira. Suivez les instructions de l'Assistant.

Vous pouvez créer une tâche de vérification des mises à jour pour le groupe d'administration sélectionné ou pour l'ensemble d'ordinateurs. Les ordinateurs, sur lesquels la tâche de vérification des mises à jour se réalise, s'appellent les *ordinateurs d'essai*.

En tant que les ordinateurs d'essai, il est recommandé d'utiliser les 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 découverte de virus sur les ordinateurs d'essai, la tâche de vérification des mises à jour est considérée comme ratée).

4. Fermez la fenêtre des propriétés de la tâche de téléchargement des mises à jour dans le stockage, en cliquant sur le bouton **OK**.

Finalement, dans le cadre d'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 répertoire 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 répertoire 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 référentiel** ne sont pas lancées. Ces opérations sont réalisées à l'exécution suivante de la tâche de téléchargement des mises à jour dans le référentiel, si la vérification du nouvel ensemble des mises à jour donne un résultat positif.

L'ensemble de mises à jour est considéré comme incorrect si sur au moins un ordinateur d'essai une des conditions suivantes est exécutée :

- 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 a changé ;
- un objet infecté a été identifié durant l'analyse à la demande ;
- une erreur de fonctionnement de l'application de Kaspersky Lab s'est produite.

Si aucune des conditions citées ne s'est manifestée sur aucun des ordinateurs de test, 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 dossier joint **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 par 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 61).
   - 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 62).

   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 **Planification** dans le champ **Planification**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage**.

Finalement, 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 **Planification**, il faut sélectionner l'option de lancement **Lors du téléchargement des mises à jour dans le stockage** dans le champ **Planification 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 par 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 de fonctionnement avec 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'APPLICATIONS 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 par 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 de fonctionnement avec 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 directement après la fin de la tâche de récupération des mises à jour par le Serveur d'administration.

     Si la case n'est pas sélectionnée, 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 de l'Agent d'administration, quand elles sont récupérées, sont installées directement après la fin de la tâche de récupération des mises à jour par le Serveur d'administration.

     Si la case n'est pas sélectionnée, les mises à jour pourront être installées manuellement seulement.

     Par défaut la case est cochée.

Immédiatement 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 dossier **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 récupération des mises à jour par 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 le travail avec les 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 paramètres de la clé sont enregistrés 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 paramètres 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**, sélectionnez le dossier joint **Clés**.

Finalement, 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 dans le dossier **Stockages**, sélectionnez le dossier joint **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.

Finalement 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 dans le dossier **Stockages**, sélectionnez le dossier joint **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.

Finalement, l'Assistant de création de la tâche de diffusion de la clé sera 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 sélections 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. Dans l'arborescence de la console **Stockages**, σ⌠λεχτιοννεζ λε δοσσιερ φοιντ **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.

Finalement, 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 paramètres de la clé, est tenue en compte. Si la restriction est dépassée, la clé n'est pas diffusée sur le poste client.

CREATION ET CONSULTATION DU RAPPORT D'UTILISATION DES CLES

- *Pour créer le 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.

Finalement, la zone de travail du rapport d'utilisation des clés affichera les informations sur les clés actives et complémentaires utilisées sur les postes clients. La 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 paquets d'installation qui sont utilisés pour l'installation à distance des applications sur les postes clients ;
- 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 101) ;
- les clés détectées sur les postes clients (cf. section "Travail avec les clés des applications" à la page 106) ;
- 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 dans le dossier **Stockages**, sélectionnez le dossier joint du stockage nécessaire.
2. Dans le menu contextuel de la liste des objets du stockage, sélectionnez l'option **Exporter la liste**.

   Finalement, la fenêtre **Exporter de la liste** s'ouvrira. 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 permet d'installer à distance sur les postes clients les applications Kaspersky Lab et les applications d'autres fabricants.

Afin d'installer une application par les moyens de Kaspersky Security Center, il est nécessaire de créer un paquet d'installation pour cette application. *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.

La liste des paquets d'installation créés se trouvent dans le dossier de l'arborescence de la console **Stockages**, du dossier joint **Paquets d'installation**.

Pour plus d'informations sur le fonctionnement avec les 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 découverte.

Dossier de sauvegarde est conçu pour enregistrer les copies de réserve 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 8 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 dossier joint **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 dossier joint **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 depuis 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 dossier joint **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 dossier joint **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 dans le dossier **Stockages**, sélectionnez le dossier joint **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 du lien **Analyse le fichier en quarantaine**.

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 UN TRAITEMENT DIFFERE

Les informations sur les fichiers avec un traitement différé, détectés sur les postes clients, se trouvent dans le dossier **Stockages**, dans le dossier joint **Fichiers avec un 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 UN TRAITEMENT DIFFERE

Pour lancer la réparation du fichier avec un traitement différé, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le dossier joint **Fichiers avec un traitement différé**.
2. Dans la zone de travail du dossier **Fichiers avec un 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 UN TRAITEMENT DIFFERE SUR LE DISQUE

Kaspersky Security Center permet d'enregistrer les copies des fichiers sur les postes clients avec un 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 avec un traitement différé sur le disque, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le dossier joint **Fichiers avec un traitement différé**.
2. Dans la zone de travail du dossier **Fichiers avec un 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 avec un 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 avec un traitement différé**, procédez comme suit :*

1. Dans l'arborescence de la console dans le dossier **Stockages**, sélectionnez le dossier joint **Fichiers avec un traitement différé**.

2. Dans la zone de travail du dossier **Fichiers avec un 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 avec un traitement différé**.

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

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

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

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

Formulaire de soumission de demande du Support Technique

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

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

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

Si vous n'êtes pas un utilisateur enregistré des applications de Kaspersky Lab, remplissez le formulaire d'enregistrement (https://support.kaspersky.com/ru/personalcabinet?LANG=fr). Lors de l'enregistrement, indiquez *le code d'activation* de l'application ou *le fichier de licence*.

L'opérateur du service du Support Technique vous enverra sa réponse dans votre Espace personnel (https://support.kaspersky.com/ru/personalcabinet?LANG=fr) ainsi qu'à l'adresse électronique que vous avez indiquée dans votre demande.

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

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

Support Technique par téléphone

Si le problème est urgent, vous pouvez toujours appeler le Support Technique local de Kaspersky Lab. Avant de contacter les experts du Support Technique, veuillez fournir les informations (http://support.kaspersky.com/support/details) concernant votre ordinateur. Ceci aidera nos experts à vous venir en aide le plus rapidement possible.

GLOSSAIRE

A

Administrateur de Kaspersky Security Center

Personne qui gère les travaux du programme grâce à un système d'administration centralisé à distance de Kaspersky Security Center.

Administration centralisee de l'application

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

Administration directe de l'application

Administration de l'application par l'interface locale.

Agent d'administration

Composant de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant est 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 des mises a jour

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

Application incompatible

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui n'est pas compatible avec l'administration par Kaspersky Security Center.

B

Bases

Bases de données créées par les experts de Kaspersky Lab et qui contiennent une description détaillée de toutes les menaces connues à l'heure actuelle contre la sécurité informatique, ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces surgissent.

C

Certificat du Serveur d'administration

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

Client du Serveur d'administration (poste client)

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

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

CLE COMPLEMENTAIRE

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

CONSOLE D'ADMINISTRATION KASPERSKY

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

D

DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement enregistré durant le fonctionnement de l'application de Kaspersky Lab. Il existe quatre niveaux de gravité :

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

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

DOSSIER DE SAUVEGARDE

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

DUREE DE VALIDITE DE LA LICENCE

Période durant laquelle vous pouvez utiliser l'ensemble des fonctions de l'application de Kaspersky Lab. En règle générale, la licence est valide pendant une année calendaire à partir de la date de son installation. Une fois la durée de la licence écoulée, l'application n'est plus opérationnelle : vous ne pourrez plus actualiser les bases de l'application.

E

ETAT DE PROTECTION

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

F

FICHIER DE LICENCE

Fichier possédant l'extension key qui constitue votre "clé" personnelle indispensable à l'utilisation de l'application de Kaspersky Lab. Le fichier de licence est livré avec le logiciel si vous avez acheté ce dernier chez un revendeur de Kaspersky Lab. Il est envoyé par courrier électronique si vous avez acheté le logiciel en ligne.

G

GROUPE D'ADMINISTRATION

Sélection 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 se trouver à l'intérieur d'autres groupes. Il est possible de créer dans le groupe les stratégies de groupe pour chacune des applications installées et chacune des tâches de groupe créées.

I

INSTALLATION FORCEE

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

INSTALLATION A DISTANCE

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

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

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

K

KASPERSKY SECURITY 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 des nouveaux types de menaces, augmente l'efficacité de fonctionnement de certains composants de la protection, ainsi que diminue la possibilité des faux positifs.

L

LISTE NOIRE DES FICHIERS CLES

Base de données qui contient les informations sur les fichiers clés bloqués par Kaspersky Lab. Le contenu du fichier avec la liste noire est actualisé avec les bases.

M

MISE A JOUR

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

MISE A JOUR DISPONIBLE

Paquet des mises à jour des modules de l'application Kaspersky Lab qui contient les mises à jour urgentes recueillies au cours d'un intervalle de temps et les modifications dans l'architecture de l'application.

P

PAQUET D'INSTALLATION

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

PARAMETRES DE L'APPLICATION

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

PARAMETRES DE LA TACHE

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

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

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

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

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

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

R

RESTAURATION

Transfert de l'objet original depuis la quarantaine ou du dossier de sauvegarde vers l'emplacement, où se trouvait l'objet avant qu'il ne soit placé en quarantaine, supprimé ou réparé, ou vers tout autre emplacement désigné 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

SAUVEGARDE

Création d'une copie de sauvegarde d'un fichier avant sa suppression ou la réparation et placement de cette copie dans le dossier de sauvegarde avec la possibilité de le restaurer ultérieurement, par exemple en vue de l'analyser à l'aide des bases actualisées.

SAUVEGARDE DES DONNEES DU SERVEUR D'ADMINISTRATION

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

- la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;

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

SERVEUR D'ADMINISTRATION

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

SERVEUR D'ADMINISTRATION SECONDAIRE

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 Serveur d'administration secondaire peut être le Serveur virtuel. Par rapport aux Serveurs d'administration secondaires physiques, les possibilités des Serveurs d'administration virtuels sont partiellement limitées.

SERVEUR D'ADMINISTRATION VIRTUEL

(ci-après Serveur virtuel) Le composant 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.

SERVEURS DE MISE A JOUR KASPERSKY LAB

Liste des serveurs HTTP et FTP de Kaspersky Lab depuis lesquels l'application copie les bases et les mises à jour des modules sur votre ordinateur.

SEUIL DE L'ACTIVITE DU VIRUS

Nombre maximum d'événements d'un certain type admis au cours d'un intervalle déterminé, dont le dépassement sera considéré comme une augmentation de l'activité du virus et l'apparition de la menace d'attaque de virus. Ces données peuvent être utiles en période d'épidémie et permettent à l'administrateur de réagir opportunément à la menace d'une attaque de virus.

STOCKAGE DES COPIES DE SAUVEGARDE

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

STRATEGIE

Sélection des paramètres de fonctionnement de l'application dans le groupe d'administration en cas d'administration à l'aide de Kaspersky Security Center. Les paramètres de fonctionnement de l'application peuvent varier en fonction des

groupes. Une stratégie propre à chaque application peut être définie. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

T

TACHE

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

TACHE DE GROUPE

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

TACHE LOCALE

Tâche définie et exécutée sur un poste client particulier.

TACHE POUR UNE SELECTION D'ORDINATEURS

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

U

UTILISATEUR DE KASPERSKY SECURITY CENTER

Utilisateur qui est responsable de l'état et du fonctionnement du système de protection administré à l'aide de Kaspersky Security Center.

KASPERSKY LAB

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 propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et 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 actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (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.fr
Encyclopédie de 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 – la marque Cisco Systems, Inc. déposée aux Etats-Unis et aux autres pays, et/ou ses compagnies affiliées.

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

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

Mac, Mac OS – les marques déposées Apple Inc.

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

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

INDEX

A

C

E

G

I

K

M

N

P

R

S

T