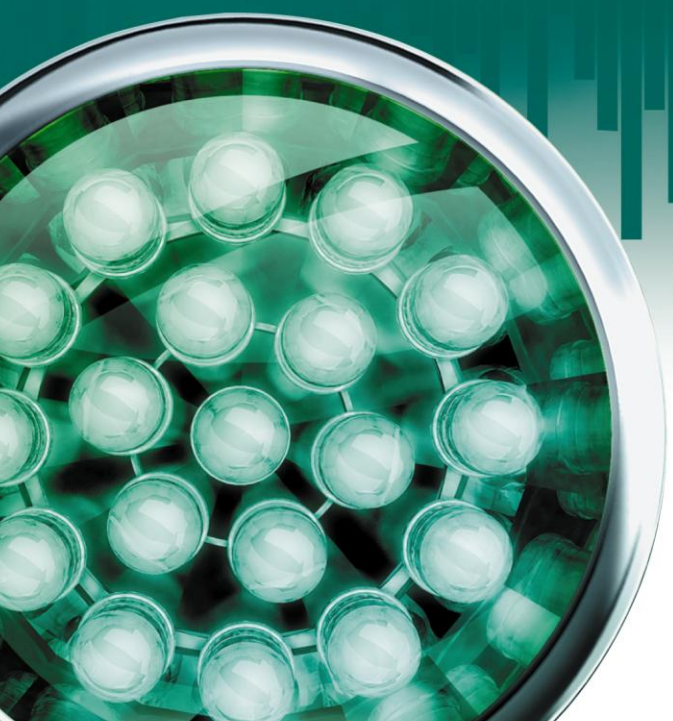
Kaspersky Administration Kit 8.0

MANUEL D'ADMINISTRATEUR

VERSION DU LOGICIEL : 8.0



KASPERSKY lab

Cher utilisateur !

Merci d'avoir choisi notre produit. On espère que cette documentation vous aidera dans votre travail et répondra à plusieurs questions qui vous intéressent.

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

Date d'édition : 14/09/09

http://www.kaspersky.fr
http://enterprise.kaspersky.fr

CONTENU

KASPERSKY ADMINISTRATION KIT

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

Kaspersky Administration Kit est un outil pour les administrateurs de réseaux d'entreprise et pour les responsables de la sécurité antivirus.

DANS CETTE SECTION

DISTRIBUTION

Le logiciel 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).

SERVICES POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab, Ltd. propose à ses utilisateurs enregistrés un large éventail de services qui leur permettent de profiter au maximum de leur Produits.

Lorsque vous achetez une licence pour un des logiciels de Kaspersky Lab appartenant à la suite Kaspersky Open Space Security, vous devenez un utilisateur enregistré de Kaspersky Administration Kit. Vous bénéficierez des services suivants pendant la durée de validité de la licence :

- mise à jour toutes les heures des bases de l'application et mise à jour gratuite vers les nouvelles versions ;
- accès à la Base de connaissances sur l'installation, la configuration et la prise en main du logiciel, ainsi qu'au support téléphonique ou e-mail ;

> Lors de tout contact avec le service du Support Technique, renseignez les informations relatives à la licence des Produits de Kaspersky Lab que vous administrez avec l'Administration Kit.

- notification sur la sortie des nouvelles versions des Produits Kaspersky Lab ainsi que l'actualité sur les nouveaux virus. Ce service est offert aux utilisateurs abonnés à la lettre d'informations de Kaspersky Lab sur le site du service du Support Technique (http://support.kaspersky.com/fr/subscribe).

Aucun support sur le fonctionnement et l'utilisation des systèmes d'exploitation ne sera dispensé par le Support Technique.

OBTENTION DE L'INFORMATION SUR L'APPLICATION

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

Kaspersky Lab propose 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 (Base de connaissances) ;
- système d'aide électronique ;
- documentation.

Page sur le site Web de Kaspersky Lab

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

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 l'application. Ils sont regroupés par thèmes tels que "Administration des licences", "Configuration des mises à jour des bases" ou "Résolution des problèmes". Les articles peuvent répondre à des questions qui concernent non seulement cette application mais également d'autres logiciels de Kaspersky Lab ainsi que contenir des nouvelles du 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 d'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, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse, ou sur la touche **<F1>** du clavier.

Documentation

La documentation qui accompagne l'application contient la majorité des informations indispensables à l'utilisation de celle-ci. Elle contient les éléments suivants :

- **Manuel de l'administrateur** décrit le but, les notions principales, les fonctions et le mode de fonctionnement général de Kaspersky Administration Kit.
- **Manuel de déploiement** décrit l'installation des composants de Kaspersky Administration Kit, ainsi que l'installation à distance des applications dans un réseau informatique de configuration simple.
- **Début du fonctionnement** contient une description des étapes qui permettront à l'administrateur de la sécurité antivirus de l'entreprise de commencer à utiliser rapidement Kaspersky Administration Kit et de déployer la protection antivirus dans tout le réseau sur la base des applications de Kaspersky Lab.
- **Manuel de référence** contient une description du rôle de Kaspersky Administration Kit et une description pas à pas de ses fonctions.

Ces documents sont au format PDF et sont livrés avec Kaspersky Administration Kit (cédérom d'installation).

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

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

Vous pouvez obtenir des informations sur nos produits auprès des experts du service du Support Technique par téléphone ou via Internet. Lors de tout contact avec le service du Support Technique, renseignez les informations relatives à la licence du produit Kaspersky Lab que vous utilisez.

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 le malware ainsi que ses conséquences associées.

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 service d'assistance 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.

Support Technique par téléphone

Si le problème est urgent, vous pouvez toujours appeler le Support Technique de votre Partenaire/Revendeur Kaspersky Lab, ou encore si vous disposez d'un Contrat de Support Kaspersky (http://support.kaspersky.com/fr/support/details), référez-vous aux coordonnées indiquées sur celui-ci. Vous pouvez aussi joindre notre Support International Kaspersky Lab (http://support.kaspersky.com/support/international) ou Support Kaspersky Lab en langue russe (http://support.kaspersky.ru). Ceci aidera nos experts à vous venir en aide le plus vite possible.

FORUM SUR LES APPLICATIONS KASPERSKY LAB

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

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

FONCTION DU DOCUMENT

Ce manuel contient la description des notions principales et des fonctions de Kaspersky Administration Kit, ainsi que le mode de son fonctionnement général. Le manuel d'aide de Kaspersky Administration Kit contient la description pas à pas de ses fonctions. Les fonctions, décrites dans le manuel d'aide, sont indiquées dans le texte par les soulignements.

POSSIBILITES DE L'APPLICATION

Les possibilités offertes par l'application à l'administrateur sont les suivantes :

- Installation et suppression centralisée à distance des applications de Kaspersky Lab sur les postes du réseau. Cette fonction permet à l'administrateur de copier les distributions d'applications Kaspersky Lab nécessaires dans un ordinateur prédéfini puis de les déployer sur d'autres à travers le réseau.

- Administration centralisée à distance des applications de Kaspersky Lab. L'administrateur peut créer un système de protection antivirus à plusieurs niveaux et gérer toutes les applications à partir d'un même poste de travail administratif. Cette particularité est particulièrement importante dans le cas de sociétés de grande taille utilisant un réseau local avec de nombreux postes répartis dans plusieurs bâtiments ou bureaux séparés. Cette caractéristique permet à l'administrateur de :

  - créer une hiérarchie des Serveurs d'administration ;

  - grouper les postes en tant que groupes d'administration, en fonction de leurs prestations et du nombre d'applications qui y sont installées ;

  - configurer les applications de manière centralisée en créant et en appliquant des stratégies ;

  - configurer des paramètres isolés de l'application dans le cas de postes séparés, à l'aide des paramètres de l'application ;

  - administrer de façon centralisée le fonctionnement de l'application grâce à la création et au lancement de tâches de groupe et de tâches pour une sélection d'ordinateur et au Serveur d'administration ;

  - créer des modèles individualisés de fonctionnement d'une application, avec la création et l'exécution de tâches sur plusieurs postes appartenant à différents groupes d'administration.

- Mettre à jour automatiquement la base et les modules de programme sur les ordinateurs. Cette fonction permet d'assurer une mise à jour centralisée de la base de toutes les applications Kaspersky Lab installées, sans avoir à se connecter au serveur de mises à jour de Kaspersky Lab sur Internet pour faire les mises à jour mise individuelles. La mise à jour peut s'effectuer automatiquement conformément à la planification définie par l'administrateur. L'administrateur peut surveiller l'installation des mises à jour sur les postes client.

- Schéma de la réception des rapports. Cette fonction permet de récupérer de manière centralisée des données statistiques sur toutes les applications Kaspersky Lab installées, de surveiller leur bon fonctionnement et de créer des rapports d'après les informations obtenues. L'administrateur peut créer un rapport d'activité d'une application, récapitulatif pour l'ensemble du réseau, ou pour chaque poste où l'application est installée.

- Utiliser le système de notification d'événements. Système d'envoi de notifications par messagerie. Cette fonction permet à l'administrateur de créer une liste des événements liés à l'activité des applications, sur lesquels il

souhaite être informé. La liste de ces événements peut correspondre à la détection d'un nouveau virus, d'une erreur apparue en essayant de mettre à jour la base de l'application sur un ordinateur ou d'un nouvel ordinateur sur le réseau.

- Gestion des licences. Cette fonction permet d'installer des licences pour toutes les applications Kaspersky Lab de manière centralisée, de surveiller le respect du Contrat de licence (c'est à dire, que le nombre de licences correspond au nombre d'applications en cours d'exécution sur le réseau), ainsi que leur date de péremption.

COMPOSITION DE L'APPLICATION

L'application Kaspersky Administration Kit se présente sous forme de trois composants principaux :

- **Serveur d'administration** est un entrepôt centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau local de la société et un outil efficace de gestion de ces applications.

- **Agent d'administration** coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant est unique pour toutes les applications Windows de la ligne de produits Kaspersky Open Space Security. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

- **Console d'administration** fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur et de l'Agent. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console). La Console d'administration permet de se connecter au Serveur d'administration distant via Internet.

CONFIGURATION LOGICIELLE ET MATERIELLE REQUISE

Serveur d'administration

- Configuration logicielle :
  - Microsoft Data Access Components (MDAC) version 2.8 ou suivante.
  - MSDE 2000 avec Service Pack 3, Microsoft SQL Server 2000 avec Service Pack 3 ou suivant, ou MySQL Enterprise version 5.0.32 ou 5.0.70, ou Microsoft SQL 2005 et suivant ; ou Microsoft SQL Express 2005 et suivant, Microsoft SQL Express 2008, Microsoft SQL 2008.

    Il est recommandé d'utiliser Microsoft SQL 2005 avec Service Pack 2, Microsoft SQL Express 2005 avec Service Pack 2 et les versions plus récentes.

  - Microsoft Windows 2000 avec Service Pack 4 ou suivant ; Microsoft Windows XP Professional avec Service Pack 2 ou suivant ; Microsoft Windows XP Professional x64 ou suivant ; Microsoft Windows Server 2003 ou suivant ; Microsoft Windows Server 2003 x64 ou suivant ; Microsoft Windows Vista avec Service Pack 1 ou suivant ; Microsoft Windows Vista x64 avec Service Pack 1 et tous les SP actuels, pour Microsoft Windows Vista x64 Microsoft Windows Installer 4.5 doit être installé ; Microsoft Windows Server 2008 ; Microsoft Windows Server 2008 déployé en mode Server Core ; Microsoft Windows Server 2008 x64 avec Service Pack 1 et tous les SP actuels, pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé ; Microsoft Windows 7.

    Pendant le fonctionnement sous Microsoft Windows 2000 avec Service Pack 4, avant le déploiement du Serveur d'administration il est nécessaire d'installer les mises à jour Microsoft Windows suivantes : 1) ensemble de mises à jour cumulatives 1 pour Windows 2000 SP4 (KB891861) ; 2) mise à jour de la sécurité pour Windows 2000 (KB835732).

- Configuration matérielle :
  - Processeur Intel Pentium III, 800 Mhz minimum ;

- 256 Mo de mémoire vive ;
- 1 Go d'espace disque disponible.

Console d'administration Kaspersky

- Configuration logicielle :
  - Microsoft Windows 2000 avec Service Pack 4 ou suivant ; Microsoft Windows XP Professional avec Service Pack 2 ou suivant ; Microsoft Windows XP Home Edition avec Service Pack 2 ou suivant ; Microsoft Windows XP Professional x64 ou suivant ; Microsoft Windows Server 2003 ou suivant ; Microsoft Windows Server 2003 x64 ou suivant ; Microsoft Windows Vista avec Service Pack 1 ou suivant ; Microsoft Windows Vista x64 avec Service Pack 1et tous les SP actuels, pour Microsoft Windows Vista x64 Microsoft Windows Installer 4.5 doit être installé ; Microsoft Windows Server 2008, 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 7.
  - Microsoft Management Console version 1.2 ou suivante.
  - L'utilisation sous Microsoft Windows 2000 requiert Microsoft Internet Explorer 6.0.
  - L'utilisation sous 7 E Edition et Microsoft Windows 7 N Edition requiert Microsoft Internet Explorer 8.0 ou suivante.
- Configuration matérielle :
  - Processeur Intel Pentium III, 800 Mhz minimum ;
  - 256 Mo de mémoire vive ;
  - 70 Mo d'espace disque disponible.

Agent d'administration

- Configuration logicielle :
  - Pour les systèmes Windows :

    Microsoft Windows 2000 avec Service Pack 4 ou suivant ; Microsoft Windows XP Professional avec Service Pack 2 ou suivant ; Microsoft Windows XP Professional x64 ou suivant ; Microsoft Windows Server 2003 ou suivant ; Microsoft Windows Server 2003 x64 ou suivant ; Microsoft Windows Vista avec Service Pack 1 ou suivant ; Microsoft Windows Vista x64 avec Service Pack 1et tous les SP actuels, pour Microsoft Windows Vista x64 Microsoft Windows Installer 4.5 doit être installé ; 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 7.
  - Pour les systèmes Novell :

    Novell NetWare 6 SP5 ou suivant, Novell NetWare 6.5 SP7 ou suivant.
  - Pour les systèmes Linux :

    La version du système d'exploitation supporté est fixée par l'exigence de l'application compatible de Kaspersky Lab sur le poste client.
- Configuration matérielle :
  - Pour les systèmes Windows :
    - Processeur Intel Pentium, 233 Mhz minimum ;

- 32 Mo de mémoire vive ;
- 20 Mo d'espace disque disponible.

- Pour les systèmes Novell :
  - Processeur Intel Pentium, 233 Mhz minimum ;
  - 32 Mo de mémoire vive ;
  - 32 Mo d'espace disque disponible.
- Pour les systèmes Linux :
  - Processeur Intel Pentium, 133 Mhz minimum ;
  - 64 Mo de mémoire vive ;
  - 100 Mo d'espace disque disponible.

Agent des mises à jour

- Configuration logicielle pour les systèmes Windows :

  Microsoft Windows 2000 avec Service Pack 4 ou suivant ; Microsoft Windows XP Professional avec Service Pack 2 ou suivant ; Microsoft Windows XP Professional x64 ou suivant ; Microsoft Windows Server 2003 ou suivant ; Microsoft Windows Server 2003 x64 ou suivant ; Microsoft Windows Vista avec Service Pack 1 ou suivant ; Microsoft Windows Vista x64 avec Service Pack 1et tous les SP actuels, pour Microsoft Windows Vista x64 Microsoft Windows Installer 4.5 doit être installé ; Microsoft Windows Server 2008, 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 7.

- Configuration matérielle pour les systèmes Windows :
  - Processeur Intel Pentium III, 800 Mhz minimum ;
  - 256 Mo de mémoire vive ;
  - 500 Mo d'espace disque disponible.

NOUVEAUTES

Les modifications apportées dans la version 8.0 de Kaspersky Administration Kit. par rapport à la version 6.0 de Kaspersky Administration Kit :

- Mode d'installation simplifiée.
- Possibilité d'afficher plusieurs comptes dans la tâche d'installation à distance.
- Le fichier de distribution Microsoft SQL Express 2005 fait partie de l'application. L'installation de Microsoft SQL Express 2005 s'effectue automatiquement dans le cas de sélection de l'installation standard.
- Ajout de la possibilité de la surveillance SNMP des paramètres généraux de la protection antivirus du réseau de la société.
- La possibilité de création du paquet autonome d'installation pour les applications de Kaspersky Lab est ajoutée.
- L'interface utilisateur de l'application est remaniée considérablement : panneau des résultats, types de rapports, barres d'informations (cf. section "Fenêtre principale de l'application" à la page 27).

- Le mécanisme de collecte des informations sur les applications installées sur les postes clients est ajouté (registre des applications).
- Le système des privilèges d'accès est remanié et élargi.
- Ajout du support des technologies Microsoft NAP.
- Ajout de la possibilité de la permutation des clients nomades entre les Serveurs d'administration.
- Elargissement des critères de permutation des clients entre les stratégies mobiles et normales.
- Les possibilités de déplacement automatique des ordinateurs dans les groupes d'administration sont élargies.
- La possibilité de création des groupes d'administration à la base de la structure Active Directory est ajoutée.
- Les nouveaux rapports sont ajoutés, maintenant il est possible d'ajouter vos propres systèmes de compte, l'information, affichée dans les rapports, est élargie.
- Ajout de la possibilité d'exporter les rapports dans les fichiers en format PDF et XML (Microsoft Excel).
- Ajout de la possibilité de collecter des données détaillées lors d'une construction des rapports généraux.
- Réalisation du mécanisme de mise en cache de l'information pour la construction des rapports généraux, qui contiennent les données des Serveurs d'administration secondaires.
- Le support de deux ensembles des colonnes dans la console d'administration est ajouté, ainsi que l'ensemble des colonnes est élargie (cf. section "Panneau des résultats" à la page 33).
- Les nouveaux colonnes pour la liste des ordinateurs sont ajoutées : " Redémarrage ", " Description de l'état ", " Version de l'Agent d'administration ", " Version de la protection ", " Version des bases ", " Heure de l'activation ".
- Ajout de nouveaux critères, à l'aide desquels les états des ordinateurs sont formés.
- Les nouvelles sélections d'ordinateurs, formés par défaut, sont ajoutées ; la possibilité de création des sélections d'ordinateurs à l'aide des données des Serveurs d'administration secondaires est ajoutée.
- La possibilité de gestion de la liste des notes de l'administrateur est ajoutée.
- La possibilité de visionnage des sessions et des contactes d'utilisateurs disponibles sur l'ordinateur est ajoutée.
- L'interface graphique pour l'utilitaire de sauvegarde et de restauration des données est ajoutée.
- Les fichiers des stratégies et des tâches de groupes se propagent à l'aide d'une diffusion IP multiadresse.
- Le paramètre Wake On Lan est en accès libre pour les clients situés dans les sous-réseaux et différents du sous-réseau du Serveur d'administration, et dans le cas du lancement manuel de la tâche.
- Vous pouvez définir les paramètres de redémarrage pour les postes clients dans les configurations de la tâche d'installation à distance.
- Le mécanisme de restriction du nombre des notifications envoyées en unité de temps est modifié : maintenant les restrictions sont comptées d'un air indépendant pour chaque type d'événements.
- La possibilité de recherche de groupes et de Serveurs d'administration secondaires selon la hiérarchie des Serveurs est ajoutée.
- Elargissement des statistiques des agents des mises à jour.
- La tâche de suppression des applications étrangères permet maintenant de supprimer plusieurs applications à la fois.

- Elaboration de l'utilitaire de préparation à l'installation à distance des ordinateurs.
- Réalisation du mécanisme d'obtention des mises à jour nécessaires à l'application directement après la création de son paquet d'installation.
- Réalisation des statistiques des applications connectées aux Serveurs d'administration secondaires lors d'obtention des mises à jour nécessaires.
- Instauration du classement des erreurs possibles du sous-système de l'installation à distance de l'application, ajout des conseils de résolution des problèmes types.
- Ajout du mécanisme d'application automatique des mises à jour des modules pour les composants du système d'administration.

NOTIONS PRINCIPALES

Cette section contient les définitions détaillées des notions principales, concernant **Kaspersky Administration Kit**. Les définitions de ces notions, ainsi que de quelques termes, sont présentées dans la section **Glossaire**.

DANS CETTE SECTION

SERVEUR D'ADMINISTRATION. GROUPES D'ADMINISTRATION

Les composants de Kaspersky Administration Kit permettent de réaliser l'administration à distance des applications de Kaspersky Lab dans le cadre du réseau de l'entreprise.

On appellera les ordinateurs, sur lesquels est installé le composant **Serveur d'administration**, les Serveurs d'administration (ci-après aussi Serveurs).

La multitude des ordinateurs du réseau de l'entreprise peut être divisée en groupes, qui créent une certaine hiérarchie de la structure. On appellera ces groupes les groupes d'administration. La structure des groupes d'administration est affichée dans l'arborescence de la console dans le nœud du Serveur d'administration.

Le Serveur d'administration s'installe sur l'ordinateur en tant que service avec une sélection d'attributs suivante :

- le nom de Kaspersky Administration Server ;
- le lancement automatique lors du démarrage du système d'exploitation ;
- le compte utilisateur **Système local**, soit le compte utilisateur en vertu de la sélection, effectuée lors de l'installation du composant.

Les fonctions du Serveur d'administration, notamment le composant installé **Serveur d'administration**, consistent en :

- sauvegarde de la structure des groupes d'administration ;
- sauvegarde de la copie de l'information de configuration des postes clients ;
- organisation des stockages des distributifs des applications de Kaspersky Lab ;
- installation et désinstallation à distance des applications sur les ordinateurs ;
- mise à jour des bases et des modules de l'application ;

- administration des stratégies et des tâches sur les postes clients ;
- sauvegarde des informations sur les événements ;
- formation des rapports de fonctionnement des applications ;
- extension des licences sur les postes clients, sauvegarde des informations sur les licences ;
- envoi des notifications sur l'exécution en cours de la tâche. Ces notifications peuvent signaler, par exemple, les virus détectés sur l'ordinateur.

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 secondaires comme sur un seul niveau de hiérarchie, ainsi que sur les niveaux imbriqués. Le niveau d'intégration des Serveurs secondaires n'est pas limité. Cela dit, 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 isolés et indépendants les uns des autres peuvent être administrés par différents Serveurs d'administration qui, à leur tour, sont administrés par le Serveur principal.

La possibilité de sous-structurer la hiérarchie des Serveurs peut être utilisée pour :

- Limiter la charge sur le Serveur d'administration (par rapport à un Serveur installé dans le réseau).
- Diminuer le trafic dans le réseau et simplifier le fonctionnement avec les bureaux distants. Il n'est pas nécessaire d'établir la connexion entre le Serveur principal et tous les ordinateurs du réseau, qui peuvent être situés, par exemple, dans d'autres régions. Il suffit d'installer dans chaque segment du réseau un Serveur d'administration secondaire, répartir les ordinateurs dans les groupes d'administration des Serveurs secondaires et fournir aux Serveurs secondaires la connexion avec le Serveur principal par les canaux de liaisons rapides.
- Répartir plus clairement les responsabilités entre les administrateurs de la sécurité antivirus. Alors, toutes les possibilités de l'administration centralisée et de la surveillance de la sécurité antivirus du réseau corporatif seront maintenues.

Chaque ordinateur, inclus dans la structure du groupe d'administration, peut être connecté à un seul Serveur d'administration. L'administrateur doit lui-même contrôler la correction de connexion des ordinateurs aux Serveurs d'administration en utilisant la fonction de recherche d'ordinateurs par les attributs de réseau dans les groupes d'administration des différents Serveurs.

POSTE CLIENT. GROUPE

L'interaction entre le Serveur d'administration et les ordinateurs s'opère via l'Agent d'administration. C'est à dire :

- affichage de l'information sur l'état actuel des applications ;
- envoi et réception des commandes d'administration ;
- synchronisation de l'information de configuration ;
- envoi de l'information sur le Serveur sur les événements dans le fonctionnement des applications ;
- fonctionnement de l'*agent de mise à jour* ;

L'Agent d'administration doit être installé sur tous les ordinateurs où l'administration des applications de Kaspersky Lab se réalise à l'aide de Kaspersky Administration Kit.

Ce composant s'installe sur l'ordinateur en tant que service avec une sélection d'attributs suivante :

- nom de Kaspersky Network Agent ;
- lancement automatique lors du démarrage du système d'exploitation ;
- 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, quand l'application Cisco Trust Agent est installée sur l'ordinateur. Les paramètres de collaboration avec Cisco NAC sont indiqués dans les propriétés du Serveur d'administration.

En collaboration avec **Cisco NAC**, le Serveur d'administration joue le rôle du 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, serveur ou poste de travail sur lequel l'Agent d'administration est installé ainsi que les applications administrées de Kaspersky Lab, on appellera – **client du serveur d'administration** (ou tout simplement *poste client*).

En vertu de la stratégie de l'entreprise (d'organisation ou territoriale), des fonctions exécutées et de l'ensemble d'applications de Kaspersky Lab installées, les postes clients peuvent être organisés dans les groupes d'administration. Ce groupement s'effectue pour permettre l'administration de tous les ordinateurs en tant que groupe unique. Lors du groupement des postes clients, n'importe quelle association des principes ci-dessus peut être utilisée, ainsi que d'autres critères selon le choix de l'administrateur. Par exemple, les groupes correspondant aux départements peuvent composer le niveau supérieur. Au niveau suivant, à l'intérieur de chaque département, les ordinateurs se réunissent selon les fonctions exécutées : un groupe d'ordinateurs peut contenir toutes les stations de travail, un autre – tous les serveurs fichiers, etc.

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 s'installent :

- 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 (de fonctions de l'application) avec l'ensemble établi de 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.

L'administrateur peut créer une hiérarchie des Serveurs et des groupes de n'importe quel degré de complexité, si cela lui simplifie la tâche d'administration des applications. On peut avoir à un niveau de la hiérarchie les Serveurs d'administration secondaires, les groupes et les postes clients.

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

On appellera les ordinateurs, sur lesquels est installé le composant de la Console d'administration : **les postes administrateurs**. A partir de ces ordinateurs, les administrateurs peuvent administrer, à distance de manière centralisée, la configuration de toutes les applications de Kaspersky Lab installées sur les postes clients.

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

Le poste administrateur n'est pas un objet du groupe d'administration, mais pourtant, il peut être inclus dans le groupe en tant que poste client. Aucune restriction n'est imposée sur le nombre des postes administrateurs. Les postes administrateurs peuvent coïncider pour différents Serveurs d'administration, chacun peut administrer les groupes d'administration de n'importe quel Serveur d'administration dans la structure du réseau de l'entreprise.

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

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

L'interface pour administrer le fonctionnement de l'application concrète via la Console d'administration est présentée par un composant spécialisé – **plug-in d'administration de l'application**. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide Kaspersky Administration Kit. Le plug-in d'administration est spécifique à chaque application. Il est installé sur le poste administrateur et assure :

- sélection des boîtes de dialogue (interface) pour créer et rédiger les stratégies de l'application ;
- sélection des boîtes de dialogue (interface) pour créer et rédiger les paramètres de l'application ;
- sélection des boîtes de dialogue (interface) pour créer et rédiger les paramètres des tâches réalisées par l'application ;
- fourniture des renseignements sur les tâches réalisées par l'application ;
- fourniture des renseignements sur les événements générés par l'application ;
- prestation de fonctions pour la Console d'administration de l'affichage de l'information reçue des postes clients sur les événements et les statistiques de fonctionnement de l'application.

STRATEGIES, PARAMETRES DE L'APPLICATION ET TACHES

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

L'ensemble de paramètres de fonctionnement de l'application lors de son exécution correspond à une tâche. L'ensemble de paramètres de fonctionnement de l'application, unique pour tout type 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**. Les paramètres de l'application et les paramètres de la tâche ne se croisent pas.

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

Afin d'activer l'exécution de la fonction nécessaire, il est conseillé de configurer les paramètres de fonctionnement de l'application, de créer et de configurer la tâche correspondante et la mettre en exécution.

On appellera les paramètres de l'application définis pour le poste client particulier via l'interface locale, ou à distance via la Console d'administration : **les paramètres locaux de l'application**.

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

La stratégie c'est l'ensemble de paramètres de fonctionnement de l'application dans le groupe. La stratégie ne définit pas tous les paramètres de l'application.

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

Chaque paramètre, présenté dans la stratégie, a pour attribut : le " cadenas ", qui 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). 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 de paramètres locaux de l'application" à la page 18). La case décochée **Hériter des paramètres de la stratégie de niveau supérieur** annule l'action du " cadenas " pour les stratégies héritées.

Une stratégie propre à chaque application peut être définie dans le groupe. Plusieurs stratégies avec les valeurs différentes des paramètres peuvent être définies pour une application, mais une seule stratégie pour l'application peut être active.

Il y a la possibilité d'activer la stratégie, qui n'est pas active, selon l'événement. Cela permet, par exemple, d'installer les 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. Elle va entrer en vigueur lorsque l'ordinateur est déconnecté du réseau de l'entreprise.

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 sous-groupes et les Serveurs d'administration secondaires héritent des stratégies du groupe du niveau plus élevé de la hiérarchie.

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

- **la tâche de groupe** : la tâche qui définit les paramètres de fonctionnement de l'application, installée sur les ordinateurs, inclus dans le groupe d'administration ;
- **la tâche locale** : la tâche pour l'ordinateur individuel ;
- **la tâche pour la sélection d'ordinateurs** : la 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 est installée.

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.

Les tâches, créées pour le poste client de manière locale, seront exécutées uniquement pour cet ordinateur. Lors de la synchronisation du 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, c'est le nom du disque, les masques des fichiers analysés, etc.

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 les notifications sur l'exécution de telle ou telle tâche, ainsi que parcourir les rapports détaillés.

L'information sur les stratégies, les paramètres de l'application, les tâches pour les sélections d'ordinateurs et les tâches de groupe est enregistrée sur le Serveur et diffusée sur les postes clients lors de la synchronisation. Cela dit, les modifications locales (réalisées sur les postes clients et autorisées par la stratégie), à leur tour, sont enregistrées dans les données du Serveur d'administration. Outre cela, 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 pour tous les ordinateurs inclus dans le groupe, les valeurs identiques des paramètres de fonctionnement de l'application peuvent être établies.

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 " chez le paramètre de la stratégie :

- si la modification du paramètre est interdite, sur tous les postes clients est utilisée la même valeur : définie par la stratégie ;
- si ce n'est pas interdit, sur chaque poste client l'application n'utilise pas la valeur, indiquée dans la stratégie, mais la valeur locale du paramètre. Cela dit, la valeur du paramètre peut être modifiée via les paramètres locaux de l'application.

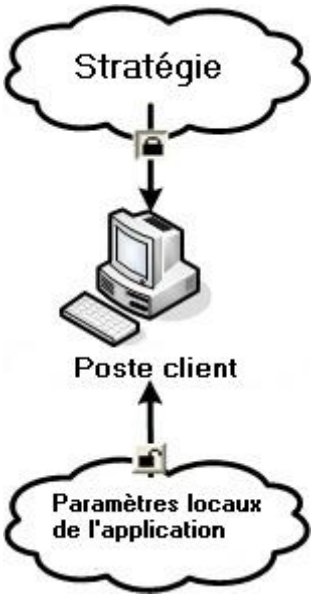


Illustration 1. Stratégie et paramètres locaux de l'application

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.

CONCEPTION DU FONCTIONNEMENT DE KASPERSKY ADMINISTRATION KIT

Cette section décrit les principes de base du fonctionnement de l'application, ainsi que les modes de résolution des tâches particulières, ainsi que donne une brève description de l'interface utilisateur et des modes de son utilisation.

DANS CETTE SECTION

DEPLOIEMENT DU SYSTEME DE PROTECTION ANTIVIRUS

Il existe deux types de déploiement du système de protection antivirus, administré à l'aide de Kaspersky Administration Kit :

- Grâce à l'installation à distance centralisée des applications sur les postes clients. Cela dit, l'installation des applications et la connexion au système d'administration à distance centralisé s'opère automatiquement, ne demande aucune intervention de l'administrateur et permet d'installer le logiciel antivirus sur n'importe quel nombre de postes clients.

- Grâce à l'installation locale des applications sur chaque poste client. Dans ce cas, l'installation des composants requis sur les postes clients et sur le poste administrateur s'opère manuellement. Les paramètres de connexion des clients au Serveur seront définis lors de l'installation de l'Agent d'administration. Cette option de déploiement est utilisée dans le cas, où il n'est pas possible d'exécuter une installation à distance centralisée.

L'installation à distance peut être utilisée pour installer n'importe quelle application au choix de l'utilisateur. Cependant, il ne faut pas oublier que Kaspersky Administration Kit supporte l'administration que par les applications de Kaspersky Lab, dont le distributif contient le composant spécialisé : le plug-in d'administration par l'application.

COMPATIBILITE AVEC LE SYSTEME CISCO NETWORK ADMISSION CONTROL (NAC)

Kaspersky Administration Kit offre la possibilité d'indiquer une concordance entre les conditions de la protection antivirus de l'ordinateur et les états de sécurité du système Cisco Network Admission Control (NAC).

Pour ce faire, il faut définir les conditions, dans lesquelles le poste client recevra les états de sécurité Cisco Network Admission Control (NAC) : **Healthy**, **Checkup**, **Quarantine** ou **Infected**. Si le poste client ne remplit aucune des conditions précédentes, il recevra l'état **Unknown**. L'état **Healthy** est octroyé uniquement quand toutes les conditions sont remplies, les états **Checkup**, **Quarantine** ou **Infected** – sont attribués, si au moins une des conditions est remplie.

COMPATIBILITE AVEC MICROSOFT NETWORK ACCESS PROTECTION (NAP)

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

Afin d'intégrer Kaspersky Administration Kit, il est nécessaire d'exécuter les actions suivantes :

1. Déployer Kaspersky Administration Kit dans le réseau de façon habituelle.

2. Installer sur le PVS Kaspersky Lab System Health Validator (SHV). Pour ce faire, lors de l'installation de Kaspersky Administration Kit, à l'étape de la sélection des composants de l'application, cochez la case en face du mode d'analyse des fonctions du système Kaspersky Lab System Health Validator (SHV).

   L'Agent d'administration sera alors installé sur les postes clients. Cet agent joue le rôle de l'agent des fonctions du système dans Microsoft NAP Kaspersky Lab System Health Agent (SHA), en transmettant à l'agent Microsoft NAP l'information sur les paramètres de la protection antivirus et leurs modifications sur les postes clients.

   Finalement, Kaspersky Lab System Health Validator (SHV) apparaîtra dans la liste des SHV accessibles dans la console PVS, où il sera possible de configurer les règles d'analyse des données des postes clients, réunis par l'Agent d'administration.

CREATION DU SYSTEME DE GESTION CENTRALISEE DE LA PROTECTION ANTIVIRUS

La conception de la structure des groupes d'administration est la première étape de la construction du système de gestion centralisée de la protection antivirus du réseau de l'entreprise à l'aide de la suite logicielle Kaspersky Administration Kit. Cette étape exige de prendre les décisions suivantes :

1. Sélectionner dans le réseau les parties isolées et définir, quel nombre de Serveurs d'administration il est nécessaire d'installer.

2. Définir, quels ordinateurs dans le réseau de l'entreprise exécuteront les fonctions du Serveur d'administration principal et des Serveurs secondaires, lesquels - les fonctions des postes administrateurs et des postes clients. Tous les ordinateurs, sur lesquels on suppose d'installer les applications de Kaspersky Lab, doivent devenir des postes clients.

3. Décider, selon quel critère le groupement des postes clients sera exécuté, et définir la hiérarchie des groupes.

4. Sélectionner, quel type de déploiement du système de protection antivirus sera utilisé : l'installation à distance ou locale.

A l'étape suivante, l'administrateur doit créer une structure des dossiers du Serveur d'administration par une installation des composants appropriés de Kaspersky Administration Kit sur les ordinateurs du réseau de l'entreprise, notamment :

1. Installer le Serveur d'administration sur les ordinateurs, inclus dans le réseau de l'entreprise.

2. Installer la Console d'administration sur les ordinateurs, depuis lesquels sera exécutée la gestion.

3. Prendre la décision de nommer les administrateurs de Kaspersky Administration Kit, définir, quelles catégories d'utilisateurs vont travailler avec le système, et réserver pour chaque catégorie la liste des fonctions exécutées.

   Le système admet le travail simultané des administrateurs avec les mêmes ressources. Les derniers paramètres selon l'heure d'application seront considérés comme réels. Dans ce cas toutes les actions, effectuées par les administrateurs, doivent être concertées.

4. Former les groupes utilisateurs et fournir à chaque groupe les privilèges d'accès nécessaires à l'exécution des fonctions, dont les utilisateurs sont chargés.

Après cela, il est nécessaire de créer une hiérarchie des Serveurs d'administration, et pour chaque Serveur construire une hiérarchie des groupes d'administration et répartir les ordinateurs dans les groupes appropriés.

A l'étape suivante l'installation est exécutée sur les postes clients du composant de l'Agent d'administration, des applications nécessaires de Kaspersky Lab, ainsi que sur le poste administrateur des plug-ins appropriés de la gestion des applications.

Pas toutes les applications de Kaspersky Lab, dont la gestion est accessible via Kaspersky Administration Kit, ne peuvent être installées à distance sur les postes clients. Consultez les informations détaillées à ce propos dans les manuels des applications correspondantes.

Lors de l'installation à distance, l'Agent d'administration peut être installé conjointement avec n'importe quelle application. Dans ce cas, l'installation à part de l'Agent d'administration n'est pas requise.

Pour compléter, configurez les applications installées par la définition et l'application des stratégies de groupes (cf. section "Administration des stratégies" à la page 48) et la création des tâches nécessaires (cf. section "Paramètres locaux de l'application" à la page 52).

L'application offre la possibilité de créer le système de la gestion centralisée de protection antivirus avec les paramètres minimum à l'aide de l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale" à la page 39). La structure des groupes d'administration, identique à la structure de domaine du réseau Windows, est alors créée. Et le système de protection antivirus se forme, en utilisant Kaspersky Anti-Virus pour Windows Workstations version 6.0 MP4.

Après avoir créé la structure des dossiers du Serveur d'administration, l'installation et la configuration de la protection antivirus, il est recommandé aux administrateurs de réaliser les mesures du service du réseau (cf. section "Maintenance" à la page 66).

CONNEXION DES POSTES CLIENTS AU SERVEUR D'ADMINISTRATION

La coopération des postes clients avec les Serveurs d'administration s'effectue au cours du processus de connexion des clients au Serveur. Cette fonction est assurée par l'Agent d'administration installé sur les postes clients.

La connexion est réalisée afin d'exécuter les opérations suivantes :

- synchronisation de la liste des applications installées sur le poste client ;
- synchronisation des stratégies, des paramètres de l'application, des tâches et des paramètres des tâches ;
- obtention par le Serveur des informations en cours sur l'état des applications et de l'exécution des tâches ;
- transmission des informations sur les événements, que le Serveur doit traiter.

Le mode de connexion principal des postes clients au Serveur consiste en la connexion du client au Serveur. Ce type de connexion est exécuté lors de la synchronisation automatique des données du client et du Serveur, ainsi que lors de la transmission sur le Serveur des informations sur les événements dans le fonctionnement des applications.

La synchronisation automatique s'effectue périodiquement, en fonction des paramètres de l'Agent d'administration (par exemple, une fois toutes les 15 minutes). L'administrateur définit l'intervalle des connexions.

L'information sur un événement est envoyée sur le Serveur tout de suite après qu'il a eu lieu.

Le paramètre **Maintenir la connexion avec le Serveur d'administration** est prévu pour le poste client. Ce paramètre définit, si la connexion du client au Serveur sera terminée à l'achèvement de toutes les opérations énumérées ci-dessus. Une connexion permanente est nécessaire dans le cas, où le contrôle d'état des applications est requis, et que le Serveur ne peut pas établir la connexion avec le client pour des raisons quelconques (la connexion est protégée par un pare-feu, il est interdit d'ouvrir les ports sur le client, l'adresse IP du client est inconnue, etc.).

La synchronisation peut être exécutée par l'administrateur manuellement à l'aide de la commande **Synchroniser** du menu contextuel (cf. section "Menu contextuel" à la page 34) du poste client. Dans ce cas, le mode auxiliaire de connexion est utilisé. Le Serveur initie la connexion en ce mode. Pour ce faire, le port UDP s'ouvre sur le poste client. Le Serveur envoie une demande de connexion sur le port UDP. En réponse, l'analyse des privilèges du Serveur à une connexion au client est exécutée (en vertu de la signature numérique du Serveur d'administration), et dans le cas de leur existence une connexion est exécutée.

Le deuxième mode de connexion est aussi utilisé au cours de l'appel aux données du client sur le Serveur : pour recevoir les informations en cours sur l'état des applications, des tâches et des statistiques du fonctionnement des applications.

CONNEXION SECURISEE AU SERVEUR D'ADMINISTRATION

L'échange d'informations entre les postes clients et le Serveur d'administration, ainsi que la connexion de la Console au Serveur d'administration peut être exécutée en utilisant le protocole SSL (Secure Socket Layer). Il permet d'identifier les parties coopérants, 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 est à la base du protocole SSL, utilisé en cours de la connexion sécurisée.

CERTIFICAT DU SERVEUR D'ADMINISTRATION

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

Le certificat du Serveur d'administration est créé en cours de l'installation du composant du Serveur d'administration et sauvegardé sur le Serveur d'administration dans le dossier d'installation du programme dans le sous-dossier **Cert**.

Le certificat du Serveur d'administration n'est créé qu'une fois, à l'installation. Il est recommandé de le sauvegarder à l'aide de l'assistant d'installation. Dans le cas, si le certificat du Serveur d'administration est perdu, pour le restaurer, il est nécessaire de réinstaller le composant du serveur d'administration et de restaurer les données (cf. section "Copie de sauvegarde et restauration des données du Serveur d'administration" à la page 85).

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

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

Si l'installation de l'Agent d'administration est locale, le certificat du Serveur d'administration peut être sélectionné par l'administrateur manuellement.

En vertu de la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée durant les connexions ultérieures.

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

Si le Serveur d'administration initie la connexion, la demande de connexion via le port UDP reçue du Serveur d'administration est vérifiée de la même manière.

L'AUTHENTIFICATION DU SERVEUR LORS DE LA CONNEXION DE LA CONSOLE

Lors de la première (après l'installation) connexion au Serveur, la Console d'administration demande le certificat du Serveur d'administration et le sauvegarde localement sur le poste administrateur. En vertu de la copie reçue du certificat, lors des connexions suivantes au Serveur d'administration avec ce nom, l'identification du Serveur sera exécutée.

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

IDENTIFICATION DES POSTES CLIENTS SUR LE SERVEUR D'ADMINISTRATION

L'identification des postes clients se réalise sur la base des noms de postes clients. Le nom du 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. 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, à la fin du nom du nouveau poste client sera ajouté le numéro d'ordre, par exemple : **<Nom>-1**, **<Nom>-2**, etc. Sous ce nom le poste client est inclus dans le groupe d'administration.

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

Dans Kaspersky Administration Kit les types suivants sont prévus afin d'autoriser l'accès aux fonctions de l'application :

- **Lecture** :
  - connexion au Serveur d'administration ;
  - affichage de la structure des dossiers du Serveur d'administration ;
  - affichage des valeurs des paramètres des stratégies, des tâches et des paramètres de l'application.
- **Écriture** :
  - création de groupes d'administration, ajout de sous-groupes et de postes clients ;
  - installation du composant Agent d'administration sur les postes clients ;
  - mise à jour de la version des applications installées sur les postes clients ;

  - création de stratégies, de tâches pour les groupes ou les ordinateurs isolés, configuration des paramètres de l'application ;

  - contrôle centralisé des applications, réception de rapports d'activités à l'aide des services du Serveur d'administration, de l'Agent d'administration et de la Console d'administration.

- **Exécution** : lancement et arrêt des tâches existantes pour les groupes, les sélections d'ordinateurs ; génération des rapports.

- **Modification des privilèges d'accès** : attribution aux utilisateurs et aux groupes d'utilisateurs des droits d'accès aux fonctions de Kaspersky Administration Kit.

- **Modification des paramètres d'enregistrement des événements**.

- **Modification des paramètres d'envoi des notifications**.

- **Installation à distance des applications de Kaspersky Lab**.

- **Installation à distance d'autres applications** : préparation des paquets d'installation et installation à distance sur les postes clients des applications des éditeurs tiers.

- **Modification des paramètres de la hiérarchie des Serveurs d'administration**.

Après avoir installé le Serveur d'administration par défaut, ce sont les utilisateurs, inclus dans les groupes **KLAdmins** et **KLOperators**, qui possèdent des privilèges de connexion au Serveur et peuvent travailler avec ses objets.

Ces groupes sont formés en cours de l'installation du composant du Serveur d'administration. Ils sont créés en fonction du compte utilisateur qui était sélectionné afin de lancer les services du Serveur d'administration :

- dans le domaine, auquel est inclus le Serveur d'administration, et sur l'ordinateur du Serveur d'administration, si le Serveur d'administration est lancé sous un compte utilisateur inclus dans le domaine ;

- seulement sur l'ordinateur du Serveur d'administration, si le Serveur est lancé sous un compte du système.

Tous les privilèges sont accordés au groupe **KLAdmins**, au groupe **KLOperators** – les privilèges de lecture. Il est impossible de modifier l'ensemble de privilèges, accordés au groupe **KLAdmins**.

On appellera les utilisateurs du groupe **KLAdmins** - **les administrateurs de Kaspersky Administration Kit**, les utilisateurs du groupe **KLOperators** – **les opérateurs de Kaspersky Administration Kit**.

La consultation des groupes **KLAdmins** et **KLOperators** et l'insertion des modifications nécessaires est réalisée à l'aide des méthodes traditionnelles d'administration de Windows – **Administration** / **Utilisateurs locaux et groupes**.

A part les utilisateurs du groupe **KLAdmins**, les privilèges d'administrateur sont accordés aux :

- administrateurs du domaine, dont les ordinateurs sont inclus dans ce groupe d'administration de ce Serveur ;

- administrateurs locaux des ordinateurs, sur lesquels le Serveur d'administration est installé.

  Les administrateurs locaux peuvent être exclus de la liste d'utilisateurs qui possèdent les privilèges d'administrer le Serveur d'administration.

Toutes les opérations initiées par les administrateurs de Kaspersky Administration Kit seront exécutées avec les privilèges du compte du Serveur d'administration. Pour chaque Serveur d'administration un propre groupe **KLAdmins** peut être formé. Ce groupe possédera les privilèges uniquement dans le cadre du travail avec ce Serveur.

Si les ordinateurs appartiennent au même domaine et constituent les groupes d'administration des Serveurs différents, l'administrateur est l'administrateur de Kaspersky Administration Kit dans le cadre de tous les groupes. Cela dit, le groupe **KLAdmins** est unique pour ces groupes d'administration et est créé lors de l'installation du premier Serveur d'administration. Son enrichissement peut être réalisé par les moyens d'administration du système d'exploitation. Toutes les opérations initiées par les administrateurs de Kaspersky Administration Kit seront exécutées avec les privilèges du compte du Serveur d'administration.

Les privilèges des utilisateurs (cf. section "Affectation de droits" à la page 36) dans l'application Kaspersky Administration Kit sont établis en vertu de l'authentification d'utilisateurs de Windows.

Après l'installation de l'application, l'administrateur de Kaspersky Administration Kit peut :

- modifier les privilèges, accordés aux groupes **KLOperators** ;
- attribuer des privilèges d'accès aux fonctions de l'application Kaspersky Administration Kit aux autres groupes d'utilisateurs et aux utilisateurs particuliers enregistrés sur l'ordinateur, où la Console d'administration est installée ;
- accorder différents privilèges d'accès afin de pouvoir travailler dans chaque groupe d'administration.

CONCEPTION DE L'INTERFACE UTILISATEUR

La consultation, la création, la modification et la configuration des groupes d'administration, l'administration centralisée du fonctionnement de toutes les applications de Kaspersky Lab installées sur les postes clients est exécutée 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), donc, l'interface Kaspersky Administration Kit est standard pour MMC.

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

Pour travailler localement avec les postes clients, l'application prévoit la possibilité d'installer une connexion à distance avec l'ordinateur via 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 sur le poste client la connexion à distance au poste de travail.

CONFIGURATION DE L'INTERFACE

Kaspersky Administration Kit permet de configurer l'interface de la Console d'administration.

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

1. Passez au menu **Affichage** →**Configuration de l'interface**. Cela entraîne l'ouverture de la fenêtre du même nom (cf. ill. ci-après).

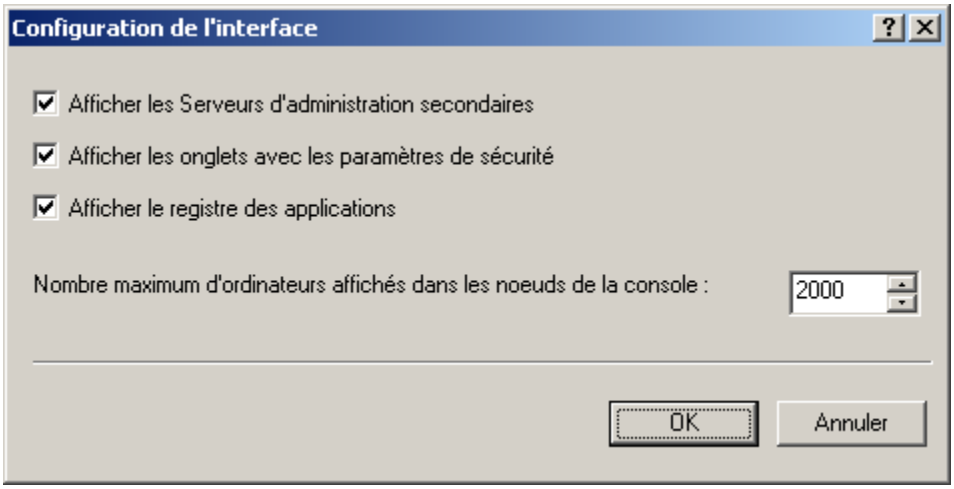


Illustration 2. Affichage des propriétés du groupe. Fenêtre ***Configuration de l'interface***

2. Dans la fenêtre ouverte vous pouvez spécifier les paramètres suivants :

   - **Afficher les Serveurs d'administration secondaires**.
   - **Afficher les onglets avec les paramètres de sécurité**.
   - **Afficher le registre des applications**.
   - **Nombre maximum d'ordinateurs affichés dans les nœuds de la console**. Ce paramètre détermine le nombre d'ordinateurs affichés sur le panneau des résultats de la Console d'administration pour les entrées de groupes et de domaines. La valeur par défaut est égale à 2000.

     Si le nombre d'ordinateurs dans le groupe dépasse la valeur définie, l'avertissement approprié s'affiche. Pour afficher la liste de tous les ordinateurs, il faut augmenter la valeur.

La définition dans les paramètres d'un groupe (ou d'un domaine) de la valeur du nombre maximum d'ordinateurs à afficher entre en vigueur pour tous les groupes de tous les niveaux de la hiérarchie, ainsi que pour tous les domaines.

DEMARRER L'APPLICATION

Le lancement de l'application Kaspersky Administration Kit s'effectue par la sélection du point **Kaspersky Administration Kit** dans le groupe d'application **Kaspersky Administration Kit** du menu standard **Démarrer** → **Applications**. Ce groupe de programme est créé uniquement sur les postes administrateurs pendant l'installation de la Console d'administration.

Pour accéder aux fonctions de Kaspersky Administration Kit, il faut que le Serveur d'administration Kaspersky Administration Kit soit lancé.

FENETRE PRINCIPALE DU PROGRAMME

La fenêtre principale du programme (cf. ill. ci-dessous) contient le menu, la barre d'outils, la barre de consultation et la zone d'information, qui peut être représentée par la barre des tâches ou la barre des résultats.

Le menu assure la gestion des fenêtres et offre l'accès au système d'information. Le point du menu **Action** reprend les commandes du menu contextuel pour le nœud actuel ou pour le dossier de l'arborescence de la console.

L'ensemble de boutons de la barre d'outils assure l'accès direct à certains points du menu principal. Le contenu de la barre d'outils change selon le nœud actuel de l'arborescence de la console.

La barre de consultation reflète l'étendue des noms de **Kaspersky Administration Kit** en guise de l'arborescence de la console (cf. section "Arborescence de la console" à la page 28).

La zone d'information du menu contextuel peut être représentée par la barre des tâches, la barre des résultats ou par leurs combinaisons. Pour certains nœuds de l'arborescence de la console, la zone d'information a deux types de présentations : étendu et standard. Le passage entre ces types est accessible par les onglets du même nom.

La barre des tâches contient un ou plusieurs onglets, qui représentent les pages avec les liens d'accès rapide aux opérations principales, envisagées pour le nœud sélectionné dans l'arborescence de la console. Voir les détails sur le travail avec la barre des tâches dans la section Barre des tâches (à la page 30).

La barre des résultats représente la liste des éléments du nœud sélectionné dans l'arborescence de la console ou l'ensemble des zones d'information. Cela peut être la liste des ordinateurs dans les groupes, la liste des rapports, des requêtes d'événements ou d'ordinateurs, etc. Pour obtenir de plus amples informations sur l'utilisation du panneau des résultats, consultez la section Panneau des résultats (page 33).

Illustration 3. Fenêtre principale de Kaspersky Anti-Virus

ARBORESCENCE DE LA CONSOLE

L'arborescence de la console (cf. ill. ci-dessous) est conçue pour refléter la hiérarchie (formée dans le réseau de l'entreprise) des Serveurs d'administration, de la structure de leurs groupes d'administration, ainsi que d'autres objets de l'application, tels que stockages, requêtes, etc.

L'étendue des noms de **Kaspersky Administration Kit** peut inclure plusieurs nœuds avec les noms des serveurs qui correspondent aux Serveurs d'administration installés et inclus dans la structure.

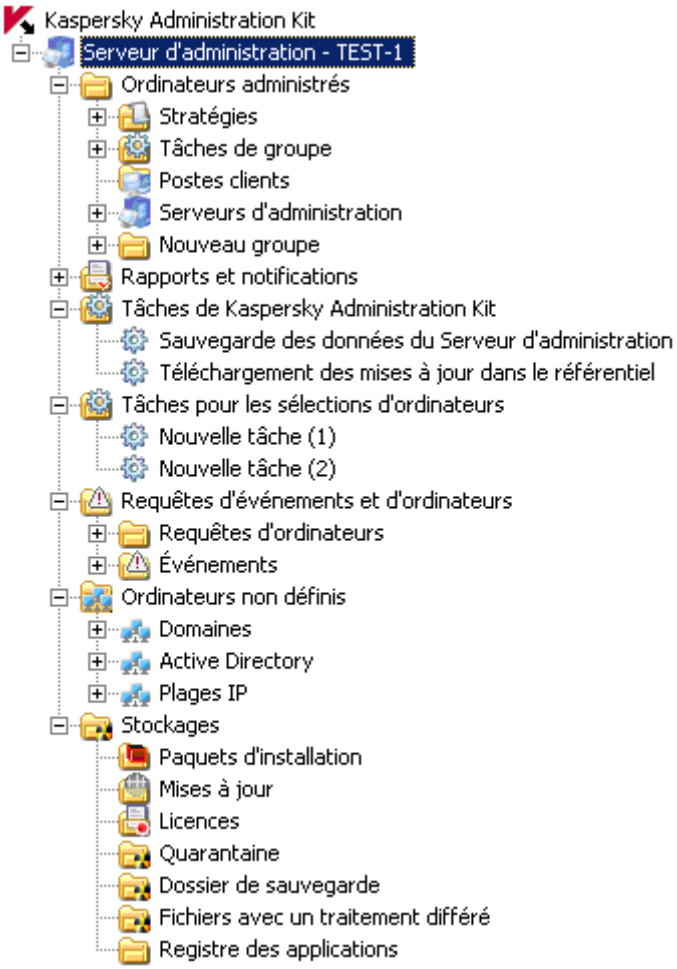


Illustration 4. Arborescence de la console

Le nœud **Serveur d'administration – <nom de l'ordinateur>** est un container et reflète la structure des dossiers du Serveur d'administration indiqué. Le container **Serveur d'administration – <nom de l'ordinateur>** inclut les nœuds suivants :

- **Ordinateurs administrés** ;
- **Rapports et notifications** ;
- **Tâches de Kaspersky Administration Kit** ;
- **Tâches pour les sélections d'ordinateurs** ;
- **Requêtes d'événements et d'ordinateurs** ;
- **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.

Les objets, situés à la racine du dossier **Ordinateurs administrés**, correspondent au niveau supérieur de la hiérarchie. Citons les dossiers obligatoires pour chaque objet qui reflète le groupe : **Stratégies**, **Tâches de groupe**, **Postes clients**

et **Serveurs d'administration**. Ces dossiers sont conçus pour travailler avec les Serveurs d'administration, les postes clients, les stratégies et les tâches de groupe du niveau supérieur de la hiérarchie.

Le dossier **Tâches de Kaspersky Administration Kit** 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 et le téléchargement de la mise à jour par le Serveur d'administration.

Le dossier **Tâches pour les sélections d'ordinateurs** contient l'ensemble de tâches, définies pour la sélection d'ordinateurs dans le groupe d'administration ou dans le nœud **Ordinateurs non définis**. Ces tâches sont commodes pour les petits groupes des postes clients, qui ne peuvent pas être unis dans un groupe d'administration séparé.

Le nœud **Rapports et notifications** de l'arborescence de la console contient l'ensemble de modèles pour former les rapports d'état du système de protection antivirus sur les postes clients des groupes d'administration. Les modèles sont accessibles dans l'onglet **Statistiques** de la barre des tâches du nœud. Sur l'onglet **Notifications** vous pouvez configurer les paramètres des notifications sur le fonctionnement du système. Lors de la sélection d'un modèle dans l'arborescence de la console dans la barre de résultats, le rapport formé s'affiche.

Le nœud **Requêtes d'événements et d'ordinateurs** inclut les sous-dossiers suivants :

- **Requêtes d'ordinateurs** : est conçu pour rechercher les postes clients selon les critères définis et dans la barre des résultats.
- **Événements** : contient les requêtes d'événements, qui présente l'information sur les événements, enregistrés dans le fonctionnement des applications, ainsi que sur les résultats de l'exécution de la tâche.

Le nœud **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 régulières 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 barre des résultats des sous-dossiers correspondants : **Domaines**, **Plages IP** et **Active Directory**.

Le nœud **Stockages** permet de manipuler les objets utilisés pour la surveillance de l'état des postes client et les entretenir. Le nœud inclut les dossiers suivants :

- **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 récupérées par le Serveur d'administration qui peuvent être déployées sur les postes client.
- **Licences** : contient la liste des licences installées 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.
- **Registre des applications** : contient la liste des applications installées sur les postes clients, sur lesquels l'Agent d'administration est installé.

PANNEAU DES TACHES

Le panneau des tâches est une zone de la fenêtre, qui reprend une série de liens pour l'administration des objets du Serveur d'administration et du Serveur lui-même.

Il existe deux types de panneaux des tâches : le panneau standard et le panneau étendu.

Le panneau étendu (cf. ill. ci-après) est accessible à la majorité des nœuds et des objets de l'arborescence de la console. Il s'agit d'une page HTML contenant des liens, qui permettent d'exécuter diverses opérations et d'accéder à d'autres objets du Serveur d'administration, ainsi que de brèves informations sur l'objet ou le nœud sélectionné.

Il peut exister plusieurs panneaux des tâches pour un nœud. Ils se présentent alors sous la forme d'onglets dont le titre figure dans la partie supérieure de la zone d'information.

Pour faciliter la navigation entre les nœuds et les objets du Serveur d'administration, la partie supérieure du panneau des tâches propose la chaîne de navigation suivante : **Début → <nom du nœud> → ... → <nom du dossier> → <nom de l'objet>**. Les liens peuvent être regroupés en blocs pour une meilleure organisation du panneau.

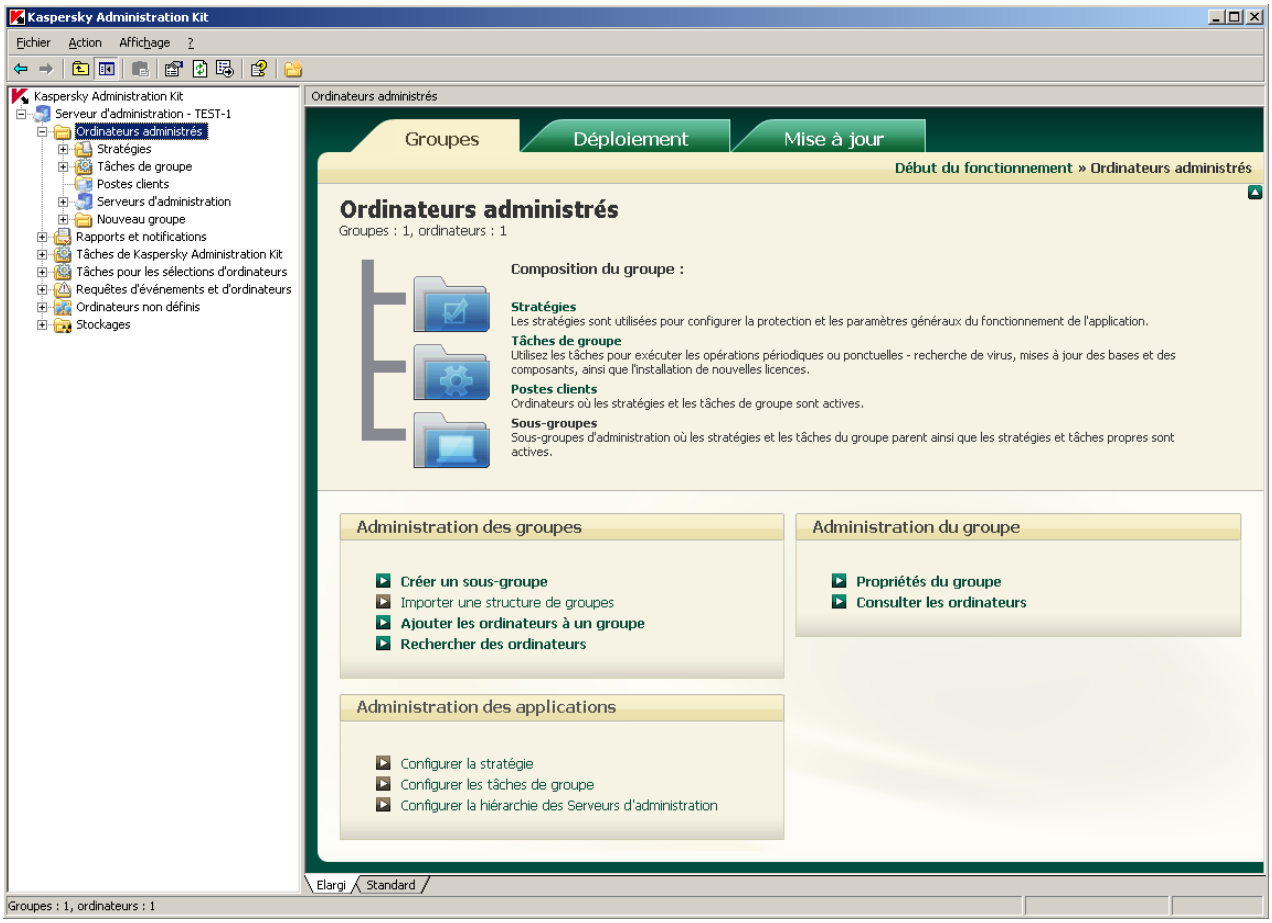


*Illustration 5. Panneau des tâches élargi. Nœud **Ordinateurs administrés***

Pour certains objets de l'arborescence de la console, il est possible de trouver dans le panneau des tâches des informations de synthèse telles que les résultats de l'application d'une stratégie, par exemple (cf. ill. ci-dessous). Dans ce cas, le panneau des tâches remplit la même fonction que le panneau des résultats (cf. section "Panneau des résultats" à la page 33).

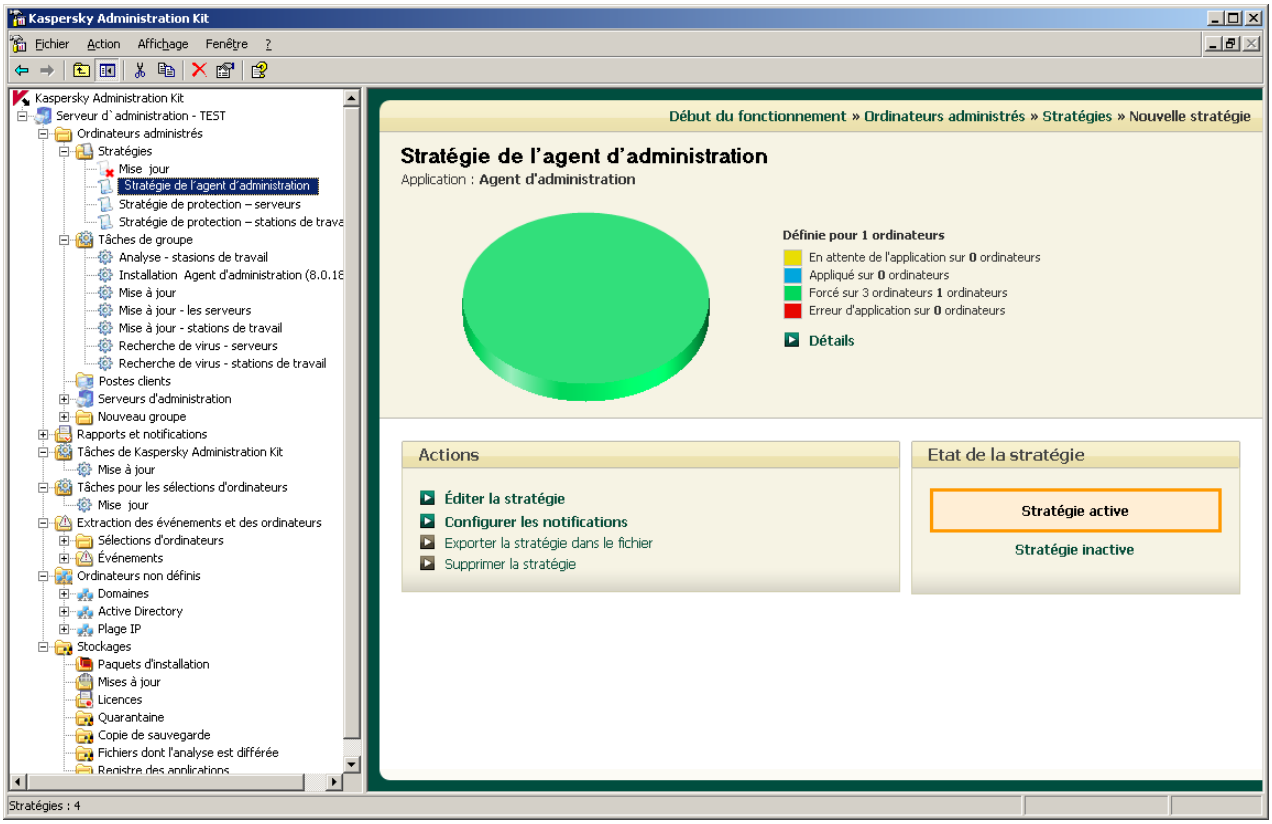


Illustration 6. Panneau des tâches pour la stratégie

Le panneau des tâches standard est prévu pour certains nœuds, qui ne possèdent pas de panneau des tâches étendu. Il reprend une série de liens dans la partie gauche du panneau des résultats (cf. ill. ci-dessous). À l'instar des liens du panneau des tâches étendu, les liens du panneau des tâches standard permettent d'exécuter les opérations, de consulter les propriétés d'un objet ou de les modifier. Le panneau des résultats, comprenant le panneau des tâches, est accessible sur l'onglet portant le nom du nœud ou du dossier.

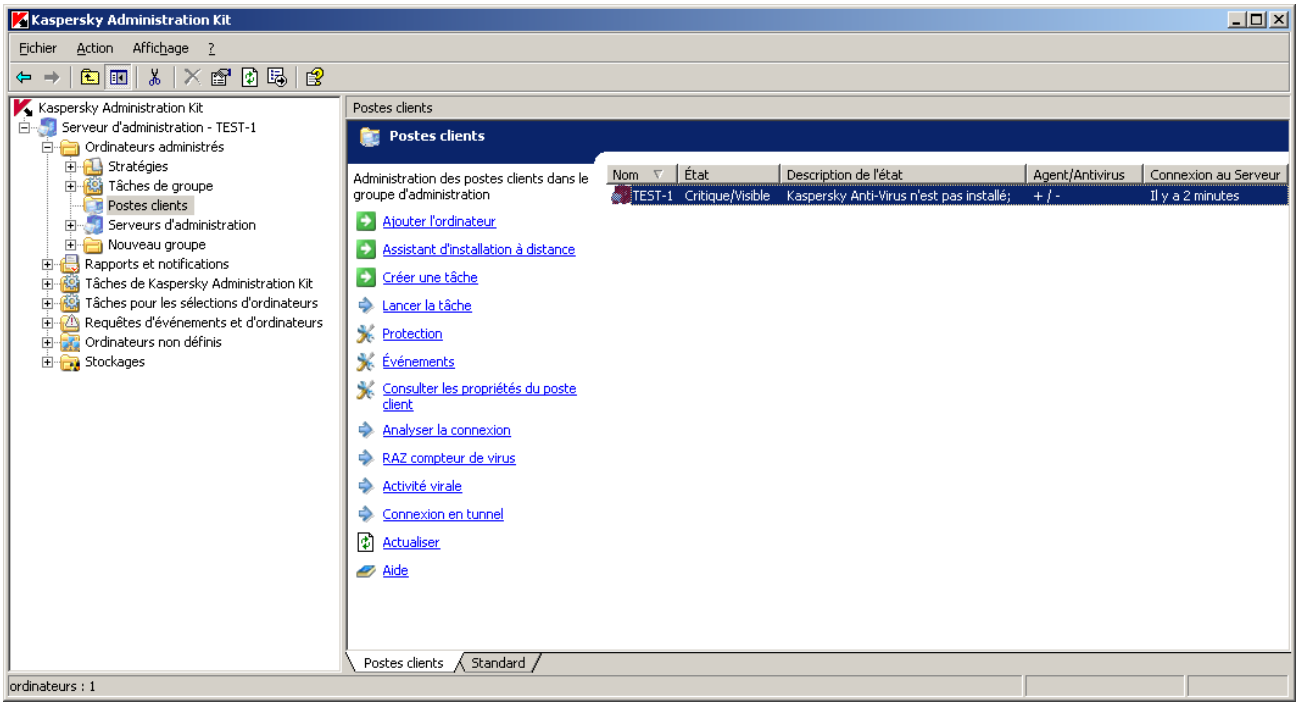


Illustration 7. Panneau des tâches standard pour le nœud ***Postes clients***

Dans la documentation qui accompagne Kaspersky Administration Kit, le terme panneau des tâches fait référence au panneau des tâches élargi. En cas de référence faite au panneau des tâches standard, ses éléments sont décrits comme faisant partie du panneau des résultats.

PANNEAU DES RESULTATS

Le panneau des résultats est une partie de la fenêtre, qui affiche diverses informations : liste des ordinateurs, des stratégies ou des tâches, rapports composés sur la base de modèles définis, etc.

Il existe deux types de panneau des résultats : panneau standard et panneau étendu. Ils sont tous deux accessibles via l'onglet du même nom.

Pour les rapports existants, le panneau des résultats propose des diagrammes, ainsi que des informations synthétiques et détaillées présentées sous forme de tableaux (cf. ill. ci-après).

Le panneau des résultats peut être composé de panneaux d'information (cf. ill. ci-après), qui constituent chacun une page séparée. Les données des panneaux d'information peuvent être représentées sous forme de tableaux ou de diagrammes (camemberts ou barres). L'administrateur peut modifier la sélection de pages et de panneaux d'information, ainsi que la composition des données et le mode de représentation :

- Pour modifier la composition des pages contenant les panneaux d'informations, cliquez sur le bouton  situé dans le coin supérieur droit de l'onglet **Statistiques**.

- Pour configurer la composition des panneaux d'information sur la page, cliquez sur le bouton  situé à côté du nom de la page et définissez les paramètres requis dans la fenêtre qui s'ouvre.

- Pour définir les paramètres de représentation d'un panneau d'information en particulier, cliquez sur le bouton situé à côté du nom du panneau.

- Il est possible de déployer et de réduire les panneaux à l'aide des boutons et

Dans le panneau des résultats standard, les données sont présentées sous forme d'un tableau (cf. ill. ci-après). La liste des colonnes pour les différents nœuds est reprise dans l'aide.

Illustration 8. Panneau des résultats standard

Les informations présentées dans la Console d'administration sont actualisées uniquement pour les entrées. Pour actualiser les informations dans le panneau des résultats, il faut appuyer sur la touche **F5** ou utiliser la commande **Actualiser** du menu et du menu contextuel ou cliquer sur le lien **Actualiser** dans le panneau des tâches.

MENU CONTEXTUEL

Dans l'arborescence de la console, chaque catégorie d'objets de l'espace des noms **Kaspersky Administration Kit** possède son propre menu contextuel. Outre les commandes standards du menu contextuel de 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'aide.

Le panneau des résultats de 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. Les principaux types d'éléments et les commandes supplémentaires associées figurent dans l'aide.

ADMINISTRATION DES ORDINATEURS DU RESEAU

Dans le cadre des mesures d'administration des ordinateurs du réseau de l'entreprise, on détermine les entités suivantes :

- Serveurs d'administration (cf. section "Connexion au Serveur d'administration" à la page 35) et leur hiérarchie (cf. section "Serveurs d'administration secondaires" à la page 45) ;
- Privilèges d'accès au Serveur d'administration (cf. section "Affectation de droits" à la page 36) ;
- Composition et hiérarchie des groupes d'administration (cf. section "Création, consultation et modification de la structure du groupe d'administration" à la page 39).

DANS CETTE SECTION

CONNEXION AU SERVEUR D'ADMINISTRATION ;

Vous pouvez utiliser la Console d'administration pour la connexion des postes clients à distance au Serveur d'administration via Internet.

Après le lancement de Kaspersky Administration Kit, la fenêtre principale du programme présente l'arborescence de la console avec le niveau supérieur de la hiérarchie de l'espace de noms **Kaspersky Administration Kit**. Pour que la fenêtre principale illustre la structure des dossiers du Serveur d'administration, il faut ajouter l'objet – Serveur à l'arborescence de la console et établir la connexion avec le Serveur d'administration requis (cf. ill. ci-après).

Vous pouvez connecter les postes clients distants au Serveur d'administration à l'aide de la Console d'administration via Internet.

Le programme reçoit les informations sur la structure des dossiers depuis le Serveur d'administration et la représente dans l'arborescence de la console.

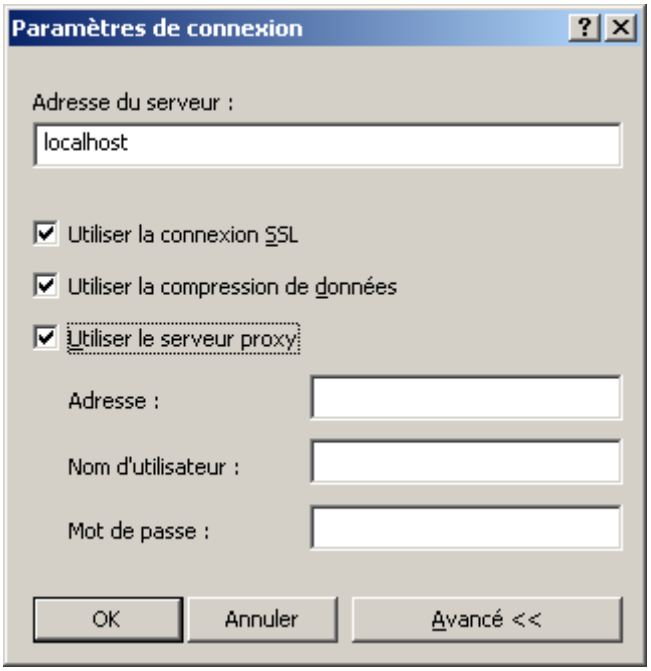


Illustration 9. Etablissement de la connexion au Serveur d'administration

Les utilisateurs qui ne jouissent pas des privilèges de connexion ne pourront pas accéder au Serveur d'administration. La vérification des privilèges s'opère sur la base de l'authentification Windows de l'utilisateur dans le réseau.

Si plusieurs Serveurs d'administration sont installés dans la structure du réseau, vous pouvez travailler avec chacun d'eux depuis le poste de travail de l'administrateur. Pour **passer** aux groupes d'administration d'un autre Serveur, vous pouvez soit vous connecter au Serveur requis, soit ajouter plusieurs Serveurs à l'arborescence de la console et établir la connexion avec chacun d'eux.

L'utilisation en parallèle de plusieurs Serveurs d'administration est uniquement possible, si vous êtes l'utilisateur ou l'administrateur de Kaspersky Administration Kit pour chaque Serveur ou si vous jouissez des privilèges requis sur chaque Serveur.

AFFECTATION DE DROITS

Une fois que le Serveur d'administration a été installé, les utilisateurs appartenant aux groupes (cf. section "Privilèges d'accès au Serveur d'administration et à ses objets" à la page 24) **KLAdmins** et **KLOperators** jouissent des privilèges de connexion au Serveur et d'utilisation de celui-ci.

Vous pouvez modifier les privilèges d'accès pour le groupe **KLOperators**, octroyer des privilèges d'utilisation du Serveur pour d'autres groupes d'utilisateurs ou les utilisateurs particuliers enregistrés sur l'ordinateur, où se trouve la Console d'administration.

L'octroi de privilèges d'accès à tous les objets du Serveur d'administration s'opère dans la fenêtre de configuration des paramètres du Serveur d'administration sur l'onglet **Sécurité** (cf. ill. ci-après).

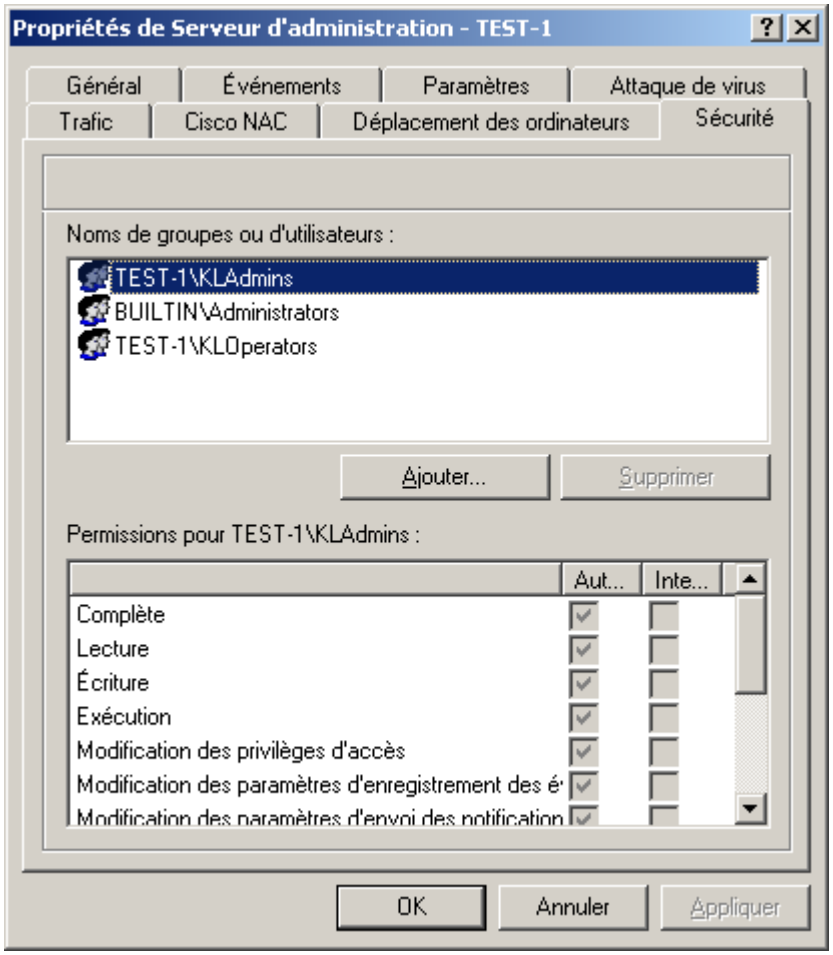


Illustration 10. Attribution de privilèges d'accès au Serveur d'administration

Il est possible de désigner les privilèges d'accès pour chaque groupe d'administration individuel ou pour d'autres objets du Serveur d'administration, par exemple, les tâches du Serveur d'administration. Cette configuration est réalisée dans la fenêtre des propriétés de l'objet à l'onglet **Sécurité**.

L'administrateur peut surveiller l'activité de l'utilisateur à l'aide des événements survenus pendant l'utilisation du Serveur d'administration et consignés dans les journaux des événements. Ces événements possèdent le degré d'importance **Message d'information**, les types d'événement commencent par le mot **Audit**. Dans le nœud **Événements** de l'arborescence de la console, ils figurent dans le dossier **Événements d'audit**.

AFFICHAGE DES INFORMATIONS DU RESEAU D'ORDINATEURS DOMAINES, PLAGES D'ADRESSES IP ET GROUPES ACTIVE DIRECTORY

Les informations relatives à la structure du réseau informatique et aux ordinateurs qui en font partie sont reprises dans le nœud **Ordinateurs non définis** de l'arborescence de la console.

Le dossier **Ordinateurs non définis** contient trois sous-dossiers :

- **Domaines**.

- **Active Directory**.
- **Plages IP**.

Le dossier **Domaines** contient la hiérarchie des dossiers qui représentent la structure des domaines et des groupes de travail du réseau Windows de l'entreprise. Au dernier niveau de chacun des dossiers, se trouve la liste des postes appartenant au domaine ou groupe de travail, mais qui n'appartiennent pas à la structure des groupes d'administration. Dès qu'un ordinateur est intégré à un quelconque, les informations qui le concernent sont aussitôt supprimées. Dès qu'un ordinateur est exclu du groupe d'administration, les informations qui le concernent apparaissent à nouveau dans le dossier correspondant du nœud **Ordinateurs non définis** / **Domaines**.

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

La représentation des ordinateurs dans le dossier **Plages IP** repose sur la structure des sous-réseaux IP créés dans le réseau. La structure du dossier **Plages IP** peut être composée par l'administrateur par création des sous-réseaux IP et par modification des paramètres existants.

Seules les plages d'adresses IP contenant le Serveur d'administration sont affichées par défaut en tant que sous-réseaux IP.

Le panneau des tâches du nœud **Ordinateurs non définis** contient les liens qui mènent à la configuration des paramètres et à la consultation du contenu des sous-dossiers.

Le contenu de chacun des dossiers **Domaines**, **Active Directory** ou **Plages IP** est présenté dans le panneau des résultats sous forme de tableaux. La liste complète des colonnes du panneau des résultats pour chaque objet de la Console d'administration est reprise dans l'aide. S'il s'agit d'une structure à plusieurs niveaux, c.-à-d. s'il y a des sous-dossiers, ceux-ci figurent dans l'arborescence de la console. Les éléments finaux de la hiérarchie (les postes clients) ne sont pas représentés dans l'arborescence de la console.

La création du groupe **Ordinateurs non définis** et son maintien à jour sont réalisés via le Serveur d'administration. Conformément aux paramètres définis, il sonde le réseau de l'entreprise à intervalles réguliers afin d'identifier les nouveaux ordinateurs ajoutés ou la déconnexion des anciens.

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

- *Sondage du réseau Windows*. Il existe deux types de sondage : rapide et complet. Lors du sondage rapide, seule la liste des noms NetBIOS des hôtes connectés aux domaines et groupes de travail du réseau sera actualisée. Lors du sondage complet, des informations complémentaires sont obtenues : système d'exploitation, adresse IP, nom DNS, etc.

  Pour consulter ou modifier les paramètres de sondage du réseau Windows, cliquez sur le lien **Configurer** situé dans le groupe **Balayage de l'environnement de réseau** du panneau des tâches du nœud **Ordinateurs non définis**.

- *Sondage du sous-réseau 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 à l'intervalle.

  Pour consulter ou modifier les paramètres de sondage des sous-réseaux IP, cliquez sur le lien **Configurer** situé dans le groupe **Balayage des sous-réseaux IP** du panneau des tâches du nœud **Ordinateurs non définis**.

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

  Pour consulter et modifier le sondage des groupes Active Directory, cliquez sur le lien **Configurer** situé dans le groupe **Balayage d'Active Directory** dans le panneau des tâches du nœud **Ordinateurs non définis**.

Sur la base des informations obtenues et des données relatives à la structure du réseau informatique, le Serveur d'administration actualise le contenu des dossiers du nœud **Ordinateurs non définis**. Sachez que les ordinateurs découverts dans le réseau peuvent être automatiquement inclus dans certains groupes d'administration. Il est possible de désactiver le sondage des ordinateurs repris dans les dossiers du nœud **Ordinateurs non définis**.

Les dossiers du nœud **Ordinateurs non définis** du Serveur d'administration principal reprennent, entre autres, les ordinateurs faisant partie du réseau informatique, auquel appartient le Serveur d'administration secondaire.

ASSISTANT DE CONFIGURATION INITIALE

L'application Kaspersky Administration Kit 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. L'Assistant de configuration initiale permettra de créer :

- les licences, que vous pouvez diffuser automatiquement sur les ordinateurs dans les groupes administratifs, en cochant la case dans le champ du même nom ;
- les paramètres de diffusion des notifications par courrier électronique et via NET SEND sur les événements survenus pendant l'utilisation du Serveur d'administration ainsi que pendant l'utilisation de toutes les autres applications de Kaspersky Lab. (Afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les ordinateurs le Messenger doit être lancé) ;
- les stratégies et les tâches du niveau le plus haut de la hiérarchie pour Kaspersky Anti-Virus for Windows Workstations et Windows Servers 6.0 MP4 sont créées, ainsi que les tâches du Serveur d'administration : récupération des mises à jour et copie de sauvegarde des données.

  Les stratégies pour Kaspersky Anti-Virus for Windows Workstations 6.0 MP4 ne seront pas créées, si le dossier **Ordinateurs administrés** contient déjà des stratégies pour ces applications. Si les tâches de groupe pour le groupe **Ordinateurs administrés** et les tâches de mise à jour et de copie de sauvegarde du Serveur d'administration portant le même nom ont déjà été créées, elles ne seront pas non plus créées.

L'invitation à lancer l'Assistant de configuration initiale est affichée lors de la première connexion au Serveur d'administration après son installation. A la fin du travail de l'Assistant, l'application vous propose de lancer l'Assistant d'installation à distance.

CREATION, CONSULTATION ET MODIFICATION DE LA STRUCTURE DES GROUPES D'ADMINISTRATION

Structure des groupes d'administration : la hiérarchie des Serveurs d'administration secondaires, ainsi que la liste et la composition des groupes d'administration sont définies à cette étape du projet. La création des groupes d'administration a lieu dans la fenêtre principale de l'application Kaspersky Administration Kit dans le nœud spécial **Ordinateurs administrés** (cf. ill. ci-après) par le biais de la création d'une hiérarchie de groupes et l'ajout dans ceux-ci des postes clients et des Serveurs d'administration secondaires.

Directement après l'installation de Kaspersky Administration Kit, le dossier **Ordinateurs administrés** ne contient aucun autre objet, les dossiers **Serveurs d'administration**, **Stratégies**, **Tâches de groupe** et **Postes clients** sont vides. Lorsque l'administrateur met en place les structures des groupes d'administration, des postes clients et des sous-groupes peuvent être ajoutés au dossier **Ordinateurs administrés**.

Les groupes d'administration se présentent sous forme de dossiers. Chaque groupe possède une structure similaire à celle du nœud **Ordinateurs administrés** :

- lors de la création de chaque groupe, les sous-dossiers **Serveurs d'administration**, **Stratégies**, **Tâches de groupe** et **Postes clients** sont créés automatiquement pour la conservation et l'utilisation des Serveurs d'administration secondaires, des stratégies et des tâches du groupe sélectionné ;
- lorsqu'un poste client est intégré à un groupe, les informations à son sujet sont reprises dans un tableau sur le panneau des résultats du sous-dossier **Postes clients** ;
- lorsque des grappes ou des massifs de serveurs sont ajoutés au groupe, les informations à leur sujet sont reprises dans un tableau dans le panneau des résultats du sous-dossier **Grappes et matrices de serveurs** ;

- lorsqu'un sous-groupe est ajouté, le dossier proposant une structure identique est créé.

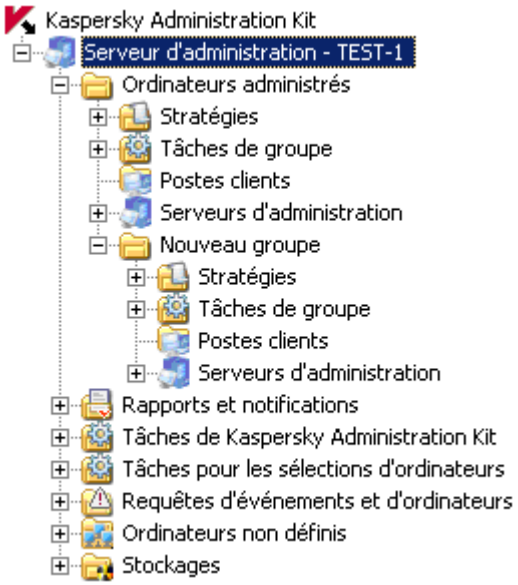


Illustration 11. Affichage de la structure des dossiers du Serveur d'administration

Lorsqu'un dossier est sélectionné dans l'arborescence de la console, son contenu est repris dans le panneau des résultats. La liste complète des colonnes du panneau des résultats pour chaque objet de la Console d'administration est reprise dans l'aide.

Les manipulations sur les objets du dossier **Ordinateurs administrés** s'opèrent à l'aide des commandes du menu contextuel (cf. section "Menu contextuel" à la page 34) et des liens du panneau des tâches.

Si la structure des groupes d'administration est identique à la structure des domaines et des groupes de travail du réseau Windows, vous pouvez utiliser l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale" à la page 39).

Afin de créer manuellement la structure construite, procédez comme suit :

1. Connectez-vous au Serveur d'administration nécessaire.
2. Organisez la hiérarchie des groupes en créant les sous-dossiers.
3. Ajoutez les postes clients au groupe.
4. Ajoutez les Serveurs d'administration secondaires.

La structure des groupes d'administration est illustrée dans le dossier **Ordinateurs administrés**. Vous pouvez obtenir des informations sur chacun des objets qui en fait partie, qu'il s'agisse des serveurs secondaires, des groupes ou des postes clients. Les données proposées indiquent la date de la création de l'objet et la date de la modification la plus récente de ses paramètres (cf. ill. ci-après). Vous pouvez également consulter et modifier les paramètres de l'interaction avec les objets (Serveur secondaire, poste client ou tous les postes clients du groupe) et le Serveur d'administration.

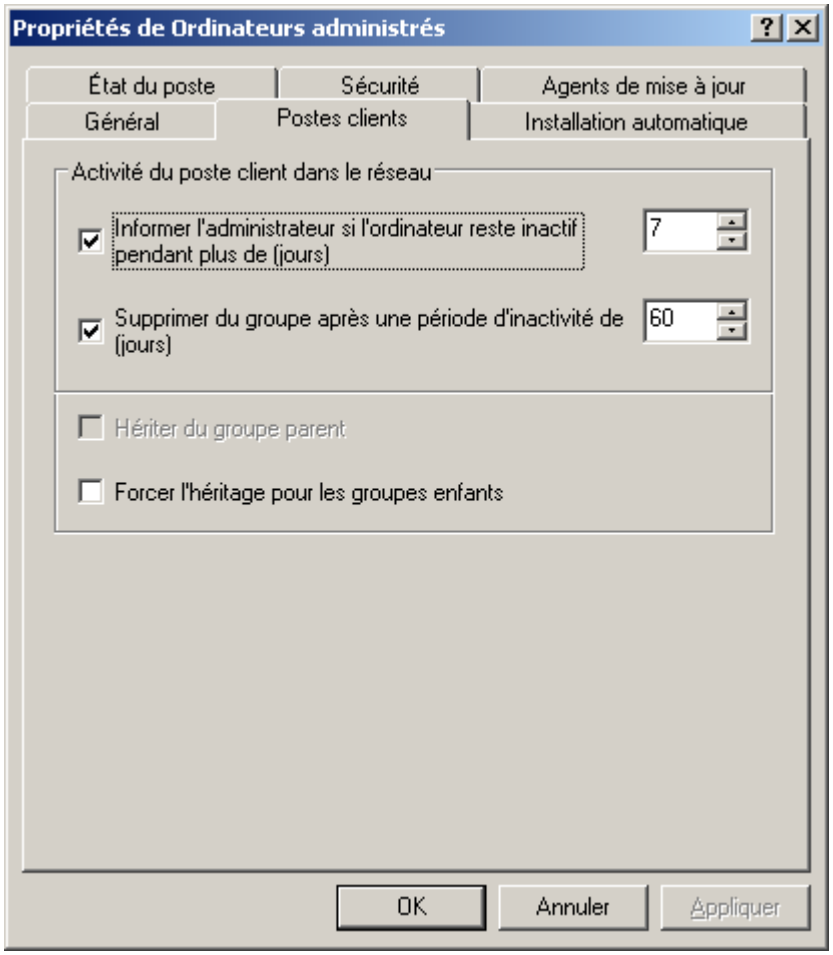


Illustration 12. Affichage des propriétés du groupe

Pour obtenir des informations sur des postes clients en particulier, vous pouvez utiliser la fonction de recherche de postes (cf. section "Recherche d'un poste" à la page 77) dans le réseau de l'entreprise sur la base de critères définis. La recherche peut être réalisée sur la base d'informations relatives aux Serveurs d'administration secondaires. Pour rechercher les informations relatives à des ordinateurs dans un dossier en particulier de l'arborescence de la console, pour les enregistrer et pour les afficher, utilisez la fonction de création de sélections (cf. section "Sélections d'ordinateurs" à la page 79).

En cas de modification de la configuration du réseau informatique de l'entreprise, il faut introduire opportunément les modifications correspondantes dans la structure des groupes d'administration. Vous pouvez :

- ajouter à la composition d'un groupe d'administration le nombre aléatoire de groupes de n'importe quel niveau (les Serveurs d'administration secondaires et les sous-groupes qui forment le niveau hiérarchique suivant peuvent être ajoutés au groupe) ;
- Définir les applications de Kaspersky Lab qui seront installées automatiquement sur tout nouveau poste client ajouté au groupe ;

  Pour activer l'installation automatique des applications de Kaspersky Lab sur des ordinateurs sous MS Windows 98 / ME nouveaux sur le réseau, il faut installer sur ces derniers l'outil Agent d'administration.

- ajouter au groupe des postes clients ;

- modifier la hiérarchie des objets des groupes d'administration en déplaçant des postes clients individuels ou des groupes entiers dans d'autres groupes ;
- supprimer d'un groupe les sous-groupes et les postes clients ;
- ajouter des Serveurs d'administration secondaires dans le but de réduire la charge sur le Serveur principal, de réduire le trafic interne et d'accroître la fiabilité du système d'administration à distance ;
- déplacer les postes clients des groupes d'administration d'un Serveur vers les groupes d'un autre.

GROUPES

Kaspersky Administration Kit offre la possibilité de créer ses propres groupes. Pour ajouter un nouveau groupe, cliquez sur le lien **Créer un sous-groupe** situé dans le panneau des résultats. Un nouveau dossier portant le nom défini apparaît dans le groupe que vous avez sélectionné dans le nœud **Ordinateurs administrés** (cf. ill. ci-après) de l'arborescence de la console. Les sous-dossiers sont créés automatiquement dans le dossier :

- **Stratégies** ;
- **Tâches de groupe** ;
- **Postes clients** ;
- **Serveurs d'administration**.

> Le dossier **Serveurs d'administration** s'affichera dans le dossier créé, si la case **Afficher les Serveurs d'administration secondaires** est cochée dans les paramètres de l'interface.

Les dossiers sont remplis lors de la définition des stratégies du groupe, lors de la création de tâches de groupe ou de Serveurs secondaires.

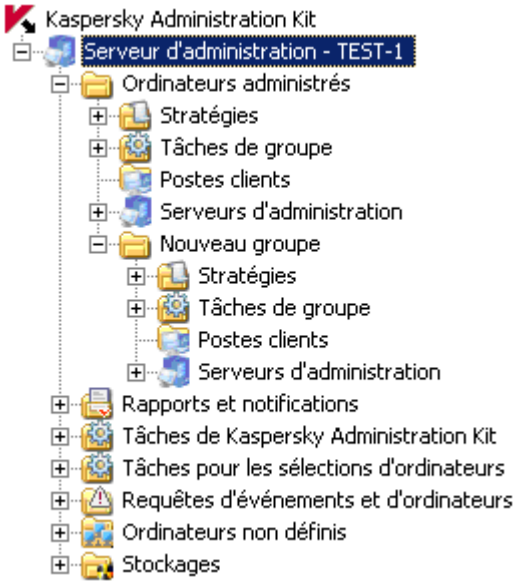


Illustration 13. Affichage de la structure des dossiers du Serveur d'administration

Les groupes peuvent reprendre les postes clients et les sous-groupes ajoutés formant le niveau hiérarchique suivant. Il est possible de configurer la représentation des stratégies et des tâches de groupe héritées dans les sous-groupes.

Vous pouvez également définir les applications de Kaspersky Lab qui seront installées automatiquement sur tout nouveau poste client ajouté au groupe.

Pour activer l'installation automatique des applications de Kaspersky Lab sur des ordinateurs sous MS Windows 98 / ME nouveaux sur le réseau, il faut installer sur ces derniers l'outil Agent d'administration.

Vous pouvez ensuite renommer le groupe, le déplacer vers un autre groupe ou le supprimer.

Le groupe 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 déplacement des groupes est exécuté à l'aide des commandes traditionnelles **Couper / Coller** du menu contextuel ou des commandes similaires du menu **Action**. Vous pouvez également déplacer les groupes à l'aide de la souris.

Lors du déplacement des groupes, il convient de respecter la règle de l'unicité des noms de groupe au sein d'un même niveau hiérarchique. Pour résoudre les conflits des noms, il faut modifier le nom avant de le déplacer. Si la règle de l'unicité des noms n'est pas respectée, le suffixe **_1**, **_2**, etc. sera ajouté au nom.

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

Un groupe pourra être supprimé d'un dossier du Serveur d'administration s'il ne contient pas de Serveurs d'administration secondaires, de sous-groupes ou de postes clients, et si aucune stratégie ou tâche de groupe n'a été composée. Pour supprimer un groupe, sélectionnez-le puis choisissez la commande **Supprimer** du menu contextuel ou la commande similaire du menu **Action**.

POSTES CLIENTS

L'ajout d'un poste client à un groupe permet de lui appliquer les stratégies et les tâches créées dans le groupe. Pour ajouter des postes clients à un groupe, cliquez sur le lien **Ajouter un ordinateur** situé dans le panneau des tâches du groupe, au sein duquel l'ordinateur est ajouté. Cette action lance un Assistant. Si l'opération réussit, les ordinateurs sont ajoutés au groupe et figurent dans le panneau des résultats du dossier **Postes clients** sous les noms choisis pour eux par le Serveur d'administration (cf. ill. ci-après). Si pour une raison quelconque le Serveur d'administration n'a pas découvert le poste client, il faut y installer l'Agent d'administration et se connecter au Serveur d'administration. Le Serveur d'administration placera cet ordinateur dans le nœud **Ordinateurs non définis**, d'où vous allez pouvoir le déplacer dans le groupe qu'il vous est nécessaire.

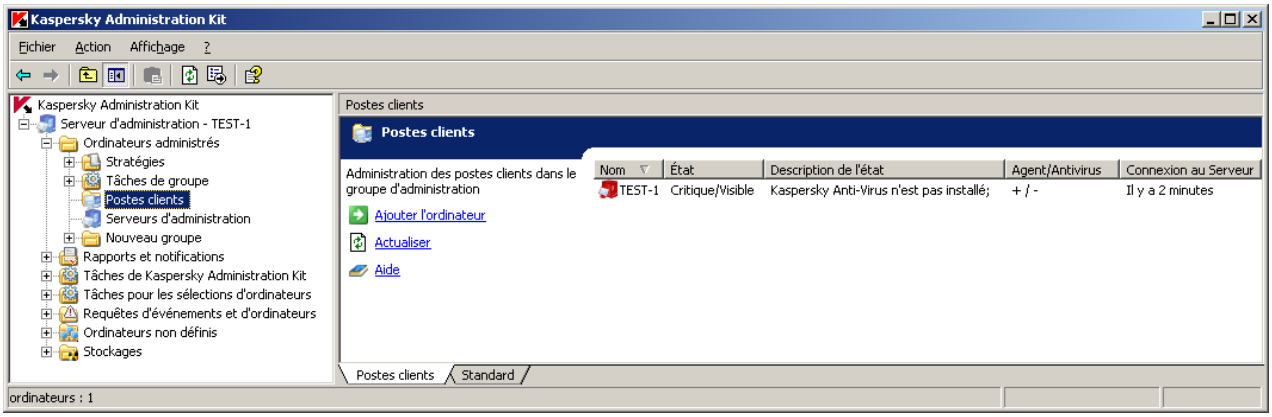


Illustration 14. Postes clients dans le groupe

Une icône caractérisant l'état du poste client figure à côté du nom du poste dans le panneau des résultats. La liste des icônes et des états correspondant figure dans l'annexe de l'aide.

L'ajout de postes clients aux groupes d'administration peut être configuré de telle sorte, que le Serveur d'administration inclue automatiquement tous les nouveaux postes découverts sur le réseau dans un groupe d'administration déterminé. Il faut pour ce faire définir les paramètres correspondant dans les propriétés du Serveur d'administration (cf. ill. ci-après).

Pour ajouter un ordinateur à un groupe, faites glisser l'icône correspondante du dossier **Ordinateurs non définis** vers le dossier cible du groupe administratif requis, à l'intérieur de la fenêtre principale de Kaspersky Administration Kit.

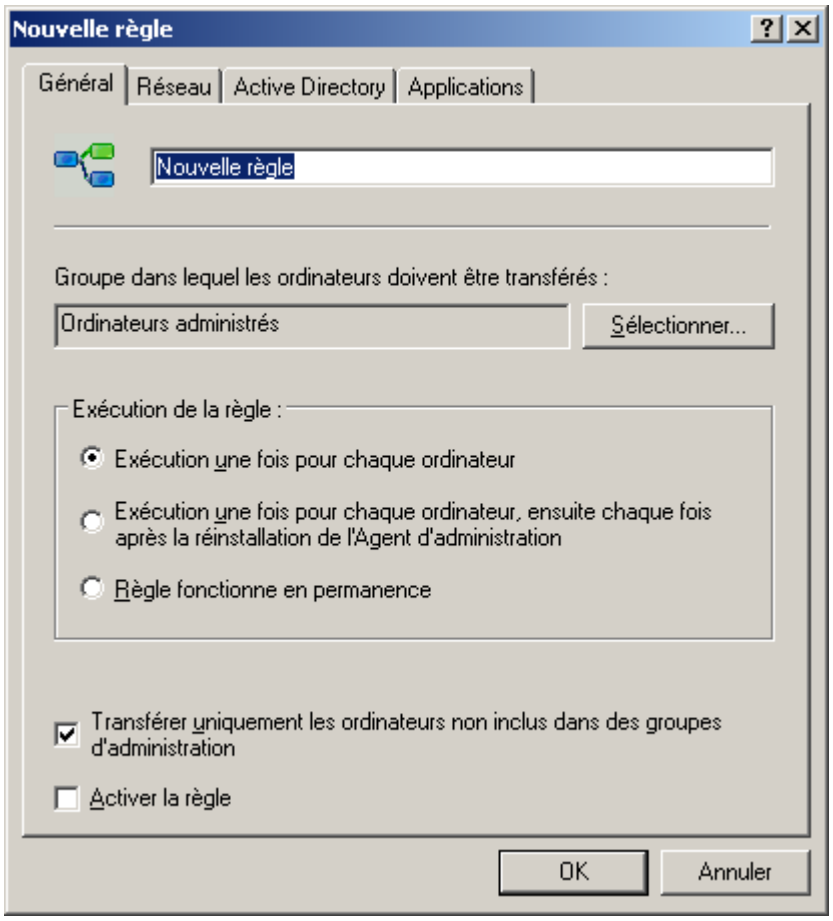


Illustration 15. Configuration de l'ajout automatique des nouveaux ordinateurs dans le groupe

Vous pouvez déplacer les postes clients d'un groupe vers un autre ou les exclure de la composition de groupes d'administration à l'aide des commandes standard **Couper / Coller** et **Supprimer** du menu contextuel ou des options similaires du menu **Action**. Les ordinateurs supprimés d'un groupe sont déplacés dans le nœud **Ordinateurs non définis**. Vous pouvez également faire glisser les ordinateurs vers leur emplacement cible avec votre souris.

Il est possible de déplacer les postes clients depuis les groupes d'administration d'un Serveur d'administration vers les groupes d'un autre Serveur. Par exemple, en cas d'ajout d'un Serveur d'administration secondaire, vous pouvez déplacer les postes clients depuis les groupes d'administration du Serveur principal vers les groupes du Serveur secondaire. Il faut pour ce faire connecter les postes clients au nouveau Serveur d'administration.

Vous pouvez connecter un poste client à un autre Serveur d'administration localement depuis un poste client. Cette opération est exécutée à l'aide de l'utilitaire klmover.exe inclus dans la distribution de l'Agent d'administration. Cet utilitaire s'installe dans la racine du dossier d'installation du composant après l'installation de l'Agent d'administration.

La connexion d'un poste client à un autre Serveur d'administration s'opère à l'aide de la création et du lancement de la tâche **changement de Serveur d'administration**. Il est possible de déplacer des ordinateurs individuels en créant une tâche pour les sélections d'ordinateurs ou pour tous les postes clients d'un groupe d'administration défini à l'aide d'une tâche de groupe. Suite à l'exécution réussie de la tâche de changement de Serveur d'administration, les postes clients pour lesquels la tâche avait été créée sont déconnectés de l'ancien Serveur d'administration et apparaissent dans le nœud **Ordinateurs non définis** du nouveau Serveur. Le déplacement des ordinateurs vers les groupes d'administration du nouveau Serveur depuis le groupe de l'ancien Serveur s'opère manuellement via la Console d'administration.

SERVEURS D'ADMINISTRATION SECONDAIRES

Les opérations suivantes peuvent être réalisées à l'aide de la hiérarchie des Serveurs pour tous les Serveurs d'administration secondaires et les postes clients qui y sont connectés depuis le Serveur d'administration principal :

- création et diffusion de *stratégies pour les applications* ;
- rédaction et diffusion de *tâches de groupe* (y compris les tâches d'installation à distance) ;
- diffusion des *mises à jour* et des *paquets d'installation* récupérés par le Serveur principal ;
- création de *rapports* présentant les informations sur tous les Serveurs d'administration secondaires.

Les stratégies et les tâches héritées du Serveur d'administration principal ne peuvent pas être modifiées sur le Serveur secondaire.

Pour ajouter un Serveur secondaire, utilisez l'option **Créer** / **Serveur d'administration** pour l'objet du Serveur d'administration dans le groupe qui vous intéresse. Cette action entraîne le lancement de l'Assistant d'ajout de serveur secondaire. Cet assistant exécute les opérations suivantes :

- ajout du Serveur d'administration secondaire ;
- connexion de la Console d'administration au Serveur secondaire ;
- configuration des paramètres de connexion au Serveur principal ;
- ajout des informations relatives au Serveur secondaire dans la base de données du Serveur d'administration principal.

Les étapes de connexion et de configuration ne sont pas obligatoires. Dans ce cas, il faudra les exécuter manuellement : connectez-vous au Serveur qui deviendra le Serveur secondaire via la Console d'administration et définissez les paramètres de connexion au Serveur principal (cf. ill. ci-après).

Si l'ajout du Serveur secondaire réussit, l'icône et le nom du Serveur apparaissent dans le dossier **Serveurs d'administration** du groupe correspondant.

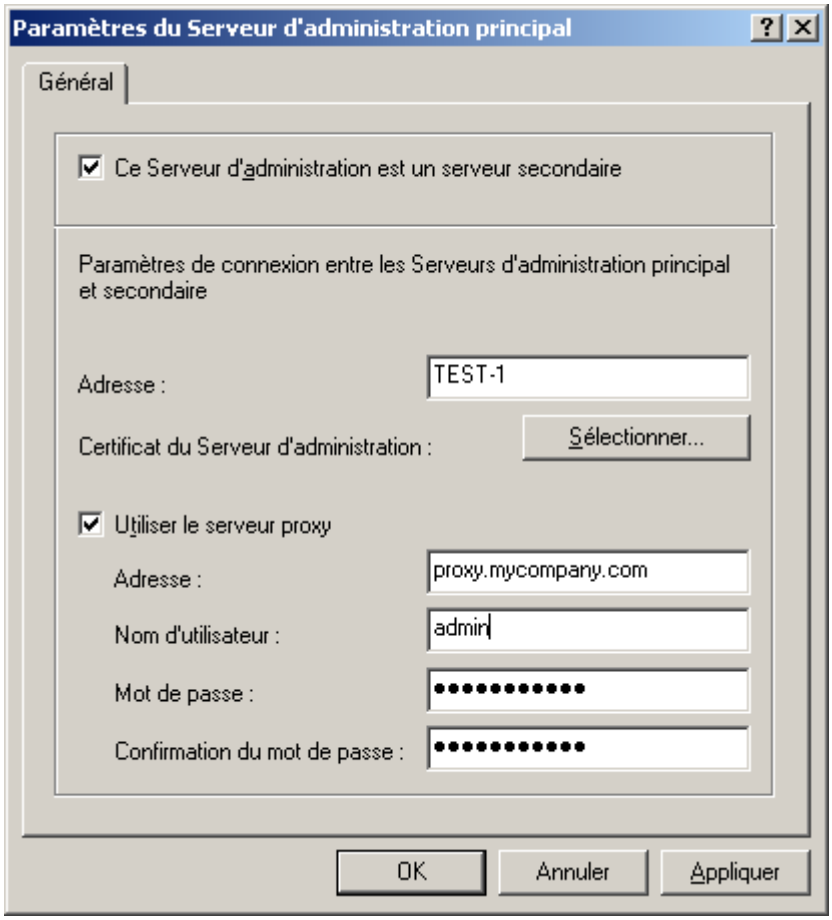


Illustration 16. Configuration dans le Serveur principal des infos du Serveur secondaire

Il est possible de manipuler les groupes d'administration du Serveur d'administration secondaire via le nœud **Serveurs d'administration** du Serveur principal ou directement en ajoutant le Serveur dans l'arborescence de la console en guise de nouveau Serveur d'administration.

Le Serveur secondaire est un Serveur d'administration à part entière et exécute toutes les fonctions du Serveur d'administration dans le cadre de ses propres groupes d'administration.

Le Serveur d'administration secondaire hérite des tâches de groupe et des stratégies du groupe du Serveur d'administration principal, dans lequel il se trouve. Les stratégies et les tâches héritées sont représentées sur le Serveur secondaire de manière suivante :

- L'icône (icône normale de la stratégie :) apparaît à côté du nom de la stratégie obtenue du Serveur d'administration principal.
- Les valeurs des paramètres des stratégies héritées ne peuvent pas être modifiées sur le Serveur secondaire.
- Les paramètres dont la modification est impossible dans la stratégie héritée (icône) ne peuvent être modifiés dans toutes les stratégies de l'application sur le Serveur secondaire et utilisent les valeurs définies dans la stratégie héritée.
- Les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie héritée, peuvent être changées (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page 18) dans les stratégies du Serveur secondaire (icône). Si le paramètre n'était pas " verrouillé " dans la stratégie du Serveur secondaire, il pourra également être modifié (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page 18) dans les paramètres de l'application et dans les paramètres de la tâche.

- L'icône  (icône normal de la stratégie : ) apparaît à côté du nom de la tâche de groupe obtenue du Serveur d'administration principal.

Les tâches d'installation à distance pour la sélection d'ordinateurs ne sont pas transmises aux Serveurs secondaires. Le transfert des tâches de groupe est configuré dans les propriétés de la tâche.

La mise à jour des postes clients du Serveur d'administration secondaire (cf. section "Mise à jour des Serveurs secondaires et de leurs postes clients" à la page 63) peut être configurée de telle sorte que dès la récupération des mises à jour par le Serveur principal, une tâche de récupération des mises à jour par le Serveur secondaire sera lancée automatiquement. Après son exécution réussie, les tâches de mise à jour des applications sur les postes clients du Serveur secondaire seront exécutées.

ADMINISTRATION A DISTANCE DES APPLICATIONS

Kaspersky Administration Kit prend uniquement en charge l'administration des applications dont la distribution contient un composant spécial baptisé module externe d'administration de l'application.

L'administration des applications s'effectue par deux moyens :

- l'administration des paramètres de l'application via la définition de stratégies (cf. section "Administration des stratégies" à la page 48) et la modification des paramètres locaux (cf. section "Paramètres locaux de l'application" à la page 52) des applications ;
- la création et l'exécution de tâches (cf. section "Administration du fonctionnement de l'application" à la page 52).

DANS CETTE SECTION

ADMINISTRATION DES STRATEGIES

La création de stratégies 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 créer une stratégie, cliquez sur le lien **Nouvelle stratégie** situé dans le panneau des tâches du groupe, pour lequel vous créez la stratégie. Lors de la création de la stratégie, une sélection minimum de paramètres est configurée, sans laquelle l'application ne fonctionnera pas. Tous les autres paramètres prendront les valeurs par défaut, correspondant à celles définies lors de l'installation locale de l'application. Pour créer rapidement une stratégie pour certaines applications, cliquez sur les liens, **Créer une nouvelle stratégie de Kaspersky Anti-Virus pour Windows Workstations** et **Créer une nouvelle stratégie de Kaspersky Anti-Virus pour Windows Servers** dans le panneau des tâches.

Les stratégies composées pour les applications dans le groupe apparaissent dans l'arborescence de la console dans le dossier correspondant. Une icône représentant le statut de la stratégie apparaît à côté du nom de celle-ci. La liste des icônes et leur signification figure dans l'aide.

Vous pourrez modifier les valeurs des paramètres, interdire la modification de certains d'entre eux dans les stratégies des sous-groupes et dans les paramètres de l'application (cf. ill. ci-après).

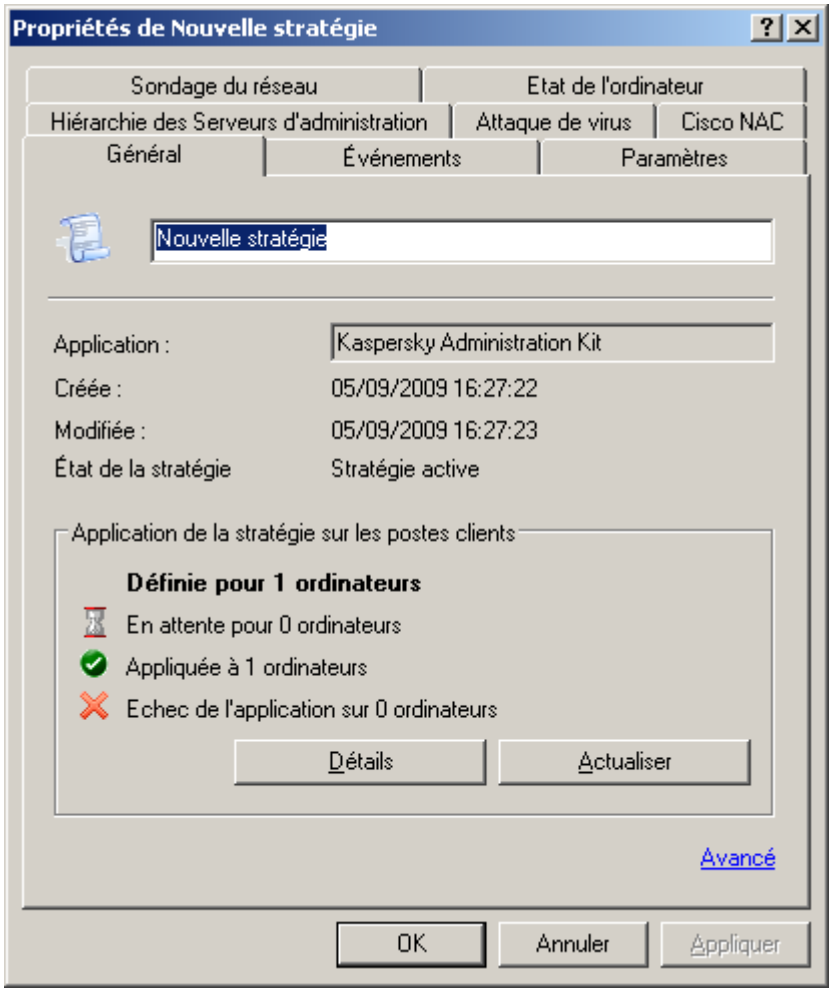


Illustration 17. Fenêtre des propriétés de la stratégie

Les paramètres de la stratégie dont les valeurs peuvent être verrouillées sont accompagnés de l'icône . Pour verrouiller, cliquez sur l'icône avec le bouton gauche de la souris. L'icône deviendra . Ces paramètres ne pourront pas être modifiés dans la configuration de l'application, des tâches ou des stratégies des sous-groupes et des Serveurs d'administration secondaires. Il est toutefois possible de lever l'interdiction de modification des paramètres pour les stratégies héritées.

La stratégie possède la priorité sur les paramètres locaux uniquement dans le cas d'interdiction de modification des paramètres (verrouillage).

Une fois que la stratégie a été créée, elle est ajoutée au dossier **Stratégies** (cf. ill. ci-après) du groupe correspondant, apparaît dans l'arborescence de la console et est diffusée à tous les sous-groupes du groupe et aux Serveurs d'administration secondaires en qualité de stratégie héritée.

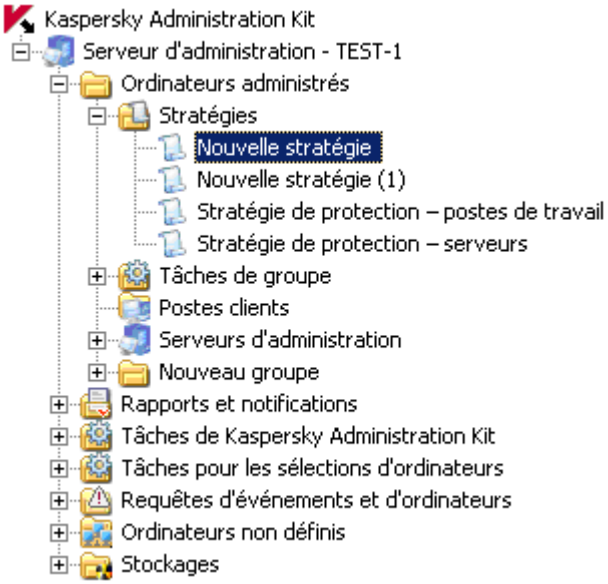


Illustration 18. Affichage de la liste des stratégies

Les stratégies ainsi créées peuvent être supprimées, copiées, exportées ou importées d'un groupe vers un autre à l'aide des commandes du menu contextuel de la stratégie sélectionnée dans le panneau des résultats. Pour importer une stratégie depuis un fichier extérieur, cliquez sur le lien **Importer la stratégie du fichier** situé dans le panneau des tâches du nœud **Stratégies**. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier doté de l'extension *.klp qui contient les paramètres de la stratégie.

Il est possible de définir plusieurs stratégies de groupe pour chaque application. Toutefois, il ne peut y avoir qu'une seule stratégie active. Dans la configuration de cette stratégie, le paramètre **Stratégie active** doit être sélectionné.

L'activation d'une stratégie peut se produire suite au déclenchement de l'événement **Attaque de virus**. Dans ce cas, le retour à la stratégie précédente s'opère manuellement.

Il est également possible de créer une stratégie pour les utilisateurs nomades qui entrera en vigueur dès que l'ordinateur est déconnecté du Serveur d'administration. Vous pouvez configurer les critères d'activation de la stratégie pour les utilisateurs nomades à l'aide des profils de l'Agent d'administration.

Un ordinateur est considéré comme déconnecté du Serveur d'administration après trois tentatives de connexion échouées. L'intervalle d'attente entre les tentatives est défini dans les paramètres de l'Agent d'administration via le champ **Période de synchronisation (min)** et est égal à 15 minutes par défaut.

Les résultats de l'application de la stratégie sont visibles via la Console d'administration dans la fenêtre de configuration des paramètres (cf. ill. ci-après).

La modification des paramètres locaux s'opère automatiquement conformément aux paramètres de la stratégie lors de la première application de la stratégie sur le poste client, c-à-d. :

- lors de l'ajout d'un client dans le champ d'application de la stratégie ;
- lors de l'activation d'une stratégie ;
- lors de l'installation sur un client d'une application antivirus, pour laquelle une stratégie a été établie.

Après la suppression d'une stratégie ou la fin de ses effets, l'application continue de fonctionner selon les paramètres définis dans la stratégie. Ceux-ci pourront être modifiés manuellement.

L'application d'une stratégie se déroule de 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) maintiennent les anciennes valeurs. Le lancement suivant sera réalisé avec des paramètres modifiés. Les valeurs des paramètres de fonctionnement de l'application définis après l'application de la stratégie peuvent être affichées via la Console d'administration dans la fenêtre des propriétés d'un poste client concret.

Dans 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. Ensuite, les Serveurs d'administration secondaires modifient comme il se doit leurs stratégies et les diffusent vers les postes clients connectés.

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 de configuration de la stratégie sur le Serveur d'administration principal.

Il est possible également de consulter les résultats de la diffusion de la stratégie sur les postes clients dans la fenêtre des propriétés de la stratégie du Serveur d'administration secondaire après s'y être connecté.

Vous trouverez une description détaillée de la configuration des stratégies pour chacune des applications de Kaspersky Lab dans les documentations respectives. La configuration d'une stratégie pour l'Agent d'administration et le Serveur d'administration est décrite dans l'aide de Kaspersky Administration Kit.

PARAMETRES LOCAUX DE L'APPLICATION

Le système d'administration Kaspersky Administration Kit permet d'administrer à distance les paramètres locaux des applications sur les postes clients via la Console d'administration (cf. ill. ci-après). Vous pouvez définir les valeurs individuelles des paramètres de fonctionnement de l'application pour chaque poste client du groupe. Vous pouvez uniquement modifier les paramètres dont la modification n'est pas interdite par une stratégie de groupe pour cette application : le paramètre n'est pas "verrouillé" dans la stratégie.

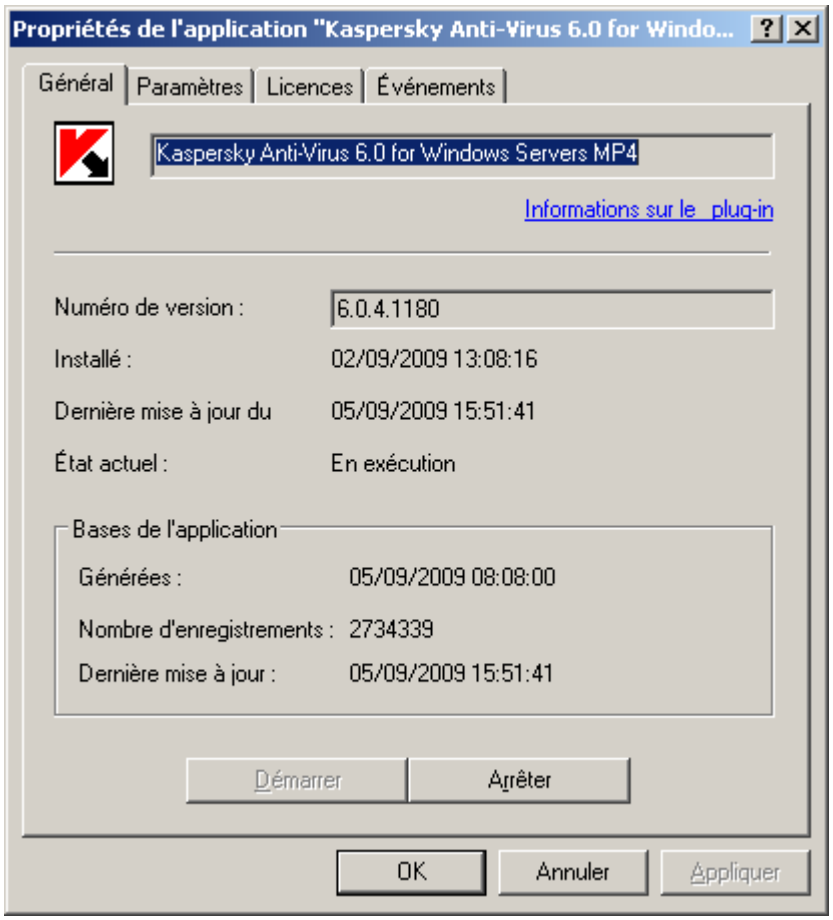


*Illustration 19. Affichage des propriétés d'un poste client. Onglet **Général***

La configuration des paramètres locaux s'opère séparément pour chaque poste client dans la fenêtre **Paramètres de l'application <Nom de l'application>**. Cette fenêtre est accessible via l'onglet **Applications** de la fenêtre **Propriétés de <nom de l'ordinateur>** qui s'ouvre depuis le menu contextuel du poste client requis.

La sélection des paramètres locaux est propre à chaque application de l'éditeur Kaspersky Lab. La description détaillée est fournie dans la documentation de chacune de ces applications.

La description détaillée des paramètres de l'Agent d'administration et du Serveur d'administration figure dans l'aide de Kaspersky Administration Kit.

ADMINISTRATION DU FONCTIONNEMENT DE L'APPLICATION

L'administration du fonctionnement des applications installées sur les postes clients s'opère via la création et l'exécution de tâches qui prennent en charge les principales fonctions : installation d'applications, installation de licences, analyse des fichiers, mise à jour des bases et des modules de l'application, etc.

Les tâches créées apparaissent dans l'arborescence de la console dans le dossier correspondant. Une icône représentant le statut de la tâche apparaît à côté du nom de celle-ci. La liste des icônes et leur signification figure dans l'aide.

Kaspersky Administration Kit est compatible avec tous les types de tâches prévues dans le cadre d'une utilisation locale de l'application. Il est également possible de lancer et d'arrêter des applications à distance à l'aide des tâches d'administration correspondantes pour l'Agent d'administration. La description détaillée des types de tâches pour chaque application de Kaspersky Lab est présentée dans les manuels.

La Console d'administration permet de réaliser le lancement et l'arrêt à distance d'une application à l'aide des tâches correspondantes.

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 garantir la protection du réseau, l'administrateur peut créer le nombre de tâches différentes qu'il souhaite (sauf les tâches créées en un exemplaire) pour toutes les applications administrées via Kaspersky Administration Kit.

Par exemple, pour soumettre les postes clients qui remplissent les fonctions de poste de travail à la recherche de programmes malveillants, il faut créer une tâche d'analyse à la demande pour Kaspersky Anti-Virus for Windows Workstations.

Les fonctions d'administration des applications et les services d'opération généraux sont pris en charge par les tâches des composants de Kaspersky Administration Kit que sont le Serveur d'administration et l'Agent d'administration. Les tâches suivantes ont été définies pour ces composants :

- **Changement du Serveur d'administration** ;
- **Lancement ou arrêt de l'application** ;
- **Installation à distance de l'application** ;
- **Tâche de désinstallation à distance de l'application** ;
- **Administration du poste client** ;
- **Message pour l'utilisateur** ;
- **Diffusion du paquet d'installation** ;
- **Envoi du rapport** ;
- **Sauvegarde des données du Serveur d'administration** ;
- **Téléchargement des mises à jour dans le référentiel**.

La création et le lancement des tâches des types énumérés ont certaines particularités. La description détaillée de l'utilisation de celles-ci figure dans l'aide de Kaspersky Administration Kit.

Pour ces types de tâches, vous pouvez créer des tâches de groupe et des tâches locales, des tâches pour une sélection d'ordinateurs et des tâches pour Kaspersky Administration Kit.

Pour une tâche d'installation à distance, il est possible de créer des tâches de groupe et des tâches pour des sélections d'ordinateurs. Pour les tâches de récupération des mises à jour, de création des copies de sauvegarde et de diffusion des rapports, il est possible de créer uniquement des tâches du Serveur d'administration.

Les tâches Récupération des mises à jour et Création d'une copie de sauvegarde du Serveur d'administration peuvent être créées uniquement en un exemplaire. Elles sont créées et exécutées uniquement pour un ordinateur, à savoir l'ordinateur du Serveur d'administration.

Les tâches de groupe sont placées dans les sous-dossiers **Tâches de groupe** des groupes correspondant (cf. ill. ci-après). Pour créer une tâche de groupe, ouvrez le dossier **Tâches de groupe** du groupe, pour lequel vous créez la tâche dans l'arborescence de la console, et cliquez sur le lien **Nouvelle tâche** situé dans le panneau des tâches.

Les tâches pour une sélection d'ordinateurs sont conservées dans le nœud **Tâches pour les sélections d'ordinateurs** de l'arborescence de la console. Pour créer une telle tâche, sélectionnez le nœud **Tâches pour les sélections d'ordinateurs** dans l'arborescence de la console et cliquez sur le lien **Création d'une tâche** du panneau des tâches.

Les tâches du Serveur d'administration sont conservées dans le conteneur **Tâches de Kaspersky Administration Kit**. Pour créer une tâche du Serveur d'administration, ouvrez le nœud **Tâches de Kaspersky Administration Kit** dans l'arborescence de la console et utilisez la commande **Nouveau / Tâche**.

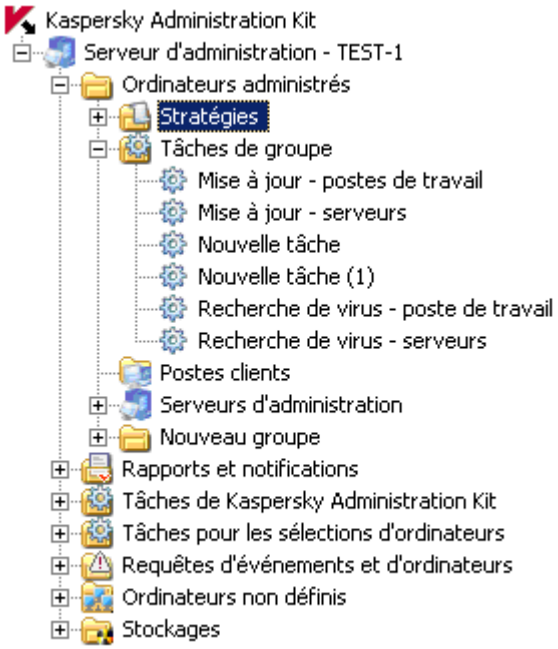


Illustration 20. Tâches de groupe

La fenêtre des propriétés d'un poste client affiche la liste des tâches locales sur celui-ci. Pour ce faire, exécutez les opérations suivantes :

1. Dans l'arborescence de la console, ouvrez le dossier **Postes clients** du groupe contenant l'ordinateur requis.

2. Sélectionnez l'ordinateur dans la liste reprise dans le panneau des résultats.

3. Ouvrez la fenêtre des propriétés de l'ordinateur à l'onglet **Tâches**, qui reprend la liste des tâches locales pour l'ordinateur sélectionné. Pour ce faire, cliquez sur le lien **Tâches** situé à gauche de la liste des ordinateurs dans le panneau des résultats ou choisissez l'option **Tâches** dans le menu contextuel de l'ordinateur sélectionné.

L'échange d'informations relatives aux tâches entre l'application locale et la base d'information de Kaspersky Administration Kit a lieu au moment de la connexion de l'Agent d'administration au Serveur. Dans ce cas, les informations relatives aux tâches créées localement sont reprises dans la base du Serveur d'administration.

Vous pouvez modifier les paramètres des tâches, suivre leur exécution, les copier, les exporter ou les importer d'un groupe dans un autre, ainsi que les supprimer à l'aide des commandes du menu contextuel et des liens du panneau des tâches.

Les paramètres de fonctionnement de l'application lors de l'exécution des tâches sur chaque poste client sont définis conformément à la stratégie de groupe (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page 18), aux paramètres de la tâche et aux paramètres de cette application sur le poste client.

La majeure partie des paramètres est définie à l'aide d'une stratégie de l'application qui exécute cette tâche. Si la modification de ces paramètres est bloquée dans la stratégie, la modification sera également impossible dans la tâche (cf. ill. ci-après).

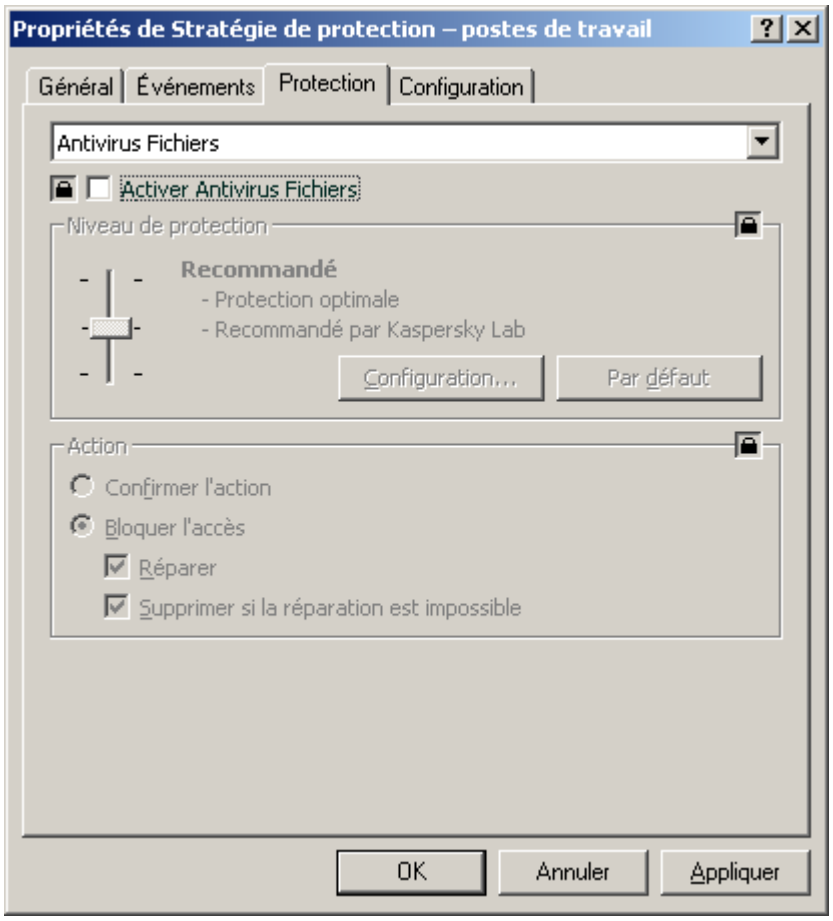


Illustration 21. Paramètres de la tâche ne pouvant pas être modifiés dans la stratégie

Toutefois, une partie des paramètres est propre à une tâche concrète : planification de l'exécution de la tâche, compte utilisateur, sous lequel la tâche est lancée, couverture d'analyse pour les tâches d'analyse à la demande, etc. Les valeurs de ces paramètres sont définies pour chaque tâche et peuvent être modifiées après la création de la tâche (cf. ill. ci-après).

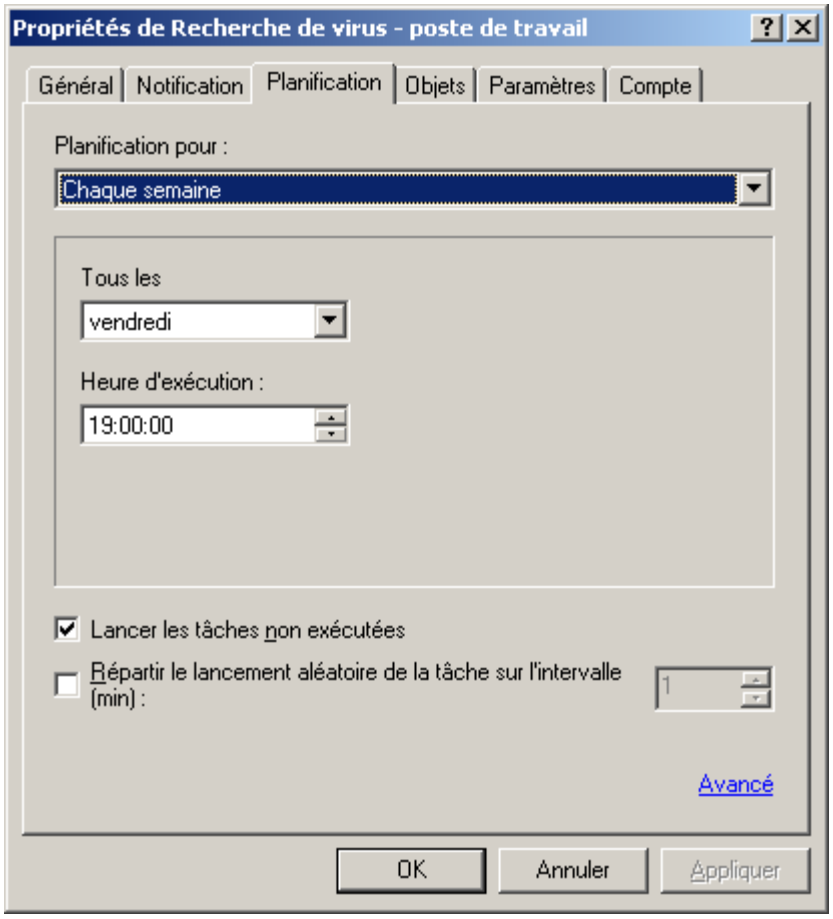


*Illustration 22. Modification des propriétés de tâche. Onglet **Planification***

Les tâches sont exécutées selon l'horaire défini. Les ordinateurs, éteints au moment où le lancement de l'application est prévu, peuvent être automatiquement démarrés à l'aide de la fonction Wake On Lan. Il suffit pour ce faire de cliquer sur le bouton **Avancé** de l'onglet **Planification** (cf. ill. ci-dessus) afin d'ouvrir la fenêtre, dans laquelle il faudra cocher la case adéquate (cf. ill. ci-après).

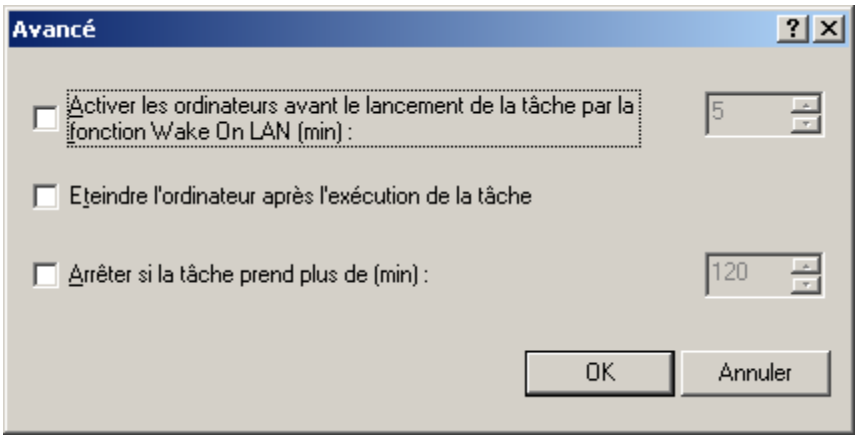


Illustration 23. Activation du démarrage automatique du système d'exploitation

Il est possible de programmer l'arrêt automatique de l'ordinateur après l'exécution de la tâche programmée.

La durée d'exécution de la tâche peut être limitée. Dans ce cas, la tâche s'arrêtera dès que l'intervalle défini dans les paramètres aura écoulé. Il est possible de désactiver le lancement des tâches programmées. La tâche n'est pas supprimée. Elle ne sera tout simplement pas exécutée.

Vous pouvez lancer une tâche, l'interrompre, la suspendre ou la reprendre à l'aide des commandes du menu contextuel ou depuis la fenêtre de consultation des paramètres de la tâche (cf. ill. ci-après). Les liens situés dans le groupe **Administration de la tâche** du panneau des résultats permettent de lancer ou d'arrêter une tâche.

Les tâches ne sont lancées sur un client que l'application correspondante est en exécution. Si l'application est désactivée, toutes les tâches courantes sont annulées.

Il est possible de suivre l'exécution d'une tâche et de consulter ses résultats dans la fenêtre des propriétés de la tâche (cf. ill. ci-après) ou dans la partie supérieure du panneau des tâches dans le groupe portant le nom de la tâche.

Les résultats d'exécution de la tâche sont enregistrés et consignés conformément aux paramètres définis dans les journaux des événements de Windows et Kaspersky Administration Kit, de façon centralisée sur le Serveur d'administration et localement sur chaque poste client. Il est aussi possible de notifier l'administrateur et autres utilisateurs des résultats. La forme et le mode de notification sont également définis via les paramètres de la tâche.

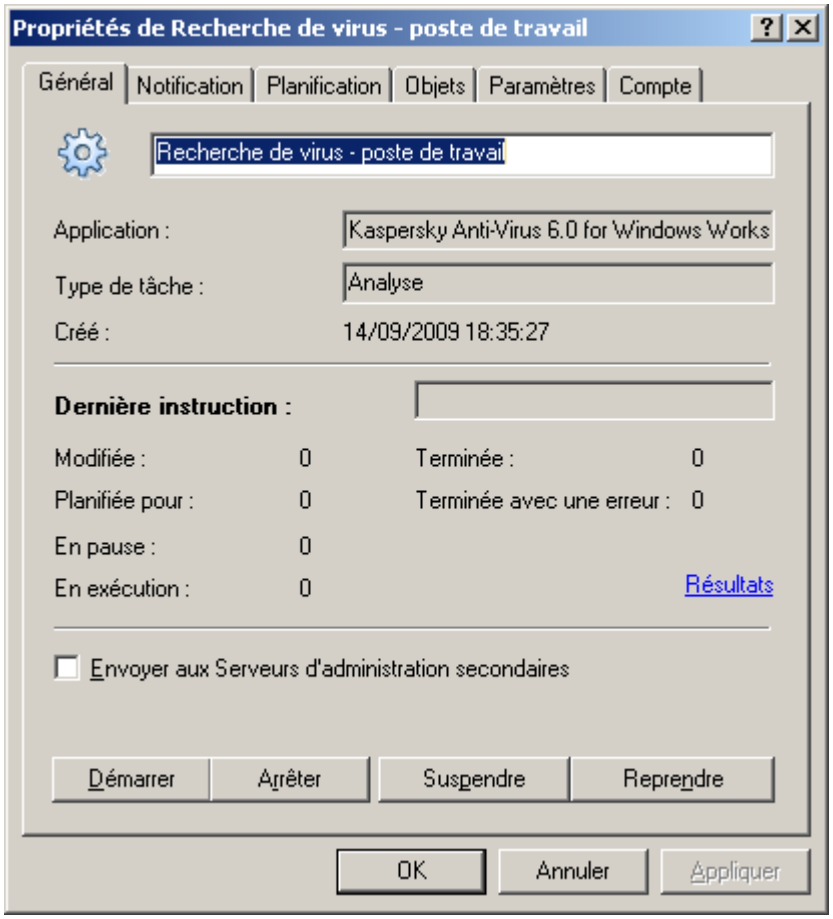


*Illustration 24. Modification des propriétés de la tâche. Onglet **Général***

Vous pouvez voir les résultats de l'exécution des tâches consignés dans le journal des événements de Kaspersky Administration Kit via le nœud **Événements** de l'arborescence de la console. Vous pouvez prendre connaissance des résultats de l'exécution de la tâche pour chaque poste client dans la fenêtre de consultation des propriétés.

Dans le cadre d'une structure hiérarchique des Serveurs d'administration, si le paramètre correspondant est activé dans les paramètres de la tâche (cf. ill. ci-dessus), les Serveurs secondaires reçoivent les tâches de groupe depuis le Serveur d'administration principal et les diffusent vers les postes clients. Les paramètres d'une tâche de groupe peuvent être modifiés sur le Serveur d'administration principal. Ensuite, les Serveurs d'administration secondaires modifient en conséquence leurs tâches de groupe et les diffusent vers les postes clients connectés.

Les résultats de la diffusion de la tâche de groupe vers les Serveurs d'administration secondaire figurent dans la fenêtre **Résultats de la tâche** de la fenêtre des propriétés de la tâche de groupe du Serveur d'administration.

De la même manière, il est possible de consulter les résultats de la diffusion de la tâche de groupe vers les postes clients dans la fenêtre des propriétés de la tâche de groupe du Serveur d'administration secondaire après s'y être connecté.

MISE A JOUR DES BASES ET DES MODULES DE L'APPLICATION

La mise à jour opportune des bases des applications utilisées lors de l'analyse des objets infectés, l'installation des mises à jour critiques des modules logiciels de l'application et l'actualisation fréquente de leur version figurent parmi les facteurs importants, qui exercent une influence sur la fiabilité de la protection antivirus.

La mise à jour des bases des applications situées sur les serveurs de mise à jour de Kaspersky Lab a lieu toutes les heures. Nous vous conseillons de réaliser les mises à jour avec la même fréquence et d'installer immédiatement toutes les mises à jour critiques des modules des applications.

Pour actualiser les bases et les modules logiciels des applications administrées via Kaspersky Administration Kit, il faut créer une tâche de téléchargement des mises à jour dans le référentiel. Quand la tâche est exécutée, les bases et les mises à jour des modules logiciels sont téléchargées depuis la source de la mise à jour conformément aux paramètres de la tâche. Les données récupérées sont stockées dans le dossier **Updates** du dossier partagé sur le Serveur d'administration et peuvent être diffusées vers les postes clients et les Serveurs d'administration secondaires automatiquement dès la fin de la mise à jour. Le dossier partagé est créé lors de l'installation du Serveur d'administration. Par défaut, le dossier partagé est le dossier **KLShare** situé dans le dossier d'installation sélectionné lors de l'installation du composant Serveur d'administration (**<Disque>:\Program Files\Kaspersky Lab\ Kaspersky Administration Kit**).

Les mises à jour sont déployées sur les postes client à l'aide des tâches de mise à jour pour les applications. La mise à jour des Serveurs secondaires s'opère à l'aide de la tâche de récupération des mises à jour par le Serveur d'administration. Ces tâches peuvent être exécutées automatiquement directement après la réception des mises à jour par le Serveur principal, quelle que soit la planification définie dans les paramètres des tâches.

L'exactitude des mises à jour peut être vérifiée avant la diffusion vers les postes clients. Il existe pour cela la fonction de vérification des mises à jour. La vérification des mises à jour prévoit de diffuser les mises à jour sur une sélection d'ordinateurs d'essai puis vers les autres postes clients, si aucune erreur n'a été détectée.

DANS CETTE SECTION

TELECHARGEMENT DES MISES A JOUR DANS LE REFERENTIEL DU SERVEUR D'ADMINISTRATION

La tâche de récupération des mises à jour par le Serveur d'administration est une tâche globale, qui existe en un seul exemplaire. Cette tâche est créée et lancée uniquement pour un ordinateur, à savoir l'ordinateur, sur lequel le composant Serveur d'administration est installé.

Si vous avez utilisé l'Assistant de configuration initiale, la tâche **Téléchargement des mises à jour dans le référentiel** est déjà créée et placée dans le nœud **Tâches de Kaspersky Administration Kit**.

Pour créer une tâche de récupération des mises à jour par le Serveur d'administration, lancez l'Assistant de création de tâche pour le nœud **Tâches de Kaspersky Administration Kit** et choisissez **Téléchargement des mises à jour dans le référentiel** (cf. ill. ci-après) en guise de type de tâche.

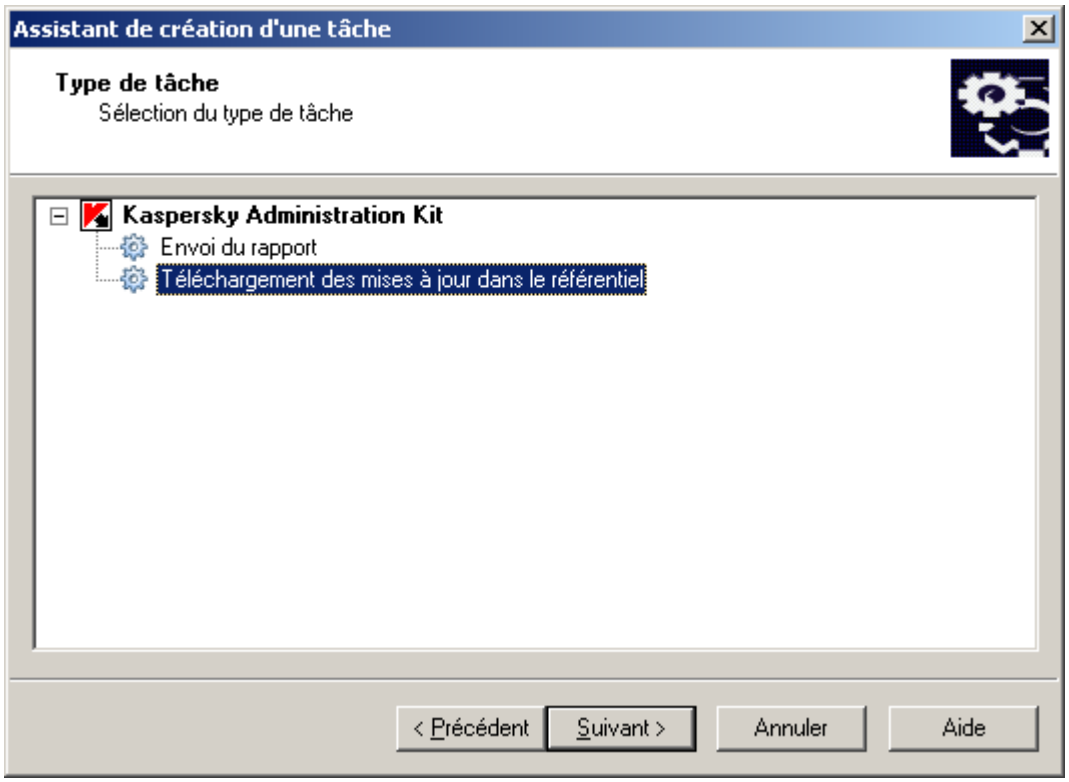


Illustration 25. Création d'une tâche de téléchargement des mises à jour dans le référentiel

S'il existe une hiérarchie des Serveurs d'administration dans le réseau (ou s'il est prévu d'instaurer une telle hiérarchie), il faut cocher la case **Forcer la mise à jour des Serveurs secondaires** (cf. ill. ci-après) dans les paramètres de la tâche sur le Serveur principal pour la diffusion automatique des mises à jour sur les Serveurs secondaires. Dans ce cas, les tâches de mise à jour des Serveurs secondaires seront lancées directement après la mise à jour du Serveur principal (si cette tâche a été créée).

Si la case **Forcer la mise à jour des Serveurs secondaires** est cochée, la création automatique des tâches de récupération des mises à jour sur les Serveurs d'administration secondaires n'a pas lieu. Il faudra les créer manuellement pour chaque Serveur secondaire.

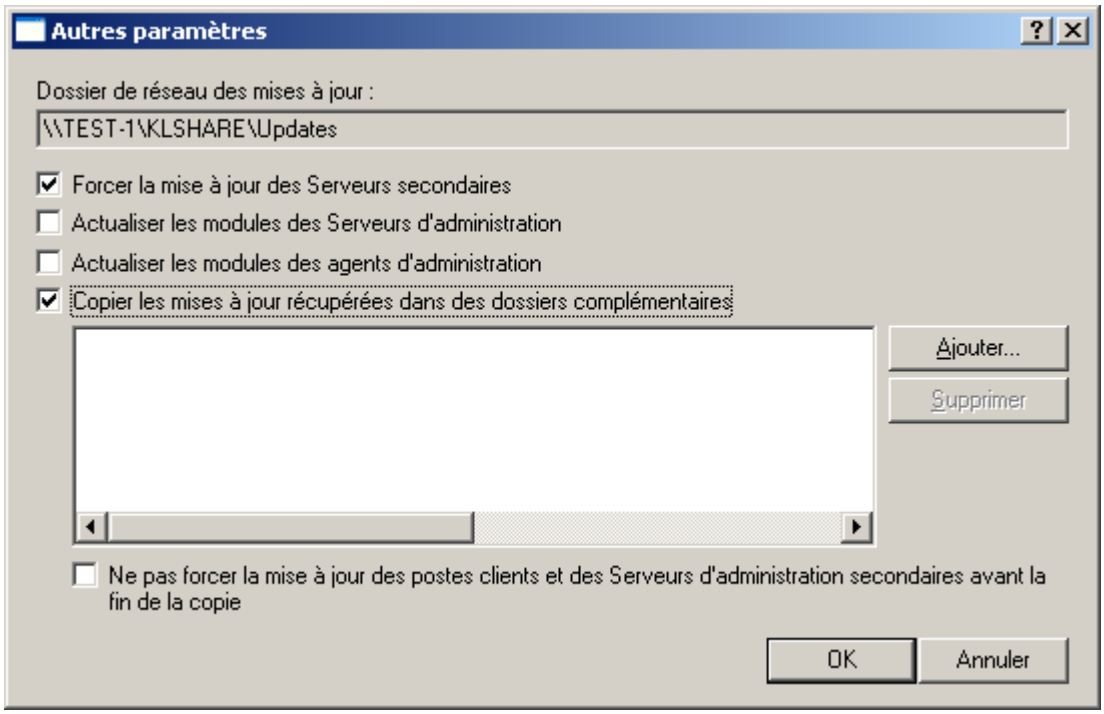


Illustration 26. Configuration d'autres paramètres de la tâche

Suite à l'exécution de la tâche **Téléchargement des mises à jour dans le référentiel** les mises à jour des bases et des modules des applications sont copiées depuis la source définie vers le dossier partagé.

Depuis le dossier partagé, les mises à jour seront diffusées vers les postes clients (cf. section "Diffusion des mises à jour sur les postes clients" à la page 62) et les Serveurs d'administration secondaires (cf. section "Mise à jour des Serveurs secondaires et de leurs postes clients" à la page 63).

Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

- Serveurs de mise à jour Kaspersky Lab ;
- Serveur d'administration principal ;
- Serveur ftp ou http ou dossier de réseau de mise à jour.

La sélection de la ressource dépend des paramètres de la tâche.

En cas de mise à jour depuis un serveur FTP ou HTTP ou depuis un dossier de réseau, la mise à jour correcte du Serveur requiert que la structure des dossiers contenant les mises à jour reste fidèle à la structure formée lors de la copie des mises à jour à par les logiciels de Kaspersky Lab.

Il est possible de consulter les informations relatives aux mises à jour récupérées dans le dossier **Mises à jour** du nœud **Stockages** de l'arborescence de la console. La liste des mises à jour figure dans le panneau des résultats (cf. ill. ci-après).

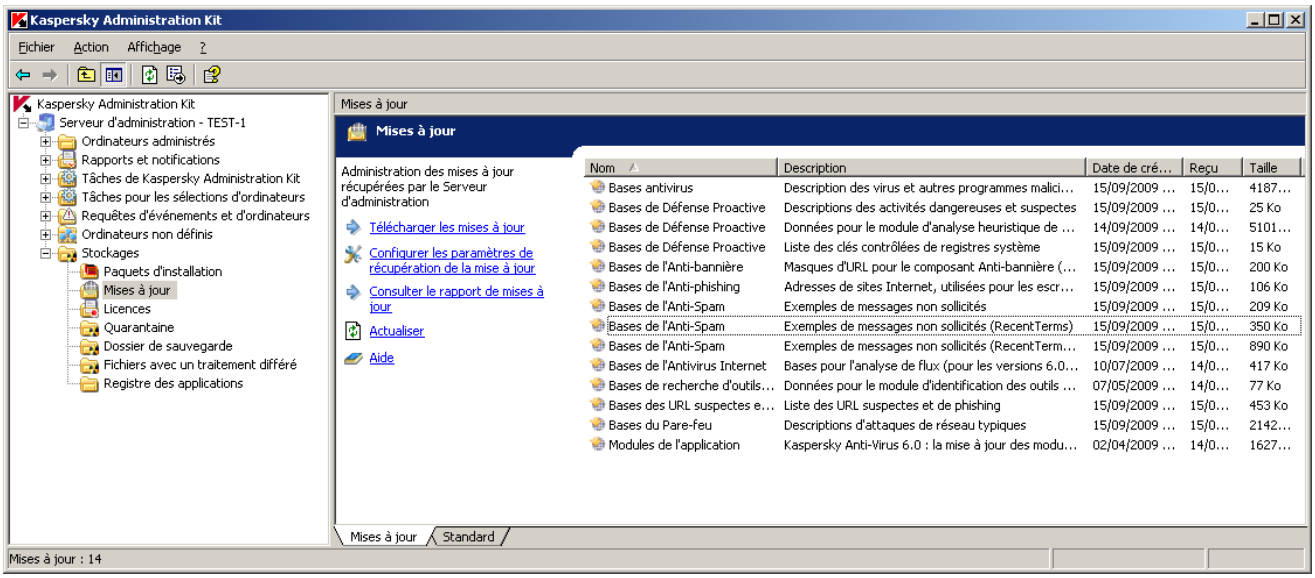


Illustration 27. Affichage des mises à jour récupérées

DIFFUSION DES MISES A JOUR VERS LES POSTES CLIENTS

Pour accroître la fiabilité de la protection antivirus, il faut créer des tâches de groupe de récupération des mises à jour pour toutes les applications antivirus repris dans le système de protection antivirus des postes clients.

Pour que des versions identiques des bases et des mises à jour des modules de l'application soient installées sur les postes clients, il faut sélectionner le Serveur d'administration en guise de source des mises à jour dans les paramètres des tâches de récupération des mises à jour par les applications.

Si le Serveur d'administration est choisi en tant que source des mises à jour dans la tâche de mise à jour de l'application, dans la structure hiérarchique des Serveurs les postes clients seront actualisés depuis le Serveur, auquel ils sont connectés, c-à-d. depuis le Serveur secondaire au lieu du Serveur principal.

La composition des tâches de mise à jour pour les applications est présentée en détails dans les documentations respectives.

Pour les tâches de mise à jour, il est possible de sélectionner sur l'onglet **Planification** (cf. ill. ci-après) l'option de lancement **Lors du téléchargement des mises à jour dans le référentiel**. Ceci permet de réduire le volume du trafic et le nombre de requêtes des postes clients vers le Serveur d'administration, ainsi que d'éviter les imprécisions et les erreurs lors de la création de tâches de mise à jour pour les groupes d'administration contenant un grand nombre de postes clients.

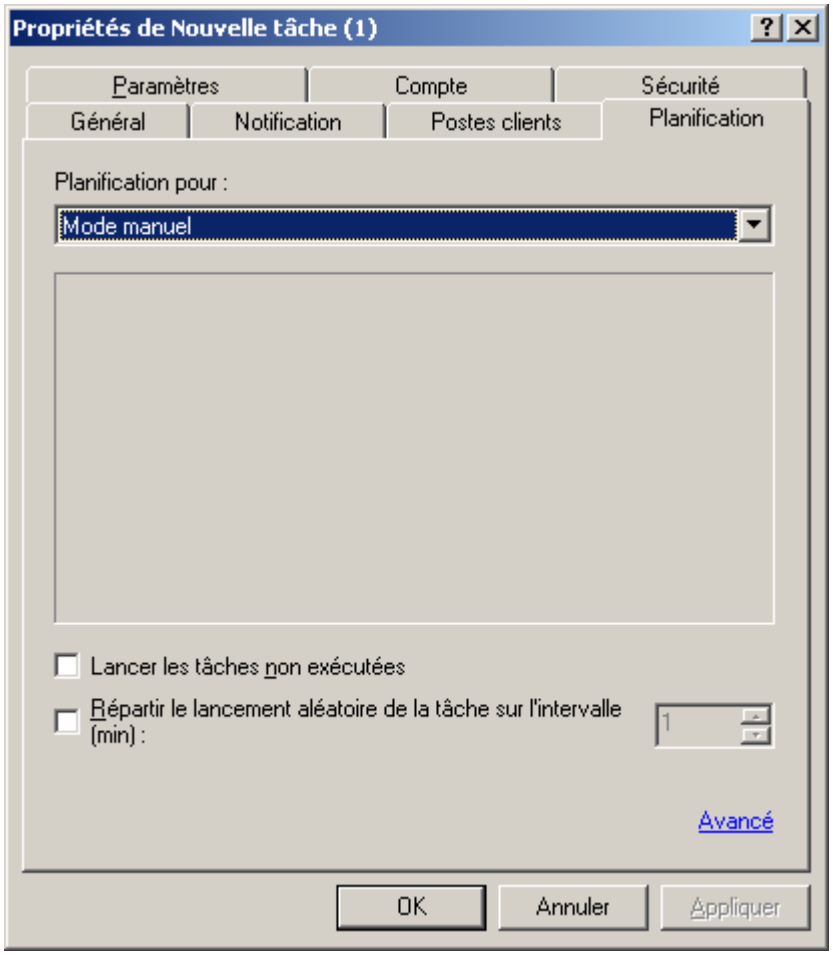


Illustration 28. Planification d'une tâche de mise à jour

Pour diminuer la charge des Serveurs d'administration, il est conseillé d'utiliser les agents de mise à jour (cf. section "Diffusion des mise à jour à l'aide des agents de mise à jour" à la page 65) qui permettra la diffusion des mises à jour dans les limites du groupe d'administration. En cas de diffusion multiadresses IP, les agents de mise à jour diffusent également les paramètres des stratégies et des tâches.

MISE A JOUR DES SERVEURS SECONDAIRES ET DE LEURS POSTES CLIENTS

La récupération des mises à jour par les applications a lieu depuis le Serveur d'administration, auquel le poste client est connecté, à savoir, depuis le Serveur secondaire au lieu du Serveur principal.

S'il existe une hiérarchie des Serveurs d'administration dans le réseau informatique, pour que les Serveurs secondaires puissent récupérer les mises à jour et les diffuser sur les postes clients connectés, il faut :

- Créer une tâche de récupération des mises à jour pour chaque Serveur d'administration secondaire ;

- Dans les paramètres de la tâche de récupération des mises à jour pour les Serveurs secondaires, sélectionner **Serveur d'administration principal** (cf. ill. ci-après) en guise de source des mises à jour ;

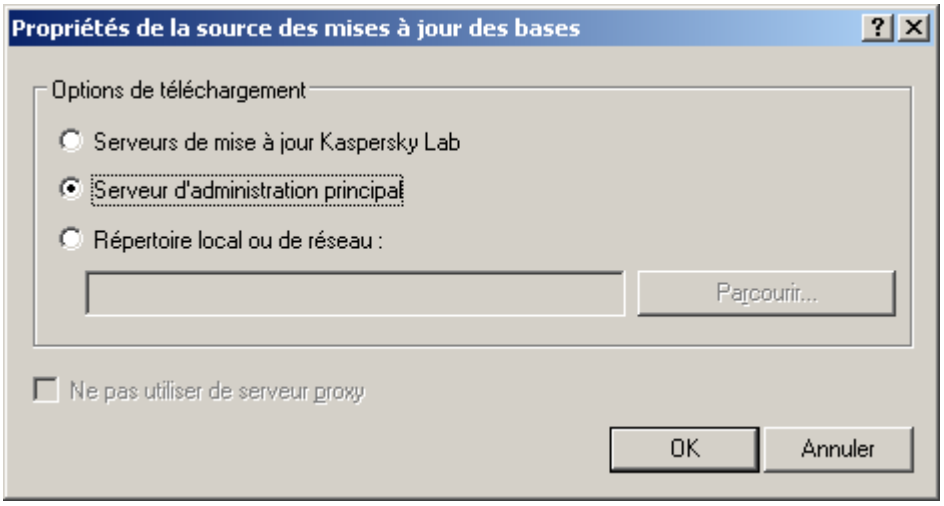


Illustration 29. Mise à jour depuis le Serveur d'administration principal

- Dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration principal, activer le mode de diffusion automatique des mises à jour sur les Serveurs secondaires en cochant la case **Forcer la mise à jour des Serveurs secondaires** (cf. ill. ci-après) ;

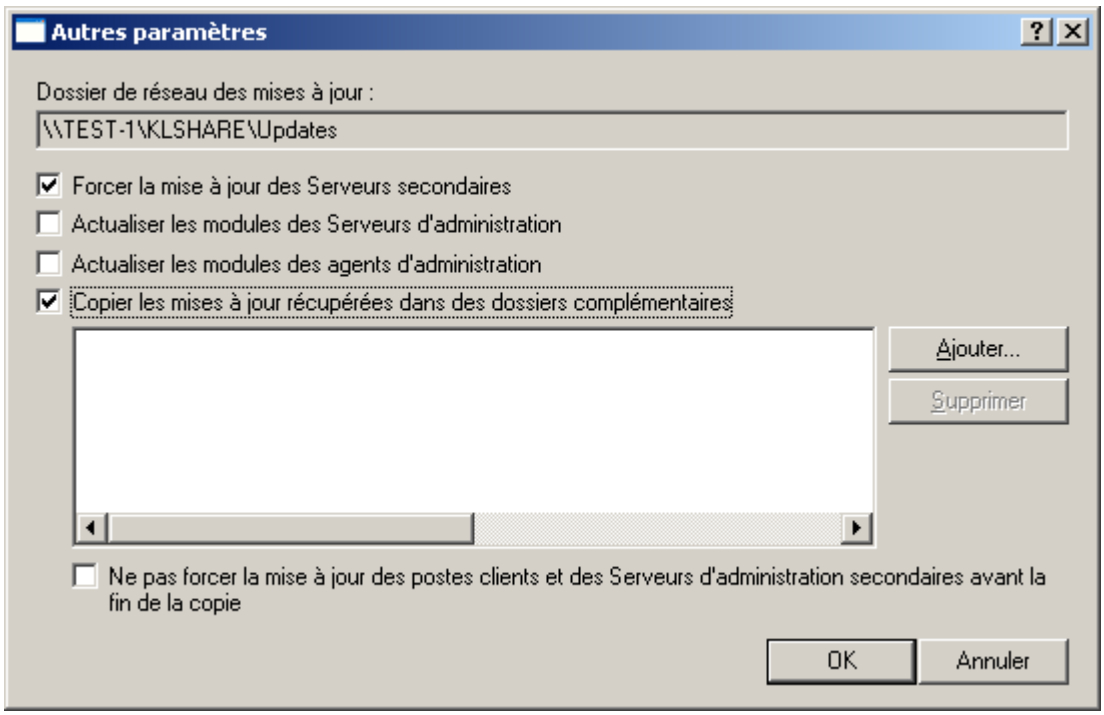


Illustration 30. Configuration d'autres paramètres de la tâche

- Déterminer les agents de mise à jour (cf. section "Diffusion des mises à jour à l'aide des agents de mise à jour" à la page 65) dans les limites des groupes d'administration.

DIFFUSION DES MISES A JOUR A L'AIDE DES AGENTS DE MISE A JOUR

Pour diffuser les mises à jour vers les postes clients du groupe, il est possible d'utiliser les agents de mise à jour, à savoir les ordinateurs qui jouent le rôle du centre intermédiaire de diffusion des mises à jour et des paquets d'installation dans les limites du groupe d'administration. Ils récupèrent les mises à jour depuis le Serveur d'administration et les placent dans le dossier désigné lors de l'installation de l'application. Le dossier peut être modifié dans les propriétés de l'agent de mise à jour. Seules les mises à jour requises dans les limites du groupe sont copiées. Par la suite, les postes clients du groupe contactent les agents pour les mises à jour.

La composition de la liste des agents de mise à jour et leur configuration a lieu dans la fenêtre des propriétés du groupe, sous l'onglet **Agents de mise à jour** (cf. ill. ci-après). Outre les paquets de mise à jour, les agents diffusent les paramètres des stratégies et les tâches de groupe sur les postes clients.

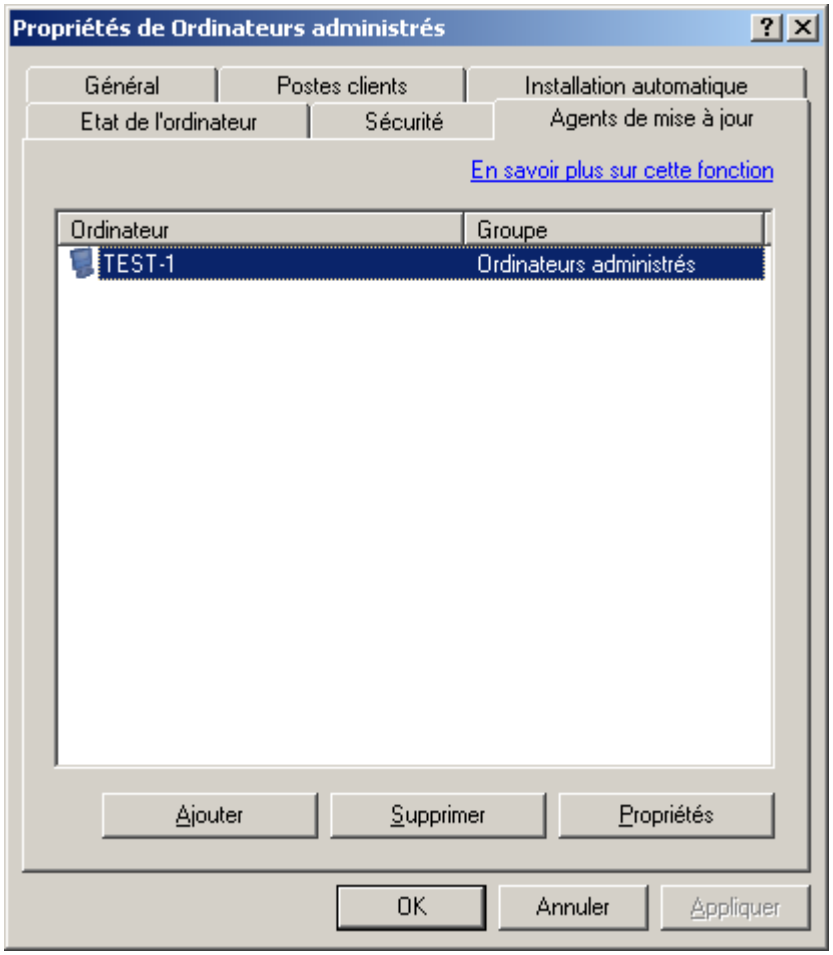


Illustration 31. Création de la liste des agents de mise à jour

MAINTENANCE

Dans le cadre de la maintenance des groupes d'administration, il est conseillé de réaliser une série d'opérations à intervalles réguliers :

- Créer et consulter périodiquement les rapports de fonctionnement des applications sur les postes clients (cf. section "Rapports" à la page 74).
- Lire les notifications envoyées depuis les postes clients et le Serveur d'administration.

  La liste complète des notifications envoyées par les applications de Kaspersky Lab est reprise dans les documentations respectives.

- Si une situation qui justifie la notification survient, l'administrateur peut l'envoyer depuis son poste de travail, par exemple réparer les fichiers infectés sur cet ordinateur.
- Actualiser en temps opportuns (cf. section "Mise à jour des bases et des modules de l'application" à la page 59) les bases de l'application et les modules logiciels des applications installées sur les postes clients.
- Surveiller la taille des bases de données pour le stockage des informations en provenance des postes clients concernant le fonctionnement des applications et l'existence de l'espace suffisant sur le Serveur d'administration.
- Ajouter opportunément aux groupes d'administration les nouveaux ordinateurs du réseau de l'entreprise et y installer les applications antivirus requises.
- Réaliser à intervalles réguliers une copie de sauvegarde des données du système d'administration (cf. section "Copie de sauvegarde et restauration des données du Serveur d'administration" à la page 85).
- Surveiller l'état des licences des applications installées sur le réseau et, le cas échéant, les renouveler (cf. section "Renouvellement des licences" à la page 67).
- Consulter les informations relatives aux événements du Serveur d'administration et des applications qu'il gère (cf. section "Journaux des événements. Sélection d'événements" à la page 70).
- Surveiller l'état de la quarantaine (cf. section "Quarantaine et sauvegarde" à la page 68) et les informations relatives aux fichiers dont l'analyse a été différée (cf. section "Fichiers avec un traitement différé" à la page 85).

Il existe dans Kaspersky Administration Kit plusieurs fonctions qui simplifient considérablement la maintenance du réseau :

- recherche d'ordinateurs, de groupes d'administration et de Serveurs d'administration secondaires selon des paramètres définis (cf. section "Recherche d'un poste" à la page 77) ;
- tenue d'un registre des applications (cf. section "Registre des applications" à la page 81) ;
- contrôle de l'émergence d'épidémies de virus (page 82).

DANS CETTE SECTION

RENOUVELLEMENT DE LA LICENCE

Le droit d'utilisation d'une application de Kaspersky Lab repose sur un contrat de licence conclu au moment de l'achat de l'application.

Vous bénéficiez des services suivants durant la validité de la licence :

- utilisation des fonctions antivirus de l'application ;
- mise à jour des bases des applications ;
- mise à niveau de la version de cette application ;
- consultations sur des questions liées à l'installation, à la configuration et à l'utilisation de l'application. Cette aide peut être obtenue par téléphone ou en remplissant le formulaire de demande en ligne du service du Support Technique, accessible sur le site de Kaspersky Lab ;
- possibilité d'envoyer les objets infectés et suspects découverts à Kaspersky Lab en vue d'une analyse plus poussée.

Aucune licence n'est requise pour Kaspersky Administration Kit ! En cas de contact avec le service du Support Technique, utilisez les informations relatives à la licence de n'importe quelle application de Kaspersky Lab que vous avez achetée et qui est administrée à l'aide de Kaspersky Administration Kit.

L'application Kaspersky Administration Kit détermine la présence d'une licence qui est une partie intégrante de n'importe quel logiciel de Kaspersky Lab et qui détermine sa durée de validité. L'application ne peut disposer que d'une seule licence active. Cette licence contient les restrictions d'utilisation de l'application, qui peuvent être vérifiées par des mécanismes spéciaux.

Les possibilités citées ci-dessus sont limitées une fois que la licence a expiré. Le renouvellement de la licence consiste à acheter et à installer une nouvelle licence.

L'application Kaspersky Administration Kit permet d'installer de façon centralisée les licences sur les postes clients, d'observer leur état et de les renouveler.

Lors de l'installation d'une licence à l'aide des services de Kaspersky Administration Kit, toutes les données relatives à celle-ci sont stockées sur le Serveur d'administration. Ces informations servent à créer les rapports d'état des licences installées et permettent de signaler la fin de la validité ou le dépassement du nombre d'ordinateurs utilisant cette application tel que défini dans la licence. Les paramètres de notification sur l'état des licences sont modifiés dans les paramètres du Serveur d'administration.

Pour créer un rapport sur l'état des licences installées sur les postes clients, vous pouvez utiliser le modèle **Rapport de licences** ou créer un nouveau modèle du même type.

Le rapport créé selon le modèle **Rapport de licences** reprend les informations complètes sur toutes les licences installées sur les postes clients, qu'elles soient actives ou non, ainsi que le nom des ordinateurs, sur lesquels elles sont utilisées et les restrictions qu'elles imposent.

La liste complète des licences installées sur les postes clients figure dans le nœud **Stockages** du dossier **Licences** (cf. ill. ci-après). Les informations détaillées sont reprises dans le panneau des résultats pour chacune d'elles. La liste complète des colonnes du panneau des résultats pour le dossier **Licences** est reprise dans l'aide.

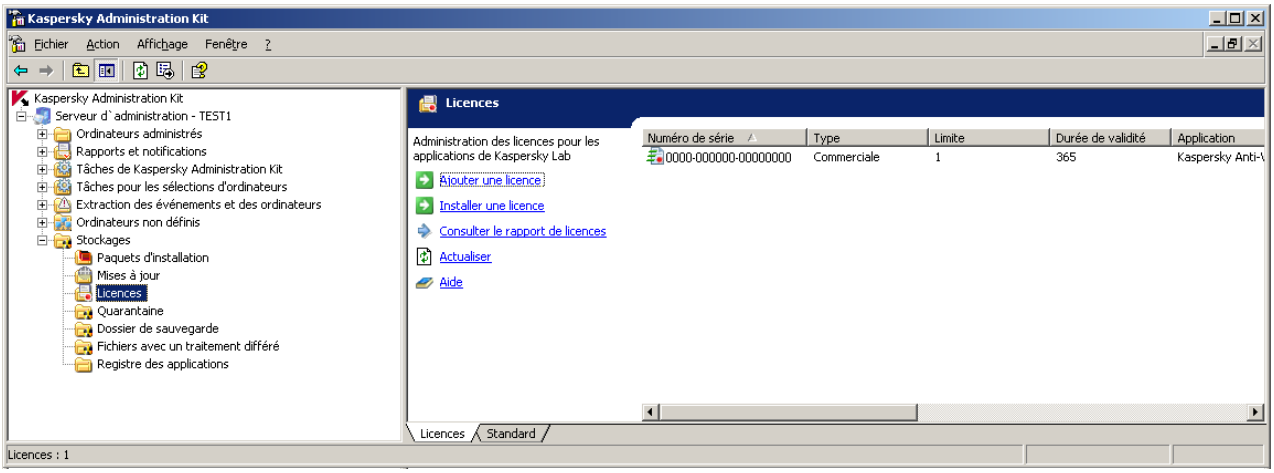


Illustration 32. Licences

Les informations relatives à la nature des licences installées pour les applications sur un poste client concret sont visibles dans la fenêtre des propriétés de l'application.

Afin d'installer une licence, il est nécessaire de créer et de lancer la tâche d'installation de la licence.

La tâche d'installation des licences peut être créée en tant que tâche de groupe, en tant que tâche locale ou en tant que tâche pour une sélection d'ordinateurs. La tâche d'installation des licences peut être créée à l'aide de l'Assistant.

Pour remplacer une licence qui est déjà installée ou pour installer une licence en tant que licence active, vous pouvez utiliser une tâche existante en veillant toutefois à en modifier les paramètres.

QUARANTAINE ET DOSSIER DE SAUVEGARDE

L'utilisation de la quarantaine et du dossier de sauvegarde est accessible à Kaspersky Anti-Virus for Windows Workstations et Kaspersky Anti-Virus for Windows Servers 6.0 MP4.

Les logiciels antivirus proposent une fonction, qui permet d'enregistrer les objets dans des dossiers spéciaux. Il existe pour chaque ordinateur les dossiers individuels de quarantaine et de sauvegarde, situés sur l'ordinateur. La quarantaine accueille les objets suspects, tandis que le dossier de sauvegarde est prévu pour la copie de sauvegarde des objets infectés avant leur réparation ou leur suppression.

L'application Kaspersky Administration Kit permet de tenir une liste centralisée d'objets placés dans la sauvegarde par les applications de Kaspersky Lab. Ces informations sont transmises depuis les postes clients via les Agents de réseau et conservées dans la base d'informations du Serveur d'administration. Il est possible, via la Console d'administration, de

consulter les propriétés des objets dans les stockages sur les ordinateurs locaux, de lancer une analyse antivirus des référentiels et d'en supprimer les objets.

Pour activer la fonction d'administration à distance des objets des stockages locaux, dans la stratégie de l'application il faut cocher les cases dans le bloc d'informations **Informer le Serveur d'administration** (cf. ill. ci-après) :

- **Sur les objets en quarantaine**.
- **Sur les objets du dossier de sauvegarde**.
- **Sur les objets avec le traitement différé**.

La configuration des paramètres des stockages est réalisée individuellement pour chaque application : dans la stratégie ou dans les paramètres de l'application.

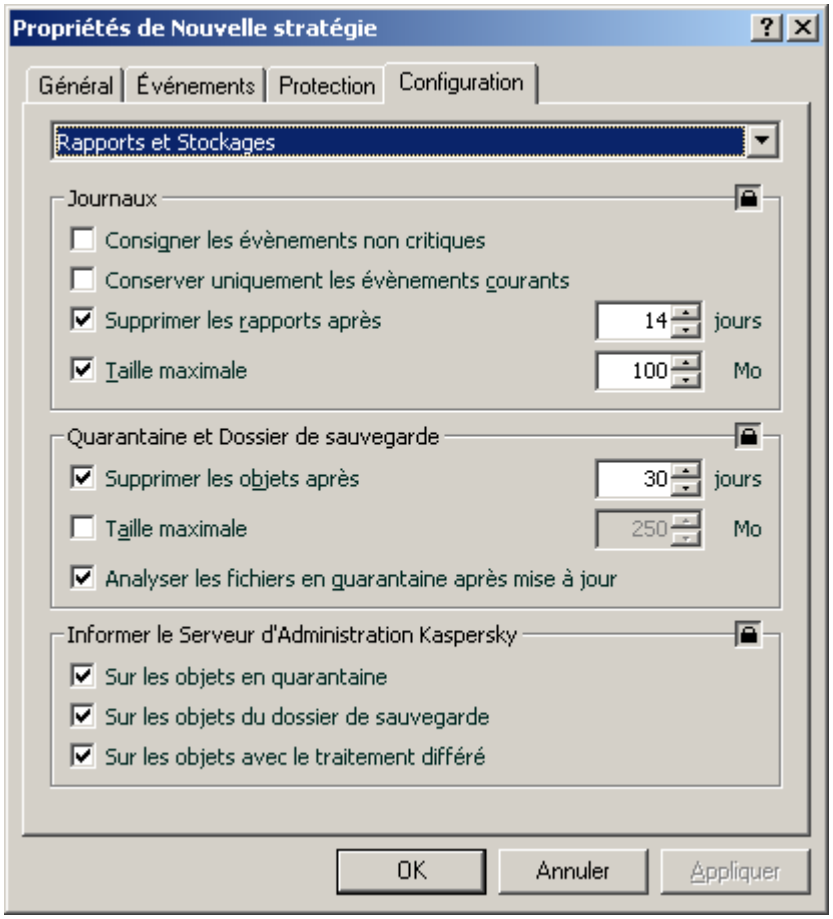


Illustration 33. Configuration des stockages distants

La consultation des objets placés dans les stockages des postes clients des groupes d'administration et la manipulation de ces objets s'opèrent dans le dossier **Stockages** (cf. ill. ci-après).

Kaspersky Administration Kit ne copie pas les objets sur le Serveur d'administration. Tous les objets sont placés dans les stockages locaux des postes clients. La restauration des objets s'opère sur l'ordinateur, où est installée l'application antivirus, qui a placé l'objet dans le stockage défini par l'administrateur.

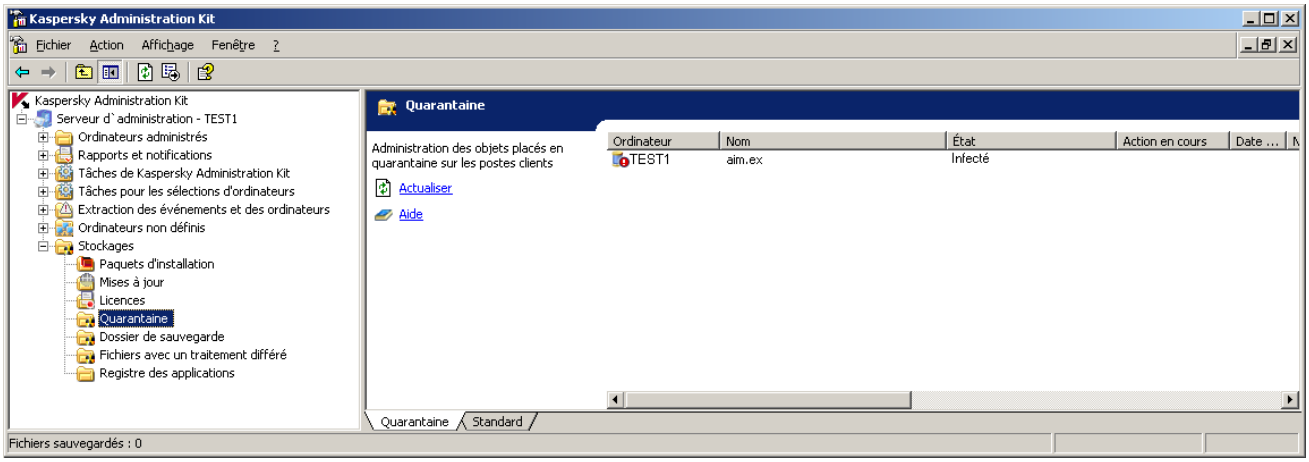


Illustration 34. Affichage du contenu du stockage

JOURNAUX DES EVENEMENTS SELECTIONS D'EVENEMENTS

L'application Kaspersky Administration Kit propose un large éventail de fonctions pour observer le fonctionnement du système de protection antivirus.

Il est possible de tenir un journal des événements survenus durant le fonctionnement du Serveur d'administration et de toutes les applications administrées à l'aide de Kaspersky Administration Kit. Les données peuvent être enregistrées dans le journal système de Microsoft Windows ou dans le journal des événements de Kaspersky Administration Kit.

Les événements survenus durant l'utilisation des applications et les résultats des tâches sont consignés dans les journaux.

Vous pouvez définir la liste des événements enregistrés durant le fonctionnement de chaque application, ainsi que l'ordre de notification de l'administrateur et des autres utilisateurs pour chaque groupe d'administration. Ces paramètres sont définis par la stratégie de groupe pour l'application. La définition des paramètres a lieu dans la fenêtre des propriétés de la stratégie de groupe sous l'onglet **Événements** (cf. ill. ci-après).

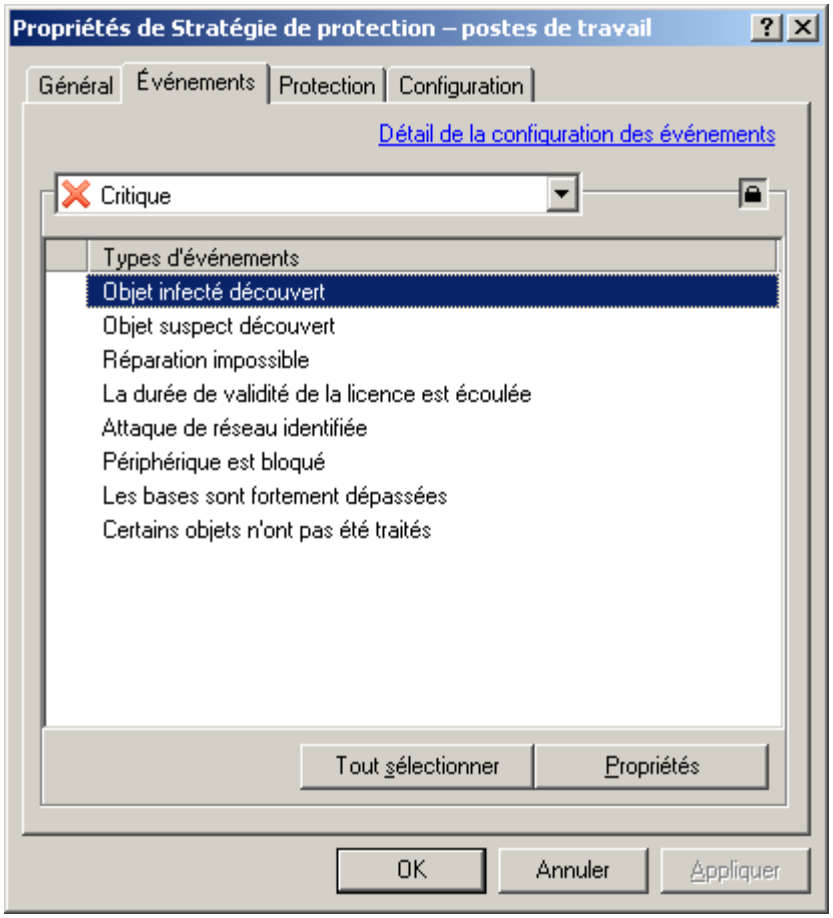


*Illustration 35. Modification d'une stratégie. Onglet **Événements***

Les paramètres de la tâche permettent de définir l'ordre d'enregistrement des résultats de l'exécution des tâches, ainsi que la forme et le moyen de notification.

La notification peut être réalisée via la diffusion de messages par courrier électroniques ou par le réseau, ainsi qu'à l'aide de l'exécution d'un programme ou d'un script particulier.

Les informations relatives aux événements et aux résultats de l'exécution des tâches peuvent être conservées de façon centralisée sur le Serveur d'administration, ainsi que sur chaque poste client.

La consultation des informations reprises dans le journal des événements de Microsoft Windows s'opère à l'aide des outils standards **Affichage des événements** de MMC. La consultation des informations reprises dans le journal des événements de Kaspersky Administration Kit conservé sur le Serveur d'administration s'opère via le nœud **Extraction des événements et des ordinateurs / Événements** de l'arborescence de la console (cf. ill. ci-après).

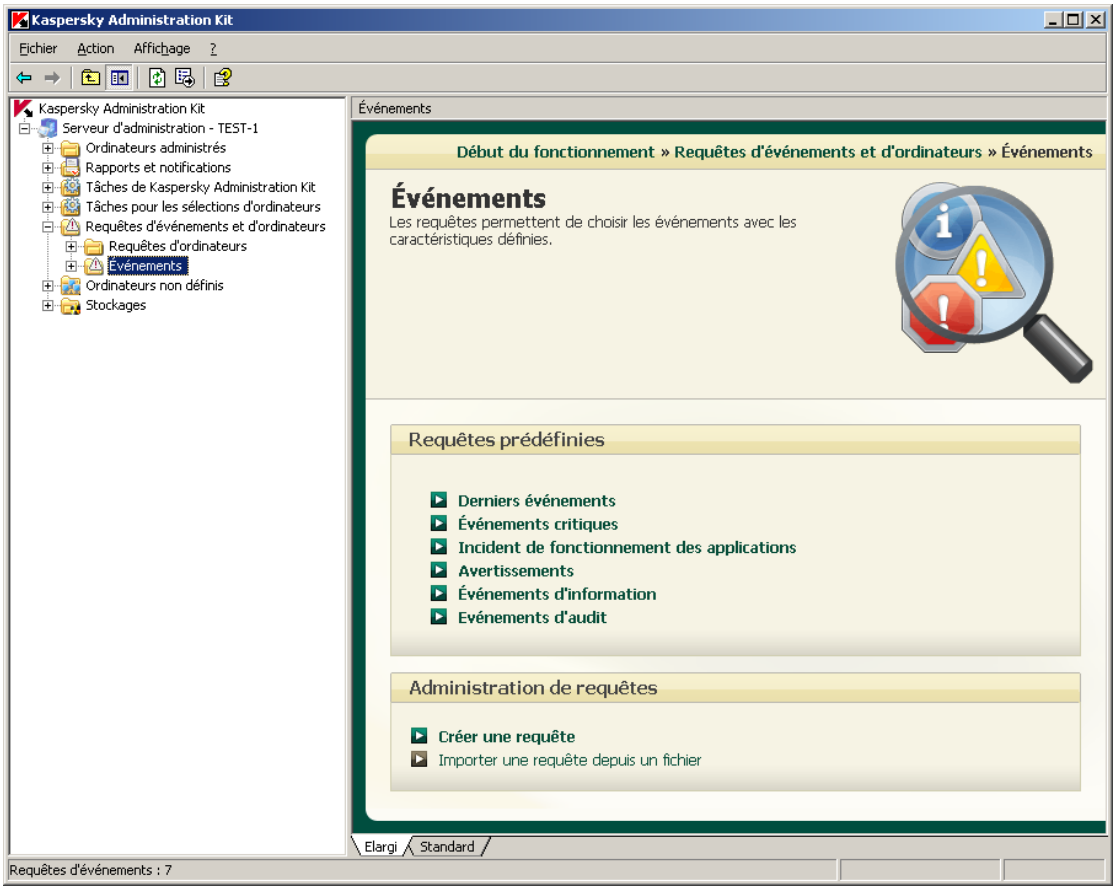


Illustration 36. Consultation des informations reprises dans le journal des événements de Kaspersky Anti-Virus

Pour simplifier la consultation et la recherche, les informations du nœud **Événements** sont regroupées par requête. Par défaut, les requêtes suivantes sont proposées : **Derniers événements**, **Événements critiques**, **Erreurs**, **Avertissements**, **Informations** et **Événements d'audit**. La requête permet de réaliser la recherche et de structurer les informations sur les événements consignés, car après l'établissement de la requête, seules les informations qui répondent à des critères spécifiés sont proposées. Ceci est assez important vu le grand volume des informations conservées sur le Serveur. Il est possible de créer des requêtes supplémentaires, de modifier la sélection des colonnes affichées et d'enregistrer la requête des événements dans un fichier au format .txt.

Pour créer une requête, utilisez la commande **Créer** / **Nouvelle requête** du menu contextuel du nœud **Événements**. Un nouveau dossier portant le nom de la requête apparaîtra dans le nœud **Événements** de l'arborescence de la console. Il reprendra tous les événements et les résultats de l'exécution des tâches. Pour pouvoir modifier la composition des informations, configurez les paramètres de la requête (cf. ill. ci-après).

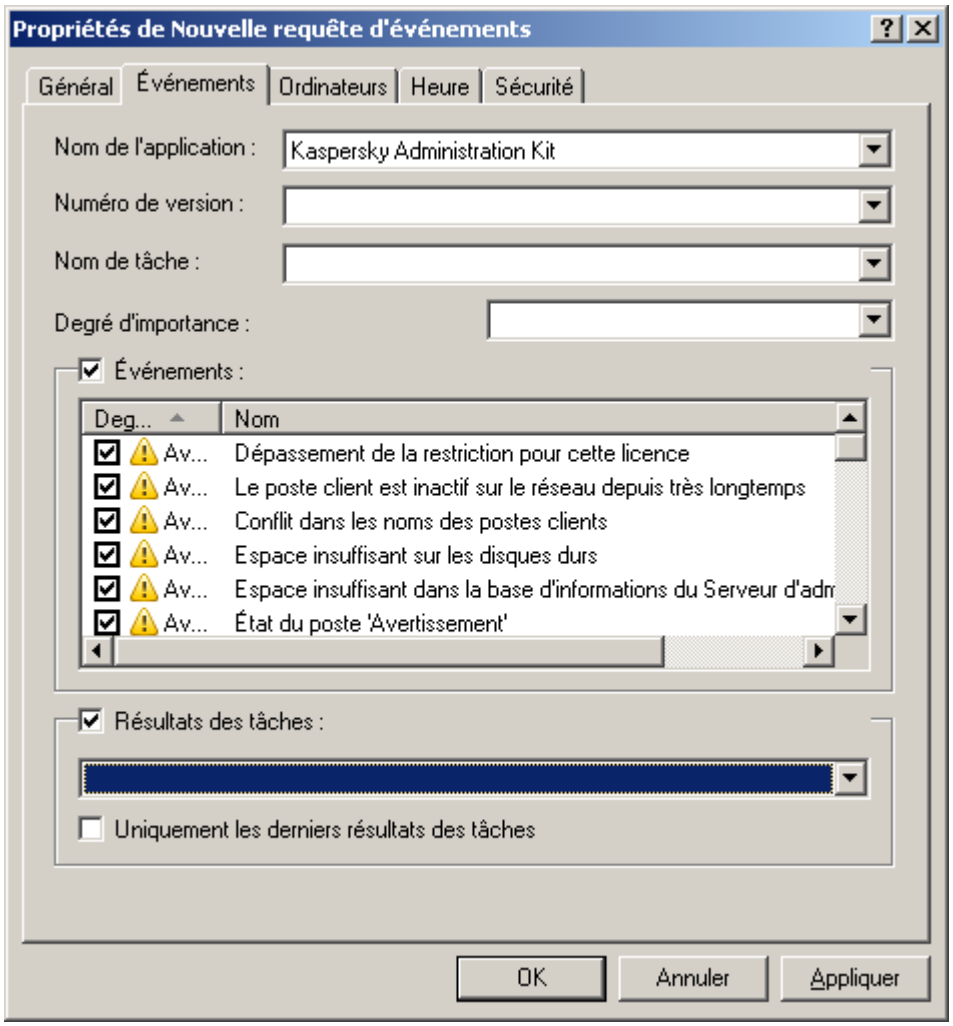


*Illustration 37. Configuration d'une requête d'événements. Onglet **Événements***

La suppression des événements consignés survient automatiquement à l'expiration du délai de conservation, défini par la stratégie, ou manuellement à l'aide de la commande **Supprimer** du menu contextuel. Vous pouvez supprimer un événement individuel sélectionné dans le panneau des résultats, tous les événements ou les événements qui satisfont à des conditions déterminées.

La liste des événements consignés durant le fonctionnement de l'application pour chaque poste client est visible dans la fenêtre **Événements** (cf. ill. ci-après) qui s'ouvre depuis le menu contextuel **Événements**. Les informations sont proposées par le journal des événements de Kaspersky Administration Kit, conservés sur le Serveur d'administration. Pour rechercher les informations, vous pouvez utiliser le filtre des événements.

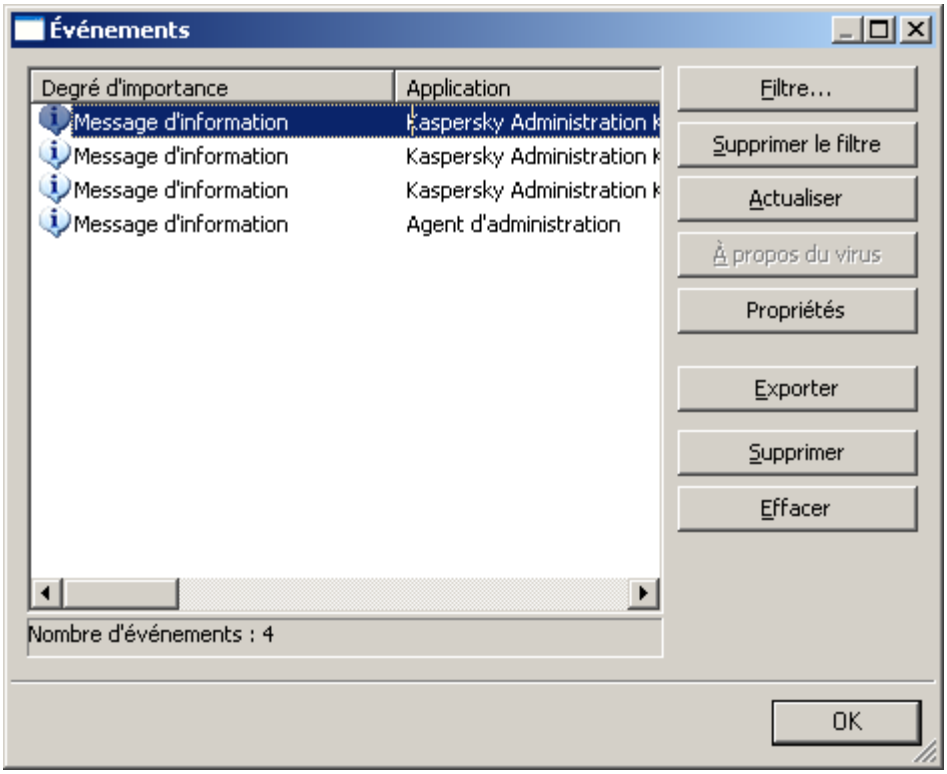


Illustration 38. Affichage des événements entreposés sur le Serveur d'administration

RAPPORTS

Vous pouvez obtenir des rapports sur l'état du système de protection antivirus, rédigés sur la base des informations du Serveur d'administration.

Il est également possible de vérifier l'état de la protection antivirus sur le poste client à l'aide des informations consignées par l'Agent d'administration dans le registre système.

Il existe les rapports pour les objets suivants :

- le système de protection antivirus dans son ensemble ;
- les ordinateurs appartenant à un groupe d'administration déterminé ;
- la sélection de postes clients issus de divers groupes d'administration ;
- le système de protection antivirus des Serveurs d'administration secondaires.

Les rapports de type suivant sont prévus :

- **Etat de protection** :
  - **Rapport d'état de protection** contient des informations sur les postes clients, qui ne jouissent pas d'une protection antivirus suffisante.

- **Rapport sur les erreurs** contient des informations sur les erreurs (refus de fonctionnement) enregistrées durant le fonctionnement des applications installées sur les postes clients.

- **Rapport sur les événements** contient la liste des événements des applications pour le groupe sélectionné. La liste reprend uniquement les événements indiqués lors de la création du rapport.

- **Rapport sur le fonctionnement des agents de mise à jour** contient les statistiques de fonctionnement des agents de mise jour dans le cadre des groupes d'administration sélectionnés.

- **Rapport sur les Serveurs d'administration secondaires** contient les informations sur les Serveurs d'administration secondaires inclus dans les groupes d'administration sélectionnés.

- **Déploiement** :

  - **Rapport sur l'utilisation des licences** contient des informations sur l'état des licences utilisées par les applications et sur le respect des restrictions qu'elles imposent.

  - **Rapport sur les versions des logiciels de Kaspersky Lab** reprend les informations sur les versions des applications antivirus de Kaspersky Lab installées sur les postes clients.

  - **Rapport sur les applications incompatibles** contient des informations sur les applications antivirus d'autres éditeurs installés sur les postes clients ou sur les applications de Kaspersky Lab qui ne sont pas compatibles avec l'administration via Kaspersky Administration Kit.

  - **Rapport sur le déploiement de la protection** contient une liste des ordinateurs dans le réseau et les informations sur les applications antivirus qui y sont installées.

- **Mise à jour** :

  - **Rapport sur les bases utilisées** contient les informations sur les versions des bases utilisées par les applications.

  - **Rapport sur les versions des mises à jour des modules logiciels des applications de Kaspersky Lab** contient les informations de synthèse sur les versions des mises à jour des modules logiciels installés, le nombre de mises à jour installées, ainsi que le nombre d'ordinateurs ou de groupes, où l'installation a eu lieu.

- **Statistiques antivirus** :

  - **Rapport sur les virus** reprend les informations relatives aux résultats de l'analyse antivirus des postes clients.

  - **Rapport sur les ordinateurs** les plus infectés contient les informations sur les postes clients dont l'analyse s'est soldée par le plus grand nombre d'objets suspects découverts.

  - **Rapport d'attaques réseau** reprend les informations relatives aux attaques de réseau enregistrées sur les postes clients.

  - **Rapport sur les applications pour la protection des postes de travail et des serveurs de fichiers** contient les informations détaillées sur les logiciels antivirus installés pour la protection des postes de travail et des serveurs de fichiers, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.

  - **Rapport sur les applications pour la protection des systèmes de messagerie** contient les informations détaillées sur les logiciels antivirus installés pour la protection des systèmes de messagerie, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.

  - **Rapport sur les applications antivirus pour la protection des passerelles** contient les informations détaillées sur les logiciels antivirus installés pour la protection du périmètre, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.

- **Rapport de synthèse sur les types d'application** contient les informations sur les types de logiciels antivirus installés sur les postes clients, ainsi que les informations sur les objets infectés découverts par ces applications et les actions associées.

- **Rapport sur les utilisateurs des ordinateurs infectés** contient les informations sur les utilisateurs les plus dangereux du réseau.

- **Autres** :

  - **Rapport sur le registre des applications** contient les informations sur toutes les applications installées sur les postes clients des groupes d'administration.

  - **Rapport sur les notes de l'administrateur** reprend la liste des remarques de l'administrateur enregistrées dans le groupe pendant l'intervalle indiqué.

Vous pouvez créer des rapports sur la base de modèles créés au préalable. La majorité des rapports créés sur la base des modèles par défaut sont repris dans le nœud **Rapports et notifications** (cf. ill. ci-après) de l'arborescence de la console. L'Assistant de création des rapports permet également de sélectionner certains modèles supplémentaires.

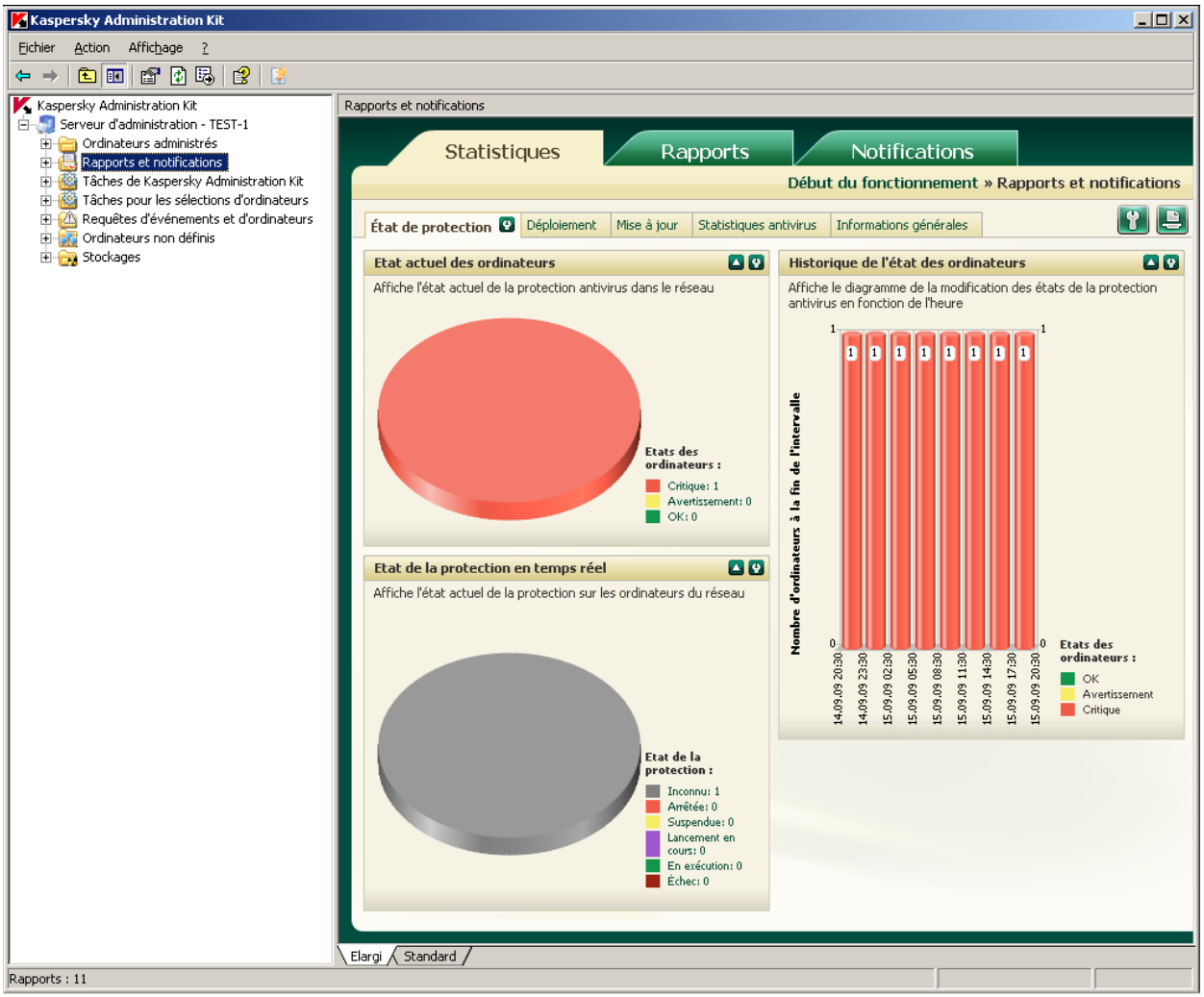


Illustration 39. Affichage de la liste des rapports

Il existe plusieurs modèles standards, qui correspondent aux types de rapport d'état du système de la protection antivirus.

Vous pouvez créer des modèles, en supprimer ceux qui existent ou consulter et modifier leurs paramètres.

Les rapports sont consultés à l'aide du panneau des résultats du nœud correspondant au modèle de création du rapport ou du navigateur installé par défaut dans le système.

Lors de l'utilisation d'une structure hiérarchique des Serveurs d'administration, il est possible de créer les rapports généraux, qui contiennent les informations relatives aux Serveurs d'administration secondaires.

Si certains Serveurs d'administration sont inaccessibles, les informations à ce sujet seront consignées dans le rapport.

Pour enregistrer un rapport, sélectionnez-le dans l'arborescence de la console, ouvrez le menu contextuel du rapport puis sélectionnez l'option **Enregistrer**. Dans l'Assistant qui s'ouvre, indiquez le dossier, où seront enregistrés les rapports, et dans la liste déroulante, sélectionnez le format, dans lequel le rapport sera enregistré. Cliquez sur **Terminer**.

RECHERCHE D'UN POSTE

Pour obtenir des informations relatives à un ordinateur concret ou à un groupe d'ordinateurs, vous pouvez exploiter la fonction de recherche de postes sur la base des critères définis. Les informations des Serveurs d'administration secondaires peuvent intervenir dans la recherche. Les résultats de la recherche peuvent être enregistrés dans un fichier texte.

La fonction de recherche permet de trouver :

- les postes clients appartenant aux groupes d'administration du Serveur d'administration et des Serveurs secondaires ;
- les ordinateurs, qui n'appartiennent pas au groupe d'administration, mais qui appartiennent aux ordinateurs du réseau doté du Serveur d'administration et de ses Serveurs secondaires ;
- tous les ordinateurs de tous les réseaux où est installé le Serveur d'administration et ses Serveurs secondaires, que l'ordinateur appartienne ou non au groupe d'administration.

La recherche des ordinateurs requiert l'utilisation de la commande **Recherche** du menu contextuel du nœud **Serveur d'administration**, des dossiers **Ordinateurs non définis** ou **Ordinateurs administrés** (cf. ill. ci-après) ou les dossiers des sous-groupes d'administration sélectionnés dans l'arborescence de la console. Vous pouvez également cliquer sur les liens suivants du panneau des tâches : **Rechercher des ordinateurs non définis** pour le nœud **Ordinateurs non définis** et **Rechercher des ordinateurs** selon les critères définis pour les dossiers du nœud **Ordinateurs administrés**.

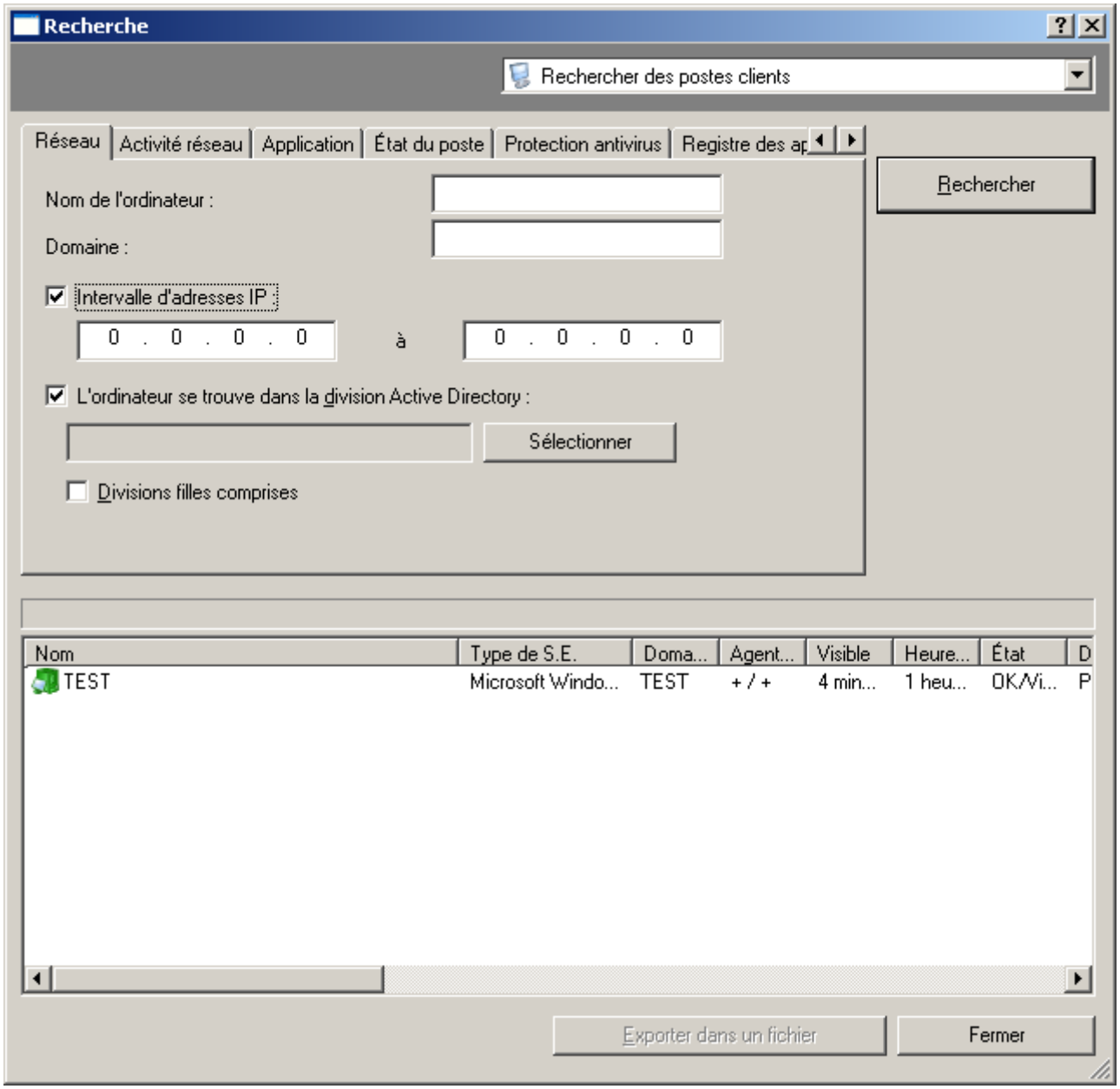


*Illustration 40. Recherche d'un poste. Onglet **Réseau***

Les résultats suivants seront proposés en fonction du nœud, pour lequel la recherche est lancée :

- Nœud **Ordinateurs administrés** ou n'importe lequel de ses dossiers : recherche des postes clients connectés au Serveur d'administration, auquel appartient le groupe sélectionné.

  La recherche se déroule sur la base des informations relatives à la structure des dossiers du Serveur d'administration et des Serveurs secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** a été cochée dans les paramètres de la recherche).

- Nœud **Ordinateurs non définis** : recherche des ordinateurs, qui ne sont pas repris dans les groupes d'administration du réseau, où est installé le Serveur d'administration.

La recherche s'effectue sur la base des données récupérées lors du sondage du réseau par le Serveur d'administration et les Serveurs secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** a été cochée dans les paramètres de la recherche).

Les résultats de la recherche représenteront les ordinateurs appartenant au dossier du nœud **Ordinateurs non définis** choisi pour la recherche et du nœud **Ordinateurs non définis** de tous les Serveurs secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** est cochée dans les paramètres de recherche).

- **Serveur d'administration <nom du serveur>** : recherche globale des ordinateurs.

  La recherche s'exécute sur la base des informations relatives à la structure des groupes d'administration et des données obtenues lors du sondage du réseau informatique par le Serveur d'administration sélectionné et les Serveurs d'administration secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** est cochée).

  La recherche donnera les résultats suivants :

  - Les postes clients appartenant aux groupes d'administration du Serveur d'administration et de tous ses Serveurs secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** est cochée).

  - Les ordinateurs du groupe **Ordinateurs non définis** du Serveur d'administration sélectionné et des groupes **Ordinateurs non définis** de tous ses Serveurs secondaires (si la case **Y compris les données des Serveurs secondaires jusqu'au niveau** a été cochée dans les paramètres de la recherche).

Pour rechercher, enregistrer et afficher les informations relatives aux ordinateurs dans un dossier distinct de l'arborescence de la console, utilisez la fonction de la création de requêtes.

REQUETES D'ORDINATEURS

Pour obtenir un contrôle plus souple sur l'état des postes clients, les informations relatives aux ordinateurs sur les critères différents sont reprises dans un nœud séparé de l'arborescence de la console : **Requêtes d'ordinateurs et d'événements** dans le dossier **Requêtes d'ordinateurs** (cf. ill. ci-après).

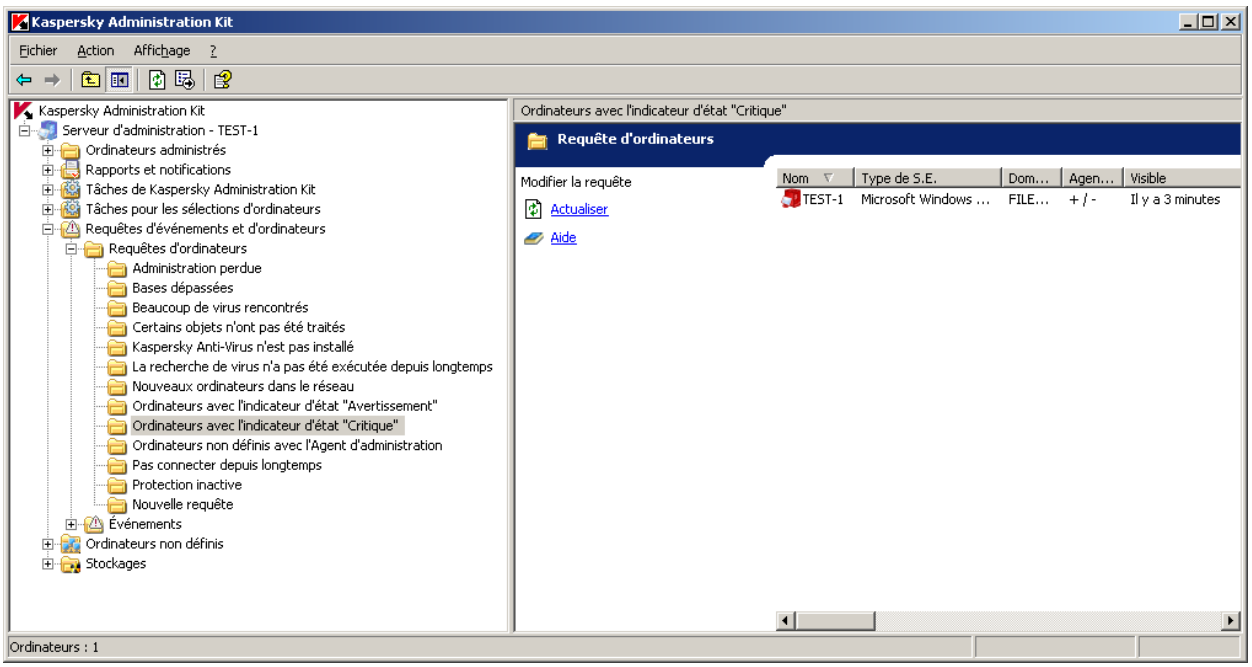


Illustration 41. Requêtes d'ordinateurs

Le diagnostic de l'état des postes clients s'opère sur la base des informations sur l'état de la protection antivirus de l'ordinateur et des données relatives à son activé dans le réseau. La configuration des paramètres du diagnostic s'effectue pour chaque groupe administratif séparément sur l'onglet **Etat du poste** (cf. ill. ci-après).

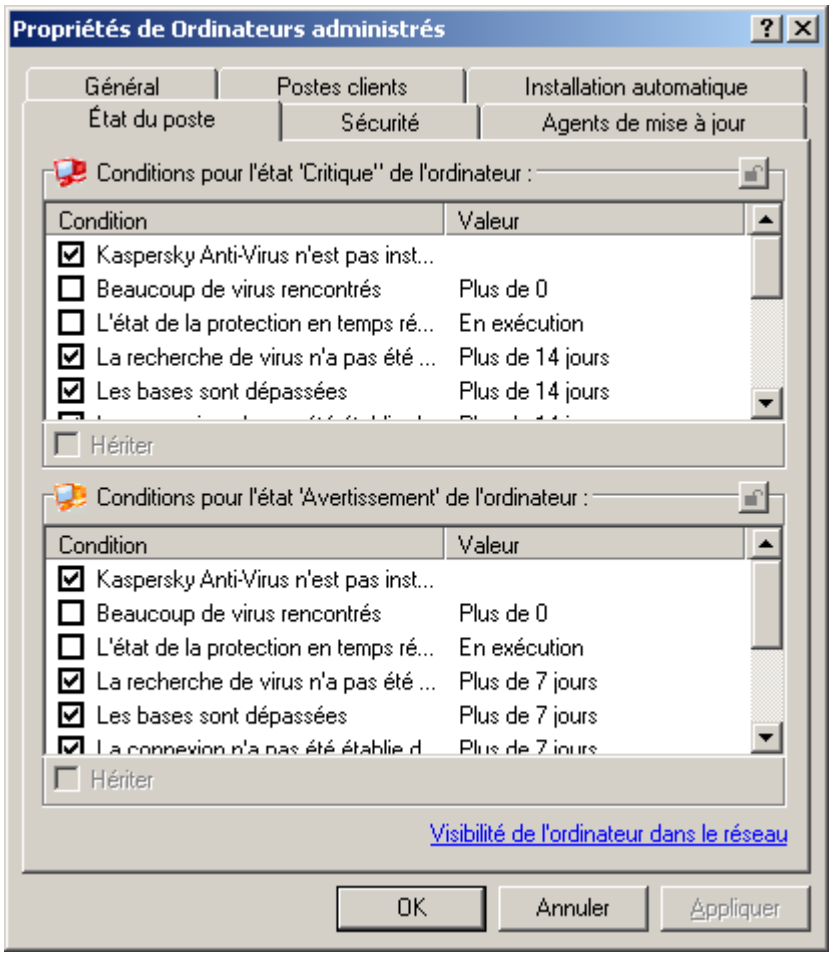


Illustration 42. La configuration de diagnostic de l'état du poste client

Les informations relatives aux nouveaux ordinateurs sont présentées suite au sondage du réseau par le Serveur d'administration.

Il est possible de créer des requêtes complémentaires, de modifier la sélection des colonnes affichées et d'enregistrer la requête d'ordinateurs dans un fichier au format .txt. Pour ajouter des ordinateurs à la requête, configurez les paramètres de la requête (cf. ill. ci-après). La requête peut servir à la recherche et au déplacement des ordinateurs découverts dans les groupes d'administration : Le déplacement est réalisé à l'aide de la souris.

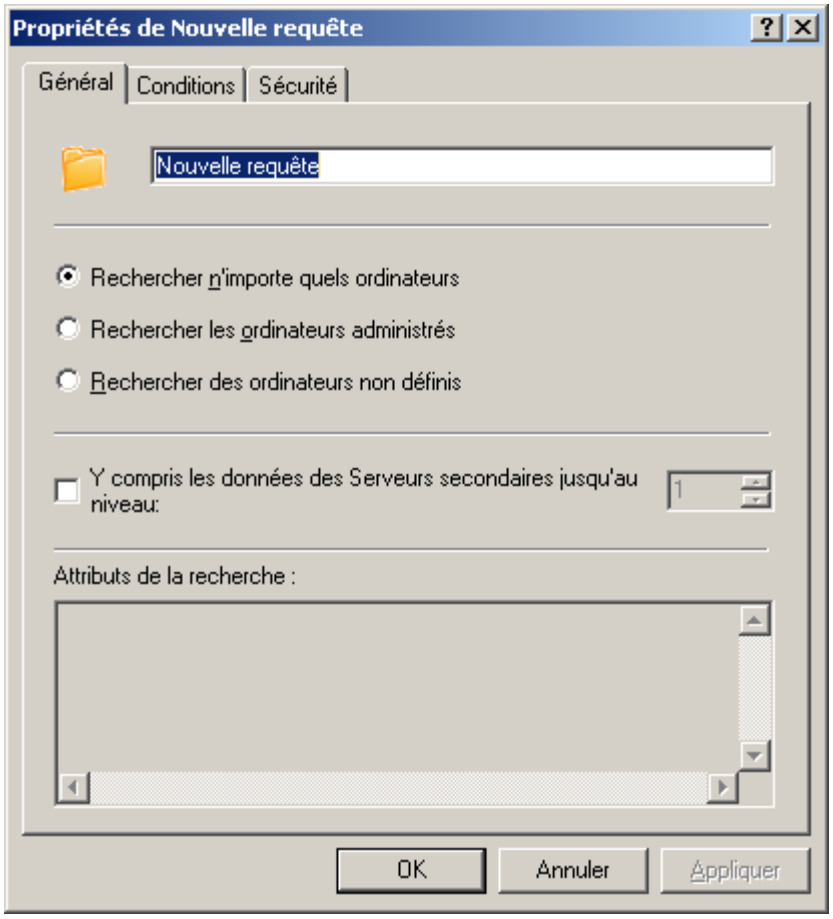


*Illustration 43. Configuration de la requête d'ordinateurs. Onglet **Général***

REGISTRE DES APPLICATIONS

Ce bloc est désactivé par défaut. Pour activer le registre des applications, cochez la case dans les paramètres de l'interface du Serveur d'administration.

Pour consulter le registre des applications installées sur les ordinateurs du réseau, ouvrez le dossier **Registre des applications** du nœud **Stockages**. Les informations relatives aux applications proviennent du registre des postes clients du réseau local et sont présentées dans un tableau contenant les champs suivants :

- **Nom** : nom de l'application ;
- **Version** : numéro de la version de l'application ;
- **Editeur** : nom de la société, qui produit l'application ;
- **Nombre d'hôtes** : nombre d'ordinateurs du réseau, sur lesquels l'application est installée ;
- **Commentaires** : brève description de l'application ;
- **Service du Support Technique** : adresse du site web du service du Support Technique ;

- **Téléphone du service du Support Technique** : numéro de téléphone du service du Support Technique.

Les champs **Commentaires**, **Service du Support Technique** et **Téléphone du service du Support Technique** peuvent être vides, si l'éditeur de l'application n'a pas prévu la possibilité de fournir ces informations dans le registre lors de l'installation de l'application.

Pour consulter les données relatives aux applications qui satisfont à un critère défini, utilisez un filtre. Il est possible, pour les applications de la liste, de consulter la liste des ordinateurs, sur lesquels l'application est installée.

CONTROLE DE L'EMERGENCE D'EPIDEMIES DE VIRUS

Kaspersky Administration Kit permet de contrôler l'activité virale sur les postes clients à l'aide de l'événement **Attaque de virus** consigné pendant le fonctionnement du composant Serveur d'administration.

Cette fonction est primordiale en cas d'épidémie, car elle permet de réagir opportunément aux menaces émergentes d'attaques de virus.

Les critères, qui déclenchent l'événement **Attaque de virus**, sont définis dans les paramètres du Serveur d'administration sous l'onglet **Attaque de virus** (cf. ill. ci-après).

L'événement peut être fixé par plusieurs types d'applications. Pour enclencher le mécanisme d'identification des attaques de virus, cochez les cases en regard des types d'applications requis :

- **Antivirus pour postes de travail et serveurs de fichiers** ;
- **Antivirus pour passerelles** ;
- **Antivirus pour systèmes de messagerie**.

Pour chaque type d'applications, spécifiez le seuil de l'activité virale, au-dessus duquel un événement Attaque de virus sera généré :

- Le champ **Virus** indique le nombre de virus trouvés par des applications de ce type ;

- Le champ **pendant (min)** indique l'intervalle de temps, qu'il a fallu pour détecter la quantité de virus dont il est question ci-dessus.

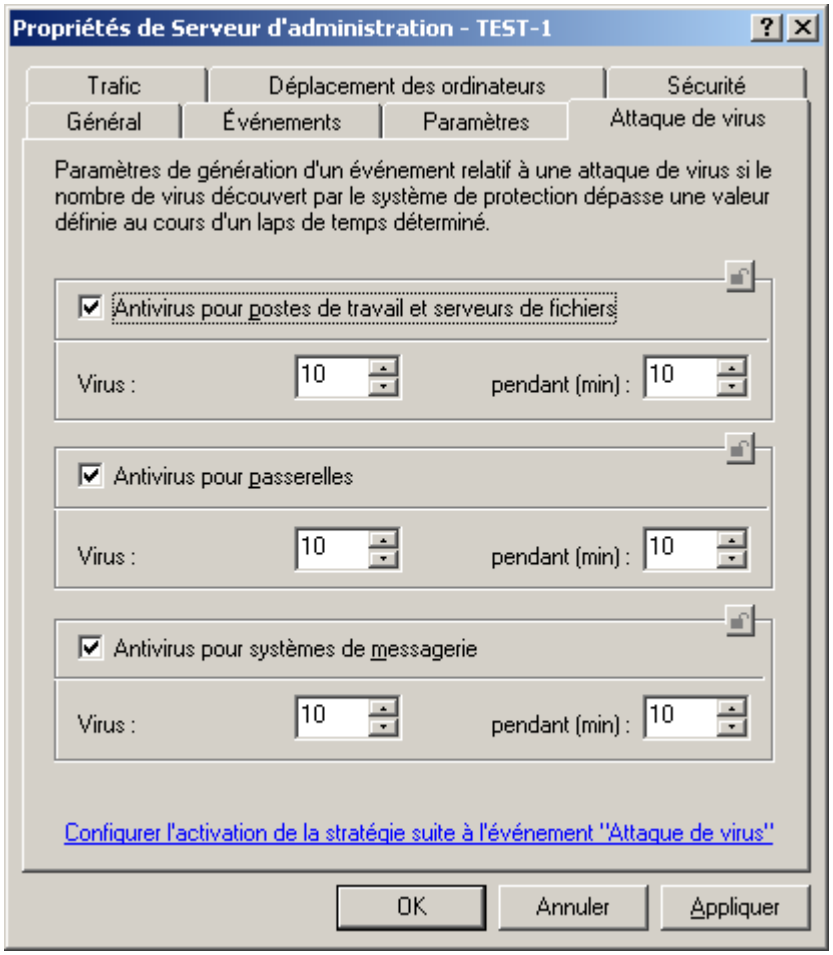


*Illustration 44. Affichage des propriétés du Serveur d'administration. Onglet **Attaque de virus***

L'événement **Attaque de virus** est déclenché sur la base des événements **Détection de virus, de vers, de chevaux de Troie et de programmes nuisibles** et **Virus découvert** dans le fonctionnement des applications antivirus. Par conséquent, pour pouvoir identifier correctement une épidémie de virus, toutes les informations relatives à ces événements doivent être enregistrées sur le Serveur d'administration. Il faut pour cela cocher les paramètres correspondant dans les stratégies pour toutes les applications antivirus. Dans la fenêtre des propriétés des événements **Détection de virus, de vers, de chevaux de Troie et de programmes nuisibles** et **Virus découvert** la case **Sur le Serveur d'administration pendant (jours)** doit être cochée.

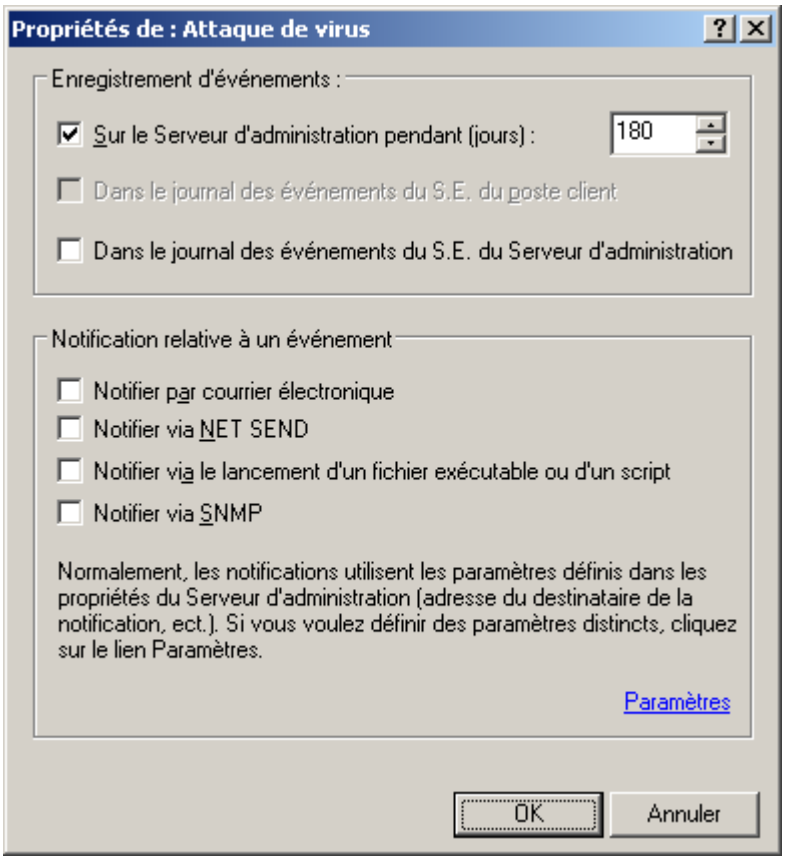


Illustration 45. Configuration de l'enregistrement de l'événement

L'ordre de notification sur l'événement **Attaque de virus** est défini sur le Serveur d'administration dans les propriétés de l'événement sous l'onglet **Notification** (cf. ill. ci-après).

En guise de réaction face à une épidémie émergente, il est possible de définir le remplacement automatique de la stratégie en cours pour les applications. La sélection de stratégies pour chaque type d'attaque de virus est définie dans la fenêtre **Activation des stratégies** ouverte à l'aide du lien **Configurer l'activation de la stratégie suite à l'événement "Attaque de virus"** situé dans la fenêtre de configuration du Serveur d'administration sous l'onglet **Attaque de virus**.

Sous le titre **Détection de virus, de vers, de chevaux de Troie et de programmes nuisibles** et **Objet infecté découvert** on trouvera uniquement les informations en provenance des postes clients du Serveur d'administration principal. L'événement **Attaque de virus** est configuré individuellement pour chaque Serveur secondaire.

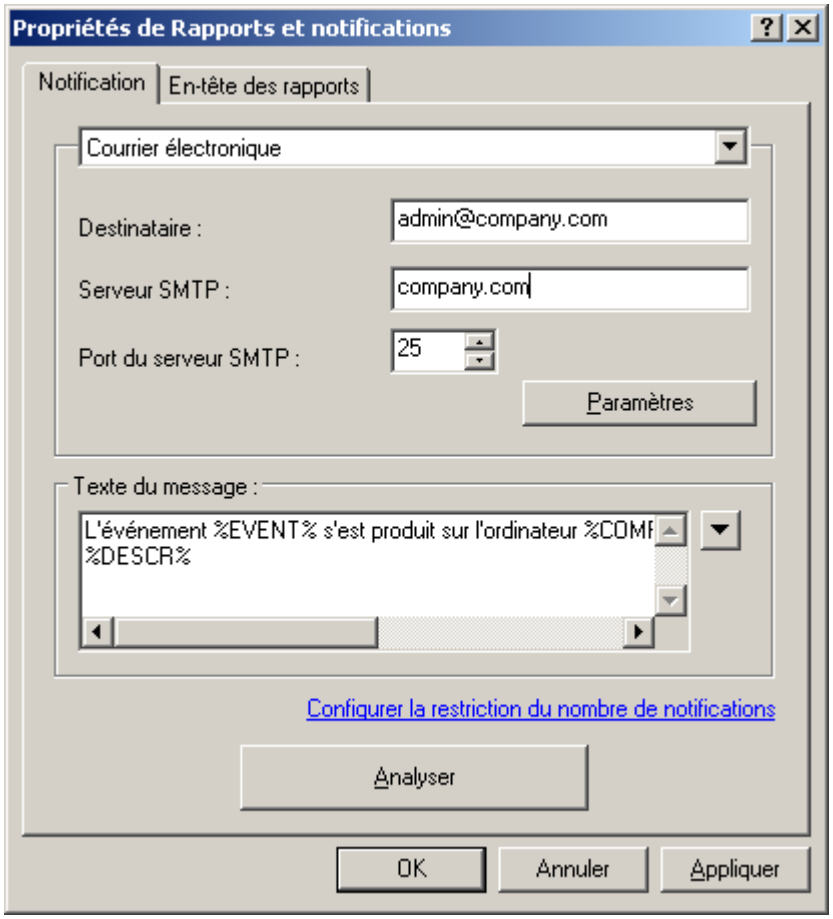


Illustration 46. Modification des paramètres de notification par courrier électronique

FICHIERS AVEC UN TRAITEMENT DIFFERE

Les informations relatives aux fichiers, dont l'analyse et la réparation ont été différées, figurent dans le dossier **Fichiers avec un traitement différé** du nœud **Stockages**. L'information sur tous ces fichiers sur les Serveurs d'administration et les postes clients s'accumule dans le dossier.

L'analyse et la réparation différées ont lieu à la demande ou après la réalisation d'un événement déterminé. Il est possible de configurer les paramètres pour la réparation différée d'une sélection de fichiers.

COPIE DE SAUVEGARDE ET RESTAURATION DES DONNEES DU SERVEUR D'ADMINISTRATION

La copie de sauvegarde permet de déplacer le Serveur d'administration d'un ordinateur vers un autre sans perte l'information et de restaurer les données lors du déplacement de la base d'informations du Serveur d'administration sur un autre ordinateur ou lors du passage à une version plus récente de l'application Kaspersky Administration Kit.

Lors de la suppression du Serveur d'administration d'un ordinateur, Kaspersky Administration Kit propose toujours de créer une copie de sauvegarde.

En cas de copie de sauvegarde, les éléments suivants sont enregistrés ou peuvent être restaurés :

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

La restauration des données en cas de passage à une version plus récente de l'application est prise en charge à partir de Kaspersky Administration Kit version 5.0 Maintenance Pack 3.

Si le chemin d'accès au dossier partagé a été modifié au moment de la restauration des données du Serveur d'administration, il faut vérifier le bon fonctionnement des tâches, où ce dossier est utilisé (tâches de mise à jour, d'installation à distance) et, le cas échéant, introduire les modifications requises dans les paramètres.

La copie des données du Serveur d'administration pour la copie de sauvegarde et la restauration ultérieure peut être réalisée par la tâche **de copie de sauvegarde des données** ou manuellement à l'aide de l'utilitaire *klbackup* repris dans la distribution de Kaspersky Administration Kit. La restauration des données a lieu uniquement à l'aide de l'utilitaire *klbackup*.

Après l'installation du Serveur d'administration, l'utilitaire *klbackup* est enregistré dans le dossier d'installation du composant désigné pendant l'installation, et copie ou restaure les données en fonction de l'argument saisi dans la ligne de commande pour lancer son exécution.

La tâche de copie de sauvegarde est créée manuellement dans le nœud **Tâches de Kaspersky Administration Kit**. Pour que la copie de sauvegarde des données ait lieu, il faut configurer les paramètres de cette tâche. Vous pouvez également créer une tâche de copie de sauvegarde des données manuellement : en guise d'application, pour laquelle la tâche est créée, sélectionnez **Kaspersky Administration Kit** ; en guise de tâche, sélectionnez **Sauvegarde des données du Serveur d'administration**.

GLOSSAIRE

A

Administrateur de Kaspersky Administration Kit

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

Administration centralisee de l'application

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

Administration directe de l'application

Administration de l'application via l'interface locale.

Agent d'administration

Composant de l'application Kaspersky Administration Kit qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant est unique pour toutes les applications Windows de la ligne de produits de la société. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

Agent de mise 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 via Kaspersky Administration Kit.

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. Afin d'améliorer la détection des menaces, il est conseillé de copier fréquemment la mise à jour des bases depuis les serveurs de mises à jour de Kaspersky Lab.

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 lors de l'installation du Serveur d'administration et enregistré dans le sous-dossier Cert du dossier d'installation de l'application.

Client du Serveur d'administration (poste client)

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

Console d'administration Kaspersky

Composant de l'application Kaspersky Administration Kit, 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 créées 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 depuis 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 LA 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 Administration Kit.

INSTALLATION A L'AIDE D'UN SCENARIO DE LANCEMENT

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.

L

LICENCE ACTIVE

Licence utilisée pour l'instant par l'application de Kaspersky Lab. Elle définit la durée de validité de l'ensemble des fonctions, ainsi que la politique de licence vis-à-vis de l'application. L'application ne peut compter plus d'une licence dont l'état est " active ".

LICENCE COMPLEMENTAIRE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais pas encore activée. La licence complémentaire entrera en vigueur à la fin de la durée de validité de la licence en cours.

M

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application) récupérés 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.

O

OPERATEUR DE KASPERSKY ADMINISTRATION KIT

Utilisateur, qui est responsable de l'état et du fonctionnement du système de protection administré à l'aide de Kaspersky Administration Kit.

P

PAQUET D'INSTALLATION

Sélection de fichiers pour l'installation à distance de l'application Kaspersky Lab à l'aide du système d'administration à distance Kaspersky Administration Kit. Le paquète 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 sa 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, paramètres des performances de l'application, paramètres de génération des rapports, 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 via 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 Kaspersky Administration Kit.

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 Administration Kit - 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 Administration Kit – élaborer et 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 de données 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 référentiel des paquets d'installation des applications pour l'installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;
- le certificat du Serveur d'administration.

REFERENTIEL 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.

S

SAUVEGARDE

Création d'une copie de sauvegarde d'un fichier avant sa suppression ou sa 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 de données 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 référentiel 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 Administration Kit, qui remplit la fonction d'enregistrement centralisé d'informations sur les applications Kaspersky Lab, installées sur le réseau local de la société, et d'un outil efficace de gestion de ces applications.

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 VIRALE

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 virale 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.

STRATEGIE

Sélection des paramètres de fonctionnement de l'application dans le groupe d'administration en cas d'administration à l'aide de Kaspersky Administration Kit. 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.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège se trouve en Fédération de Russie, et les bureaux sont ouverts au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, Pologne, Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches anti-virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus. Grâce à l'analyse continue de l'activité virale, nous savons prévoir les tendances dans le développement des programmes malveillants et fournir à l'avance à nos utilisateurs la protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement des systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Kaspersky® Anti-Virus, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : postes de travail, serveurs de fichiers, systèmes de messagerie, pare-feu et passerelles Internet, ordinateurs de poche. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants internationaux utilisent le noyau Kaspersky Anti-Virus dans leurs produits : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirus pour entreprise. Nos bases antivirus sont mises à jour toutes les heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site officiel de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie de virus :	http://www.viruslist.com/fr
Laboratoire Anti-Virus :	newvirus@kaspersky.com (uniquement pour l'envoi des objets suspects archivés) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les demandes auprès des experts en virus)

INDEX