KASPERSKY LAB

Kaspersky® Administration Kit version 6.0

Manuel de l'administrateur

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Manuel de l'administrateur

Consultez notre site Web : http://www.kaspersky.com/

Date de révision : février 2007

Sommaire

CHAPITRE 1. KASPERSKY ADMINISTRATION KIT

1.1. Présentation de Kaspersky Administration Kit

Kaspersky® Administration Kit est une application conçue pour centraliser les tâches d'administration les plus importantes, en rapport avec la sécurité antivirus de réseaux corporatifs utilisant les applications Kaspersky Lab fournies avec les produits Kaspersky Anti-Virus Business Optimal et Kaspersky Corporate Suite. Kaspersky Administration Kit prend en charge toutes les configurations réseau utilisant le protocole TCP/IP.

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

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

- Déployer des applications à travers le réseau sur des ordinateurs distants sous Windows. 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.
- Contrôle des licences. Cette fonction permet d'installer des clés de licence pour toutes les applications Kaspersky Lab de manière centralisée, de surveiller la bonne application du Contrat de licence (c'est à dire, que le nombre de licences est en accord avec le nombre d'applications en cours d'exécution sur le réseau) ainsi que leur date de péremption.
- Gérer à distance des applications Kaspersky Lab à travers un réseau permettant de connecter des ordinateurs Windows. 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 sur plusieurs édifices ou bureaux séparés. Cette caractéristique permet à l'administrateur de :
    - Grouper les postes en tant que *groupes administratifs*, 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 de groupe*.

- Configurer des paramètres isolés de l'application dans le cas de postes séparés, à l'aide des *Paramètres d'application*.
- Gérer l'activité des applications de manière centralisée en créant et en exécutant des *tâches locales ou de groupe*.
- Créer des modèles individualisés de fonctionnement d'une application, avec la création et l'exécution de tâches sur plusieurs postes appartenant à différents groupes administratifs.

- Mettre à jour automatiquement la base antivirus et les modules de programme sur les ordinateurs. Cette fonction permet d'assurer une mise à jour centralisée de la base antivirus 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.
- Recevoir des rapports à l'aide d'un poste dédié. 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 sur l'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, par exemple, correspondre à la détection d'un nouveau virus, d'une erreur apparue en essayant de mettre à jour la base antivirus sur un ordinateur, ou d'un nouvel ordinateur sur le réseau.
- Collaborer avec le système Cisco Network Admission Control (NAC). Cette fonction permet d'introduire les correspondances entre les conditions de protection antivirus de l'ordinateur et les états Cisco NAC.

Kaspersky Administration Kit se présente sous la forme de trois composants principaux :

- **Le serveur d'administration (Administration Server)** 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.
- **L'agent réseau (Réseau Agent)** 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 prend en charge toutes les applications Windows présentes dans Kaspersky Lab Business Optimal et Kaspersky Corporate Suite. Il existe des versions de l'agent réseau spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

- **La console d'administration** fournit l'interface utilisateur nécessaire pour les services administratifs du serveur d'administration et de l'agent réseau. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console).

1.2. Spécifications matérielles et logicielles

Serveur d'administration

- Configuration logicielle :
    - Microsoft Data Access Components (MDAC) version 2.8 ou supérieur
    - MSDE 2000 SP 3 ; MS SQL Server 2000 SP 3 ou supérieur ; MySQL version 5.0.22 (page de code UTF-8 par défaut) ; MS SQL 2--5 ou supérieur ou MS SQL 2005 Express ou supérieur ;MSDE 2000 SP 3, MS SQL Server 2000 SP 3,[1] ou supérieur
    - Microsoft Windows 2000 SP 1 ou supérieur ; Microsoft Windows XP Professional SP 1 ou supérieur ; Microsoft Windows XP Professional x64 et supérieur ; Microsoft Windows Server 2003 ou supérieur ; Microsoft Windows Server 2003x64 ou supérieur ; Microsoft Windows NT4 SP 6a ou supérieur ; Microsoft Windows Vista.
- Configuration matérielle :
    - Processeur Intel Pentium III de 800 MHz ou supérieur
    - 128 Mo de RAM
    - 400 Mo d'espace disponible sur le disque

Console d'administration

- Configuration logicielle :
    - Microsoft Windows 2000 SP 1 ou supérieur ; Microsoft Windows NT4 SP 6a ; Microsoft Windows XP Professional SP 1 ou supérieur ; Microsoft Windows XP Home Edition SP1 ou supérieur ; Microsoft Windows XP Professional x64 ou

[1] Vous pouvez installer MSDE depuis la distribution de Kaspersky Administration Kit.

supérieur. Microsoft Windows Server 2003 ou supérieur ; Microsoft Windows Server 2003 x64 et supérieure ; Microsoft Windows NT 4 SP 6a ou supérieur ; Microsoft Windows Vista , Microsoft Windows Vista x64;

- Microsoft Management Console version 1.2 ou supérieur

- Configuration matérielle :
  - Processeur Intel Pentium II de 400 MHz ou supérieur
  - Au moins 64 Mo RAM.
  - 10 Mo d'espace de disque libre.

Agent réseau

- Configuration logicielle :
  - Pour les systèmes Windows :

    Microsoft Windows 98 ; Microsoft Windows ME ; Microsoft Windows 2000 SP 1 ou supérieur ; Microsoft Windows NT4 SP 6a ou supérieur ; Microsoft Windows XP Professional x64 ou supérieur ; Microsoft Windows XP Professional SP 1 ou supérieur et and Windows Server 2003 ou supérieur ; Microsoft Windows Server 2003 x64 ou supérieur ; Microsoft Windows Vista.
  - Pour les systèmes Novell :

    Novell NetWare 6 SP3 ou supérieur ; Novell NetWare 6.5 SP3 ou supérieur.
- Configuration matérielle :
  - Pour les systèmes Windows :
    - Processeur Intel Pentium à 233 MHz ou supérieur
    - 32 Mo de RAM
    - 10 Mo d'espace disponible sur le disque
  - Pour les systèmes Novell :
    - Processeur Intel Pentium à 233 MHz ou supérieur
    - 12 Mo de RAM
    - 32 Mo d'espace disponible sur le disque

1.3. Contenu de la distribution

Ce progiciel est accompagne gratuitement toutes les applications de Kaspersky Lab distribuées avec Kaspersky Antivirus Business Optimal et Kaspersky Corporate Suite (version vendue en boîte) et se trouve également disponible pour la vente sur le site corporatif de Kaspersky Lab à l'adresse www.kaspersky.com.

1.4. Services réservés aux utilisateurs inscrits

Kaspersky Lab propose un large éventail de services à ses utilisateurs inscrits leur permettant d'utiliser plus efficacement les produits Kaspersky Lab .

Quand vous achetez la licence de l'un des produits Kaspersky Lab inclus dans Kaspersky Antivirus Business Optimal ou dans Kaspersky Corporate Suite, vous devenez un utilisateur inscrit de Kaspersky Administration Kit. Par la suite vous pourrez bénéficier des services suivants pour la durée de votre licence :

- Nouvelles versions de ce logiciel antivirus, fournies gratuitement ;
- Assistance téléphonique et par formulaire pré-rempli sur le Web sur l'installation, la configuration et l'utilisation de l'application antivirus ;

  Avant de soumettre une consultation au service d'assistance technique, assurez-vous de connaître les informations de licence relatives aux applications de Kaspersky Lab utilisée avec Kaspersky Administration Kit.

- Informations sur les nouveaux produits Kaspersky Lab et les nouveaux virus d'ordinateurs (pour les abonnés au bulletin).

Kaspersky Lab ne fournit pas d'informations concernant l'administration ou l'utilisation de votre système d'exploitation ou d'autres technologies.

1.5. Objectif du document

Ce guide décrit les objectifs, les concepts généraux, les fonctions et les schémas de fonctionnement généraux de l'application Kaspersky Administration Kit. Vous trouverez une description pas à pas des actions dans le livre de référence de Kaspersky Administration Kit. Les fonctions décrites dans le manuel de référence sont soulignées.

Pour lire les questions les plus fréquentes que nos utilisateurs posent aux spécialistes du service support de Kaspersky Lab, visitez notre site Web et suivez le lien **Services →Base de connaissances**. Cette section contient des informations sur l'installation, la configuration et le fonctionnement des applications Kaspersky Lab, sur la suppression des virus les plus répandus, ainsi que sur la désinfection des fichiers infectés.

1.6. Conventions

Plusieurs conventions ont été adoptées dans ce guide en fonction du contenu et de l'intérêt de chaque section particulière. Le tableau ci-après illustre les conventions utilisées dans ce manuel.

Convention	Usage
Gras	Titres de menus, commandes, titres de fenêtres, éléments de boîtes de dialogue, etc.
Note	Information complémentaire, remarques.
Attention!	Informations essentielles.
Pour exécuter une action : 1. Étape 1. 2. …	Description de la succession des étapes que l'utilisateur doit suivre et des actions possibles.
[option] - nom du paramètre	Paramètre de ligne de commande.
`Texte des messages d'information et de la ligne de commande`	Texte des fichiers de configuration, des messages d'information et de la ligne de commande.

CHAPITRE 2. PRESENTATION DE KASPERSKY ADMINISTRATION KIT

2.1. Réseau logique

2.1.1. Réseau logique. Serveur d'administration.

Le réseau logique est une structure hiérarchique de *groupes administratifs* contenant des *postes clients*. Les applications Kaspersky Lab installées sur les postes clients sont contrôlées par Kaspersky Administration Kit.

Un serveur d'administration est un ordinateur équipé du composant Administration Server.

Le serveur d'administration est installé sur un ordinateur en tant que service avec les attributs suivants :

- Nommé Kaspersky Administration Server ;
- Avec lancement automatique au démarrage du système d'exploitation ;
- Utilise le profil système Local ou utilisateur en fonction du choix réalisé lors de l'installation du composant.

Les fonctions du serveur d'administration (ou, plus exactement, de l'application serveur d'administration installée sur ce poste) sont les suivantes :

- Entreposer la description de la structure logique du réseau (configuration réseau) ;
- Conserver des copies de sauvegarde des données de configuration des postes du réseau logique ;
- Entreposer les fichiers de distribution des applications Kaspersky Lab ;
- Installer et désinstaller à distance des applications sur les ordinateurs ;
- Mettre à jour la base antivirus et les modules de programme ;
- Contrôler les stratégies et les tâches sur les ordinateurs du réseau logique ;
- Entreposer des informations sur les événements qui se sont produits sur les ordinateurs du réseau logique ;

- Générer des rapports sur l'exécution des applications à travers le réseau logique ;
- Distribuer des clés de licence sur les ordinateurs du réseau logique, conserver les données des clés de licence ;
- Envoyer des alertes à partir de tâches exécutées sur les ordinateurs du réseau logique. Vous pouvez être informé, par exemple, de la détection d'un virus sur un poste client.

2.1.2. Hiérarchie des serveurs d'administration

Les serveurs d'administration peuvent former une hiérarchie sur le modèle **« serveur principal – serveur secondaire ».** Chaque serveur d'administration peut avoir plusieurs serveurs secondaires sur le même niveau de hiérarchie ou sur des niveaux imbriqués. Le niveau d'imbrication des serveurs secondaires n'est pas limité. Dans ce cas, la structure du réseau logique du serveur principal inclura les réseaux logiques de tous les serveurs secondaires. Cette façon de procéder permet à différents serveurs d'administration de gérer des sections individuelles du réseau indépendamment des autres et d'être à leur tour contrôlés par le serveur principal (pour plus de détails, voir section 3.5.1 à la page 46).

Il est possible de créer une hiérarchie de serveurs :

- Pour réduire la charge du serveur d'administration (par rapport à un seul serveur exploité sur le réseau) ;
- Pour réduire le trafic réseau et simplifier l'interaction avec des bureaux décentralisés. Il n'est pas nécessaire d'établir de connexion entre le serveur principal et tous les ordinateurs du réseau situés, par exemple, dans d'autres régions. Il suffit d'installer un serveur d'administration secondaire sur chacun des segments du réseau, de distribuer les postes sur les réseaux logiques des serveurs secondaires et d'assurer une connexion entre les serveurs secondaires et le serveur principal par des voies de communication rapide ;
- Pour garantir une subdivision claire des responsabilités entre les administrateurs de sécurité. Toutes les caractéristiques de contrôle centralisé et de gestion de la sécurité antivirus du réseau corporatif seront préservées.

Chaque ordinateur inclut dans une structure de réseau logique ne doit être connecté qu'à un seul et unique serveur d'administration.

L'administrateur doit contrôler les connexions des postes clients aux serveurs d'administration, en se servant de la fonction de recherche d'ordinateurs d'après leurs attributs réseau, à travers les réseaux logiques de multiples serveurs.

2.1.3. Poste client et Groupe

Les interactions entre le serveur d'administration et les ordinateurs, à savoir :

- Production d'informations sur l'état actuel des applications ;
- Envoi et réception de commandes de contrôle ;
- Synchronisation des données de configuration ;
- Envoi d'informations sur les événements au cours de l'exécution des applications sur le serveur ;
- Fonctionnement de l'agent de mises à jour ;

sont prises en charge par l'agent réseau. Ce component doit être installé sur tous les ordinateurs dont des applications Kaspersky Lab sont sous le contrôle de Kaspersky Administration Kit.

L'agent réseau est installé dans l'ordinateur en tant que service, avec les attributs suivants :

- son nom est **Kaspersky Network Agent** ;
- lancement automatique au démarrage du système d'exploitation ;
- utilise le profil **système Local**.

Un plug-in permettant la collaboration avec le système Cisco NAC est installé en même temps que l'agent réseau. Ce plug-in est actif lorsque l'application Cisco Trust Agent est présente sur l'ordinateur. Les paramètres relatifs à la collaboration avec le système Cisco NAC doivent être définis dans les propriétés du serveur d'administration.

Un ordinateur (serveur ou poste de travail) sur lequel sont installés l'agent réseau et des applications Kaspersky Lab contrôlées est appelé **client du serveur d'administration** (ou plus simplement *poste client*).

En fonction de l'organisation ou de la structure géographique de la société, des opérations effectuées et de la sélection d'applications Kaspersky Lab installées, les postes clients peuvent s'organiser en tant que *groupes administratifs*. Cette solution peut intervenir pour simplifier la gestion des ordinateurs appartenant au groupe, considérés comme une entité simple ; l'administrateur peut alors librement combiner les ordinateurs en groupes selon n'importe quel principe ou attributs. Par exemple, le niveau supérieur peut être composé de groupes correspondants aux divers départements. Sur le niveau suivant, sous chaque

département, les ordinateurs sont regroupés d'après les fonctions qu'ils assurent : un premier groupe inclut tous les postes de travail, un second groupe, uniquement les serveurs de fichiers, etc.

Un **groupe** est une sélection de postes clients regroupés par un attribut commun, permettant de les gérer comme s'il s'agissait d'une entité simple. Tous les postes clients d'un même groupe partagent :

- Des paramètres communs de fonctionnement des applications, par des *stratégies de groupe* ;
- Un mode fonctionnement des applications commun – par la création de *tâches de groupe* (fonctions d'applications) employant un ensemble défini de paramètres (par exemple, pour la création et l'installation d'un unique *paquet d'installation*, pour la mise à jour de la base antivirus et des modules d'application, pour l'analyse à la demande de l'ordinateur et pour la protection en temps réel).

Un poste client ne peut appartenir qu'à un seul groupe.

L'administrateur peut ainsi créer une hiérarchie de serveurs et de groupes avec un nombre quelconque d'imbrications, si cela lui simplifie les tâches d'administration des applications. Les serveurs d'administration secondaires, les groupes et les ordinateurs peuvent figurer sur le même niveau hiérarchique.

2.1.4. Postes de travail des administrateurs

Les ordinateurs du réseau d'entreprise sur lesquels la console d'administration est exécutée, sont eux-mêmes désignés comme **postes administrateurs**. À partir de ces postes, les administrateurs peuvent contrôler à distance tous les composants Kaspersky Antivirus installés sur l'ensemble du réseau logique.

Après son installation, l'icône de la console d'administration apparaît dans le menu **Démarrer/Programmes/Kaspersky Administration Kit**.

Le poste de travail de l'administrateur n'est pas un objet du réseau logique. Cependant, ils peuvent être ajoutés au réseau logique en tant que postes clients. Le nombre de postes administrateur est potentiellement illimité. Les postes administrateurs de différents réseaux logiques peuvent coïncider – n'importe quel réseau logique peut être administré à partir de n'importe quel poste administrateur disponible sur votre réseau local.

Sur un réseau logique, un même ordinateur peut figurer en tant que poste client, serveur d'administration et poste administrateur.

2.1.5. Plug-in d 'administration des applications

Plug-in de console pour l'agent réseau, un composant spécial qui fournit l'interface de gestion de chaque application via la console d'administration, il est distribué avec les applications Kaspersky Lab contrôlées par Kaspersky Administration Kit . Chaque application dispose de son propre plug-in, installé sur le poste administrateur. Les plug-ins fournissent :

- Des boîtes de dialogue pour créer et modifier les stratégies d'applications
- Des boîtes de dialogue pour créer et modifier la configuration des applications
- Des boîtes de dialogue pour la configuration de tâches
- Des renseignements sur les tâches exécutées par une application
- Des informations sur les événements générés par une application
- Des informations sur les événements et les statistiques de chaque poste client, transmis à la console d'administration.

2.1.6. Stratégies, paramètres, et tâches

Une **tâche** est une action effectuée par une application de Kaspersky Lab. Il y a plusieurs types de tâches, qui sont classées d'après leurs fonctions. À chaque tâche correspondent des paramètres spécifiques d'application.

Une sélection de paramètres de fonctionnement de l'application est associée à la tâche, puis appliquée lors de son exécution. L'ensemble des paramètres de l'application qui sont communs à tous les types de tâches, définissent les paramètres de l'application. Les paramètres de fonctionnement de l'application qui sont propres à chacune des tâches, constituent les paramètres de tâche. Les paramètres d'application et les paramètres de tâche ne se superposent pas.

Pour plus d'informations sur les types de tâche, reportez-vous à la documentation des applications Kaspersky Lab.

Pour qu'une application puisse réaliser une action, il faut configurer les paramètres de l'application, créer et configurer une tâche associée puis l'exécuter.

Les paramètres d'application définis pour chaque poste client individuel depuis l'interface locale, ou à distante depuis une console d'administration, seront appelés les **paramètres locaux de l'application**.

La configuration centralisée des paramètres de fonctionnement des applications installées sur les postes clients du réseau logique est assurée par la définition de stratégies.

Une stratégie – est un ensemble de paramètres d'une application dans un groupe. **Une stratégie** contient la configuration complète de toutes les fonctions de l'application, à l'exclusion des paramètres liés aux tâches individuelles. Les paramètres de planification sont un bon exemple de ce type de configuration.

Par conséquent, une stratégie inclut les paramètres suivants :

- Paramètres communs à tous les types de tâches ou paramètres d'application ;
- Paramètres communs à toutes les tâches individuelles, de chaque type – soit la plupart des paramètres de tâche.

Ceci signifie qu'une stratégie de application antivirus (Figure 1) contenant des tâches comme la protection en temps réel et l'analyse à la demande, inclut tous les paramètres nécessaires à l'application, pour exécuter ces deux types de tâches, mais ne contient pas, par exemple, la planification de l'exécution de ces tâches, ni les paramètres permettant de définir la portée de l'analyse.

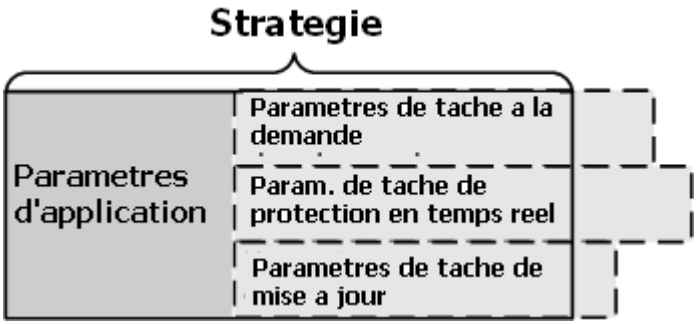


Figure 1. Stratégie

Chaque paramètre de stratégie possède un attribut de verrouillage qui indique si ce paramètre est modifiable aux niveaux imbriqués de la stratégie (dans le cas de groupes imbriqués et de serveurs d'administration secondaires), et figure dans les paramètres de tâche et les paramètres locaux de l'application. S'il existe un tel "verrou" associé ce paramètre, vous ne pourrez pas redéfinir sa valeur (voir section 2.1.6 à la page 16).

Chacune des applications d'un groupe possède sa propre définition de stratégie. De nombreuses stratégies avec des paramètres différents peuvent être définies pour la même application. Mais chacune des applications ne peut avoir qu'une seule stratégie active.

Il est prévu de permettre à un utilisateur d'activer une stratégie inactive après un événement, ce qui permet, par exemple, de renforcer la configuration de la protection antivirus en périodes de virulences.

Vous pouvez également créer des stratégies pour des utilisateurs mobiles. Ce type de stratégie est mis en œuvre quand l'ordinateur se déconnecte du réseau logique corporatif.

Selon les groupes les paramètres de fonctionnement de l'application peuvent être différents. Il est possible de créer dans chaque groupe une stratégie séparée pour une application.

Les groupes et serveurs d'administration secondaires imbriqués héritent des stratégies de groupe définies au niveau supérieur de la hiérarchie.

La création et la configuration de tâches sur le réseau logique sont centralisées. Une tâche attribuée à un groupe administratif est une **tâche de groupe** ; une tâche attribuée à un poste client individuel est une **tâche locale** ; et celle attribuée à de multiples postes clients, appartenant à différents groupes du réseau logique, est une **tâche globale**.

Une tâche de groupe peut être affectée à un groupe, même si l'application Kaspersky Lab n'est installée que sur certains postes clients du groupe. Dans ce cas, la tâche de groupe ne sera exécutée que sur les ordinateurs où l'application est exploitée.

Les groupes et serveurs d'administration secondaires imbriqués héritent des tâches de leurs groupes parent. Une tâche définie dans un groupe sera donc partagée par tous les postes client de ce groupe, mais aussi par tous les postes des groupes et par les serveurs secondaires des niveaux inférieurs de la hiérarchie.

Les tâches attribuées localement sur un poste client en particulier ne sont exécutées que sur cet ordinateur. Les tâches locales sont ajoutées à la liste des tâches courantes du client, lors de la synchronisation de ce poste avec le serveur d'administration.

Étant donné que les paramètres d'application sont régis par la stratégie, vous ne pourrez redéfinir que les paramètres définis comme modifiables par cette stratégie, ou encore, ceux qui sont spécifiques à une tâche particulière. Par exemple, pour une analyse à la demande d'une unité, vous devez pouvoir indiquer le nom du disque, les masques de fichier, etc.

Il est possible de planifier le démarrage automatique de tâches, ou les exécuter à la demande. Les comptes-rendus d'activité des tâches sont enregistrés sur le serveur d'administration ainsi que sur le poste client. L'administrateur peut être averti des comptes-rendus d'activité, ou afficher des rapports détaillés.

Les informations sur les stratégies, la configuration des applications et les tâches globales ou de groupe sont stockées sur le serveur et distribuées vers les postes clients pendant la synchronisation. En provenance des clients, le serveur d'administration reçoit des informations sur les modifications locales autorisées

par la stratégie, sur les applications exploitées sur les postes clients, sur leurs comptes-rendus et sur les tâches affectées.

2.1.7. Rapports entre stratégies et paramètres locaux des applications

Par l'utilisation de stratégies pour tous les ordinateurs appartenant à un groupe, vous pouvez définir les mêmes valeurs pour les paramètres de fonctionnement de l'application.

Les valeurs des paramètres définis par une stratégie peuvent être redéfinies dans le cas d'ordinateurs individuels du groupe, à l'aide des paramètres locaux de l'application. Cependant, vous pouvez seulement modifier les valeurs des paramètres dont la modification n'est pas interdite par la stratégie : c'est à dire que ces paramètres ne doivent pas être « verrouillés ».

La valeur utilisée sur le poste client (Figure 2) dépendra du « verrouillage » du paramètre par la stratégie.

- Si toutes les modifications du paramètre sont interdites, tous les postes clients utiliseront la même valeur définie par la stratégie ;
- Si les modifications du paramètre sont autorisées, alors chaque poste client utilise une valeur locale de ce paramètre, au lieu de la valeur définie par la stratégie. Dans ce cas, la valeur du paramètre peut être modifiée depuis les paramètres locaux de l'application.

Par conséquent, lorsqu'une tâche est en exécution sur un poste client, les paramètres d'application sont déterminés par :

- Les paramètres de tâche et les paramètres locaux de l'application, si la stratégie n'interdit pas la modification du paramètre ;
- Une stratégie de groupe, si la stratégie n'interdit pas la modification du paramètre.

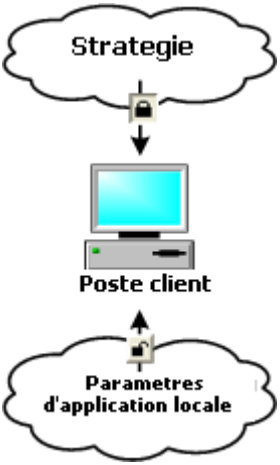


Figure 2. Stratégie et paramètres locaux de l'application

La fenêtre **Avancé** (Figure 14) de l'option de configuration de la stratégie de l'application permet de modifier ultérieurement les paramètres locaux de l'application, après une première application de la stratégie.

2.2. Connexion de clients au serveur d'administration

Pour permettre aux clients et au serveur d'administration de communiquer entre eux, les postes clients doivent être reliés au serveur (voir section 2.1 à la page 12). L'installation de l'agent réseau sur les clients assure cette fonctionnalité.

Les opérations suivantes exigent la connexion au serveur :

- Rafraîchissement de la liste des applications installées sur les postes clients
- Synchronisation des stratégies, des paramètres d'application, des tâches, et des paramètres de tâches
- Mise à jour de l'information sur les applications et les tâches fonctionnant sur des postes clients
- Transfert des événements à traiter sur le serveur

Dans la plupart des cas, les clients sont connectés au serveur. Cette connexion est utilisée pour échanger automatiquement des données entre les clients et le serveur, et pour retourner vers les serveurs des notifications sur les événements d'application.

La synchronisation automatique est exécutée à intervalles réguliers, définis dans la configuration de l'agent réseau (par exemple, une fois toutes les quinze minutes). L'intervalle de temps est défini par l'administrateur.

Des informations sur un événement sont envoyées au serveur juste après l'événement.

Dans les paramètres client, vous pouvez cocher/annuler la case **Maintenir la connexion** pour conserver ou terminer la connexion client-serveur après la fin des opérations précédentes. Une connexion permanente est préférable si la connexion d'un client s'avère difficile pour n'importe quelle raison (le client se trouve derrière un pare-feu, l'adresse IP du client n'est pas connue, etc.) ou si vous avez besoin de surveiller constamment l'exécution des applications Kaspersky Lab.

L'administrateur peut forcer le démarrage de la synchronisation avec la commande **Forcer synchronisation** du menu contextuel (voir section 2.10.4 à la page 32). Dans ce cas, la connexion est établie par le serveur. Pour permettre la connexion, le port UDP est ouvert sur le poste client. Le serveur envoie une requête de connexion au port UDP du client. En réponse, l'autorisation de connexion du serveur est vérifiée (d'après une signature numérique), et, si la signature est valide, la connexion est établie.

Le deuxième type de connexion est également utilisé pour récupérer des données sur les postes clients : mise à jour des listes d'applications et de tâches fonctionnant sur le client et rafraîchissement des statistiques d'application.

2.3. Connexion sécurisée au serveur d'administration

L'échange de données entre clients et serveur d'administration, ainsi que les connexions de la console avec le serveur d'administration sont sécurisées par le protocole SSL (Secure Socket Layer). Le protocole SSL est responsable de l'authentification de la communication aux extrêmes, de l'encodage des données transférées, et d'éviter la modification des données pendant le transfert. Les techniques d'intégrité de données vérifient que les données n'ont pas été endommagées ou modifiées pendant le transfert. Une connexion SSL implique l'authentification des deux extrêmes de la session de communication réseau, et l'encodage des données en utilisant la méthode de clé ouverte.

2.3.1. Certificat du serveur d'administration

Le certificat du serveur d'administration permet d'authentifier la console d'administration au moment où celle-ci établit la connexion au serveur d'administration, ou lorsque les données sont transférées depuis les postes

clients. Le certificat est également utilisé pour l'authentification entre les serveurs d'administrations primaires et secondaires.

Le certificat du serveur d'administration est créé pendant l'installation du serveur d'administration. Le certificat est conservé dans le serveur d'administration, dans le dossier **Cert** du répertoire d'installation.

Le certificat du serveur d'administration ne peut être créé qu'une seule fois, lors de l'installation du serveur. Il est recommandé de le sauvegarder durant l'installation du serveur d'administration, à l'aide de l'assistant d'installation. Pour restaurer le certificat, vous devez réinstaller le serveur d'administration et restaurer les données perdues à partir de celles sauvegardées.

2.3.2. Authentification du serveur d'administration (connexion de la console d'administration au serveur)

Quand la console d'administration se connecte au serveur d'administration pour la première fois, elle demande et enregistre en local le certificat du serveur, sur le poste administrateur. Lors des connexions suivantes de la console avec le serveur du même nom, le serveur sera authentifié en utilisant ce certificat.

Si l'authentification du serveur échoue (le certificat actuel diffère de celui stocké sur le poste administrateur), la console informe l'utilisateur et demande un nouveau certificat au serveur. Si la connexion est réussie et qu'un nouveau certificat est reçu, la console d'administration enregistre celui-ci sur disque, afin de l'utiliser pour authentifier le serveur lors de futures sessions.

2.3.3. Authentification du serveur d'administration au cours de la connexion avec un client

Quand un client se connecte au serveur d'administration pour la première fois, il demande et enregistre en local le certificat du serveur.

Si Agent Réseau est installé en local sur un client, l'administrateur peut sélectionner manuellement le certificat du serveur d'administration.

Quand le client se connecte au serveur la fois suivante, l'agent réseau demande le certificat du serveur d'administration et le compare au certificat local. Si les certificats diffèrent, l'accès du serveur d'administration au poste client est refusé.

Si c'est le serveur d'administration qui lance la connexion, l'agent réseau vérifie de manière similaire la demande d'une connexion UDP par le serveur.

2.4. Identification d'ordinateurs sur le réseau logique

Les postes clients du réseau logique sont identifiés par leurs **noms d'hôte**. Un nom d'hôte doit être unique parmi tous ceux utilisés pour se connecter au serveur d'administration.

Le nom du poste client est transféré au serveur d'administration quand un nouvel ordinateur est détecté sur le réseau Windows, ou quand une instance de l'agent réseau se connecte au serveur pour la première fois après son installation sur le client. Par défaut, le nom d'hôte est le même que celui de l'ordinateur sur le réseau Windows (nom NetBIOS). Si un hôte existe déjà avec ce nom, le serveur attribuera à l'hôte un nom terminé par un nombre, par exemple, **Nom-1**, **Nom-2**, etc. Ce nom d'hôte sera utilisé pour identifier l'ordinateur sur le réseau logique.

2.5. Droits d'accès au réseau logique

Kaspersky Administration Kit offre les types d'autorisation d'accès aux caractéristiques de l'application suivants :

- **Lecture :**
    - Connexion au serveur d'administration ;
    - Affichage de la structure du réseau logique (ou du groupe administratif) ;
    - Affichage des valeurs de stratégie, de tâches et de paramètres de l'application.
- **Exécution :** Démarrage et arrêt des tâches de groupe et des tâches globales existantes ; réception de rapports sur les applications installées sur les postes clients.
- **Écriture :**
    - Création d'un réseau logique, ajout de groupes et de postes clients à ce réseau (ou à un groupe administratif) ;
    - Installation du composant Agent réseau sur le poste client ;
    - Création et installation des paquets d'installation nécessaires aux applications Kaspersky Lab (avec les clés de licence correspondantes) sur les postes clients ;

- Mise à jour de la version des applications installées sur les postes clients ;
- Création de stratégies, de tâches pour des ordinateurs en groupe ou individuellement, configuration des paramètres d'application ;
- Contrôle centralisé des applications par le biais de services fournis par les composants du serveur d'administration, de l'agent réseau et de la console d'administration ;
- Attribution aux utilisateurs et aux groupes d'utilisateurs de droits d'accès aux fonctions de Kaspersky Administration Kit.

Après l'installation du serveur d'administration, les droits nécessaires pour se connecter au serveur et pour travailler dans le réseau logique sont accordés par défaut aux utilisateurs appartenant aux groupes **KLAdmins** et **KLOperators**.

Les données du groupe sont créées, lors de l'installation du composant du serveur d'administration, indépendamment du compte sélectionné pour exécuter le service « Administration Server » :

- dans le domaine contenant le serveur d'administration et sur l'ordinateur du serveur d'administration, si le serveur d'administration est exécuté sous le compte d'un utilisateur compris dans ce domaine ;
- uniquement sur l'ordinateur du serveur d'administration, si ce serveur est exécuté sous le compte système.

Le groupe **KLAdmins** reçoit tous les droits : **Lecture, Exécution, Écriture.** Le groupe **KLOperators** reçoit les droits de **Lecture** et d'**Exécution**. La sélection des droits accordés aux membres **KLAdmins** n'est pas modifiable.

Les utilisateurs compris dans le groupe **KLAdmins** sont appelés **administrateurs du réseau logique**, et les utilisateurs compris dans le groupe **KLOperators**, **opérateurs du réseau logique**.

Vous pouvez afficher les groupes **KLAdmins** et **KLOperators** et les modifier à l'aide des outils standard d'administration de Windows, **Administration / Utilisateurs et groupes locaux**.

En plus des utilisateurs du groupe **KLAdmins** les droits administratifs du réseau logique sont accordés aux :

- Administrateurs de domaine dont les ordinateurs sont incorporés à la structure de ce réseau logique ;
- Administrateurs locaux des ordinateurs équipés du serveur d'administration.

Toutes les opérations lancées par les administrateurs du réseau logique s'exécutent avec les droits du compte du serveur d'administration. Pour chaque serveur d'administration, son propre groupe **KLAdmins** est créé avec des droits exploitables uniquement à l'intérieur de ce réseau logique en particulier.

Si des ordinateurs associés à un domaine créent plusieurs réseaux logiques, l'administrateur du domaine sera aussi celui de chaque réseau logique ainsi construit. Dans ce cas, le réseau logique partagera le même groupe **KLAdmins** créé pendant l'installation du premier serveur d'administration. De nouveaux membres peuvent être ajoutés à ce groupe en utilisant les outils standard d'administration du système. Les opérations lancées par les administrateurs du réseau logique s'exécutent avec les droits du serveur d'administration correspondant.

Dans l'application Kaspersky Administration Kit, les droits d'utilisateur sont attribués conformément à l'authentification d'utilisateur de Windows sur le réseau.

Après l'installation de l'application, l'administrateur du réseau logique peut (voir section 3.2 à la page 38) :

- modifier les droits, accordés aux groupes **KLOperators** ;
- accorder des droits d'accès aux caractéristiques de l'application Kaspersky Administration Kit à d'autres groupes d'utilisateurs et à des utilisateurs individuels enregistrés sur l'ordinateur équipé de la console d'administration ;
- accorder divers droits d'accès pour travailler avec chacun des groupes administratifs.

2.6. Déploiement de la protection antivirus sur les ordinateurs du réseau logique

Deux scénarios habituels permettent d'illustrer la mise en place d'une protection antivirus fiable utilisant Kaspersky Administration Kit :

- Vous pouvez installer à distance, à partir d'un simple poste de travail, des applications sur des postes clients à travers le réseau logique. L'installation et la connexion au système de gestion à distance se font automatiquement, sans aucune interaction de l'administrateur, ce qui permet d'installer le logiciel antivirus sur un nombre quelconque de postes clients.
- Vous pouvez installer, en local, des applications sur chaque ordinateur du réseau. Dans ce cas, il faut installer manuellement tous les composants requis et le poste administrateur. Les paramètres de connexion sont définis pendant l'installation du composant Network Agent. Ce scénario de déploiement est employé seulement si un déploiement centralisé s'avère impossible.

L'installation à distance permet d'installer n'importe quelle application sélectionnée par l'utilisateur.
Cependant, tenez compte du fait que Kaspersky Administration Kit ne peut gérer que les applications Kaspersky Lab dont le paquet de distribution contient un composant spécialisé – le plugin administrateur de l'application.

2.7. Création d'un système de gestion centralisée de la protection antivirus

La première étape pour construire un système de gestion centralisée d'un réseau d'entreprise couvert par Kaspersky Administration Kit, est de concevoir un réseau logique. À ce stade, vous devez prendre les décisions suivantes :

1. Sélectionner des sections isolées du réseau et déterminer le nombre de serveurs d'administration à installer.
2. Quels ordinateurs dans la structure du réseau corporatif vont opérer en tant que serveur d'administration principal, postes administrateurs secondaires et postes clients ? Notez que tous les ordinateurs sur lesquels des applications Kaspersky Lab sont installées agiront en tant qu'ordinateurs de client.
3. Quel critère sera utilisé pour organiser des postes clients dans les groupes ? Quelle sera la hiérarchie du groupe ?
4. Quel scénario de déploiement va-t-il être utilisé : installation à distance ou locale ?

À l'étape suivante, l'administrateur doit construire un réseau logique, c'est à dire, installer les composants suivants de Kaspersky Administration Kit sur les ordinateurs du réseau :

1. Installer le serveur d'administration sur les ordinateurs du réseau corporatif.
2. Installer la console d'administration sur les ordinateurs destinés aux tâches de gestion.
3. Prendre des décisions sur les pouvoirs des administrateurs du réseau logique, de déterminer quelles autres catégories d'utilisateurs pourront opérer avec le système et attribuer une liste de fonctions à réaliser à chaque catégorie.
4. Créer des listes d'utilisateurs et accorder à chaque groupe des droits d'accès requis pour accéder aux fonctions attribuées à chacun.

Ensuite, il faut créer une hiérarchie de serveurs d'administration et, pour chacun d'eux, créer une structure du réseau logique de la manière suivante : créer une

hiérarchie de groupes administratifs et distribuer les ordinateurs parmi les groupes correspondants.

À l'étape suivante, vous devrez installer l'agent réseau et les applications Kaspersky Lab sélectionnées sur des postes clients, puis installer les plug-ins de console correspondants sur le poste administrateur.

Les applications Kaspersky Lab administrables à l'aide de Kaspersky Administration Kit ne peuvent pas toutes être installées à distance. Pour de plus amples détails, reportez-vous à la documentation de l'application concernée.

Si vous utilisez l'option d'installation à distance, l'agent réseau peut être installé en même temps que n'importe quelle application, sans qu'il soit nécessaire de le faire séparément.

Pour finir, il faudra configurer les applications installées : affectation et application des stratégies de groupe (voir section Chapitre 4 à la page 53) puis création de tâches (voir section 4.1.2 à la page 58).

En utilisant l'Assistant Démarrage rapide, l'administrateur peut facilement établir un système de protection antivirus pour son réseau et le configurer sommairement (pour une description détaillée de l'Assistant, (voyez 3.2 à la page 38). Pour simplifier, la configuration du système de protection antivirus équivaut à la création d'un réseau logique de structure identique à celle du domaine du réseau Windows, puis à la mise en place d'un système de protection utilisant les versions 5.0 et 6.0 de Kaspersky Antivirus 5.0 for Windows Workstation.

2.8. Maintenance d'un réseau logique

Après la création du réseau logique, puis l'installation et la configuration des applications antivirus, il est recommandé d'effectuer régulièrement les opérations suivantes :

- Examiner les comptes-rendus d'activité des applications sur les postes clients.
- Lire les alertes transmises par les postes clients et le serveur d'administration à l'adresse de messagerie de l'administrateur.

  La liste complète des notifications envoyées est disponible dans la documentation des applications Kaspersky Antivirus.
- En présence d'une situation sur l'un des postes clients, l'administrateur qui décide d'intervenir peut le faire depuis son propre poste de travail, par exemple, pour désinfecter des fichiers contaminés sur l'ordinateur en question.

- Mettre à jour régulièrement la base antivirus sur les postes clients (Chapitre 5 à la page 66) et les modules logiciels des applications installées sur des postes clients (Chapitre 5 à la page 66).
- Surveiller sur le serveur l'espace disponible pour stocker les soumissions des clients, ainsi que la mémoire libre disponible pour traiter les données soumises.
- Ajouter au réseau logique les nouveaux ordinateurs qui apparaissent sur le réseau local, et y installer régulièrement les applications antivirus nécessaires.
- Faire une sauvegarde régulière des données d'administration (voir section 6.5 à la page 83).

2.9. Coordination du travail en équipe des administrateurs

Le système permet à plusieurs administrateurs de travailler simultanément avec les mêmes ressources. Les dernières modifications remplaceront les paramètres précédemment enregistrés. Pour cette raison, le travail en équipe de multiples administrateurs sur le réseau logique doit être coordonné pour éviter les incohérences.

2.10. Interface utilisateur

À partir du poste administrateur, vous pouvez afficher, créer, modifier, et configurer le réseau logique, ainsi que contrôler toutes les applications Kaspersky Lab installées sur les clients. L'interface d'administration est fournie par le composant de la console d'administration, par un plug-in d'administration intégré dans Microsoft Management Console (MMC). L'interface de Kaspersky Administration Kit est conforme aux normes de MMC.

Pour garantir la bonne interaction avec les postes client, l'application offre la possibilité d'établir des connexions distantes avec l'ordinateur, depuis la console d'administration, en utilisant la fonction standard de connexion avec un poste de travail distant de Microsoft Windows.

Pour utiliser cette solution, il faut autoriser les connexions à distance avec le bureau du poste client.

2.10.1. Lancement de l'application

Pour exécuter Kaspersky Administration Kit, sélectionnez **Kaspersky Administration Kit** dans le groupe de programmes **Kaspersky Administration Kit** du menu standard **Démarrer \ Programmes**. Ce groupe de programme est

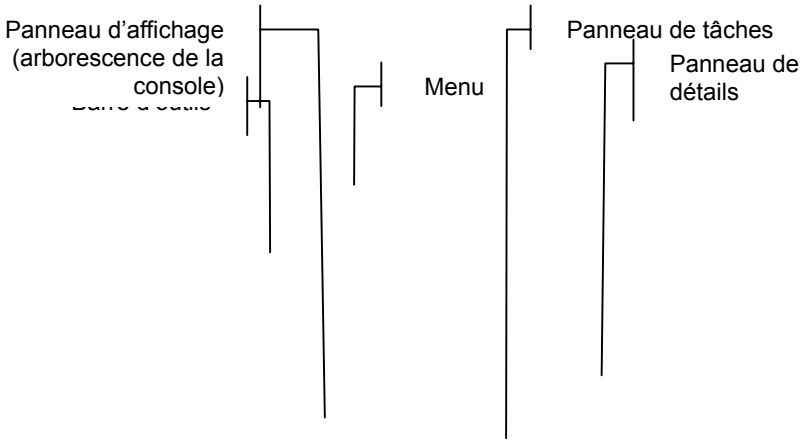
créé uniquement sur les postes administrateurs pendant l'installation de la console d'administration.

Le serveur d'administration du réseau logique doit être en exécution pour vous permettre d'utiliser les caractéristiques de Kaspersky Administration Kit.

2.10.2. Fenêtre principale

La fenêtre principale de l'application possède un menu, une barre d'outils, des panneaux d'affichage, de détails et de tâches. Le menu est utilisé pour gérer des fichiers et des boîtes de dialogue, et il permet d'accéder aux rubriques d'Aide. Les boutons de la barre d'outils fournissent un accès rapide aux options de menu les plus fréquemment utilisées. Le panneau d'affichage présente la hiérarchie de l'espace de noms de **Kaspersky Administration Kit** sous forme arborescente. Le panneau de détails affiche les détails de l'objet sélectionné dans l'arborescence de la console. Le panneau de détails contient un panneau de tâches permettant un accès rapide aux principales opérations de la console, qu'elles soient sélectionnées dans l'arborescence de la console ou dans le panneau de détails de l'objet correspondant, à travers un hyperlien. Le panneau de détails offre deux types de vue, correspondant chacun à un onglet : le premier onglet porte le nom de l'objet sélectionné dans l'arborescence de la console est le deuxième onglet est intitulé **Standard**. La seule différence est l'absence du panneau de tâches de l'onglet **Standard**.

Sous Microsoft Windows 2000, le panneau de tâches est inaccessible et n'est pas affiché dans la console d'administration.



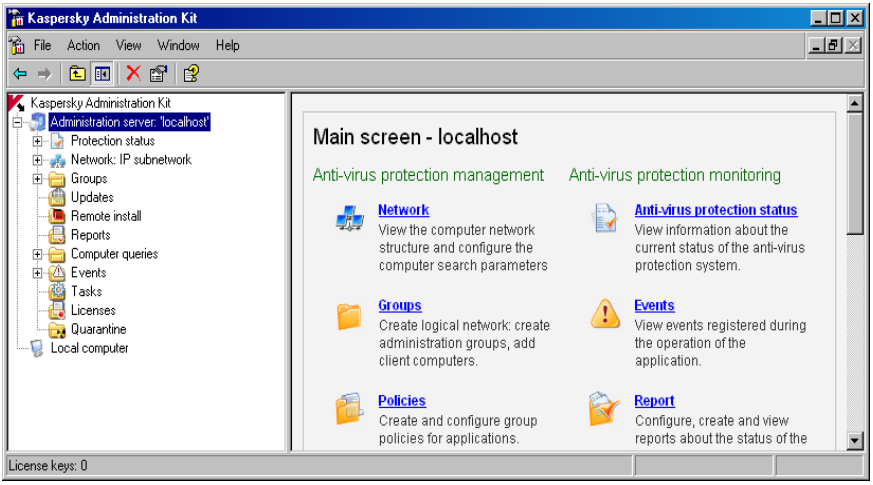


Figure 3. Fenêtre principale de Kaspersky Administration Kit

2.10.3. Arborescence de console

L'arborescence de console (voir Figure 3) affiche les réseaux logiques créés dans un réseau d'entreprise, donne accès à leurs paramètres et aux propriétés de l'ordinateur local équipé de la console d'administration est installée.

L'espace de noms **Kaspersky Administration Kit** peut avoir plusieurs postes : le **Serveur d'administration Kaspersky (<Nom du serveur>)** (d'après le nombre de serveurs d'administration) et l'objet **Ordinateur local**.

L'objet **Ordinateur local** permet d'administrer en local les applications Kaspersky Lab installées sur le poste administrateur.

Le **Serveur d'administration Kaspersky (<Nom du serveur>)** est un conteneur qui affiche la structure et les paramètres du serveur d'administration. Le **Serveur d'administration Kaspersky (<Nom du serveur>) KAV Server** contient les dossiers suivants :

- **État de protection**
- **Réseau**
- **Groupes**
- **Mises à jour**
- **Installation distante**
- **Sélections d'ordinateurs**
- **Événements**

- **Tâches**
- **Licences**
- **Stockages**

Le dossier **État de protection** offre des informations sur l'état de protection antivirus sur les postes clients et sur l'ensemble du réseau d'ordinateurs. Ce dossier contient des pages de rapports imbriqués qui gèrent la structure des informations de la manière suivante :

- **Réseau** – information sur les ordinateurs qui ne sont pas compris dans la structure du réseau logique et sur les résultats du dernier sondage du réseau par le serveur d'administration.
- **Groupes** – état de la protection antivirus sur les postes clients du réseau logique.
- **Protection antivirus** – – données statistiques sur l'activité des virus et sur les postes clients du réseau logique.
- **Mises à jour** – état de la base antivirus utilisée par les applications

Le dossier **Réseau** affiche le contenu du réseau d'ordinateurs où le serveur d'administration est installé. Le serveur d'administration crée et met à jour les informations sur la structure et sur les ordinateurs du réseau au moyen de sondages réguliers du réseau Windows et des sous-réseaux IP, créés dans le réseau corporatif. Le contenu du dossier Réseau sera mis à jour en fonction de ce sondage.

L'entrée **Groupes** est utilisée pour stocker, afficher, configurer et modifier la structure de réseau logique, les stratégies de groupe, et les tâches de groupe.

Les objets à la racine du dossier **Groupes** correspondent au niveau le plus élevé de la hiérarchie de réseau logique. Les dossiers **Serveurs d'administration, Stratégies** et **Tâches** sont obligatoires pour chaque entrée de groupe. Ces dossiers sont employés pour gérer les serveurs d'administration, les stratégies et les tâches du niveau supérieur de la hiérarchie.

Le dossier **Mises à jour** contient la liste des mises à jour reçues par le serveur d'administration et qui peuvent être distribuées aux clients.

Le dossier **Installation distante** contient la liste des paquets d'installation utilisés pour déployer des applications sur les postes clients du réseau logique.

Le dossier **Rapports** présente des modèles de rapports sur l'état de la protection de réseau logique.

Le dossier de sélection **Ordinateurs est utilisé pour rechercher des postes clients en fonction de** critères spécifiés, et pour conserver et examiner les résultats dans des dossiers séparés de l'arborescence de console.

Le dossier **Événements** affiche une liste avec des informations sur les événements enregistrés pendant le fonctionnement de l'application et sur les résultats de l'exécution des tâches.

Le dossier **Tâches globales** contient une liste de tâches globales, affectées à un groupe d'ordinateurs du réseau logique.

Le dossier **Licences** affiche les licences installées sur des postes clients.

Le dossier **Stockages** est utilisé pour la gestion des objets déplacés dans le dossier de quarantaine des postes clients et pour les copies de sauvegarde des objets conservés dans la zone de sauvegarde. Cependant, les objets eux-mêmes ne sont pas recopiés vers le serveur d'administration.

Les informations présentes dans la console d'administration ne sont mises à jour automatiquement que pour ses entrées.
Pour mettre à jour les données du panneau de résultats, utilisez la touche **F5** ou la commande **Mettre à jour** du menu, du menu contextuel ou le lien **Mettre à jour** dans le panneau des tâches.

2.10.4. Menu contextuel

Chaque type d'objets dans l'espace de noms **Kaspersky Administration Server** de l'arborescence de console possède un menu contextuel spécifique. En plus des commandes standard de MMC, ces menus contiennent des options spécifiques de traitement d'objets. D'autres commandes pour certains objets spécifiques sont énumérées dans le tableau ci-dessous.

Tableau1

Objet	Commande	Action
Kaspersky Administration Kit	**Nouveau / Kaspersky Administration Server**	Ajout d'un serveur d'administration à l'arborescence de console
Nom du serveur>	**Connexion au serveur**	Connecter au serveur d'administration
	Déconnexion	Déconnexion du serveur d'administration
	Assistant Démarrage rapide	Lancement de l'Assistant Démarrage rapide
	Assistant de déploiement d'application	Création et exécution d'une tâche de déploiement
	Rechercher un ordinateur	Ouvre une fenêtre pour l'ordinateur retrouvé :
	Propriétés	Affiche la boîte de dialogue Propriétés du serveur d'administration

Objet	Commande	Action
	Toutes les tâches/Paramètres de détection des attaques de virus	Configurer la détection des Attaques de virus contre le réseau logique ordinateurs
Réseau	**Rechercher un ordinateur**	Ouvre une fenêtre pour l'ordinateur retrouvé dans le dossier **Réseau**
	Assistant de déploiement d'application	Création et exécution d'une tâche de déploiement
	Vue/Domaines	Affiche la structure du réseau d'ordinateurs en fonction du domaine et des groupes de travail Windows
	Vue/Active Directory	Affiche la structure du réseau d'ordinateurs en fonction de la structure Active Directory
	Nouveau/Sous réseau IP	Création d'un sous-réseau IP pour afficher des ordinateurs
	Vue/Serveur d'administration	Bascule sur l'entrée du Serveur d'administration, qui contient le dossier **Réseau**
	Nouveau/Sous réseau IP	Création d'un sous-réseau IP pour afficher des ordinateurs
	Toutes les tâches/Activité de l'ordinateur	Configure les paramètres du Serveur d'administration en réponse à l'absence d'activité des ordinateurs dans le réseau
Groupes	**Installer l'application**	Création et exécution d'une tâche de déploiement pour le groupe
	Mise à jour d'application	Démarrer l'Assistant de mise à jour à distance
	Nouveau/modèle de rapport	Création d'un nouveau modèle de rapport pour le groupe sélectionné
	Rechercher un ordinateur	Ouvre une fenêtre pour l'ordinateur retrouvé dans le groupe
	RAZ compteur de virus	Remise à zéro des compteurs de détection de virus sur tous les clients dans ce groupe

Objet	Commande	Action
	Forcer synchronisation	Effectue la synchronisation des données de tous les ordinateurs d u groupe
	Nouveau/Groupe	Ajout d'un nouveau groupe à la structure du réseau logique
	Nouveau/Ordinateur	Ajout d'un nouveau client à un groupe
	Toutes les tâches/Activité de l'ordinateur	Configurer les paramètres du serveur d'administration en réponse à l'absence d'activité des ordinateurs dans le réseau
	Toutes les tâches / Sécurité	Configuration des droits d'accès du groupe
	Toutes les tâches / Stratégies	Bascule sur le dossier **Stratégies** du groupe sélectionné
	Toutes les tâches/ Tâches	Bascule sur le dossier **Tâches de groupe** du groupe sélectionné
	Toutes les tâches / Serveurs secondaires	Bascule sur le dossier **Serveurs d'administration** du groupe sélectionné
Stratégies	**Nouveau/Stratégie**	Création d'une nouvelle stratégie de groupe
	Vue/Stratégies héritées	Affiche les stratégies héritées dans le panneau de détails
Tâches de groupe	**Nouveau/Tâche**	Création d'une nouvelle tâche de groupe
	Toutes les tâches / Importer	Importation d'une tâche à partir d'un fichier
	Vue/Tâches héritées	Affiche les tâches de groupe héritées dans le panneau de détails
Installation distante	**Assistant de déploiement**	Création d'une tâche de déploiement d'application

Objet	Commande	Action
	Rapport de version des applications	Création et affichage du rapport sur les versions des applications Kaspersky Lab installées sur les ordinateurs
	Nouveau/Paquet d'installation	Création d'un nouveau paquet d'installation
	Toutes les tâches / Assistant de déploiement d'application	Création d'une tâche de déploiement d'application
Rapports	**Nouveau/modèle de rapport**	Création d'un nouveau modèle de rapport
Sélections d'ordinateurs	**Nouveau/Nouveau filtre**	Création d'un nouveau filtre de recherche d'ordinateurs
Événements	**Vue/Filtre**	Appliquer un filtre sur le tableau d'aperçu des événements
	Toutes les tâches / Importer	Importation d'une tâche à partir d'un fichier
Tâches globales	**Nouveau/Tâche**	Création d'une nouvelle tâche globale
Licences	**Ajouter clé de licence**	Installe une nouvelle clef de licence
	Rapport sur les clés de licence	Création et affichage du rapport sur les clés de licence installées sur les postes clients

Dans le panneau de détails, chaque entrée sélectionnée dans l'arborescence de console possède également un menu contextuel, avec des options de traitement spécifiques. Les principaux éléments avec leurs raccourcis correspondants sont répertoriés dans le tableau ci-dessous.

Tableau2

Élément	Commande	Action
Poste client	**Protection**	Affiche l'état de la protection antivirus du poste client
	Tâche	Ouvre une fenêtre de configuration des propriétés d'un ordinateur local sur l'onglet **Tâches**
	Applications	Ouvre une fenêtre de configuration des propriétés d'un ordinateur local sur l'onglet **Applications**

Élément	Commande	Action
	Événements	Ouvre une fenêtre pour afficher les événements enregistrés pendant l'activité de l'application sur le poste client
	Assistant de déploiement d'application	Création d'une tâche de déploiement pour le poste client
	Forcer synchronisation	Synchronisation des données du poste client et du serveur d'administration
	RAZ compteur de virus	Réinitialise les compteurs de détection de virus sur ce client
	Connecter au poste de travail distant	Ouvre une fenêtre pour la connexion au poste de travail distant
Paquet d'installation	**Installer**	Création d'une tâche de déploiement d'application
Modèle de rapport	**Générer**	Crée et affiche un aperçu du modèle de rapport choisi
	Envoi de rapports	Crée une tâche de génération automatisée et d'envoi des rapports en fonction du modèle sélectionné

CHAPITRE 3. UTILISATION DE L'APPLICATION

3.1. Connexion au serveur d'administration

Après le démarrage, la fenêtre principale de l'application affiche l'arborescence de console, avec l'espace de noms **Kaspersky Anti-Virus Administratian Kit** au niveau supérieur. Pour que le programme affiche la structure du réseau logique avec les paramètres, vous devez ajouter l'objet serveur à l'arborescence de la console et connecter au serveur d'administration requis (Figure 4). L'application reçoit des informations sur la structure du réseau logique à partir du serveur d'administration et les affiche dans l'arborescence de console.

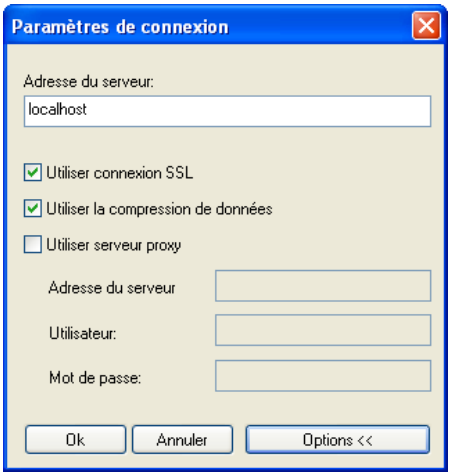


Figure 4. Établissement de connexion avec le serveur d'administration

Les tentatives de connexion seront refusées si l'utilisateur ne possède pas de droits de connexion. Les droits des utilisateurs sont vérifiés en utilisant le procédé d'authentification d'utilisateur de Windows.

Si votre réseau Windows compte plusieurs serveurs d'administration, vous pouvez contrôler ces réseaux logiques à partir d'un seul poste administrateur. Pour choisir un autre réseau logique, connectez-vous au serveur d'administration

correspondant, ou ajoutez plusieurs serveurs à l'arborescence puis connectez-vous à l'un d'eux.

Vous ne pouvez contrôler simultanément plusieurs serveurs d'administration et réseaux logiques que si vous possédez des droits d'opérateur ou d'administrateur sur chacun de ces réseaux logiques, ou si vous possédez les droits nécessaires pour chacun des réseaux.

3.2. Affectation de droits

Après l'installation du serveur d'administration, les droits nécessaires pour se connecter au serveur et pour travailler dans le réseau logique sont accordés aux utilisateurs appartenant aux groupes KLAdmins et KLOperators du réseau logique (voir section 2.5 à la page 23).

Vous pouvez modifier les droits d'accès des groupes KLOperators, accorder des droits pour opérer sur le réseau logique à d'autres groupes d'utilisateurs et à des opérateurs enregistrés sur l'ordinateur équipé de la Console d'administration.

Les droits d'accès à tous les objets des réseaux logiques sont accordés dans la boîte de dialogue **Sécurité** de la fenêtre de configuration du Serveur d'administration (Figure 5).

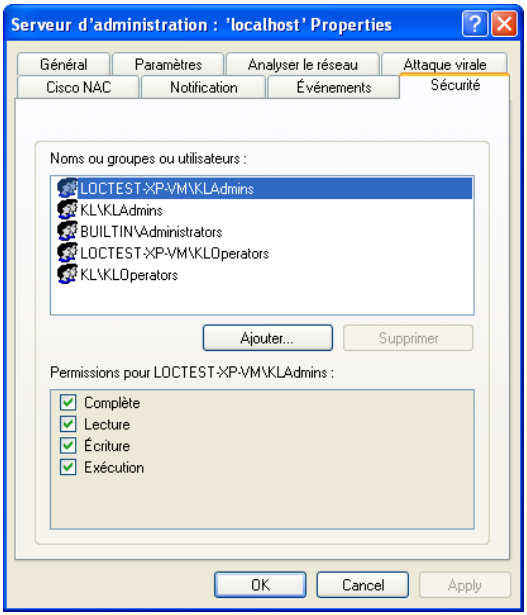


Figure 5. Affectation de droits d'accès au serveur d'administration

Il existe la possibilité d'accorder des droits d'accès séparément à chaque groupe du réseau logique. Ce paramètre est défini sur l'onglet **Sécurité** de la fenêtre de configuration du groupe.

L'administrateur peut suivre les actions de l'utilisateur d'après les événements d'activité du serveur d'administration inscrits dans les registres d'événements. Ces événements sont affectés à des **messages de type information** et qui commencent par le mot **Audit**. Ils sont affichés dans le dossier **Événements d'audit** situé dans l'entrée **Événements** de l'arborescence de console.

3.3. Affichage des informations du réseau informatique. Domaines, sous-réseaux IP et groupes Active Directory

Les informations sur la structure du réseau et sur les ordinateurs qu'il contient sont affichées dans le dossier **Réseau** de l'arborescence de console.

Après l'installation de Kaspersky Administration Kit, le dossier **Réseau** contiendra la hiérarchie des dossiers, qui reflète la structure des domaines et des postes de travail du réseau corporatif de Windows. Au dernier niveau de chacun des dossiers, se trouve la liste de postes appartenant au domaine ou groupe de travail, mais qui n'appartiennent pas à la structure du réseau logique. Dès qu'un ordinateur est ajouté dans un groupe, ses informations sont immédiatement supprimées du dossier. Dès qu'un ordinateur est enlevé du réseau logique, les informations sur cet ordinateur apparaissent à nouveau dans le dossier correspondant sous l'entrée **Réseau**.

La hiérarchie des dossiers sous l'entrée **Réseau** peut également se construire à partir des structures Active Directory ou des sous-réseaux IP créés dans le réseau. Pour ce faire, sélectionnez **Vue/Active Directory** ou **Vue/Sous-réseaux IP** dans le menu contextuel de l'entrée **Réseau**.

Si l'entrée **Réseau** est présentée par sous-réseaux IP, l'administrateur peut créer sa structure en créant des sous-réseaux IP et en modifiant les paramètres des sous-réseaux existants.

Par défaut, seuls les sous-réseaux IP auxquels appartient le serveur d'administration sont affichés dans la vue **Sous-réseaux IP**.

Quand vous sélectionnez un dossier dans l'arborescence de console, les ordinateurs contenus seront affichés dans le panneau de résultats sous forme de tableau, pouvant contenir les informations suivantes :

- **Nom** – Nom de l'ordinateur dans le réseau logique (nom NetBios ou adresse IP de l'ordinateur).

- **Type du S.E.** – Type du système d'exploitation installé sur un poste client.

  En fonction du type de système d'exploitation, une icône est affichée à côté du nom du poste :  – dans le cas d'un serveur,  – pour un poste de travail.

- **Domaine** – Domaine ou groupe de travail Windows contenant un ordinateur en particulier.
- **Agent / Antivirus** – État des applications installées sur l'ordinateur. Dans le cas de l'agent réseau ou d'une application antivirus[2] pouvant être contrôlée par Kaspersky Administration Kit,. un signe « + » (plus) sera affiché si ces logiciels sont installés sur l'ordinateur. Si ces applications ne sont pas installées, un signe « - » (moins) est affiché.
- **Visible dans le réseau** – Date où cet ordinateur a été identifié pour la dernière fois par le serveur sur le réseau.
- **Dernière mise à jour** – Date de dernière mise à jour de la base antivirus ou des applications sur cet ordinateur
- **État** – État actuel de l'ordinateur (**OK** / **Avertissement** / **Critique**) en fonction de critères définis par l'administrateur.
- **Dernière mise à jour d'informations** – Date de la dernière mise à jour des informations sur l'ordinateur.
- **Domaine DNS** – Domaine DNS auquel se rapporte l'ordinateur.
- **Nom de domaine** – Nom DNS de l'ordinateur.
- **Adresse IP** – Adresse IP de l'ordinateur.
- **Connexion avec le serveur** – Dernière connexion de l'agent d'administration installé sur le poste client, avec le serveur d'administration.

Le dossier **Réseau** reproduit les groupes de services du même nom. La création et prise en charge du groupe **Réseau** dans son état le plus récent est assurée par le serveur d'administration. Le serveur d'administration réalise un sondage périodique du réseau corporatif afin de détecter l'apparition ou la disparition d'ordinateurs.

Le serveur d'administration peut sonder le réseau de différentes manières (voir Figure 6) :

- *Sondage rapide du réseau Windows*. Seules les informations NetBIOS des ordinateurs appartenant aux domaines et groupes de travail du réseau sont collectées.

[2] Dans le cas présent, « application antivirus » désigne l'application à laquelle appartient le composant de protection en temps réel

- *Sondage complet du réseau Windows.* Dans ce cas de figure, l'entièreté des informations relatives aux ordinateurs est recherchée : système d'exploitation, adresse IP, nom DNS, etc.
- *Sondage des sous-réseaux IP*. Ici, le serveur d'administration recherche les intervalles IP à l'aide de paquets ICMP et collecte l'ensemble des informations relatives aux ordinateurs appartenant à cet intervalle.
- *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.

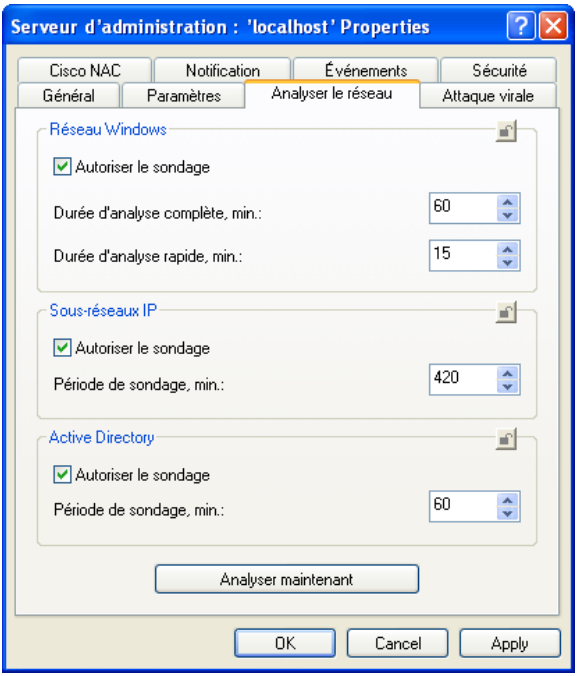


Figure 6. Configuration du sondage réseau par le serveur d'administration

En fonction des informations obtenues et des données sur la structure du réseau logique, le serveur d'administration met à jour le groupe **Réseau** ainsi que la structure et le contenu du dossier **Réseau**. Au cours de la mise à jour, les ordinateurs détectés à l'intérieur du réseau peuvent être déplacés automatiquement vers le dossier **Réseau** spécifié par l'administrateur, ou dans un Groupe administratif spécifié du réseau logique. Il existe la possibilité de

désactiver le sondage des ordinateurs présents dans la structure du groupe **Réseau** et de ses sous-groupes imbriqués.

Le dossier **Réseau** du serveur d'administration principal inclut également les ordinateurs appartenant au réseau logique du serveur d'administration secondaire, et inversement.

3.4. Assistant Démarrage rapide

Un Assistant intégré dans Kaspersky Administration Kit vous permet de configurer un ensemble de paramètres minimums afin mettre en place une administration centralisée de votre système de protection antivirus. Cet Assistant de configuration initiale permet de configurer ce qui suit :

- structure du réseau logique qui, au choix de l'administrateur, peut être :
- automatiquement créée en fonction de la structure des domaines et de groupes de travail du réseau Windows ;
- créé manuellement ;

  Si un ordinateur n'est pas enregistré dans le groupe **Réseau** quand vous créez un réseau logique (qui se trouve désactivé ou déconnecté du réseau), il ne sera pas ajouté au réseau logique. Vous pourrez ajouter manuellement cet ordinateur plus tard.

  La création d'un réseau logique avec l'Assistant Démarrage rapide ne remet pas en cause l'intégrité du réseau : de nouveaux groupes sont ajoutés ; mais ils ne remplacent pas les groupes existants. Un poste client déjà affecté à un groupe existant ne sera pas ajouté une seconde fois, parce que le groupe **Non attribué** n'affiche que les ordinateurs qui ne sont pas présents dans le réseau logique.

- Des paramètres pour envoyer des alertes par messagerie ou NET SEND sur des événements liés à la protection antivirus, enregistrés par le serveur d'administration et les autres applications Kaspersky Lab.
- La stratégie et un ensemble minimum de tâches au niveau supérieur de hiérarchie dans le cas des versions 5.0 et 6.0 de Kaspersky Antivirus pour Windows Workstation, ainsi qu'une tâche de mise à jour globale pour le serveur d'administration et la copie de sauvegarde.

  Aucune stratégie n'est créée pour les versions 5.0 et 6.0 de Kaspersky Antivirus 5.0 for Windows Workstation s'il en existait déjà une autre dans le dossier Groupes pour cette application.
  Si des tâches de groupe pour le groupe **Groupes** et les tâches de mise à jour globale et de sauvegarde ont été déjà créées avec les mêmes noms, ces tâches ne seront pas mises en place à ce moment.

Au cours de la première connexion au serveur d'administration après son installation, le programme suggère d'exécuter l'Assistant Démarrage rapide.

Pour exécuter l'Assistant plus tard, cliquez sur **Assistant Démarrage rapide** dans le menu contextuel du serveur d'administration.

3.5. Affichage, création et configuration d'un réseau logique

La structure de réseau logique ; la hiérarchie des serveurs d'administration secondaires, la liste et la structure des groupes sont définis à l'étape de conception. Le réseau logique est créé dans un dossier spécial **Groupes** (Figure 7) de la fenêtre principale de Kaspersky Administration Kit par création de la hiérarchie des groupes et ajout de postes clients et de serveurs d'administration secondaires.

Immédiatement après l'installation de Kaspersky Administration Kit le dossier **Groupes** ne contient aucun objet et les dossiers **Serveurs d'administration, Stratégies** et **Tâches de groupe** sont vides. L'administrateur peut définir la structure du réseau logique en ajoutant des postes clients et d'autres groupes imbriqués à la structure du dossier **Groupes**.

Les groupes sont affichés comme des dossiers de structure similaire à celle de ce dossier **Groupes**.

- Lors de la création de chacun des groupes, des sous-dossiers **Serveurs d'administration, Stratégies et Tâches de groupe** seront automatiquement définis pour y conserver et gérer les serveurs d'administration secondaires, les stratégies et les tâches propres à un groupe en particulier ;
- Quand des postes clients sont ajoutés à un groupe, leurs informations sont affichées dans le panneau de résultats sous forme de tableau ;
- Quand un sous-groupe est ajouté, un dossier avec la même structure est créé.

Quand un dossier est sélectionné dans l'arborescence de console, son contenu sera reproduit dans le panneau de résultats.

En plus des informations du tableau du dossier **Réseau**, les informations suivantes sur chacun des postes clients peuvent être affichées :

- **Analyse à la demande** – Date et heure de la dernière analyse antivirus complète du poste client.
- **Virus découverts** – Nombre total de virus détectés sur les postes clients depuis l'installation de l'application antivirus (première analyse) ou depuis la dernière remise à zéro de cette valeur (compteur de virus détectés). Pour remettre à zéro le compteur, cliquez sur **RAZ compteur de virus** dans le menu contextuel ou dans le menu **Action**.

- **Protection en temps réel** – État courant de la protection en temps réel du poste client.
- **Adresse IP de connexion** – Adresse IP de la connexion entre le poste client et le serveur d'administration.

Vous pouvez gérer les objets du dossier Groupes à l'aide de commandes du menu contextuel (voir section 2.10.4 à la page 32) et des liens du panneau des tâches.

Afin de créer un réseau logique avec une structure semblable à celle des domaines et des groupes d'utilisateurs du réseau Windows, vous pouvez utiliser l'Assistant de configuration initiale (voir section 3.2 à la page 38).

Pour créer manuellement la structure du réseau logique :

1. Établissez la connexion au serveur d'administration nécessaire.
2. Organisez une hiérarchie de groupes en créant des groupes imbriqués.
3. Ajoutez des postes clients aux groupes
4. Ajoutez des serveurs d'administration secondaires

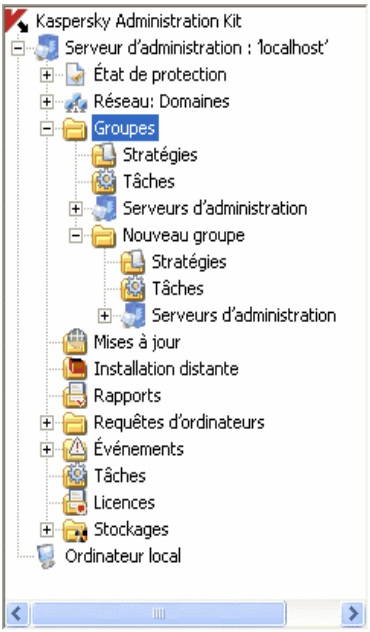


Figure 7. Affichage des objets du réseau logique

La structure de réseau logique est représentée dans le dossier **Groupes**. Vous pouvez afficher des informations sur chacun des objets du réseau logique :

serveurs secondaires, groupes et postes clients. Les données affichées concerneront la date de création de l'objet et de dernière modification. Vous pouvez également examiner et, si nécessaire, modifier les paramètres utilisés par l'objet (serveur secondaire, poste client ou tous les postes clients du groupe) pour dialoguer avec le serveur d'administration.

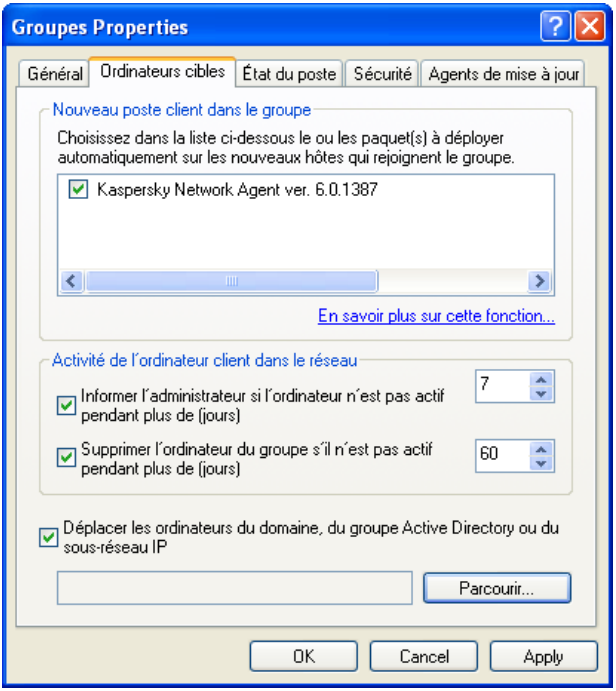


Figure 8. Affichage des propriétés du groupe.
Postes client (onglet)

Pour obtenir des informations sur des postes clients spécifiques utilisez la fonction de recherche de l'ordinateur sur le réseau logique, en utilisant les critères spécifiés. Vous pouvez utiliser les données sur les réseaux logiques des serveurs d'administration secondaires pour effectuer cette recherche. Pour effectuer cette recherche et afficher des informations sur les ordinateurs dans un dossier séparé de l'arborescence de console, utilisez la fonction de création de Filtre.

Si vous modifiez la configuration de votre réseau d'entreprise, n'oubliez pas de refléter ces modifications dans le réseau logique. Vous pouvez :

- Ajouter des groupes à votre réseau logique, quel que soit leur nombre et leur degré d'imbrication (vous pouvez ajouter des serveurs

d'administration secondaires et des groupes imbriqués pour former le niveau suivant de hiérarchie dans un groupe).

Vous pouvez également spécifier l'installation automatique des applications Kaspersky Lab sur tous les clients de ce groupe.

Pour activer l'installation automatique des applications de Kaspersky Lab sur des ordinateurs en réseau ordinateurs sous Microsoft Windows 98/ME, il faut installer sur ces derniers l'outil Network Agent.

- Ajoutez des postes clients aux groupes
- Modifiez l'ordre de la hiérarchie des objets du réseau logique, en déplaçant des postes clients individuels ou des groupes complets vers d'autres groupes.
- Ajoutez des serveurs d'administration secondaires à la structure du réseau logique afin de réduire la charge sur le serveur principal, réduire le trafic interne et améliorer la fiabilité du système d'administration à distance.
- Déplacez des postes clients d'un réseau logique vers un autre.

3.5.1. Groupes

Pour ajouter un nouveau groupe, utilisez la commande **Nouveau / Groupe** dans le menu contextuel du groupe sous lequel vous allez ajouter un groupe imbriqué. Après cela, l'arborescence de console affichera sous l'entrée **Groupes** (Figure 7) un nouveau dossier avec le nom choisi. Les sous-dossiers **Stratégies, Tâches de groupe** et **Serveurs d'administration** seront automatiquement créés dans ce nouveau dossier. Ils seront complétés à l'étape de définition des stratégies de groupe, et lors de la création de tâches de groupe et de serveurs secondaires.

Des postes client et des groupes imbriqués formant le niveau hiérarchique suivant peuvent être ajoutés dans ce groupe. Il est possible de configurer l'affichage des stratégies et tâches de groupe héritées au sein des groupes imbriqués.

Vous pouvez également définir les applications Kaspersky Lab qui seront installées automatiquement sur tous les postes clients ajoutés au groupe.

Pour activer l'installation automatique des applications Kaspersky Lab sur de nouveaux ordinateurs exploités sous Microsoft Windows 98/ME, il faut installer sur ces derniers l'outil Network Agent (agent réseau).

Par la suite, vous pourrez modifier le nom du groupe, le déplacer vers un autre groupe ou le supprimer.

Le déplacement d'un groupe vers un autre groupe se fait avec tous les groupes imbriqués, les serveurs d'administration secondaires, les postes clients, les stratégies de groupe et les tâches qui s'y rapportent. Tous les paramètres

correspondants à sa nouvelle position dans la hiérarchie des objets du réseau logique s'appliqueront à ce groupe.

Vous pouvez déplacer un groupe à l'aide des commandes standard **Copier / Coller**, avec les options équivalentes du menu **Action** ou encore, avec la souris.

Lors du déplacement d'un groupe, il faut respecter la règle de l'unicité du nom de chacun des groupes à l'intérieur du même niveau de hiérarchie. Pour résoudre un conflit dans le nom, renommez le groupe avant de le déplacer. Si vous ne respectez pas cette règle, le suffixe **_1, _2,** etc. sera ajouté automatiquement au nom.

Vous ne pouvez pas renommer le dossier **Groupes** car il s'agit d'un élément intégré à la console d'administration.

Un groupe peut être supprimé du réseau logique s'il ne contient ni serveurs d'administration secondaires, ni groupes ou postes clients imbriqués et q'aucune tâche ni stratégie n'a été créée pour lui. Vous pouvez sélectionner puis supprimer un groupe avec la commande **Supprimer** du menu contextuel ou du menu **Actions**.

3.5.2. Postes client

Pour ajouter des postes clients à un groupe, utilisez la commande **Nouveau / Ordinateur** dans le menu contextuel du groupe sous lequel vous allez ajouter les ordinateurs. Ceci lance l'Assistant correspondant. Une fois l'Assistant terminé avec succès, les ordinateurs seront inclus dans le groupe et affichés dans le panneau de résultats avec les noms définis par le serveur d'administration (Figure 9).

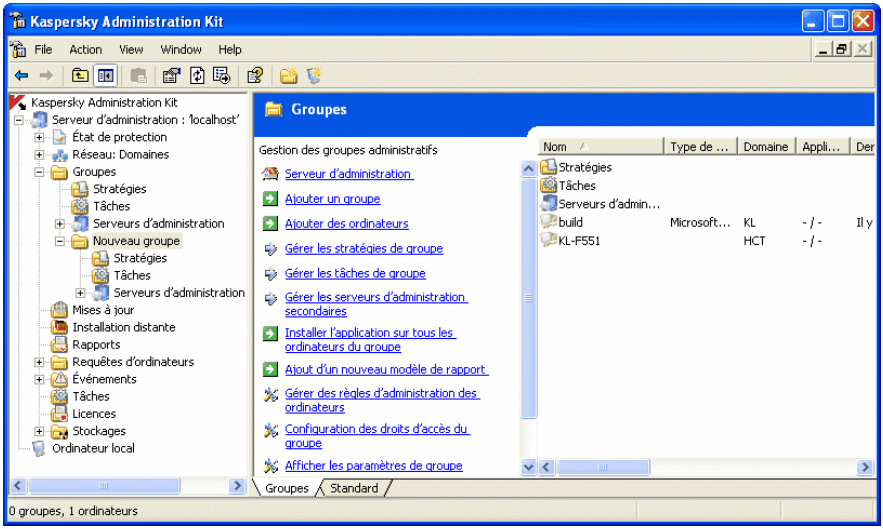


Figure 9. Postes client dans un groupe

Il est possible de configurer l'inclusion de postes clients dans les réseaux logiques de telle façon que le serveur d'administration ajoute automatiquement tous les ordinateurs détectés dans le groupe administratif désigné. Cette configuration peut se faire dans les propriétés du groupe **Réseau** (Figure 10).

Pour ajouter automatiquement un ordinateur à un groupe, faites glisser avec la souris l'ordinateur du dossier **Réseau** vers le réseau logique, à l'intérieur de la fenêtre principale de Kaspersky Administration Kit.

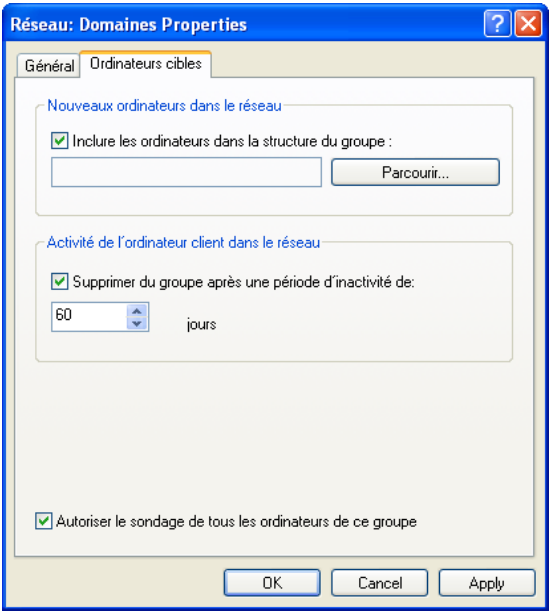


Figure 10. Configuration du déplacement automatique des nouveaux ordinateurs vers un groupe

Vous pouvez déplacer des postes clients d'un groupe à l'autre et les exclure du réseau logique, en utilisant les commandes standard **Couper/Coller** ou **Supprimer** du menu contextuel ou du menu **Action**. Les ordinateurs exclus du réseau logique sont déplacés vers le groupe **Réseau**. Le déplacement peut également se faire avec la souris.

Les postes client peuvent être déplacés d'un réseau logique vers un autre. Par exemple, quand vous ajoutez un serveur d'administration secondaire, vous pouvez déplacer les postes clients depuis le réseau logique du serveur principal vers le réseau logique d'un serveur secondaire. Pour ce faire, les postes clients doivent être connectés au nouveau serveur d'administration.

La connexion du poste client à un autre serveur d'administration se fait en créant puis en lançant une tâche de **Modification de serveur d'administration**. Il est possible de déplacer soit des ordinateurs individuels par la création d'une tâche globale, soit tous les postes clients d'un groupe administratif donné à l'aide d'une tâche de groupe. Après l'exécution de la tâche de **Modification**, les postes clients concernés par la tâche, créée et exécutée avec succès, seront déconnectés de l'ancien serveur d'administration puis réaffichés dans le groupe **Réseau** du nouveau serveur. Des postes client peuvent être supprimés des groupes administratifs de l'ancien réseau logique et ajoutés au nouveau réseau logique manuellement à l'aide de la console d'administration.

Vous pouvez connecter un poste client à un serveur d'administration différent, localement depuis ce poste client.
Cette opération s'effectue avec l'outil ***klmover.exe*** inclus dans le paquet de distribution de l'agent réseau. Après l'installation de l'agent réseau, cet outil se trouve placé à la racine du dossier d'installation du composant.

3.5.3. Serveurs d'administration secondaires

En utilisant la hiérarchie des serveurs, il est possible d'effectuer les opérations suivantes pour tous les serveurs d'administration secondaires et postes clients connectés au serveur principal :

- *des stratégies d'application* peuvent être créées et distribuées ;
- *des tâches de groupe* (y compris les tâches de déploiement) peuvent être créées et distribuées ;
- *les mises à jour et les paquets d'installation* reçus par le serveur principal peuvent être distribués ;
- *des rapports* de données récapitulatives sur tous les serveurs d'administration secondaires peuvent être créés.

Pour ajouter un serveur secondaire, utilisez la commande **Nouveau / Serveur d'administration** de l'objet serveur d'administration dans le groupe souhaité. Vous lancez ainsi l'Assistant pour l'ajout d'un serveur secondaire. Cet Assistant réalise les actions suivantes :

- ajout d'un serveur d'administration secondaire ;
- connexion de la console d'administration au serveur secondaire ;
- configuration de la connexion au serveur principal.
- ajout d'informations sur le serveur secondaire à la base de données du serveur d'administration principal.
- Vous pouvez ignorer les étapes de connexion et de configuration pour les réaliser manuellement par la suite. Pour ce faire, connectez-vous au serveur utilisé en tant que serveur secondaire depuis la console d'administration et définissez ses paramètres de connexion avec le serveur principal (Figure 11).

Après un ajout réussi du serveur d'administration secondaire, son icône et son nom s'afficheront dans le dossier **Serveurs d'administration** du groupe correspondant.

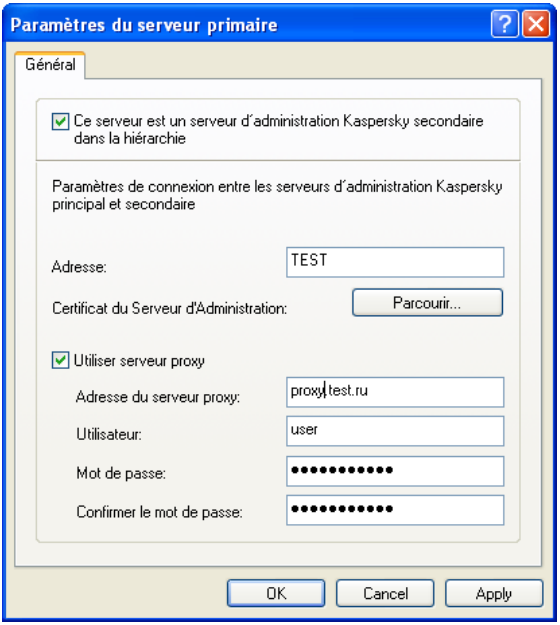


Figure 11. Configuration des paramètres de connexion au serveur d'administration principal

Vous pouvez gérer le réseau logique du serveur d'administration secondaire depuis l'entrée **Serveurs d'administration** du réseau logique du serveur principal, ou directement, en ajoutant le serveur à l'arborescence de console en tant que nouveau serveur d'administration.

Le serveur secondaire est un serveur d'administration complètement opérationnel qui peut assurer toutes les fonctions à l'intérieur de son propre réseau logique.

En outre, un serveur d'administration secondaire hérite du serveur principal toutes les tâches de groupe et stratégies du groupe dans lequel il est installé. Les stratégies et les tâches ainsi héritées sont reproduites sur le serveur secondaire de la manière suivante :

- L'icône sera affichée à côté du nom de la stratégie récupérée du serveur d'administration principal. (L'icône normale pour une stratégie est).
- Les valeurs des paramètres hérités de la stratégie ne sont pas modifiables sur le serveur secondaire.

- Les paramètres qui ne sont pas modifiables dans la stratégie héritée ne sont pas non plus modifiables (icône) dans aucune des stratégies d'application du serveur secondaire et leurs valeurs sont celles de la stratégie héritée.
- Les paramètres qui sont modifiables dans la stratégie héritée peuvent être modifiés dans les stratégies du serveur secondaire (icône). Si un paramètre n'est pas « verrouillé » dans la stratégie du serveur secondaire, il peut être modifié dans les paramètres d'application ou de tâche (voir section 2.1.7 à la page 19).
- L'icône sera affichée à côté du nom de la tâche de groupe récupérée du serveur d'administration principal. (L'icône normale pour une tâche est).

Les tâches de déploiement globales et de groupe ne peuvent pas être transférées vers les serveurs secondaires.

Il est possible de configurer la mise à jour des postes clients du serveur d'administration secondaire de telle façon que, après réception des mises à jour par le serveur principal, une tâche de réception des mises à jour sur le serveur secondaire soit automatiquement exécutée puis, une fois la tâche est terminée avec succès, des tâches de mise à jour des applications sur les postes clients du serveur d'administration secondaire soient à leur tour lancées (voir section 5.3 à la page 70).

CHAPITRE 4. GESTION DE STRATEGIES A DISTANCE

Kaspersky Administration Kit ne peut gérer que les applications Kaspersky Lab qui possèdent un composant spécialisé – - un plugin administrateur de l'application, compris dans le paquet de distribution.

4.1. Configuration des paramètres d'application

4.1.1. Administration des stratégies

Vous ne pouvez créer une stratégie pour une application que si le plug-in de console correspondant est installé sur le poste administrateur.

Pour créer une stratégie, utilisez la commande **Nouveau / Stratégie** dans le menu contextuel du dossier **Stratégie.** À cette étape de la création de la stratégie, vous ne pouvez configurer qu'un ensemble minimum de paramètres, ceux nécessaires au bon fonctionnement de l'application. Tous autres paramètres prendront des valeurs par défaut, correspondant à celles définies lors de l'installation locale de l'application.

Vous trouverez une description détaillée des paramètres de stratégie des applications Kaspersky Lab dans les Guides des applications.

Par la suite, vous pourrez modifier les valeurs des paramètres, interdire leur modification dans les stratégies des groupes imbriqués et dans les paramètres d'application (Figure 12).

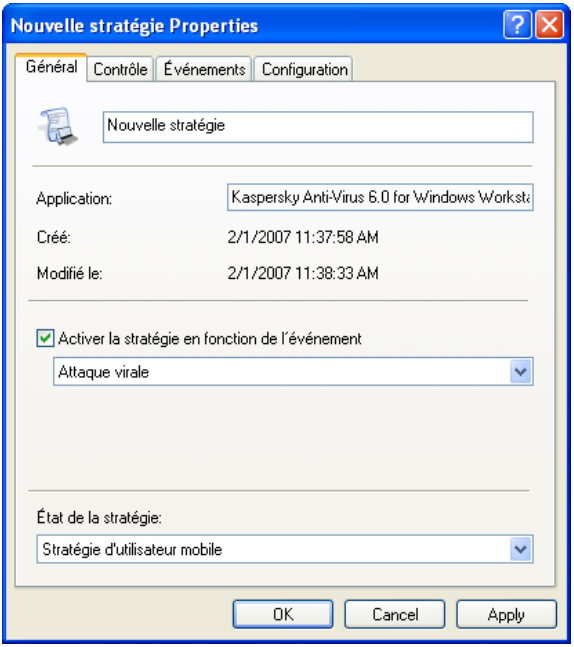


Figure 12. Modification de stratégies

Les paramètres gouvernés par la stratégie dont la modification est interdite seront signalés par l'icône . Pour interdire les modifications, cliquez dessus avec le bouton gauche. L'icône changera en Ces paramètres cesseront d'être modifiables au niveau des paramètres d'application, de tâches et des stratégies des sous-groupes et des serveurs d'administration secondaires.

Les paramètres locaux ont une priorité supérieure par rapports aux paramètres de stratégie (voir section 2.1.7 à la page 19). Si vous souhaitez utiliser une valeur définie dans la stratégie pour un paramètre en particulier, vous devez le verrouiller.

Après la création d'une nouvelle stratégie, celle-ci sera ajoutée au dossier **Stratégies** (Figure 13) du groupe correspondant et appliquée à tous les sous-groupes et serveurs d'administration secondaires compris dans ce groupe, en tant que stratégie héritée.

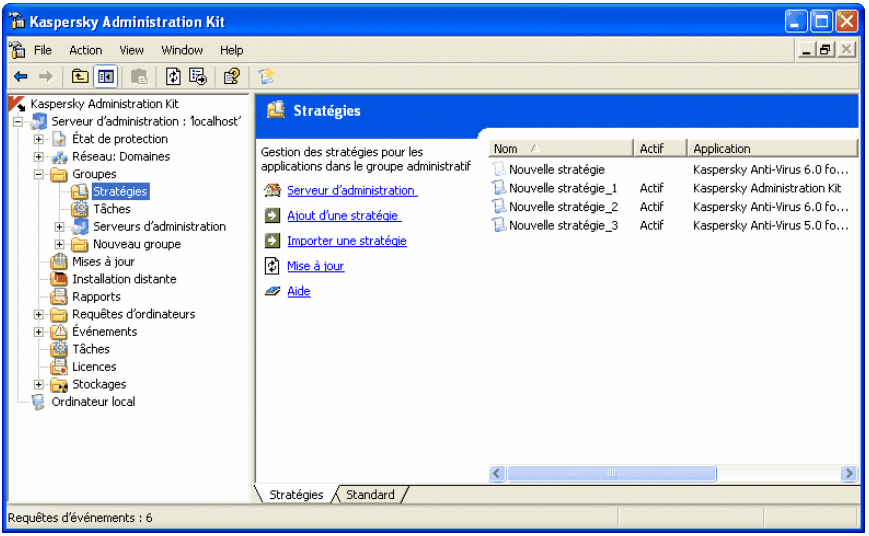


Figure 13. Le dossier **Stratégies**

Vous pouvez supprimer, copier, exporter ou importer des stratégies créées dans un groupe vers un autre, à l'aide des commandes du menu contextuel de la stratégie sélectionnée dans le panneau de résultats.

Il est possible de créer de nombreuses stratégies de groupe pour chacune des applications, mais une seule d'entre elles peut être active. Cette stratégie doit avoir le paramètre de **stratégie active** sélectionné dans sa configuration.

La stratégie peut être activée automatiquement, déclenchée par un certain événement. Cependant, vous ne pouvez revenir à la stratégie précédente que manuellement.

Vous pouvez également créer une stratégie pour utilisateurs mobiles qui sera mise en œuvre dès que l'ordinateur est déconnecté du réseau logique corporatif.

Un ordinateur est considéré comme déconnecté du réseau logique après trois tentatives infructueuses de connexion avec le serveur d'administration. L'intervalle de temps entre ces tentatives, fixé à 15 minutes par défaut, peut être modifié à l'aide du champ **Période de synchronisation (min.)** dans les paramètres de l'agent réseau.

Les résultats du déploiement de la stratégie peuvent être examinés à travers la console d'administration dans la fenêtre de propriétés de la stratégie du serveur d'administration (Figure 14).

La modification des paramètres locaux de l'application dépend de l'option sélectionnée dans la fenêtre **Avancé** (voir Figure 13). Pour ouvrir cette fenêtre, cliquez sur le lien **Avancé** dans l'onglet **Contrôle** des propriétés de stratégie.

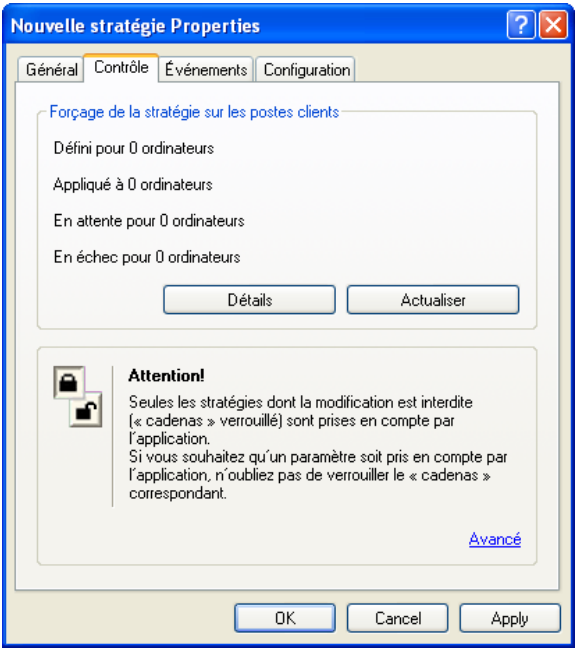


Figure 14. Configuration de l'application d'une stratégie

La modification des paramètres locaux s'opère automatiquement en fonction de l'option choisie lors de la première application de la stratégie sur l'ordinateur client, à savoir :

- Ajout d'un client dans le champ d'application de la stratégie ;
- Activation d'une stratégie ;
- Installation sur un client d'une application antivirus pour laquelle une stratégie a été établie.

Vous avez le choix parmi les options suivantes :

- **Ne pas modifier les paramètres.** Dans ce cas, seuls les paramètres en regard desquels l'icône est affiché dans les paramètres de stratégie seront d'application. Les autres paramètres seront ceux définis localement. Cette option est activée par défaut.

  Après avoir supprimé la stratégie ou suspendu son effet, les paramètres locaux de l'application sont réinitialisés à leur valeur précédente.

- **Modifier les paramètres obligatoires après un premier forçage de la stratégie.** Dans ce cas, seuls les paramètres en regard desquels

l'icône est affiché dans les paramètres de stratégie seront d'application.

Après avoir supprimé la stratégie ou suspendu son effet, seuls les paramètres dont la stratégie n'empêchait pas la modification (icône affiché en regard) sont réinitialisés à leur valeur initiale.

- **Modifier tous les paramètres après un premier forçage de la stratégie.** Tous les paramètres locaux liés à la stratégie seront modifiés.

  Après avoir supprimé la stratégie ou suspendu son effet, l'application continue à fonctionner avec les paramètres de cette stratégie. Ceux-ci pourront être modifiés manuellement.

Vous pouvez également modifier une stratégie manuellement. Pour ce faire, cliquez sur le bouton **Modifier maintenant** (voir Figure 13). La stratégie sera alors appliquée en fonction du paramètre sélectionné ci-dessus.

La stratégie est mise en place de la façon suivante. Si des tâches résidentes (protection en temps réel) se trouvaient en exécution sur un client, elles appliqueront les nouveaux paramètres de manière transparente. Si des tâches périodiques sont en cours sur un client (analyses à la demande, mise à jour de base de données), elles continueront de s'exécuter avec les anciennes valeurs des paramètres. Les nouvelles valeurs des paramètres seront appliquées lors du prochain démarrage de ces tâches. Vous pouvez afficher les paramètres de l'application, après avoir appliqué la nouvelle stratégie, à travers la console d'administration dans la fenêtre de configuration du serveur d'administration.

Dans le cas d'une structure hiérarchique, les serveurs d'administration secondaires récupèrent les stratégies depuis le serveur principal, puis les appliquent sur les postes clients. La configuration de la stratégie n'est modifiable que sur le serveur d'administration primaire. Ensuite, les serveurs secondaires modifient et déploient conformément les stratégies sur les postes clients.

En cas d'échec de connexion entre les serveurs d'administration principal et secondaire, le serveur secondaire appliquera la dernière stratégie connue. Les éventuelles modifications de stratégie effectuées sur le serveur principal seront transmises au serveur secondaire dès qu'une connexion aura pu être établie.

En cas d'échec de connexion entre le serveur d'administration et le poste client, ce dernier appliquera la stratégie pour utilisateur nomade (pour autant qu'elle soit définie) ou la dernière stratégie connue.

Les résultats du déploiement de stratégies sur les serveurs d'administration secondaires sont affichés dans la fenêtre de propriétés de stratégie du serveur d'administration primaire.

De manière similaire, vous pouvez examiner les résultats du déploiement de la stratégie sur les postes clients dans la fenêtre de propriétés de la stratégie du serveur d'administration secondaire après vous être connecté.

Vous trouverez une description détaillée des paramètres de stratégie des applications Kaspersky Lab dans les Guides des applications. La configuration de stratégie du composant Network Agent et du serveur d'administration est décrite dans le Livre de Référence de Kaspersky Administration Kit.

4.1.2. Paramètres locaux de l'application

Le système Kaspersky Administration Kit permet la configuration à distance des applications locales installées sur les postes clients, à l'aide de la console d'administration (Figure 15). Les paramètres d'application permettent de définir des paramètres de fonctionnement d'application individuels pour chaque poste client dans le groupe. Vous ne pouvez modifier que les valeurs des paramètres dont la modification n'est pas interdite par la stratégie de groupe d'une certaine application, c'est à dire, quand le paramètre n'est pas « verrouillé » par la stratégie.

La configuration des paramètres locaux est assurée séparément sur chaque poste client dans les **Paramètres d'application "<Nom de l'application>".** Cette fenêtre est invoquée depuis l'onglet **Application** de la fenêtre de **Propriétés : <Nom de poste>.**

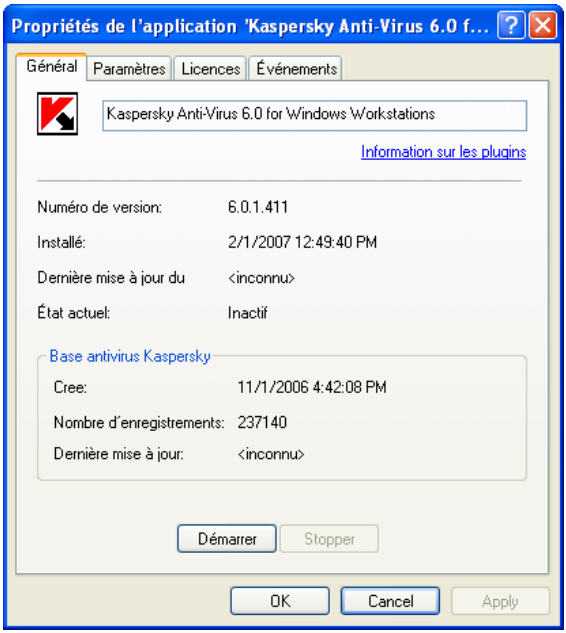


Figure 15. Fenêtre de configuration des paramètres locaux de l'application

Chaque application Kaspersky Lab possède son propre jeu de paramètres locaux. Pour une description détaillée de ces paramètres, reportez-vous au Manuel de l'application en question.

Vous trouverez une description détaillée de la configuration de l'agent réseau et du serveur d'administration dans le Guide de Référence de Kaspersky Administration Kit.

4.2. Gestion de l'application

La gestion du fonctionnement des applications installées sur les postes clients du réseau logique est assurée par la création et l'exécution de tâches qui prennent en charge la majorité de leurs caractéristiques : Installation des applications et des clés de licence, analyse de fichiers, mise à jour de la base antivirus et des modules d'application, etc.

Kaspersky Administration Kit prend en charge tous les types de tâches nécessaires à la gestion de l'application locale. En outre, l'exécution et l'arrêt à distance des applications sont prévus par les tâches d'administration correspondantes de l'agent réseau. Vous trouverez une description détaillée des types de tâches pour chaque application Kaspersky Lab dans le Guide de chaque application.

La console d'administration assure le lancement et l'arrêt à distance de l'application au moyen des tâches correspondantes.

Vous ne pouvez créer une tâche pour une application que si le plug-in d'administration de celle-ci est installé sur le poste de travail de l'administrateur.

Pour assurer la protection réseau, l'administrateur peut créer un nombre quelconque de tâches variées (à l'exception de celles qui ne peuvent être créées qu'une seule fois) pour toutes les applications gérées à partir de Kaspersky Administration Kit.

Par exemple, pour analyser des postes clients qui sont aussi des postes de travail, et y rechercher des logiciels malveillants, vous devez créer une tâche d'analyse à la demande pour Kaspersky Antivirus for Windows Workstation.

Les fonctions de gestion des applications et en général les opérations des services effectuent les tâches des composants de Kaspersky Administration Kit, du serveur d'administration et de l'agent réseau. Les types de tâches suivants sont définis pour ce composant :

- **Changement de serveur d'administration.**
- **Lancement / Arrêt de l'application.**
- **Déploiement d'applications.**
- **Désinstallation d'application à distance.**
- **Réception de mises à jour par le serveur d'administration.**
- **Création d'une copie de sauvegarde du serveur d'administration.**

- **Envoi de rapports.**
- **Distribution du paquet d'installation.**

Les tâches des types précédents ont des caractéristiques différentes selon qu'elles supposent une création ou une exécution. Vous trouverez une description détaillée de l'administration des tâches dans le Livre de Référence de Kaspersky Administration Kit.

Vous pouvez créer des tâches de groupe, globales ou locales pour chaque type de tâche.

Pour un **déploiement**, des tâches aussi bien de groupe ou globales peuvent être créées. Pour des tâches de **réception de mises à jour**, de **création d'une copie de sauvegarde** et d'**envoi de rapports**, seules des tâches globales peuvent être créés.

Les tâches de réception des mises à jour et de **création d'une copie de sauvegarde du serveur d'administration** sont uniques et ne peuvent être exécutées que par un seul ordinateur –, le serveur d'administration.

Pour créer une tâche, utilisez la commande **Nouveau / Tâche** dans le menu contextuel des dossiers **Tâches de groupe** ou **Tâches globales**.

Les tâches de groupe créées seront placées dans les sous-dossiers **Tâches de groupe** des groupes correspondants (Figure 16). Les tâches globales seront placées dans un conteneur spécial de l'arborescence de console appelé **Tâches globales**. Vous pouvez examiner la liste des tâches locales du poste client dans la fenêtre de propriétés du poste client.

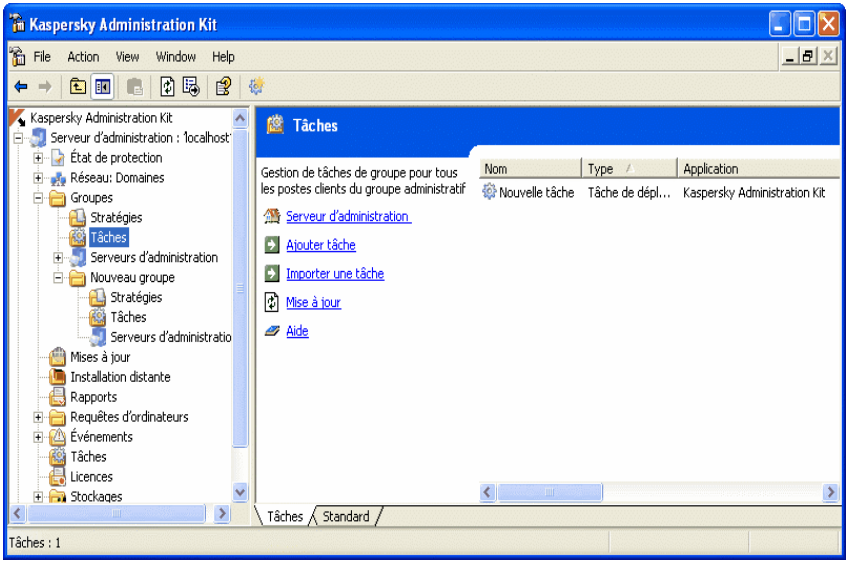


Figure 16. Tâches de groupe

L'échange des données sur les tâches entre l'application locale et la base d'informations de Kaspersky Administration Kit se produit au moment où l'agent réseau se connecte au serveur : Les tâches créées en local seront placées dans la base du serveur d'administration, tandis que celles créées à distance à l'aide de la Console, seront reproduites dans l'interface d'application sur le poste client.

Vous pouvez modifier les paramètres des tâches, observer leur exécution, copier, exporter ou importer des tâches d'un groupe à l'autre, les supprimer à l'aide des commandes du menu contextuel.

Pendant l'exécution des tâches sur chaque poste client, les paramètres de fonctionnement de l'application seront mis en place conformément à la stratégie de groupe, aux paramètres de tâche et aux paramètres de l'application concrète installée sur le poste client (pour plus de détails, voir section 2.1.7 à la page 19).

La plupart des paramètres sont définis par la stratégie de l'application qui assure cette tâche. Par exemple, les actions lors de la détection d'objets infectés, les ressources mobilisées pour mettre à jour la base antivirus, etc. Si ces paramètres sont verrouillés contre les modifications par la stratégie, ils ne sont pas non plus modifiables dans la configuration de tâche (Figure 17).

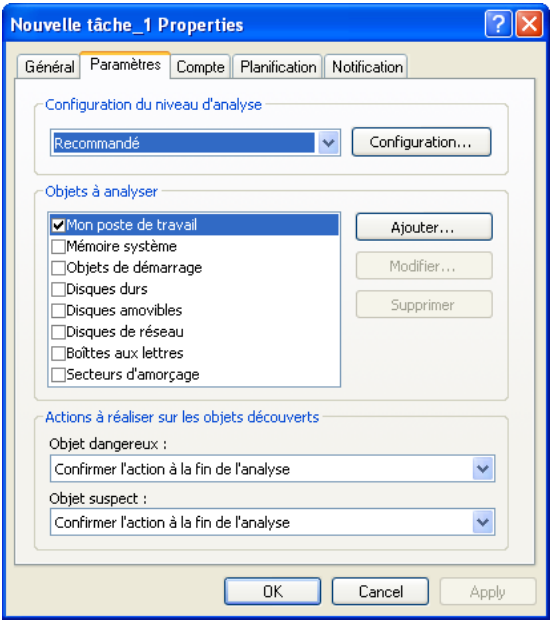


Figure 17. Paramètres de tâche verrouillés dans la stratégie

Cependant, une partie des paramètres est propre à la tâche en question : horaire du lancement planifié de la tâche, compte d'exécution de la tâche, portée des tâches d'analyse à la demande, etc. Les valeurs de ces paramètres, définis pour chaque tâche, sont modifiables une fois la tâche créée (Figure 18).

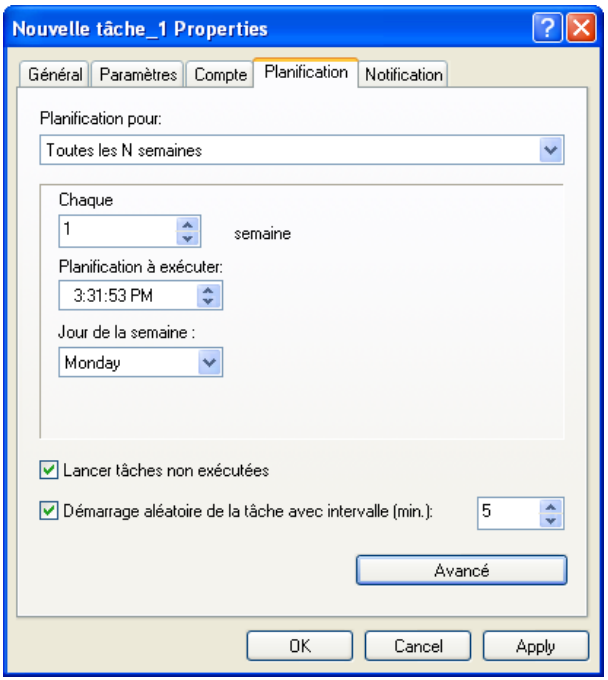


Figure 18. Planification de l'exécution d'une tâche

Les tâches seront exécutées conformément à la planification prévue. Lorsque les ordinateurs sont éteints à l'heure d'exécution prévue, le système d'exploitation peut être démarré automatiquement par la fonction Wake On Lan. Pour utiliser cette fonction, vous devez cocher la case correspondante (Figure 19) de l'onglet **Planification** (Figure 18), ouvert en cliquant sur **Avancés**.

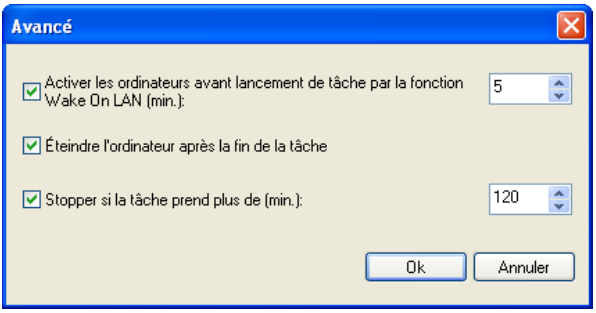


Figure 19. Activation du démarrage automatique du système d'exploitation

Vous pouvez également activer l'arrêt automatique de l'ordinateur après la fin de la tâche programmée.

La durée d'exécution de la tâche peut être contrôlée, et dans ce cas, la tâche est interrompue après un délai d'attente spécifié dans les paramètres. Il existe la possibilité de désactiver l'exécution d'une tâche programmée. Dans ce cas, la tâche, sans avoir été supprimée, ne sera pas non plus exécutée.

En outre, Vous pouvez exécuter une tâche, l'interrompre, la suspendre ou la continuer manuellement, en utilisant les commandes du menu contextuel ou depuis la fenêtre des paramètres de la tâche (Figure 20).

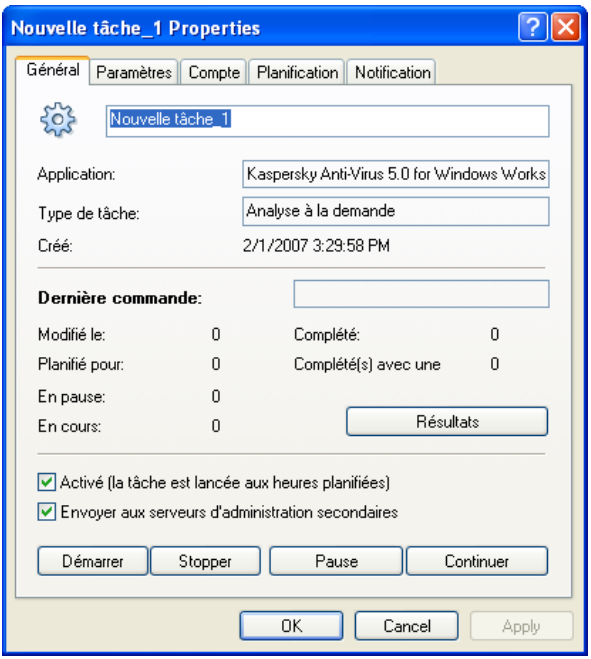


Figure 20. Contrôle de l'exécution de la tâche

Les tâches ne sont exécutées sur un poste client que si l'application correspondante est en exécution. Dès que vous refermez l'application, toutes les tâches en exécution sont interrompues.

Vous pouvez surveiller l'exécution d'une tâche ou afficher les résultats de son exécution dans la fenêtre des paramètres de la tâche (Figure 20).

Les résultats de l'exécution des tâches sont enregistrés et conservés, conformément à son paramétrage, dans les registres d'événements de Windows

ou de Kaspersky Administration Kit, aussi bien dans un emplacement centralisé sur le serveur d'administration qu'en local, sur chaque poste client. L'administrateur ou un autre utilisateur peut être informé sur les résultats de l'exécution des tâches ; le format et la méthode de notification sont également définis dans les paramètres de la tâche.

Vous pouvez afficher les résultats de l'exécution des tâches enregistrés dans Kaspersky Administration Kit sous l'entrée **Événements** de l'arborescence de console. Vous pouvez examiner les résultats de l'activité des tâches sur chaque poste client dans la fenêtre de propriétés de ce dernier.

La consultation des résultats de l'exécution des tâches conservés localement sur une poste client se fait à l'aide d'une console d'administration installée en local sur ce poste.

Grâce à la structure hiérarchisée des serveurs d'administration, et si ce paramétrage est activé dans la configuration de la tâche (Figure 20), les serveurs secondaires recevront des tâches de groupe depuis le serveur d'administration principal puis les redistribueront sur les postes clients. La configuration des tâches de groupe n'est modifiable que sur le serveur d'administration primaire. Ensuite, les serveurs d'administration secondaires modifieront leurs tâches de groupe et les redistribueront vers les postes clients connectés.

Les résultats de la distribution d'une tâche de groupe sur les serveurs d'administration secondaires sont décrits dans la fenêtre **Résultats d'exécution des tâches** de la fenêtre de propriétés de la tâche de groupe du serveur d'administration.

De manière similaire, vous pouvez examiner les résultats du déploiement de la tâche sur les postes clients depuis la fenêtre de propriétés de la tâche de groupe, sur le serveur d'administration secondaire auquel vous vous serez connecté.

CHAPITRE 5. MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES DE PROGRAMME

La mise à jour régulière de la base antivirus, l'installation de mises à jour (correctifs) aux modules de programme et la mise à niveau des versions de programme contribuent de manière essentielle à la protection permanente de votre réseau.

La base antivirus disponible sur le Web de Kaspersky Lab est mise à jour toutes les heures. Nous recommandons vivement de mettre à jour votre base antivirus aussi souvent que possible, et d'installer régulièrement tous les correctifs logiciels.

Pour procéder à la mise à jour des bases antivirus et des modules de programme des applications gérées par Kaspersky Administration Kit, vous devez créer une tâche globale dans Kaspersky Administration Kit, afin de récupérer les mises à jour. Kaspersky Administration Kit téléchargera la base de données et les modules à partir d'une source de mise à jour, en fonction des paramètres de la tâche globale. Les mises à jour téléchargées seront stockées sur le serveur d'administration dans un dossier public Mises à jour d'où elles seront redistribuées automatiquement vers les postes clients et les serveurs d'administration secondaires, après la fin de la mise à jour. Le dossier d'accès public est créé pendant l'installation du serveur d'administration. Par défaut, il s'agit du dossier **KLShare** créé avec l'installation du composant Serveur d'administration **(<Unité>:\Programmes\Kaspersky Lab\Kaspersky Administration Kit)**.

Les mises à jour son distribuées sur les postes clients au moyen de tâches de mise à jour d'application. La mise à jour des serveurs secondaires est assurée au moyen de la tâche de réception des mises à jour par le serveur d'administration. Ces tâches peuvent être démarrées automatiquement immédiatement après la réception des mises à jour sur le serveur principal, indépendamment de la planification prévue par les paramètres de la tâche.

5.1. Réception de mises à jour par le serveur d'administration

La tâche de réception de mises à jour par le serveur d'administration est une tâche globale dont une seule instance peut être créée. Cette tâche est créée et

exécutée uniquement sur un ordinateur, à savoir, celui sur lequel le serveur d'administration est installé.

Si vous utilisez l'Assistant Démarrage rapide, la tâche de réception des mises à jour par le serveur d'administration aura déjà été créée et se trouve sous l'entrée **Tâches globales** de l'arborescence de console.

Pour créer la tâche pour la réception des mises à jour par le serveur d'administration, lancez l'Assistant de création de tâches sur l'entrée **Tâches globales**. Après avoir choisi l'application cible de la tâche, sélectionnez le type de tâche **Kaspersky Administration Kit** - **Réception de mises à jour par le serveur d'administration** (Figure 21).

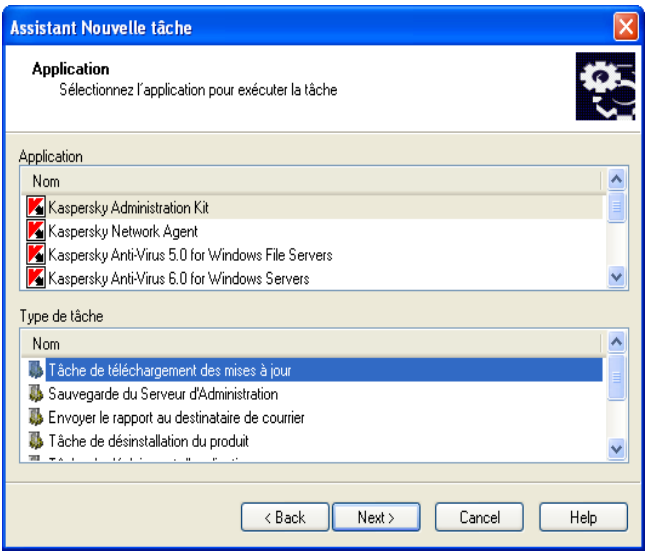


Figure 21. Création d'une tâche de mise à jour. Choix de l'application et du type de tâche

Si la hiérarchie des serveurs d'administration a été créée (ou si sa création est prévue) dans le réseau logique, alors la case **Forcer la mise à jour des serveurs secondaires** (Figure 22) doit être cochée dans les paramètres de tâche du serveur principal afin d'assurer la distribution automatique des mises à jour sur les serveurs secondaires. Dans ce cas, immédiatement après la mise à jour du serveur principal, les tâches de mise à jour des serveurs secondaires (si elles ont été créées) seront exécutées.

Si la case **Forcer la mise à jour des serveurs secondaires** est cochée, aucune création de tâche de réception de mises à jour par le serveur d'administration secondaire ne sera exécutée. Il faut créer ces tâches manuellement sur chacun des serveurs secondaires.

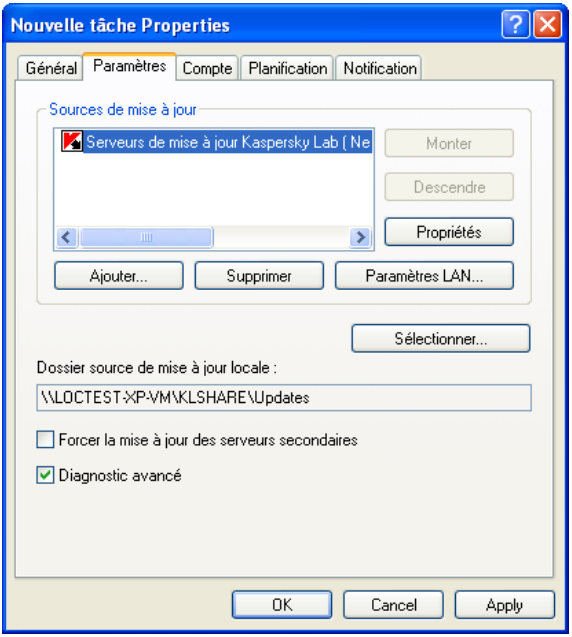


Figure 22. Configuration de la tâche de réception des mises à jour :

Après l'exécution de la tâche de réception des mises à jour par le serveur d'administration, les mises à jour de la base antivirus et des modules d'application seront téléchargées depuis les sources de mises à jour, et placées dans le dossier d'accès public.

Depuis les dossiers d'accès public, les téléchargements seront distribués vers les postes clients (voir section 5.2 à la page 69) et les serveurs d'administration secondaires (voir section 5.3 à la page 70).

Les ressources suivantes sont disponibles en tant que source de mises à jour pour le serveur d'administration :

- Serveurs de mise à jour de Kaspersky Lab ;
- Serveur d'administration principal ;
- Serveur HTTP - FTP ou dossier réseau :

L'utilisation d'une ressource en particulier dépend de la configuration de la tâche.

Si les mises à jour sont exécutées à partir de serveurs FTP- /HTTP- ou d'un dossier réseau, alors pour s'assurer de la mise à jour correct du serveur, il faut recopier la structure des dossiers contenant les mises à jour pour la faire corresponde à celle créée par les outils de Kaspersky Lab lors du téléchargement des mises à jour.

Vous pouvez examiner les informations des mises à jour réceptionnées sous l'entrée **Mises à jour** de l'arborescence de console ; la liste de mises à jour est affichée dans le panneau de résultats (Figure 23).

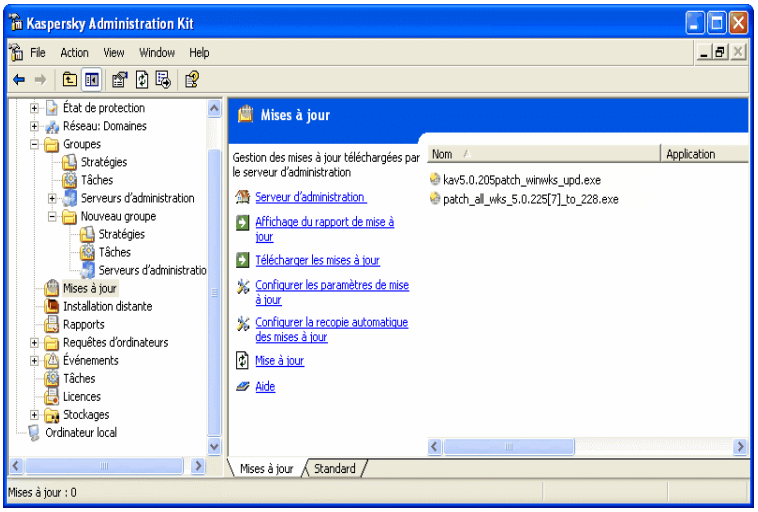


Figure 23. Examen des mises à jour réceptionnées

5.2. Distribution de mises à jour vers les postes clients

Pour améliorer la sécurité de la protection antivirus, il faut créer des tâches de mise à jour pour toutes les applications antivirus présentes dans le système de protection des ordinateurs de votre réseau logique.

Pour s'assurer que les versions des mises à jour de la base antivirus et des modules d'application installées sur les postes clients du réseau logique sont bien les mêmes, sélectionnez le serveur d'administration en tant que source de mises à jour dans les paramètres des tâches de réception des mises à jour par les applications.

Si le serveur d'administration est sélectionné en tant que source de mises à jour dans la tâche d'application, alors, en fonction de la structure hiérarchisée des serveurs, les postes clients seront mis à jour depuis le serveur auquel ils sont connectés, c'est à dire, depuis le serveur secondaire, plutôt que depuis le serveur principal.

La description de la procédure de création de tâches pour la mise à jour des applications figure dans les Guides des applications correspondantes.

Si la case est cochée, alors après chaque réception des mises à jour par le **Serveur d'administration**, deux tâches spéciales seront créées dans le dossier **Tâches de groupe** du groupe **Groups** : **Mise à jour automatique - Base antivirus** (une pour chaque application). Ces tâches seront exécutées automatiquement après chaque réception réussie des nouvelles mises à jour par le serveur. Pour désactiver le mode de distribution automatique des mises à jour (case non cochée), les tâches seront supprimées.

Pour réduire la charge des serveurs d'administration, nous vous recommandons d'utiliser les agents de mise à jour, qui se chargent de distribuer les mises à jour à l'intérieur du groupe administratif.

5.3. Mise à jour des serveurs secondaires et de leurs postes clients

Si une structure hiérarchique des serveurs d'administration est organisée dans le réseau logique, alors pour vous assurer que les serveurs reçoivent et redistribuent les mises à jour vers les postes clients connectés, vous devez :

- Créer une tâche pour la réception des mises à jour sur chacun des serveurs d'administration secondaires.
- Choisissez **Serveur d'administration principal** comme source de mises à jour dans les paramètres de la tâche de réception des mises à jour des serveurs secondaires.
- •Activez la distribution automatique des mises à jour vers les serveurs secondaires dans les paramètres des tâches de réception des mises à jour par le serveur d'administration principal : Cochez la case **Forcer la mise à jour des serveurs secondaires (**Figure 24**).**
- Si nécessaire, précisez les agents de mise à jour à l'intérieur des groupes administratifs (voir section 5.4 à la page 71).
- Activez le mode de distribution automatique des mises à jour vers les postes clients avec des installations Kaspersky Antivirus for Windows Workstation versions 5.0 et 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers et Kaspersky Anti-Virus 6.0 for Windows Servers. Pour les autres applications, les mises à jour auront été réceptionnées par les serveurs d'administration.

  Les mises à jour sont réceptionnées par les applications depuis les serveurs d'administration auxquels le poste client est connecté, c'est à dire, depuis le serveur secondaire, plutôt que depuis le serveur principal.

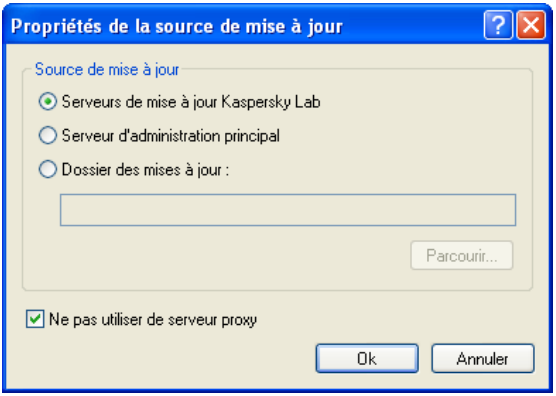


Figure 24. Mise à jour depuis le serveur d'administration principal

5.4. Distribution des mises à jour à l'aide des agents de mise à jour

Pour distribuer les mises à jour vers les postes clients du groupe, vous pouvez utiliser des *agents de mise à jour* – des ordinateurs qui opèrent comme des pôles intermédiaires de distribution des mises à jour et des paquets d'installation à l'intérieur des groupes administratifs. Ils reçoivent les mises à jour depuis le serveur d'administration et les placent dans le dossier d'installation de l'application. Seules les mises à jour nécessaires pour le groupe sont téléchargées. Par la suite, les postes clients du groupe peuvent utiliser les agents pour télécharger les mises à jour.

Il n'est pas permis de modifier l'emplacement du dossier contenant les mises à jour et les paquets d'installation ni d'établir des restrictions à la taille du dossier.

La création de la liste des agents de mise à jour et de leur configuration se fait depuis la fenêtre de propriétés du groupe de l'onglet **Agents de mise à jour** (Figure 25).

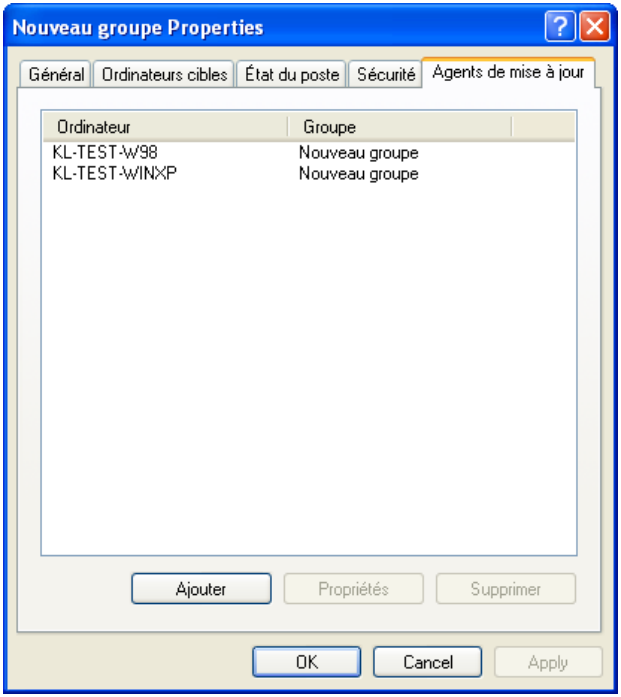


Figure 25. Création de la liste d'agents de mise à jour

CHAPITRE 6. MAINTENANCE

6.1. Renouvellement de la licence

Le droit d'utiliser le logiciel Kaspersky Lab est soumis à l'accord de licence accepté lors de l'achat du progiciel.

Pendant cette période d'autorisation, vous pouvez :

- Utiliser les fonctions antivirus de l'application
- Mettre à jour la base antivirus
- Améliorer les versions de cette application
- Obtenir une assistance technique sur l'installation, la configuration, et l'utilisation de cette application antivirus par téléphone ou par formulaire en ligne destiné aux consultations adressées au service d'assistance technique, situé sur le site Web corporatif de Kaspersky Lab.
- Envoyer les objets suspects ou infectés chez Kaspersky Lab pour une expertise.

Pour fonctionner, Kaspersky Administration Kit n'exige aucune clef de licence!

Lorsque vous contactez le service d'assistance technique, utilisez les informations de licence d'un des produits Kaspersky Lab en votre possession, pour autant qu'il soit administré par Kaspersky Administration Kit.

Le programme Kaspersky Administration Kit vérifie automatiquement les licences accordées et détermine la période d'autorisation à l'aide d'une clef de licence qui fait partie de chaque application Kaspersky Lab. Une application ne peut avoir qu'une seule clef de licence valide. La clef de licence contient les conditions d'utilisation du logiciel et elle peut être lue et vérifiée spécialement par le programme.

Après la fin de la période d'autorisation, les options énumérées ne sont plus disponibles à l'utilisation. Pour renouveler la licence, vous devez acheter et installer une nouvelle clef de licence.

Kaspersky Administration Kit permet suivre de manière centralisée la validité et le renouvellement des clés de licence installées sur les clients du réseau logique de l'entreprise.

Quand une clef de licence est installée à l'aide de Kaspersky Administration Kit, les informations correspondantes sont stockées sur le serveur d'administration. Ces informations sont utilisées pour créer des rapports sur l'état de licence et pour informer l'administrateur sur l'expiration prochaine de la licence, ou sur le dépassement du nombre d'utilisations maximum autorisé. Les paramètres de

notifications sur l'état des clés de licence peuvent être modifiés dans la configuration du serveur d'administration.

Pour créer un rapport sur l'état des clés de licence installées sur les postes clients du réseau logique, utilisez un modèle intégré de Rapport sur les licences, ou créez un nouveau modèle du type portant le même nom.

Un rapport créé sur le modèle **Rapport sur les licences** contient des informations complètes sur toutes les clés installées sur les postes clients du réseau logique, y compris les clés actives et de réserve, en indiquant les ordinateurs sur lesquels ces clés sont utilisées, avec les limitations de licence.

La liste de toutes les clés de licence installées sur les clients est affichée sous l'entrée **Licences**. Les données suivantes sont disponibles pour chaque clef :

- **Numéro de série** – Numéro de série principal de la licence
- **Type** – Type de la clef de licence (par exemple, **commerciale ou essai).**
- **Limite du compteur d'ordinateurs** – Limitation imposée par la clé de licence
- **Période de licence** – Période d'expiration de la clé de licence

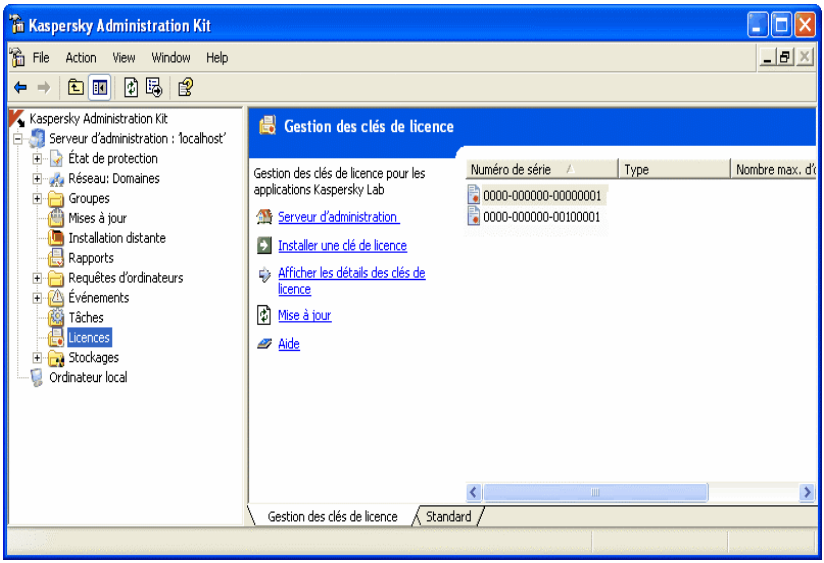


Figure 26. Gestion des clés de licence

Pour afficher les clés de licence installées pour un client spécifique, ouvrez la boîte de dialogue des propriétés de l'application.

Pour installer une clef de licence, vous devez créer la tâche **Installer la clé de licence**.

La tâche d'installation de la clé de licence peut être une tâche de groupe, une tâche globale, ou une tâche locale. Vous pouvez créer une tâche globale pour l'installation de la clé de licence en utilisant l'Assistant.

Pour remplacer la clé de licence installée ou pour changer de clé courante, utilisez une tâche que vous aurez créée auparavant en modifiant ses paramètres avant de l'utiliser.

6.2. Dossiers de quarantaine et de sauvegarde

Le travail avec ly dossier de quarantaine et de sauvegarde est accessible seulement pour Kaspersky Anti-virus pour Windows Workstations et Kaspersky Anti-virus pour Windows Servers des versions 5.0 et 6.0.

Les applications antivirus permettent de stocker des objets dans des zones de stockage spécialisées. Pour chaque ordinateur sont prévus des dossiers individuels pour la quarantaine et les zones de sauvegarde, préparés en local. La quarantaine est utilisée pour y placer des objets suspects tandis que la zone de sauvegarde permet de conserver des copies des objets infectés avant leur traitement ou leur suppression.

L'application Kaspersky Administration Kit est capable de conserver de manière centralisée une liste des objets placés dans les zones de sauvegarde par les applications Kaspersky Lab. Cette information est transmise depuis les postes clients par les agents réseau et conservée dans la base de données du serveur d'administration. Il est possible d'exécuter les fonctions suivantes à travers la console d'administration : afficher les propriétés des objets placés dans les zones de stockage, lancer l'analyse antivirus des stockages et supprimer des objets de ces stockages.

Pour activer la fonction de gestion à distance d'objets stockés en local, vous devez cocher les cases **Transfert d'informations sur les objets en quarantaine au serveur d'administration** et **Transférer des informations sur les objets sauvegardés au serveur d'administration** (Figure 27) dans la stratégie de l'agent réseau.

La définition des paramètres de sauvegarde est propre à chaque application : dans la stratégie ou dans les paramètres d'application.

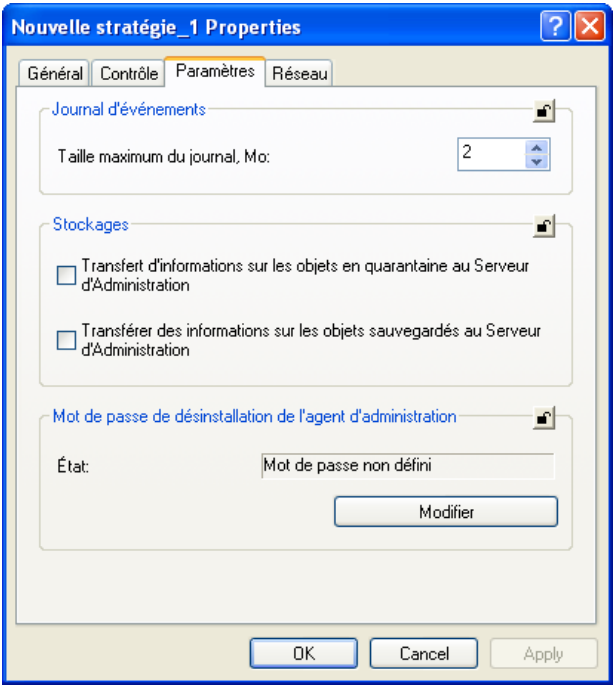


Figure 27. Configuration de zones de stockage à distance

Vous pouvez examiner des objets placés dans les zones de stockage des postes clients du réseau logique et gérer ces objets depuis le dossier **Stockages** (Figure 28).

Kaspersky Administration Kit ne recopie pas d'objets vers le serveur d'administration. Tous les objets sont placés dans des zones de stockage locales sur les postes clients.
Les objets sont restaurés dans le dossier indiqué par l'administrateur dans l'ordinateur équipé de la *console d'administration*.

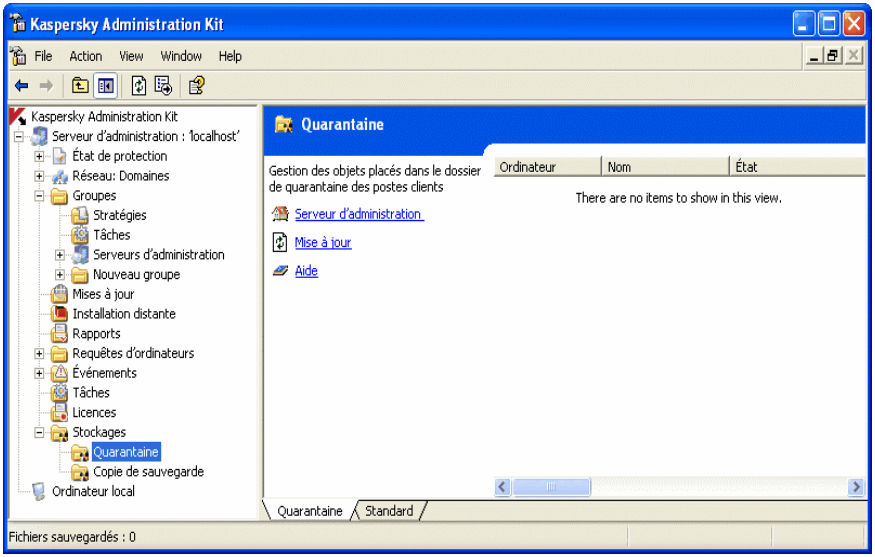


Figure 28. Affichage du contenu des stockages

6.3. Registres d'événements. Filtres d'événements.

L'application Kaspersky Administration Kit propose de nombreuses options de surveillance du système de protection antivirus :

L'application est capable de gérer des historiques des événements liés à l'activité du serveur d'administration et de toutes les applications contrôlées au moyen de Kaspersky Administration Kit. Les données peuvent être enregistrées dans le Journal système de Microsoft Windows ou dans le journal d'événements de Kaspersky Administration Kit.

Le journal contient les événements enregistrés pendant le fonctionnement de l'application et les résultats de l'exécution des tâches.

Vous pouvez configurer la liste des événements enregistrés pendant le fonctionnement de chacune des applications, ainsi que la méthode de notification employée pour en informer l'administrateur et les autres utilisateurs de chaque groupe administratif. Ces paramètres sont déterminés par les stratégies de groupe de l'application. Leur configuration se fait depuis l'onglet **Événements** de la fenêtre de configuration de la stratégie de groupe (Figure 29).

La procédure utilisée pour l'enregistrement, ainsi que le format et la méthode de notification des résultats de l'exécution des tâches sont déterminés par les paramètres de la tâche.

Les notifications peuvent se produire par l'envoi de messages électroniques, directement à travers le réseau ou par l'exécution d'une certaine application ou d'un script.

Les informations sur les événements enregistrés et les résultats de l'exécution de tâches peuvent être stockées sur le serveur d'administration (de manière centralisée) ou en local, sur l'ordinateur de chacun des postes clients.

Vous pouvez voir les informations enregistrées dans le journal de Microsoft Windows à l'aide de l'outil **Observateur d'événements** standard de MMC. Vous pouvez examiner le journal des événements de Kaspersky Administration Kit à partir de la console du poste administrateur sous l'entrée **Événements** de l'arborescence de console (Figure 30).

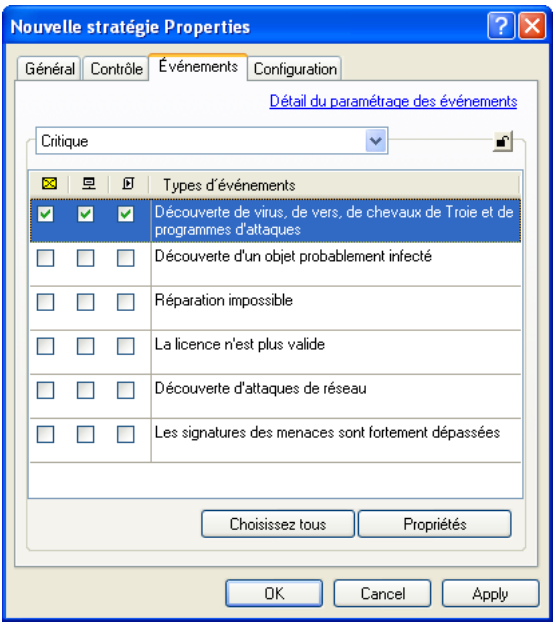


Figure 29. Modification d'une stratégie. L'onglet **Événements**.

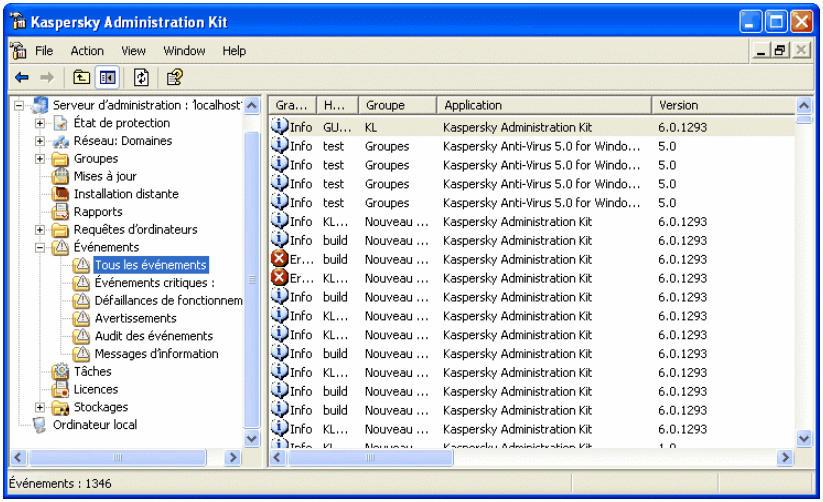


Figure 30. Affichage du journal d'événements de Kaspersky Administration Kit

Pour simplifier la recherche et la consultation, le contenu du journal **Événements** est divisé en plusieurs catégories, à savoir : **Tous les événements, Événements critiques**, **Défaillances de fonctionnement**, **Avertissements**, **Messages d'information, Événements d'audit**. L'utilisation des filtres permet d'exécuter des recherches et de structurer les données sur les événements enregistrés, du fait qu'après l'application du filtre, seules les informations qui satisfont les critères du filtre sont disponibles. Cette caractéristique devient vite indispensable pour examiner le volume d'informations conservées sur le serveur. La possibilité existe de créer des filtres supplémentaires et d'enregistrer les événements dans un fichier au format .txt. Pour examiner tous les événements et les résultats de l'exécution des tâches, sélectionnez le dossier **Tous les événements**.

Pour créer un filtre, utilisez la commande **Nouveau / Filtre** dans le menu contextuel de l'entrée **Événements**. Après cela, un nouveau dossier avec le nom indiqué sera affiché avec les résultats du filtre dans l'entrée **Événements** de l'arborescence de console. Ce dossier contiendra tous les événements et les résultats de l'exécution de la tâche. Pour modifier les informations, configurez les paramètres du filtre (Figure 31).

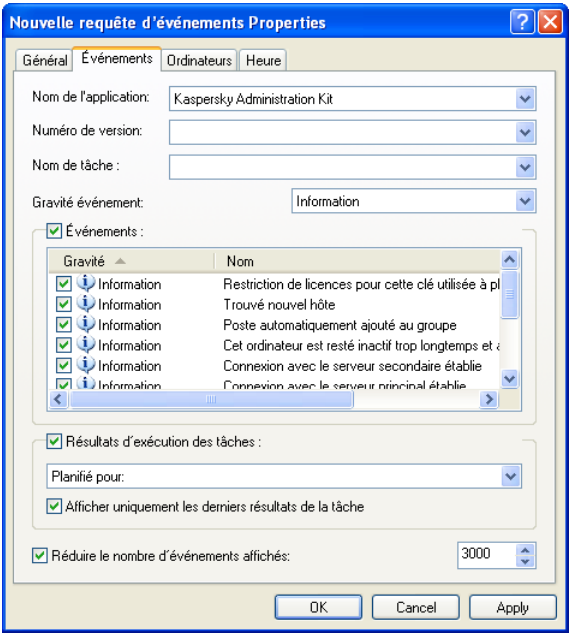


Figure 31. Configuration d'un filtre d'événements

Les événements enregistrés sont supprimés automatiquement après le délai de stockage défini par la stratégie ou l'aide de la commande du menu **Purger.** Vous pouvez supprimer un événement individuel sélectionné dans le panneau de résultats, tous les événements ou seulement les événements qui satisfont certaines conditions.

Vous pouvez examiner la liste des événements enregistrés pendant l'activité de l'application sur chaque poste client dans sa fenêtre de propriétés (Figure 32). Il affiche le journal d'événements de Kaspersky Administration Kit conservé sur le serveur d'administration. Pour rechercher des informations, utilisez le filtre d'événements.

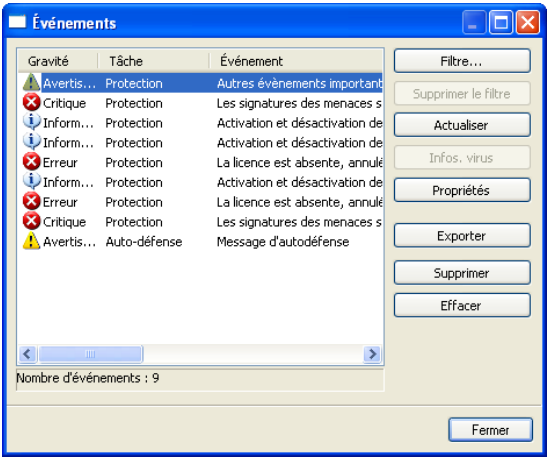


Figure 32. Affichage des événements stockés sur le serveur d'administration

6.4. Rapports

Vous pouvez recevoir des rapports sur l'état courant de la protection antivirus, construits à partir des informations stockées dans le serveur d'administration.

Il est également possible de contrôler l'état de la protection antivirus d'un poste client à l'aide d'informations inscrites par l'agent réseau dans le registre système.

Des rapports peuvent être créés pour :

- le système de protection Antivirus en général ;
- les ordinateurs appartenant à un certain groupe administratif ;
- une sélection de postes clients à l'intérieur de différents groupes administratifs ;
- le système de protection antivirus des réseaux logiques des serveurs d'administration secondaires.

Les rapports suivants peuvent être obtenus :

- **Rapport de version de la base antivirus** – Informations sur la version de la base antivirus utilisée par les applications.
- **Rapport d'erreurs** – Information sur les erreurs (défaillances de fonctionnement) enregistrées pendant l'exécution des applications installées sur les postes clients.
- **Rapports sur les clés de licence** – Informations sur l'état des clés de licence utilisées par les applications et le respect des restrictions imposées par ces licences.

- **Rapport sur les postes les plus infectés** – Informations sur les postes clients qui ont renvoyé le plus grand nombre d'objets suspects ou infectés.
- **Rapport sur le niveau de protection antivirus** – Informations sur les postes clients dont le niveau de protection antivirus est insuffisant.
- **Rapport de version du logiciel**– Informations sur les versions des applications Kaspersky Lab installées sur les postes clients.
- **Rapport sur le niveau de protection antivirus** – Informations sur les résultats de l'analyse antivirus des postes clients du réseau logique.
- **Rapport d'applications tierces** – Informations sur les logiciels d'autres fabricants ou les applications Kaspersky Lab non prises en charge par Kaspersky Administration Kit qui sont installées sur les postes clients.
- **Rapport sur les attaques réseau** – Informations sur les attaques réseau enregistrées par les postes clients.
- **Rapport sur les types d'application** – Informations sur les types d'application antivirus installées dans le réseau logique, sur les objets infectés que ces applications ont détectés et sur les actions qu'elles ont entreprises par rapport à ces objets infectés.
- **Rapport sur les applications protégeant les stations de travail et les serveurs de fichiers** – Informations détaillées sur les applications antivirus installées visant à protéger les stations de travail et les serveurs de fichiers, sur les objets infectés que ces applications ont détectés et sur les actions qu'elles ont entreprises par rapport à ces objets infectés.
- **Rapport sur les applications protégeant le périmètre informatique** – Informations détaillées sur les applications antivirus installées visant à protéger le périmètre informatique, sur les objets infectés que ces applications ont détectés et sur les actions qu'elles ont entreprises par rapport à ces objets infectés.
- **Rapport sur les applications protégeant les systèmes de messagerie** – Informations détaillées sur les applications antivirus installées visant à protéger les systèmes de messagerie, sur les objets infectés que ces applications ont détectés et sur les actions qu'elles ont entreprises par rapport à ces objets infectés.

Vous pouvez générer des rapports à partir de modèles créés par avance. La plupart des modèles de rapport générés par défaut sont placés dans le conteneur **Rapports** de l'arborescence de console (Figure 33). Quelques modèles supplémentaires sont disponibles dans l'assistant de création de rapports.

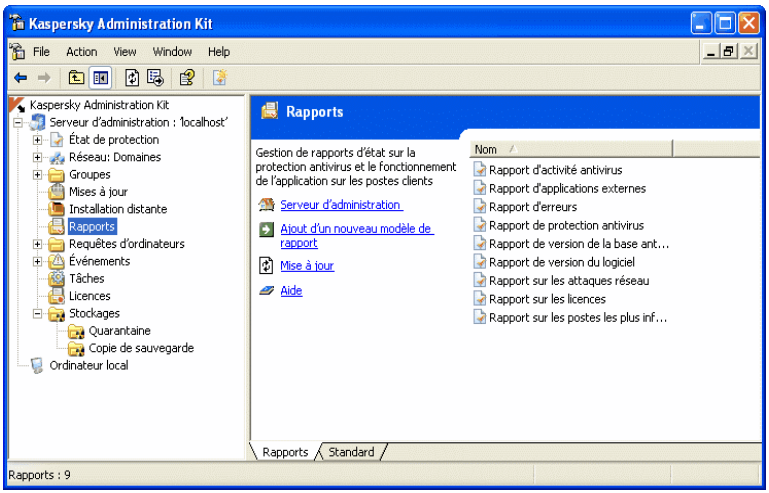


Figure 33. Affichage des résultats d'exécution des tâches stockées sur le serveur d'administration

Il existe treize (13) modèles standard qui correspondent à autant de types de rapports sur l'état du système de protection antivirus.

Vous pouvez créer de nouveaux modèles, supprimer les modèles existants, et afficher ou modifier leurs paramètres.

Les rapports sont consultés à l'aide d'un navigateur par défaut.

Si vous utilisez une structure hiérarchique des serveurs d'administration, vous pouvez créer des rapports globaux, contenant des informations sur les serveurs d'administration secondaires.

Si certains serveurs d'administration ne sont pas disponibles, le rapport en informera.

6.5. Recherche d'ordinateurs

Pour obtenir des informations sur un ordinateur spécifique ou un groupe d'ordinateurs, utilisez la fonction de recherche d'ordinateurs, en utilisant des critères. La recherche peut utiliser les informations présentes dans les serveurs d'administration secondaires. Les résultats de la recherche peuvent être enregistrés dans un fichier texte.

La fonction de recherche permet de trouver :

- Des postes clients dans le réseau logique du serveur d'administration et de ses serveurs secondaires ;

- Des ordinateurs non présents dans un réseau logique mais dans la structure des réseaux d'ordinateurs sur lesquels sont installés le serveur d'administration et ses serveurs secondaires ;
- Tous les ordinateurs des réseaux dans lesquels sont installés serveur d'administration et ses serveurs secondaires, sans tenir compte si un ordinateur en particulier appartient à la structure du réseau logique

Pour rechercher des ordinateurs, utilisez la commande **Rechercher un ordinateur** du menu contextuel correspondant à l'entrée du serveur d'administration, du dossier **Réseau** ou du groupe administratif sélectionné dans l'arborescence de console.

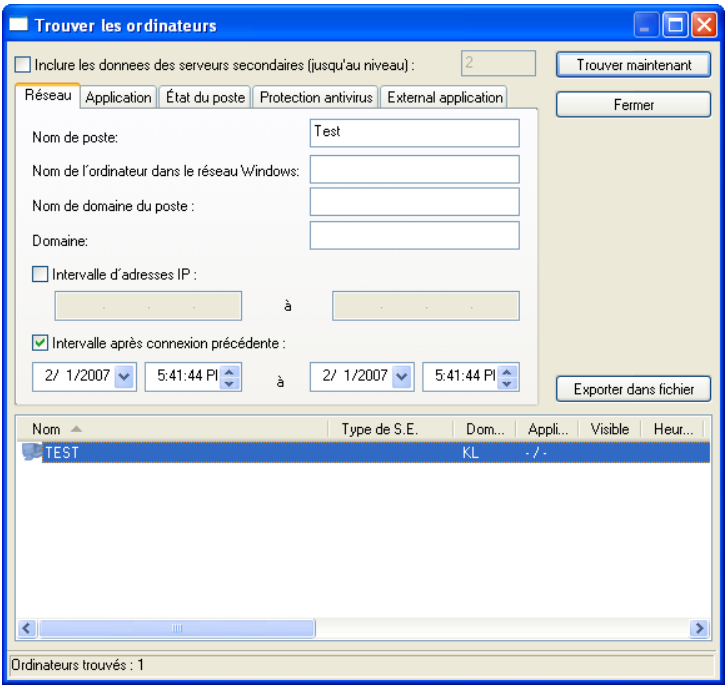


Figure 34. Recherche d'ordinateurs

En fonction de la cible choisie, les résultats de la recherche peuvent être les suivants :

- **Un groupe quelconque du réseau logique** – La recherche inclut les postes clients connectés au réseau logique du serveur d'administration auquel appartient le groupe sélectionné.

  La recherche est effectuée à partir des informations sur la structure du réseau logique et des réseaux des serveurs d'administration secondaires

(si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

Les résultats de la recherche contiendront les postes clients compris dans :

- **Tous les groupes** du réseau logique du serveur d'administration auquel appartient le groupe sélectionné ;
- **Tous les groupes** du réseau logique de **tous** les serveurs d'administration secondaires du serveur auquel appartient le groupe sélectionné (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

- Le groupe **Réseau** – La recherche s'effectue sur les ordinateurs du réseau où se trouve installé le serveur d'administration non inclus dans la structure du réseau logique.

  La recherche est effectuée à partir des données récupérées après un sondage du réseau d'ordinateurs par le serveur d'administration sélectionné et ses serveurs secondaires (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

  Les résultats incluront les postes clients du groupe **Réseau** sélectionné pour la recherche et les groupes **Réseau** de tous les serveurs secondaires (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

- Serveur d'administration <nom du serveur> – Recherche complète d'ordinateurs.

  La recherche est effectuée à partir des informations sur la structure du réseau logique et des données récupérées après un sondage du réseau d'ordinateurs par le serveur d'administration sélectionné et ses serveurs secondaires (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

  Les résultats de la recherche contiendront :

  - les postes clients du réseau logique du serveur d'administration sélectionné et tous ses serveurs secondaires (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).
  - les ordinateurs du groupe Réseau du serveur d'administration sélectionné et des groupes **Réseau** de tous ses serveurs secondaires (si la case **Inclure les données des serveurs secondaires** est cochée dans les options de recherche).

Pour rechercher, enregistrer et afficher les informations sur les ordinateurs dans un dossier séparé de l'arborescence de console, utilisez la fonction de création de filtres.

6.6. Filtres d'ordinateurs

Pour permettre une surveillance plus flexible de l'état des postes clients dans le réseau logique, les informations sur les ordinateurs à l'état **Critique** et **Avertissement** ainsi que sur les ordinateurs détectés sur le réseau au cours des dernières 24 heures, sont affichées dans un dossier séparé de l'arborescence de console appelé **Sélections d'ordinateurs** (Figure 35).

Des diagnostics sur l'état des postes clients sont effectués à partir des informations obtenues sur l'état de leur protection antivirus et sur leur activité dans le réseau. Les diagnostics sont configurés séparément pour chaque groupe administratif, à l'onglet **État de protection** (Figure 36).

Les informations sur les nouveaux ordinateurs sont fournies en fonction des résultats du sondage des ordinateurs sur le réseau, par le serveur d'administration.

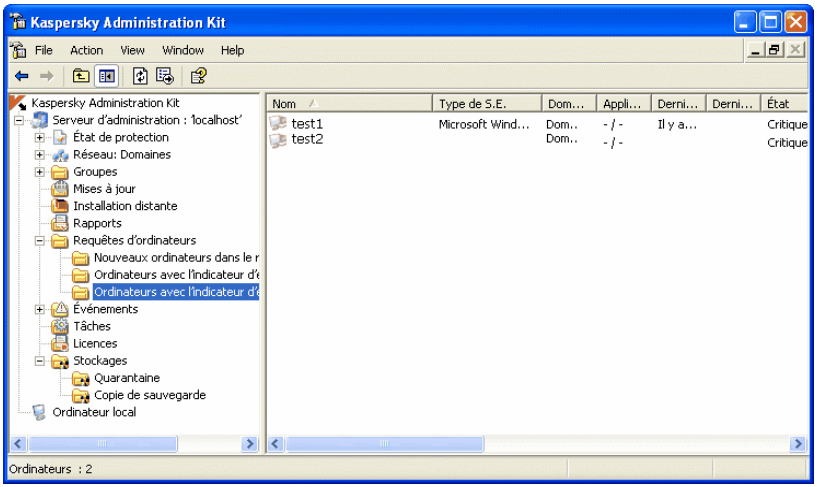


Figure 35. Sélections d'ordinateurs

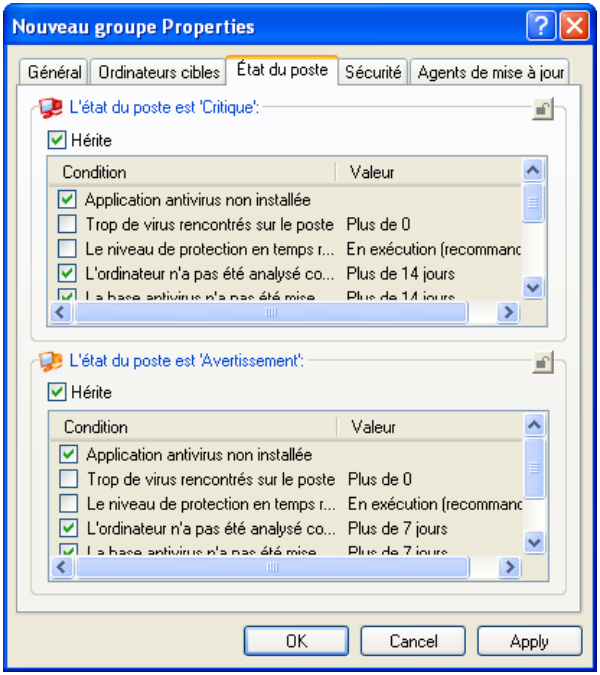


Figure 36. Configuration des diagnostics du poste client

Il est possible de créer des filtres supplémentaires. Pour créer un filtre, utilisez la commande **Nouveau / Filtre** dans le menu contextuel de l'entrée **Filtre d'ordinateurs**. Un nouveau dossier avec le nom spécifié pour le filtre apparaîtra alors sous l'entrée **Sélections d'ordinateurs** dans l'arborescence de console. Pour ajouter des ordinateurs à la sélection, configurez les paramètres du filtre (Figure 37). La sélection peut être utilisée pour la recherche puis le déplacement des ordinateurs sélectionnés vers les groupes administratifs. Le déplacement est réalisé à l'aide de la souris.

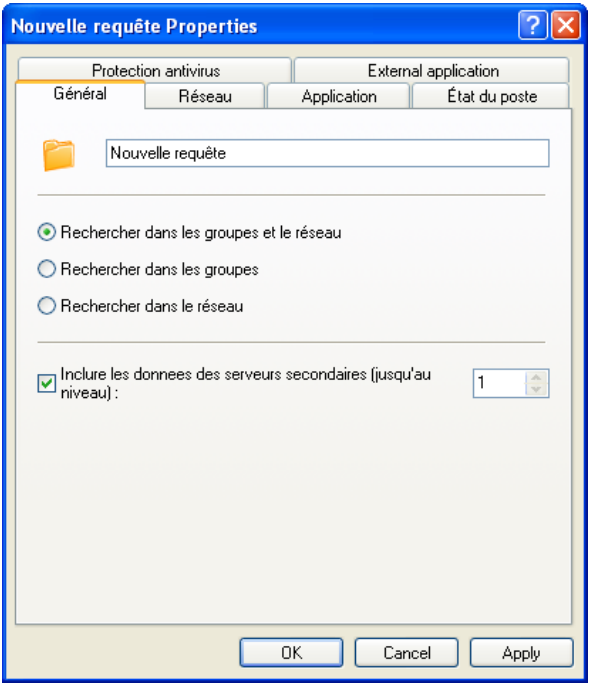


Figure 37. Configuration d'un filtre d'ordinateurs

6.7. Surveillance des attaques de virus

Kaspersky Administration Kit permet de surveiller l'activité virale sur les postes clients des réseaux logiques à l'aide de l'événement **Attaque virale** enregistré au cours de l'activité du composant serveur d'administration.

Cette caractéristique a une grande importance pendant les épidémies, car il permet de réagir à temps contre l'apparition de menaces d'attaques virales.

Les critères utilisés pour générer un événement d'**Attaque virale** sont définis dans les paramètres du serveur d'administration, sous l'onglet **Attaques de virus** (Figure 38).

Un événement peut être défini pour certains types d'applications. Pour activer le mécanisme de détection d'attaques virales, cochez la case en regard du type d'application concernée :

- **Antivirus pour les stations de travail et serveurs de fichiers** ;

- **Protections antivirus du périmètre informatique** ;
- **Antivirus pour systèmes de messagerie**.

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

- Le champ **Virus** indique le nombre de virus trouvés par des applications de ce type dans le réseau logique ;
- Le champ **Sur un laps de temps de (min.)** indique l'intervalle de temps qu'il a fallu pour détecter la quantité de virus dont il est question ci-dessus.

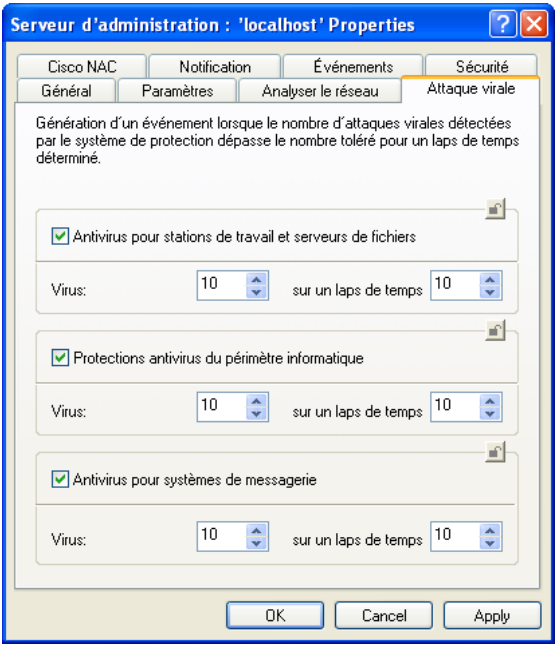


Figure 38. Configuration de la détection des attaques de virus

L'événement **Attaque virale** est défini d'après les événements **Virus détecté** et **Détection de virus, de vers, de trojans et de programmes d'intrusion** dans le fonctionnement de l'application antivirus. Par la suite, pour détecter avec succès les épidémies virales, il faut que toutes les données de ces événements soient conservées sur le serveur d'administration. Pour ce faire, les stratégies de toutes les applications antivirus doivent être correctement configurées (sous l'onglet **Enregistrement** (voir Figure 39), dans la fenêtre des propriétés des événements **Virus détecté** et **Détection de virus, de vers, de trojans et de**

programmes d'intrusion, cochez la case **Enregistrer sur le serveur pendant (jours)**).

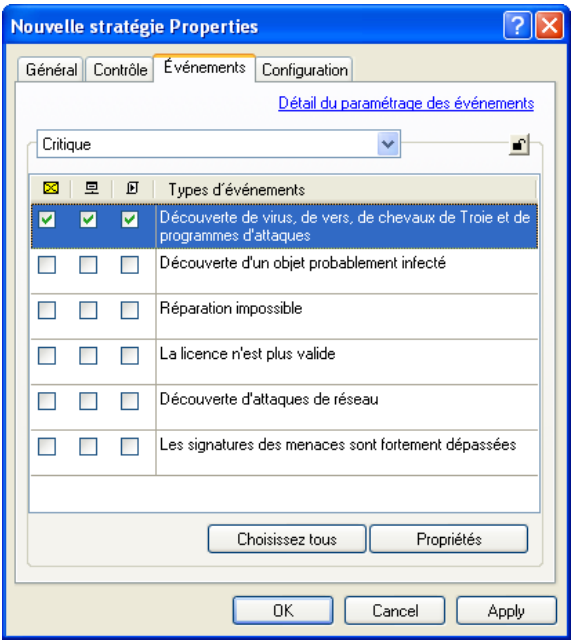


Figure 39. Configuration de l'enregistrement de l'événement

La procédure de notification de l'événement **Attaque virale** est définie dans les paramètres du serveur d'administration sous l'onglet **Notification** (Figure 40).

En outre, il est possible de définir un changement automatique dans la stratégie active, comme réaction au déclenchement d'une épidémie. Pour ce faire, il faut cocher la case **Activer la stratégie en fonction de l'événement** dans les paramètres de stratégie, et sélectionner l'événement **Attaque virale** (Figure 12).

Dans le compte des événements **Virus détecté et Détection de virus, de vers, de trojans et de programmes d'intrusion**, seules les informations sur les postes clients du serveur d'administration principal sont prises en compte.

L'événement **Attaque virale** est configuré séparément sur chaque serveur secondaire.

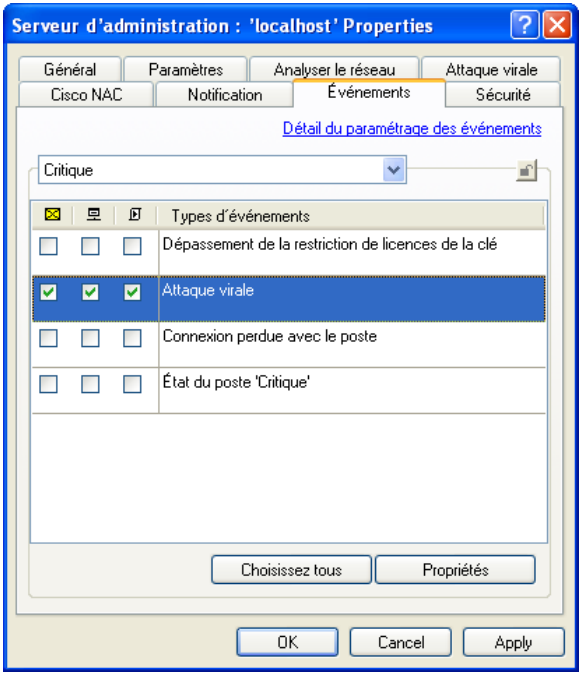


Figure 40. Configuration des paramètres de notification d'événement

6.8. Copie de sauvegarde et restauration des données du serveur d'administration

La copie de sauvegarde permet de transférer le serveur d'administration d'un ordinateur vers un autre sans perte d'informations, ainsi que de restaurer les données lors du transfert de la base du serveur d'administration vers un autre ordinateur ou pour faire la mise à jour vers une nouvelle version de Kaspersky Administration Kit.

Quand le serveur d'administration est désinstallé de l'ordinateur, Kaspersky Administration Kit suggère toujours de créer une copie de sauvegarde.

Les éléments suivants sont sauvegardés ou restaurés par une copie de sauvegarde :

- La base de données du serveur d'administration (stratégies, tâches, paramètres d'application, événements enregistrés sur le serveur d'Administration) ;
- Les données de configuration de la structure du réseau logique et des postes clients ;
- Le stock des paquets de déploiement des applications (le contenu des dossiers **Packages, Uninstall** et **Updates**) ;
- Le certificat du serveur d'administration.

La restauration des données lors de la mise à jour vers une version plus récente de l'application est prise en charge à partir de Kaspersky Administration Kit version 5.0 Maintenance Pack 3

Si l'emplacement du dossier partagé a été modifié, lors de la restauration des données, assurez-vous que les tâches utilisant le dossier partagé fonctionnement correctement (tâches de mise à jour, de déploiement) et, si nécessaire, configurez le chemin en conséquence.

La copie des données du serveur d'administration pour la copie et leur restauration postérieure peuvent être effectuées automatiquement par la tâche de sauvegarde ou manuellement, à l'aide de l'outil **klbackup** fourni dans la distribution de Kaspersky Administration Kit. La restauration des données s'effectue à l'aide de l'outil **klbackup.**

Après l'installation du serveur d'administration, l'outil **klbackup** se trouve placé dans le dossier d'installation du composant et pourra servir pour copier ou restaurer les données (en fonction des paramètres d'exécution) en le lançant depuis la ligne de commande.

La tâche de copie de sauvegarde doit être effectuée manuellement et se trouve parmi les **Tâches globales**. Pour activer la copie de sauvegarde, vous devez configurer ces paramètres de tâches. Vous pouvez également créer une tâche de copie de sauvegarde manuellement : Après avoir choisi l'application cible de la tâche, sélectionnez le type de tâche **Kaspersky Administration Kit - Réception de mises à jour par le serveur d'administration**.

ANNEXE A. GLOSSAIRE

Cette documentation utilise certains termes spécialement liés à la protection antivirus. Le glossaire présente une liste des définitions de ces termes. Les entrées de glossaire sont classées par ordre alphabétique afin d'en faciliter la consultation.

A

Administrateur de réseau logique – Utilisateur qui installe, configure et met à jour Kaspersky Administration Kit, et qui contrôle à distance les applications Kaspersky Lab installé sur les ordinateurs du réseau logique.

Agent réseau (Network Agent) – Composant de Kaspersky Administration Kit qui se charge de la communication entre le serveur d'administration et les applications Kaspersky Lab installés sur les postes réseau spécifiques (stations de travail ou serveurs). Ce composant est commun à toutes les applications Windows comprises dans Kaspersky Lab Business Optimal et Corporate Suite. Il existe des versions de l'agent réseau spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

Agents de mise à jour – ordinateurs qui opèrent comme des pôles intermédiaires de distribution des mises à jour et des paquets d'installation à l'intérieur des groupes administratifs .

Analyse complète à la demande – Mode défini par l'administrateur, qui analyse tous les fichiers de l'ordinateur à la recherche de virus et qui désinfecte ou supprime les objets infectés après leur détection.

Analyse de fichier par format – Mode d'analyse selon lequel le programme analyse le contenu d'un fichier, à savoir, l'identificateur de format de l'en-tête de fichier.

Analyse de fichiers par extension – En mode d'analyse, le programme tient compte de l'extension du fichier analysé.

Application externe ou d'autre fabricant – Une application antivirus d'un autre fabricant ou une application Kaspersky Lab non prise en charge par Kaspersky Administration Kit.

B

Base antivirus – Base de données créée par les spécialistes de Kaspersky Lab, contenant des définitions détaillées de tous les virus existants, avec des procédés de détection et de désinfection. Les applications antivirus utilisent cette base de données afin de détecter et de désinfecter les virus avec succès. La base antivirus disponible sur les sites Web de Kaspersky Lab est régulièrement mise à jour au fur et à mesure de l'apparition de nouvelles menaces de virus. Les utilisateurs enregistrés de Kaspersky Lab ont accès aux mises à jour des bases de

données. Pour conserver votre ordinateur constamment protégé contre des virus, nous recommandons de télécharger régulièrement les mises à jour.

Bases de messagerie – Bases de données contenant les messages de courrier entreposés sur votre ordinateur. Chaque message entrant/sortant est enregistré dans la base de données après sa réception/son envoi. Ces bases de données sont analysées en mode d'analyse à la demande.

Blocage d'objet – Évite que des applications externes puissent accéder à un objet. L'objet bloqué ne peut pas être lu, exécuté, modifié ni supprimé.

C

Certificat du serveur d'administration – Certificat permettant d'authentifier la connexion de la console d'administration au serveur d'administration, et les transferts de données entre le serveur et les clients. Le certificat du serveur d'administration est créé pendant l'installation du serveur d'administration. Il est placé dans le sous-dossier **Cert** du dossier d'installation.

Clé de licence – Fichier avec extension *.key* à usage de « clé » personnelle. Ce fichier est nécessaire pour un fonctionnement correct des applications Kaspersky Lab. Vous trouverez la clef de licence dans le kit de distribution si vous avez acheté l'application chez un distributeur Kaspersky Lab. Si vous avez acheté l'application en ligne, la clef de licence vous est envoyée à travers un courrier électronique. Sans clef de licence, Kaspersky Antivirus NE FONCTIONNE PAS.

Client du serveur d'administration (ou **poste client**) – un ordinateur, un serveur ou une station de travail sur lequel sont exploités le composant Network Agent et les applications Kaspersky Lab.

Console d'administration – Composant de Kaspersky Administration Kit qui fournit l'interface des services administratifs de Administration Server et de l'agent réseau.

D

Désinfection – Un procédé de traitement des objets infectés. La désinfection implique la restauration partielle ou totale des données, ou la conclusion que ces fichiers ne peuvent pas être désinfectés. Les objets sont désinfectés à l'aide de la base antivirus. Si la désinfection est la première action appliquée après la détection d'un objet suspect, le programme effectue une sauvegarde du fichier. Si des données sont perdues pendant la désinfection, la sauvegarde permet de récupérer l'objet.

Disques virtuels (disques RAM) – Partie de RAM utilisée pour simuler un disque physique normal dans un ordinateur individuel.

E

Entrepôt de sauvegarde – Dossier contenant les copies de sauvegarde des données du serveur d'administration, créées par l'outil de sauvegarde.

État de la protection antivirus – Situation actuelle de la protection antivirus qui décrit le niveau de sécurité de votre ordinateur.

Exclusions – Configuration utilisateur permettant d'exclure certains objets des analyses. Vous pouvez adapter les règles d'exclusion à la *protection en temps réel* et à l'*analyse à la demande*. Vous pouvez ainsi désactiver l'analyse des archives au cours d'une analyse complète, ou exclure des fichiers à l'aide de masques.

G

Gestion centralisée d'une application – Gestion d'une application à l'aide de Kaspersky Administration Kit.

Gestion locale – Gestion d'une application par l'intermédiaire d'une interface locale.

Groupe d'administration – Ordinateurs groupés selon des critères fonctionnels et applications de Kaspersky Lab installées. Le regroupement simplifie considérablement les procédures de gestion et permet à l'administrateur de gérer tous les ordinateurs sous la forme d'éléments simples. Un groupe peut inclure d'autres groupes. Des stratégies de groupe et des tâches de groupe peuvent être créées pour chaque application installée sur un membre du groupe.

I

IChecker – Technologie qui permet d'exclure des analyses suivantes les objets qui n'ont pas été modifiés depuis l'analyse précédente. La technologie IChecker repose sur la mise en place d'une base contenant les sommes de contrôle des objets.

Installation distante – Installation des applications Kaspersky Lab à l'aide des fonctions offertes par Kaspersky Administration Kit.

Installation par envoi – Méthode d'installation à distance (en anglais: Push) permettant d'installer le logiciel Kaspersky Lab sur des ordinateurs spécifiques de votre réseau logique. Pour exécuter la tâche d'installation par envoi avec succès, le compte chargé de lancer cette tâche doit posséder des droits d'exécution des applications sur les clients distants. Cette méthode est recommandée pour des ordinateurs sous MS Windows NT/2000/2003/XP, qui prennent en charge cette caractéristique, ou sur des ordinateurs sous MS Windows 98/Me, sur lesquels l'agent réseau est installé.

Installation par script – Méthode d'installation qui fait dépendre la tâche d'installation distante d'un ou de plusieurs comptes utilisateur spécifiques. Quand l'utilisateur spécifique ouvre une session sur le domaine, l'installation de l'application s'effectue sur poste client utilisé.

Cette méthode est recommandée pour des ordinateurs exploités sous MS Windows 95/98/Me

IStreams – Technologie qui permet d'exclure les fichiers stockés sur des disques au format NTFS, s'ils n'ont pas été modifiés depuis l'analyse précédente. La technologie IStreams est mise en œuvre grâce en conservant les sommes de contrôle des fichiers dans les flux NTFS supplémentaires.

K

Kaspersky Administration Kit – Application spécialisée dans l'exécution centralisée des tâches administratives principales. Il offre un contrôle complet sur la stratégie antivirus de l'entreprise utilisatrice d'applications Kaspersky Lab.

M

Mise à jour – Fonction de Kaspersky Anti-Virus qui met à jour des fichiers, ou en ajoute de nouveaux (base antivirus ou modules de programme), récupérés à partir des serveurs de mise à jour de Kaspersky Lab.

Mises à jour disponibles – Service Packs contenant des mises à jour urgentes, stockées pendant un certain temps, ainsi que les dernières modifications dans l'architecture de l'application.

N

Niveau de gravité – Paramètre distinctif d'un événement enregistré au cours de l'exécution de Kaspersky Anti-Virus. Il y a quatre degrés de gravité :

- **Critique**
- **Erreur**
- **Avertissement**
- **Info**

Des événements de même type peuvent avoir différents degrés de gravité, en fonction du moment spécifique.

Niveau recommandé – Niveau de protection antivirus utilisant les paramètres recommandés par les experts de Kaspersky Lab, qui assure une protection optimale de votre ordinateur. Ce niveau est celui par défaut.

O

Objet infecté – Objet contenant un virus. Nous recommandons de cesser de travailler avec ces objets qui peuvent infecter votre ordinateur.

Objet suspect – Objet contenant une mutation de code d'un virus déjà connu, ou un code ressemblant à un virus mais encore inconnu des spécialistes de Kaspersky Lab.

Objets de démarrage – Un ensemble de programmes nécessaires pour le lancement et le bon fonctionnement du système d'exploitation, et du

reste des logiciels installés dans l'ordinateur. Votre système d'exploitation lance ces objets à chaque démarrage. Certains virus tentent d'infecter ces objets et causent la défaillance du système au démarrage.

OLE (objet) – Objet lié ou incorporé dans d'autres fichiers utilisant la technologie OLE.

Opérateur de réseau logique – Utilisateur chargé de surveiller le système de protection antivirus contrôlé par Kaspersky Administration Kit.

P

Paquet d'installation – Un paquet de fichiers utilisé pour installer des applications Kaspersky Lab sur postes distants d'un réseau logique. Les paquets d'installation s'appuient sur un fichier **.kpd** spécial inclus dans le kit de distribution de l'application, avec les paramètres minimums assurant le fonctionnement de base de l'application après son installation. Ces paramètres correspondent aux paramètres par défaut des applications.

Paramètres d'application – Paramètres d'application communs à tous les types de tâches exécutées par cette application.

Paramètres de tâche – Paramètres d'application spécifiques pour chaque type de tâche.

Période de licence – Période pendant laquelle vous pouvez profiter de toutes les fonctions de Kaspersky Anti-Virus. En règle générale, la période de licence est d'un an, à compter de la date d'achat de la clé. Après l'expiration de la licence, l'application continuera de fonctionner mais il ne sera pas possible de mettre à jour la *base antivirus*.

Plug-in de console (gestion) – Composant spécial d'interface permettant de contrôler une application à distance à l'aide de la console d'administration. Les plug-ins sont spécifiques à chaque application et sont inclus dans toutes les applications Kaspersky Lab pouvant être contrôlées par Kaspersky Administration Kit.

Poste administrateur – Ordinateur sur lequel la console d'administration de Kaspersky Administration Kit est installée. Avec cette console, l'administrateur peut établir et contrôler un système de protection antivirus utilisant des applications Kaspersky Lab.

Protection en temps réel – Mode d'analyse dans lequel une application antivirus reste résidente en mémoire. Dans le mode de protection en temps réel, l'application analyse tous les objets ouverts en lecture, en écriture ou en exécution. Avant de permettre l'accès à un objet, Kaspersky Anti-Virus l'analyse et, s'il détecte un virus, bloque l'accès à l'objet, puis le désinfecte ou le supprime (selon la configuration utilisateur).

Protection Maximum – Niveau de protection qui garantit une protection complète mais pénalise légèrement le rendement.

Q

Quarantaine – Entrepôt spécial qui isole les objets infectés et suspects.

Quarantaine – Méthode de traitement d'un objet *suspect*. L'accès à l'objet est bloqué et le fichier est déplacé vers la quarantaine en vue d'un traitement postérieur.

R

Restauration – Restauration des données du serveur d'administration à l'aide d'un outil de sauvegarde. L'information de restauration est disponible dans l'entrepôt de sauvegarde. L'outil vous permet de restaurer :

Base de données du serveur d'administration qui entrepose les stratégies, les tâches, les paramètres d'application, et les événements enregistrés sur le serveur d'administration ;

Informations sur les configurations des réseaux logiques et des clients ;

Fichiers pour l'installation à distance des applications (contenu des dossiers Packages, Uninstall, Updates)

Certificat du serveur d'administration

S

Sauvegarde – de données du serveur d'administration pour leur conservation et leur postérieure restauration, par l'outil klbackup. L'outil vous permet de sauvegarder :

Base de données du serveur d'administration qui entrepose les stratégies, les tâches, les paramètres d'application, et les événements enregistrés sur le serveur d'administration ;

Informations sur les configurations des réseaux logiques et des clients ;

Fichiers pour l'installation à distance des applications (contenu des dossiers Packages, Uninstall, Updates)

Certificat du serveur d'administration

Sauvegarde (dossier de) – Répertoire contenant des copies de sauvegarde des objets effacés et désinfectés.

Serveur d'administration – Composant de Kaspersky Administration Kit qui stocke de manière centralisée des informations sur les applications Kaspersky Lab installées sur les clients, et qui contrôle ces applications.

Serveurs de mise à jour de Kaspersky Lab – Liste de sites HTTP et FTP de Kaspersky Lab, d'où vous pouvez obtenir les mises à jour pour votre ordinateur.

Seuil d'activité virale – Nombre de virus détectés dans un intervalle de temps déterminé. Si ce nombre est dépassé, la situation est identifiée comme une **Attaque virale**. Ce paramètre est important dans l'identification des épidémies, car il détermine le temps de réaction

administrative face à de nouvelles menaces, et l'application des mesures préventives destinées à protéger le réseau.

Stratégie de groupe – Ensemble des paramètres d'application d'un groupe administratif contrôlé par Kaspersky Administration Kit. Les stratégies de groupe peuvent être différentes pour chaque groupe. Les stratégies de groupe sont spécifiques pour différentes applications. La stratégie détermine la configuration de tous les paramètres des applications.

Suppression d'un objet – Méthode de traitement d'un objet. La suppression d'un objet signifier l'enlever physiquement d'un ordinateur. Cette méthode est recommandée pour traiter les objets infectés. Si la suppression est la première action appliquée sur un objet, il est nécessaire d'en créer une copie de sauvegarde avant de le supprimer. Vous pouvez utiliser la sauvegarde pour restaurer l'objet original.

Tâche – Action nommée, qui est exécutée par une application de Kaspersky Lab.

Tâche de groupe – Tâche définie et utilisée pour tous les clients d'un groupe.

Tâche globale – Tâche définie et utilisée pour un certain nombre de clients de différents groupes administratifs.

Tâche locale – Tâche créée et utilisée sur un simple client.

V

Virus inconnu – Nouveau virus non répertorié dans la *base antivirus*. En règle générale, Kaspersky Antivirus détecte les virus inconnus grâce à un *analyseur de code heuristique*, et identifie les objets contenant ces virus comme *suspects*.

Vitesse maximum – Niveau de protection qui assure une vitesse maximum mais un degré moindre de sécurité.

ANNEXE B. 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 principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. 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 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 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 d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la “météo” des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d’informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S’abonner et se désabonner aux canaux d’information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d’informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l’information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s’agit d’un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l’ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l’analyse, l’utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l’analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s’agit d’un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l’ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté

directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.
- Surveiller les modifications de la base de registres système grâce au contrôle de l'état de la base de registres.
- **Le** contrôle **des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique**. Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport,

l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.

- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont:

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel :** tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;
- **Protection contre les sms et mms indésirables.**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.

- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;
- *Génération de rapports détaillés* ;
- *Mise à jour automatique des bases* de l'application.

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors

de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable.* ;
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Blocage des fenêtres pop up et des bannières publicitaires* pendant la navigation sur Internet ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Outils de création d'un disque de démarrage* capable de restaurer le système après une attaque de virus ;
- *Système développé de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables* (technologie Intel® Centrino® Duo pour ordinateurs portables) ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de

chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Répartition de la charge entre les processeurs du serveur* ;
- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases*.

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers* ;

- *Protection des serveurs de messagerie Sendmail, Qmail, Posftix et Exim* ;
- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Prévention des épidémies de virus et des diffusions massives* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Utilisation sécurisée des réseaux sans fil* Wi-Fi ;
- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes dans le système* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les

niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;

- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;
- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™);
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Filtrage des messages non sollicités* ;
- *Analyse des messages et des pièces jointes du courrier entrant et sortant* ;
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Filtrage des messages* en fonction du type de pièce jointe ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* du logiciel ;
- *Prévention des épidémies de virus* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Système de rapports* sur l'activité de l'application ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.

- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Analyse du trafic Internet* (HTTP/FTP) en temps réel ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* ;
- *Système de rapports sur le fonctionnement de l'application* ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

B.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la

mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez,

fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

--- Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à

l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.