KASPERSKY LAB

Kaspersky® Administration Kit version 5.0

Manuel de l'administrateur

KASPERSKY® ADMINISTRATION KIT
VERSION 5.0

Manuel de l'administrateur

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

Date de révision : Décembre 2005

Sommaire

CHAPITRE 1. KASPERSKY ADMINISTRATION KIT

1.1. Présentation de Kaspersky Administration Kit

Kaspersky® Administration Kit est un logiciel conçu pour exécuter des tâches administratives de manière centralisée. Il offre un contrôle complet sur la stratégie antivirus de l'entreprise, reposant sur les applications Kaspersky Anti-Virus Business Optimal et Kaspersky Anti-Virus 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 fonctions destinées aux administrateurs sont les suivantes :

- Déployer des applications Kaspersky Lab à travers le réseau sur des ordinateurs distants sous Windows. Il est possible de créer un paquet personnalisé d'applications Kaspersky Lab sur un poste prévu à cet effet, afin d'installer ces applications en une seule opération sur un nombre quelconque d'ordinateurs distants.
- Gérer efficacement les clés de licence. Kaspersky Administration Kit permet de contrôler de manière centralisée, l'installation des clés de licence pour toutes les applications Kaspersky Lab, la correspondance entre le nombre de licences et celui des applications Kaspersky Lab installées à travers le réseau, ainsi que les dates d'expiration de licences.
- Gérer à distance plusieurs applications Kaspersky Lab installées sur des ordinateurs Windows, depuis un seul poste central. Kaspersky Administration Kit permet de construire un système de protection antivirus à plusieurs niveaux, contrôlé à partir d'un seul poste administrateur. Ceci est particulièrement important dans le cas d'entreprises disséminées sur plusieurs sièges, mais qui agissent de concert. Cette caractéristique permet aux administrateurs de :
    - Créer des *groupes administratifs* d'ordinateurs qui partagent des fonctions et des applications semblables ;

- Configurer en une seule fois les applications à l'aide de *stratégies de groupe* ;
- Ajuster les installations aux conditions spécifiques des ordinateurs individuels, à l'aide de *paramètres d'application* ;
- Gérer de multiples applications à la fois en leur affectant des *tâches de groupe ou globales* ;
- Planifier des tâches pour des applications installées sur des ordinateurs appartenant à des groupes administratifs différents.

- Mettre à jour automatiquement la base antivirus. Il est possible de mettre à jour la base antivirus de toutes les applications, sans qu'il soit nécessaire de connecter chaque ordinateur directement aux serveurs de mise à jour de Kaspersky Lab. Vous pouvez planifier la mise à jour automatique, à une heure spécifiée, pour préserver le niveau et la mise à jour de la sécurité des postes clients.
- Accumuler des rapports sur toutes les installations. Les fonctions de rapport de Kaspersky Administration Kit permettent de collecter des statistiques de fonctionnement de toutes les installations, et de créer des rapports statistiques à partir de données récentes. L'application permet de créer, à l'échelle de tout le réseau, un rapport sur une simple application Kaspersky Lab (rapports spécifiques à l'application) ou sur toutes les applications Kaspersky Lab installées sur un ordinateur individuel (rapport spécifique à un ordinateur).
- Recevoir des notifications de messagerie, sur certains événements spécifiques. Vous pouvez spécifier un éventail d'événements sur lesquels vous serez informé. Par exemple, la détection d'un virus, l'échec d'une mise à jour ou l'apparition d'un nouvel ordinateur sur le réseau sont des événements qu'une application peut transmettre pendant son fonctionnement.

Kaspersky Administration Kit possède 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.
- **Agent Réseau** coordonne Administration Server et les applications Kaspersky Lab installés sur un poste réseau particulier (un poste de travail ou un serveur). Ce composant prend en charge toutes les applications présentes dans Kaspersky Anti-Virus Business Optimal et Kaspersky Antivirus Corporate Suite.

- **La console d'administration**, une interface utilisateur destinée aux services Administration et Agent, pour simplifier le travail avec Microsoft Console d'administration (MMC).

1.2. Nouveautés de la version 5.0

Les nouvelles caractéristiques de Kaspersky Administration Kit version 5.0 sont les suivantes :

- Gestion de toutes les applications Kaspersky Lab installées sur des ordinateurs sous Windows.
- Contrôle du système de protection antivirus même sur des réseaux de grande taille (des dizaines de milliers de postes).
- Intégration de l'interface utilisateur standard de Windows dans Microsoft Console d'administration (MMC).
- Administration de la protection antivirus à travers des tâches spécifiques.
- Attribution centralisée d'une configuration générale pour un groupe d'ordinateurs appartenant au même groupe administratif.
- Création de stratégies de protection antivirus avec attribution de tâches de groupe, mise en place et suivi de l'application de ces stratégies.
- Fonctions de rapport améliorées.
- Journalisation et système de rapports améliorés. Vous pouvez afficher des informations générales sur la protection antivirus du réseau entier ou afficher des rapports pour chaque application sous surveillance, présente sur n'importe quel ordinateur individuel du réseau.
- Système de gestion centralisé de clés de licences. Ce système vous permet de contrôler la correspondance entre le nombre de licences et le nombre d'applications Kaspersky Lab installées, de vérifier les dates d'expiration des licences, et de mettre à jour les clés de licence de manière régulière.

1.3. Spécifications matérielles et logicielles

Serveur d'administration

- Configuration logicielle :

- MSDE 2000 SP 3 ou MS SQL Server 2000 SP 3[1]
- Windows 2000 SP 1 ou supérieur; Windows XP SP 1 ou supérieur, Windows 2003 Server; Windows NT4 SP 6.a

- 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 :
  - Windows 2000 SP 1 ou supérieur ; Windows NT4 SP 6a; Windows XP SP 1 ou supérieur; Windows 2003 Server; Microsoft Console d'administration 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 :
  - Windows 98; Windows ME; Windows 2000 SP 1 ou supérieur; Windows NT4 SP 6a; Windows XP SP 1 ou supérieur et Windows 2003 Server
- Configuration matérielle :
  - Processeur Intel Pentium à 233 MHz ou supérieur
  - 32 Mo de RAM
  - 10 Mo d'espace disponible sur le disque

[1] Vous pouvez installer MSDE à partir du paquet de distribution inclus dans Kaspersky Administration Kit .

1.4. Contenu de la distribution

Vous pouvez acquérir ce produit logiciel chez nos revendeurs (boîte) uniquement intégré dans Kaspersky Antivirus Business Optimal et Kaspersky Corporate Suite pour la protection de postes de travail et de serveurs sous Microsoft Windows, ainsi que en ligne (par exemple, visitez www.kaspersky.com puis cliquez sur le lien E-Store.

Le paquet au détail inclut :

- Une enveloppe cachetée avec le CD d'installation contenant les fichiers d'application;
- Guide de l'utilisateur
- Une clé de licence inscrite sur le CD d'installation ;
- Une carte d'inscription du produit logiciel principal (avec le numéro de série du produit);
- Contrat de licence

Avant d'ouvrir l'enveloppe avec le CD d'installation, lisez attentivement le Contrat de licence..

Si vous achetez Kaspersky Antivirus en ligne, vous téléchargerez le fichier d'installation depuis le site de Kaspersky Lab. Dans ce cas, le kit de distribution inclut, en plus de l'application, ce Guide de l'utilisateur. La clé de licence sera transmise par courrier électronique dès réception de votre paiement.

1.4.1. Contrat de licence

Le Contrat de licence est un contrat légal entre vous et Kaspersky Lab, où sont précisées les conditions d'utilisation du produit antivirus que vous avez acheté.

Lisez attentivement le contrat de licence !

En cas de désaccord avec les conditions du contrat de licence, vous pouvez renvoyer Kaspersky Antivirus à votre revendeur pour un remboursement. Dans ce cas, l'enveloppe contenant le CD d'installation ne doit pas avoir été ouverte.

L'ouverture de l'enveloppe cachetée contenant le CD d'installation ou l'installation du logiciel implique que vous acceptez les termes du contrat de licence.

1.5. Services réservés aux utilisateurs inscrits

Kaspersky Lab propose un large éventail de services à ses utilisateurs inscrits leur permettant d'utiliser plus efficacement les fonctions disponibles du service d'assistance de Kaspersky Anti-Virus.

Si vous vous inscrivez et achetez une souscription, vous recevrez les services suivants pour toute la période de votre inscription :

- Nouvelles versions de ce logiciel antivirus, fournies gratuitement ;
- Assistance téléphonique et par courrier électronique sur l'installation, la configuration et l'utilisation de l'application antivirus ;
- 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.

1.6. Objectif du document

Ce livre de référence présente l'usage de Kaspersky Administration Kit et contient des explications pas à pas de toutes ses fonctions. Les principes de base et le schéma de fonctionnement généraux de l'application sont décrits dans le Guide de l'administrateur de e Kaspersky Administration Kit.

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→ Knowledge base**. 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.

1.7. 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.
 Tâche ou exemple	Définition d'un problème, exemple ou démonstration des possibilités de l'application
 **Solution**	Implémentation de la tâche
[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

Kaspersky Administration Kit offre des fonctions d'administration, permettant à une société de gérer de manière centralisée des milliers d'ordinateurs à partir d'une seule interface administrateur. Pour ce faire, les ordinateurs du réseau d'entreprise sont organisés en *groupes administratifs*, selon leur utilisation et les applications Kaspersky Lab installées. Ceci facilite de manière significative la gestion parce que tous les ordinateurs du même groupe sont traités comme une unité. Par exemple, un premier groupe inclut tous les postes de travail, un second groupe, uniquement les serveurs de fichiers, etc.

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 client du serveur d'administration (*poste client*[2]) est un ordinateur, un serveur ou un poste de travail couverts par la protection antivirus. Le composant Agent Réseau et les applications Kaspersky Lab contrôlées doivent être installés sur chacun des postes clients.

Les groupes sont des groupes logiques de clients administrés par un seul serveur. Tous les ordinateurs d'un même groupe partagent :

- Les mêmes *stratégies* antivirus, spécifiques à chaque application.
- Les mêmes tâches (fonctions de l'application) et les mêmes paramètres de configuration. Il peut s'agir, par exemple, d'un *paquet d'installation* personnalisé, de la mise à jour des modules de base de données et de programme antivirus, des analyses à la demande, ou de la protection en temps réel.

L'administrateur peut créer une hiérarchie de groupes et sous-groupes imbriqués, avec n'importe quel degré de spécialisation, afin de simplifier l'administration des applications correspondantes. Les groupes et les postes

[2] Dans la suite, un poste client est un client du serveur d'administration.

clients peuvent être placés sur un même niveau hiérarchique. Chaque poste client peut être le membre d'un seul groupe.

Le Serveur d'administration est l'ordinateur du réseau d'entreprise sur lequel s'exécute l'application Administration Server. Le serveur d'administration un objet du réseau logique.

Les serveurs d'administration peuvent former une hiérarchie de type « serveur primaire ou maître – serveur secondaire ou esclave ». Le serveur d'administration primaire peut avoir de nombreux serveurs secondaires (voir section 4.5 à la page 55).

Le serveur d'administration (ou plus précisément, l'application Administration Server) est utilisé pour :

- Entreposer la description de la structure logique du réseau (configuration réseau)
- Entreposer les copies de sauvegarde des configurations client
- Entreposer les fichiers de distribution des applications Kaspersky Lab
- Installer et désinstaller à distance des applications sur les postes clients
- Mettre à jour la base antivirus et les modules de programme
- Contrôler les stratégies et les tâches de groupe sur des postes clients
- Entreposer des informations sur les événements qui se sont produits sur des postes clients
- Générer des rapports sur l'exécution des applications à travers le réseau logique
- Distribuer des clés de licence sur les postes clients ;
- Envoyer des alertes à partir de tâches exécutées sur des postes clients. Vous pouvez être informé, par exemple, de la détection d'un virus sur un poste client.

Le composant **Agent Réseau** assure la coordination entre le serveur d'administration et les postes clients. Il fournit des informations sur l'état courant de l'application, envoie et reçoit des commandes, met à jour la configuration, et informe le serveur sur des événements spécifiés. Reportez-vous à la section 2.3 à la page 16, pour savoir comment attacher Agent Réseau au serveur d'administration.

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.

Plug-in de console pour Agent Réseau: un composant spécial qui fournit l'interface de gestion de chaque application, 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.

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.

2.2. 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. Chaque tâche correspond à des paramètres spécifiques d'application.

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

Les paramètres d'application regroupent les **paramètres de fonctionnement** communs à tous les types de tâche. Les paramètres d'application spécifiques à chaque type de tâches constituent les **paramètres de tâche**. Les paramètres d'application et ceux de tâches sont toujours différents.

Pour qu'une application puisse effectuer une action, vous devez configurer des paramètres d'application, créer un tâche associée, puis exécuter cette dernière.

Vous pouvez utiliser des stratégies pour appliquer des paramètres d'application personnalisés à plusieurs postes clients du réseau logique. Une **stratégie** est un ensemble de paramètres d'application partagés par tous les ordinateurs dans un groupe. Les paramètres d'application sont différents en fonction des groupes. Une stratégie est propre à chaque application.

La mise en place d'une stratégie d'application spécifique suppose la configuration de tous les paramètres disponibles de l'application. Ainsi, la définition d'une stratégie implique à la fois la configuration des paramètres d'application et celle des paramètres des tâches spécifiques à cette application. La seule exception concerne les paramètres définis avant le démarrage de la tâche. Par exemple, la mise en place d'une stratégie de protection en temps réel *et* d'analyse à la demande, implique la configuration de paramètres pour les deux tâches sur le poste client.

Une stratégie possède une case à cocher pour indiquer si l'un de ses paramètres peut changer suite à la modification des paramètres d'application ou des paramètres de tâche, ou en raison de l'imbrication des groupes (paramètres du niveau inférieur de hiérarchie).

De nombreuses stratégies avec des paramètres différents peuvent être définies pour la même application dans un groupe. Cependant, une seule stratégie à la fois peut être appliquée dans l'application. Il est possible d'activer une stratégie qui n'est pas la stratégie active en fonction d'un événement, par exemple, pour renforcer les critères de protection antivirus au cours d'une épidémie.

Un groupe ne peut définir qu'une seule stratégie par application. Mais chaque groupe permet de créer ses propres stratégies, spécifiques à chaque application. En l'absence de stratégie définie, un groupe fils hérite de la stratégie du groupe parent.

C'est ainsi que les stratégies permettent de faire partager, à tous les ordinateurs d'un groupe, les mêmes paramètres d'application. Cependant, il reste toujours possible de modifier les paramètres d'application et de tâche pour chaque ordinateur du groupe, à moins que leurs configurations ne soient verrouillées par la stratégie du groupe.

Il est possible de créer et de configurer des tâches de manière centralisée, à travers le réseau logique. Une tâche attribuée à un groupe administratif est une **tâche de groupe** ; une tâche attribuée à un poste client individuel est appelée 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 est seulement installée sur certains des postes clients dans le groupe. Dans ce cas, la tâche de groupe ne sera exécutée que sur les ordinateurs où l'application est exploitée.

Les sous-groupes héritent des tâches de leurs groupes parent. Une tâche définie dans un groupe sera donc partagée par tous les postes de ce groupe, mais aussi par tous les postes des sous-groupes groupes de niveau inférieur.

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 une stratégie, seuls pourront être modifiés 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.

Les informations sur les stratégies, la configuration des applications, les tâches et les paramètres de tâches sont entreposées 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.

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

- Les paramètres de tâche et d'application modifiés (sauf ceux verrouillés par la stratégie courante).
- La stratégie du groupe, dans le cas des paramètres verrouillés, ou non modifiés.
- La stratégie parente, si aucune stratégie de groupe n'a pas été définie pour l'application.

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. L'administrateur peut être averti des comptes-rendus d'activité, ou afficher des rapports détaillés.

2.3. 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 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 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 section2.11.3 à la page 30). 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.

Toutes les transactions entre les postes clients et le serveur d'administration sont sécurisées par SSL (Secure Socket Layer). Le protocole SSL emploie des certificats électroniques pour l'authentification serveur et client, et assure le chiffrement des données et l'intégrité des messages au cours du transfert.

2.4. 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 des extrêmes en communication, du chiffrement des données transférées, et de la vérification de l'intégrité de données. Les techniques d'intégrité de données vérifient que les données n'ont pas été endommagées ou modifiées pendant le transfert. Une connexion SSL comporte l'authentification des deux extrêmes de la session de communication réseau, et le chiffrement des données en utilisant la méthode de clé fermée.

2.4.1. 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 les données sont transférées depuis les postes clients.

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. Pour restaurer le certificat, vous devez réinstaller le serveur d'administration et restaurer les données perdues à partir de celles sauvegardées (sur les options de sauvegarde, voir 4.14 à la page 72).

2.4.2. 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 confirmée et qu'un nouveau

certificat est reçu, la console d'administration l'enregistre sur disque, afin de l'utiliser pour authentifier le serveur lors de futures sessions.

2.4.3. 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, Agent Réseau demande le certificat du serveur d'administration et le compare au certificat local. Si les certificats diffèrent, l'accès au serveur d'administration est refusé.

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

2.5. 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.

Un nom d'hôte est attribué par le serveur d'administration quand un nouvel ordinateur est détecté sur le réseau Windows, ou quand une instance de 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.

Le serveur d'administration fait référence aux postes clients à travers leurs adresses IP. Si un client possède une installation de Agent Réseau, l'adresse IP de ce client est déterminée automatiquement par le serveur, à chaque connexion du client. Si Agent Réseau n'est pas installé, ou si ce client ne s'est pas encore connecté au serveur d'administration (par exemple, si Agent Réseau était installé

en local), le serveur d'administration détermine l'adresse IP de cet ordinateur d'après son nom NetBIOS ou DNS.

2.6. Administrateurs et opérateurs du réseau logique

Par défaut, seulement deux groupes d'utilisateurs, les **administrateurs** et les **opérateurs** de réseau logique, disposent de privilèges administratifs pour gérer des applications à l'aide de Kaspersky Administration Kit.

Un **administrateur du réseau logique** est un utilisateur qui installe et configure le progiciel Kaspersky Administration Kit sur les ordinateurs du réseau, puis qui gère les applications Kaspersky Lab sur les postes distants du réseau logique.

Un administrateur de réseau logique possède un contrôle total de toutes les fonctions disponibles de Kaspersky Administration Kit. Il a la possibilité de :

- Connecter au serveur d'administration
- Créer un réseau logique, et d'y ajouter des groupes et des postes clients à partir du réseau local de l'entreprise
- Installer le composant Agent Réseau sur des postes clients
- Créer et installer des paquets d'applications Kaspersky Lab sur des postes clients, et de contrôler leurs clés de licence
- Mettre à jour des versions d'application installées sur des postes clients
- Créer des stratégies et d'attribuer des tâches à des groupes ou à des ordinateurs différents, et de modifier des paramètres d'application
- Contrôler de manière centralisée les applications installées sur les postes clients du réseau logique et d'en examiner les rapports à l'aide des services du serveur d'administration, de Agent Réseau, et de la console d'administration.
- Autoriser à des utilisateurs ou des groupes d'utilisateurs l'accès aux fonctions de l'application, aussi bien pour le réseau logique en entier que pour des groupes administratifs séparés.

Un **opérateur du réseau logique** est un utilisateur qui surveille les performances du système de protection antivirus géré par Kaspersky Administration Kit.

L'opérateur de réseau logique possède des droits d'accès limités aux fonctions de Kaspersky Administration Kit. Il a la possibilité de :

- Connecter au serveur d'administration
- Afficher la structure du réseau logique
- Afficher les paramètres de stratégie, les tâches courantes, et les propriétés d'application
- Lancer et interrompre des tâches de groupes et des tâches globales
- Recevoir des rapports et des notifications sur les événements qui se produisent sur le réseau logique

Les privilèges d'administrateur de réseau logique sont attribués aux :

- Administrateurs de domaine dont les ordinateurs sont incorporés au réseau logique
- Administrateurs locaux des ordinateurs d'exploitation du serveur d'administration
- Utilisateurs du groupe d'administrateurs de Kaspersky Lab.

Les droits d'opérateur de réseau logique sont attribués aux utilisateurs appartenant au groupe **KLOperators**.

Les groupes **KLAdmins** et **KLOperators** sont créés pendant l'installation du composant Administration Server. L'administrateur peut créer ces groupes au choix sur le domaine du serveur d'administration, ou directement sur l'ordinateur d'exploitation du serveur d'administration. Vous pouvez afficher les groupes **KLAdmins** et **KLOperators** et les modifier à l'aide des outils standard d'administration de Windows (**Utilisateurs et groupes locaux)**.

Toutes les opérations lancées par les administrateurs de réseau logique héritent des mêmes droits d'accès que le compte de service du serveur d'administration. Un groupe **Administrateurs Kaspersky Lab** peut être créé pour chaque serveur d'administration. Ce groupe aura des privilèges d'administrateur uniquement dans ce réseau logique.

Si plusieurs ordinateurs du même domaine figurent dans plusieurs réseaux logiques, alors l'administrateur de ce domaine est un administrateur pour tous ces réseaux logiques. Il est possible de créer un seul groupe **KLAdmins** pour ces réseaux logiques pendant l'installation du premier serveur d'administration. De nouveaux membres peuvent être ajoutés à ce groupe en utilisant les outils standard d'administration de Windows. Toutes les opérations lancées par les administrateurs de réseau logique hériteront des droits d'accès du serveur d'administration.

L'administrateur d'un domaine configure et contrôle uniquement les applications Kaspersky Lab sur les ordinateurs de ce domaine. Si ce réseau logique inclut des ordinateurs de divers domaines, procédez comme suit pour attribuer des privilèges d'administrateur réseau logique à un administrateur de domaine :

- Activez des relations d'approbation entre les domaines
- Ajoutez cet administrateur au groupe d'administrateurs de chacun des domaines présents dans le réseau logique.

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

Après l'installation de l'application, l'administrateur du réseau logique peut modifier l'ensemble des droits accordés aux groupes **KLAdmins** et **KLoperators,** accorder des droits d'accès aux fonctions de l'application depuis Kaspersky Administration Kit à d'autres utilisateurs et groupes d'utilisateurs, enregistrés sur l'ordinateur où se trouve installée la Console d'administration. Il est possible d'autoriser différents droits d'accès pour travailler dans chaque groupe d'administration (voir section 4.2, page 51).

2.7. Mise en place de la protection antivirus à travers le 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 Kaspersky Lab 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. Vous pouvez installer le logiciel antivirus sur un nombre quelconque de clients sous système d'exploitation Windows.
- Vous pouvez installer, en local, des applications Kaspersky Lab 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 Agent Réseau. Ce scénario de déploiement est recommandé si un déploiement centralisé s'avère impossible.

2.8. Mise en place d'un système de gestion centralisé

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

1. Quel scénario de déploiement allez-vous choisir : installation à distance ou installation locale ? Votre décision dépendra de la présence des structures de domaine Windows sur votre réseau d'entreprise.
2. Quels ordinateurs sur votre réseau local vont fonctionner en tant que serveur d'administration, postes d'administrateurs, 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 ?

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 un ordinateur du réseau (voir section3.2 à la page 38).
2. Installer la console d'administration sur un ordinateur du réseau à partir duquel l'administrateur contrôlera les applications Kaspersky Lab (voir section3.2 à la page 38).

Ensuite, vous devrez créer la structure d'un réseau logique, définir la hiérarchie des groupes administratifs, et affecter des ordinateurs aux différents groupes.

À l'étape suivante, vous devrez installer Agent Réseau et les applications Kaspersky Lab sélectionnées sur des postes clients, puis installer les plug-ins de console correspondants sur le poste administrateur (voir Chapitre 3 à la page 36).

Pour finir, il faudra configurer les applications installées : affectation et application des stratégies de groupe (voir section 4.7 à la page 63) puis création de tâches (voir section 0 à la page 64).

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 4.2 à la page 51). Pour simplifier, la configuration du système de protection antivirus

équivaut à la création d'un réseau logique de structure similaire à celle des domaines du réseau Windows, puis à la mise en place d'un système de protection utilisant Kaspersky Antivirus 5.0, dans le cas de postes de travail sous Windows.

2.9. 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 d'applications sur les postes clients.
- Vérifier votre boîte aux lettres et lire les alertes transmises par les postes clients et le serveur d'administration à l'adresse de l'administrateur.

La liste complète des notifications envoyées est disponible dans la documentation des applications Kaspersky Antivirus.

- Effectuer à distance les tâches requises sur les clients, à partir du poste administrateur. Par exemple, suite à un événement produit par un virus sur un client, vous pouvez désinfecter les fichiers sur le client, à partir du poste administrateur.
- Mettre à jour régulièrement la base antivirus sur les postes clients (voir section 4.10 à la page 67).
- Mettre à jour régulièrement les modules de programme installés sur des postes clients (voir section 4.10 à la page 67).
- 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 4.14 à la page 72).

2.10. 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.

2.11. 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, en tant que un plug-in d'administration intégré dans Microsoft Console d'administration (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.

2.11.1. 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 sur l'objet sélectionné dans l'arborescence de console. Le panneau de détails permet un accès rapide aux principales opérations de console, qu'elle soient sélectionnées dans l'arborescente de console ou dans le panneau de détails de l'objet correspondant, à travers un hyperlien.

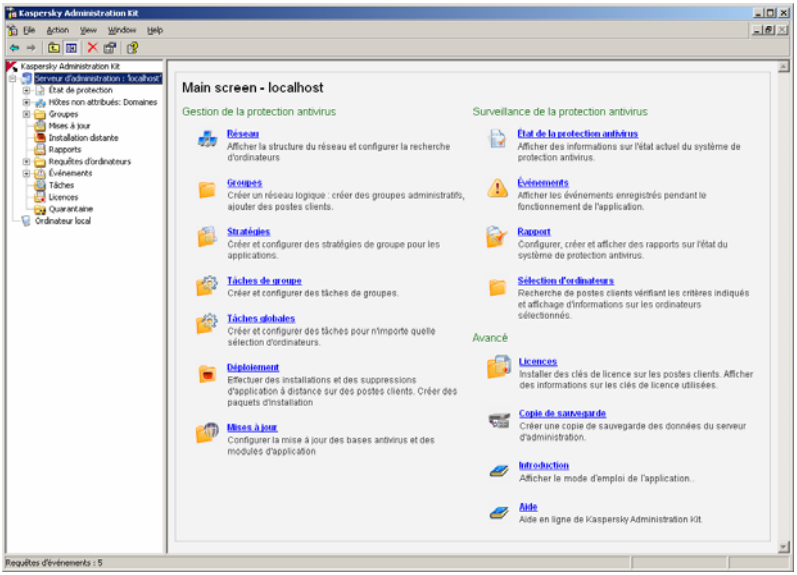

Figure 1. Fenêtre principale de Kaspersky Administration Kit

2.11.2. Arborescence de console

L'arborescence de console décrit les réseaux logiques créés dans un réseau d'entreprise et les propriétés d'un ordinateur local sur lequel la console d'administration est installée.

L'espace de noms **Kaspersky Administration Kit** peut avoir plusieurs postes : **Kaspersky Administration Server (<Nom de serveur>)** (par le nombre de postes Administration Kit Server) et un objet **Ordinateur local**.

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

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

- **État de protection**
- **Réseau**
- **Groupes**
- **Mises à jour**

- **Installation distante**
- **Requêtes d'ordinateurs**
- **Événements**
- **Tâches**
- **Licences**
- **Quarantaine**

Le dossier **État de protection** offre des informations sur l'état de protection anti-virus sur les postes clients et sur l'ensemble du réseau d'ordinateurs. Ce dossier contient des sous-dossiers imbriqués avec des informations organisées 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 administratifs**- état de la protection antivirus sur les postes clients du réseau logique.
- **Protection antivirus**- données statistiques sur l'activité des virus et sur l'état de la tâche de protection en temps réel sur les postes clients du réseau logique.
- **Mises à jour**- état de la base antivirus utilisée par les applications

Après l'installation de Kaspersky Administration Kit, l'élément **Non attribué** affiche la hiérarchie du domaine et les groupes de travail sur votre réseau Windows. Les dossiers à chaque niveau supérieur correspondent aux ordinateurs du domaine ou du groupe de travail, qui n'ont pas été affectés au réseau logique. Après avoir affecté un ordinateur à un groupe, les informations correspondantes sont supprimées de l'entrée **Non attribué**. Réciproquement, quand un ordinateur est enlevé du réseau logique, les informations sur cet ordinateur apparaissent à nouveau dans le dossier correspondant à l'entrée **Non attribué**.

La description de la hiérarchie des dossiers sous l'entrée **Réseau** et répartition des ordinateurs à l'intérieur peut être assurée par la structure Active Directory ou les sous-réseaux configurés 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.

Quand vous sélectionnez un dossier dans l'arborescence de console, le panneau de détails présente les informations suivantes sur ce dossier :

- **Nom**- Nom de poste dans le réseau logique (nom NetBios ou adresse IP de l'ordinateur (selon la méthode de présentation)
- **Type du système d'exploitation**- type du système d'exploitation installé sur un poste client (Serveur/ Station de travail).

En fonction du type de système d'exploitation, l'icône suivante est affichée à côté du nom du poste : . signale un serveur et . fait référence à un poste de travail.

- **Domaine** – Domaine ou groupe de travail Windows de l'ordinateur
- **Dernière détection** – Date où cet ordinateur a été identifié pour la dernière fois par le serveur sur le réseau logique
- **Dernière mise à jour** – Date de dernière mise à jour de la base antivirus ou des modules d'application 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 où les informations sur cet ordinateur ont été mises à jour pour la dernière fois
- **Domaine DNS** – Le domaine DNS de cet ordinateur
- **Nom DNS** – Nom DNS de l'ordinateur
- **IP**- adresse IP de l'ordinateur
- **Connexion au serveur d'administration**- Adresse IP de connexion du poste client au serveur d'administration.

Le dossier **Réseau** affiche le contenu du groupe **Réseau**. Le serveur d'administration crée et met à jour les données dans le groupe **Réseau**. Le serveur demande régulièrement des informations sur les nouveaux ordinateurs qui sont ajoutés ou retirés du réseau Windows. En fonction de cette information, le serveur rafraîchit alors le groupe **Réseau** et le dossier **Réseau**. Les nouveaux ordinateurs qui apparaissent sur le réseau sont ajoutés automatiquement à un dossier spécifié dans le groupe **Réseau** ou dans le groupe spécifié du réseau logique. Il existe une caractéristique permettant de désactiver le sondage des ordinateurs compris dans le groupe Réseau et n'importe lequel de ses sous-groupes secondaires.

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 **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.

Après l'installation de Kaspersky Administration Kit, le dossier **Groupes** ne conserve aucun élément, et les dossiers **Serveurs, Stratégies** et **Tâches** sont vides. L'administrateur peut définir la structure du réseau logique en ajoutant des postes clients et des groupes imbriqués au dossier **Groupes**.

Une liste des postes clients du dossier est affichée dans le panneau de détails sous forme de tableau. La structure et le contenu de la table sont semblables à ceux du dossier **Non attribué** (voir ci-dessus).

Les groupes sont affichés comme des dossiers de structure similaire à celle du dossier **Groupes** parent :

- Les sous-dossiers **Serveurs, Stratégies** et **Tâches** sont automatiquement créés dans le nouveau dossier du groupe. Ces dossiers, qui conservent les informations sur les serveurs, les stratégies et les tâches du groupe, sont automatiquement créés en même temps que le groupe.
- Quand des postes clients sont ajoutés à un groupe, ils sont affichés dans le panneau de détails sous la forme d'un tableau.
- Si vous créez un sous-dossier à l'intérieur du dossier courant, il aura la même structure que le dossier parent.

Le contenu du dossier choisi dans l'arborescence de console est présenté dans le panneau de détails.

En plus de l'information du dossier **Non attribué**, les données suivantes sont disponibles pour chaque client :

- **Dernière connexion** – Date et heure de dernière connexion au serveur d'administration.
- **Dernière analyse complète** – Date et heure de la dernière analyse complète antivirus de ce client.
- **Virus trouvés** – Nombre total de virus détectés entre la première analyse jusqu'à ce que le compteur de virus ait été remis à zéro pour la dernière fois. 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** – Situation actuelle de la protection en temps réel du client.
- **Connexion au serveur d'administration**- Adresse IP de connexion du poste client au serveur d'administration.

Vous pouvez manipuler des objets dans le dossier **Groupes** à l'aide de commandes de menu contextuel (voir section 2.11.3 à la page 30) ou des hyperliens du panneau des tâches.

L'entrée **Mises à jour** contient une liste de mises à jour, qui peuvent être téléchargées sur les clients.

L'entrée **Installation distante** contient la liste des paquets d'installation utilisés pour déployer des applications Kaspersky Lab sur les postes clients.

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

L'entrée **Ordinateurs** est utilisé pour les requêtes de recherche des postes clients en fonction de critères spécifiés, et pour conserver les résultats dans des dossiers séparés.

L'entrée **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.

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

L'entrée **Licences** affiche les licences installées sur des postes clients.

Le dossier **Quarantaine** est utilisé pour la gestion des objets placés dans le dossier de quarantaine des postes clients.

2.11.3. 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**	Connexion au serveur d'administration

Objet	Commande	Action
	Déconnexion	Déconnexion du serveur d'administration
	Assistant Démarrage rapide	Lancement de l'Assistant Démarrage rapide
	Assistant de déploiement d'application	Création d'une tâche de déploiement
	Rechercher un ordinateur	Ouvre une fenêtre pour l'ordinateur retrouvé dans le réseau logique du serveur d'administration
	Propriétés	Affiche la boîte de dialogue Propriétés du serveur d'administration
Réseau	**Rechercher un ordinateur**	Ouvre une fenêtre pour l'ordinateur retrouvé dans le dossier **Réseau**
	Assistant de déploiement d'application	Création 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

Objet	Commande	Action
	Nouveau/Sous réseau IP	Création d'un sous-réseau IP pour afficher des ordinateurs
Groupes	**Installer l'application**	Création 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
	Nouveau/Groupe	Ajout d'un nouveau groupe à la structure du réseau logique
	Nouveau/Ordinateur	Ajout d'un nouveau client à un groupe
Stratégies	**Nouveau/Stratégie**	Création d'une nouvelle stratégie de groupe
Tâches de groupe	**Nouveau/Tâche**	Création d'une nouvelle tâche de groupe

Objet	Commande	Action
Installation distante	**Rapport de versions 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
Rapports	**Nouveau/modèle de rapport**	Création d'un nouveau modèle de rapport
Requêtes d'ordinateurs	**Nouveau/Nouvelle requête**	Crée une nouvelle requête pour rechercher des ordinateurs
Événements	**Vue/Filtre**	Appliquer un filtre sur le tableau d'aperçu des événements
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
Ordinateur local	**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**

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	**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**
	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

Élément	Commande	Action
Modèle de rapport	**Générer**	Création et affichage d'un aperçu du modèle de rapport choisi

CHAPITRE 3. INSTALLATION DE KASPERSKY ADMINISTRATION KIT

Lors de l'installation, l'Assistant propose d'installer les composants Kaspersky Administration Kit, Administration Server et Administration Console sur l'ordinateur. Cette configuration est recommandée si vous êtes en train de créer le système de gestion à distance.

Avant l'installation, assurez-vous que votre configuration répond aux exigences matérielles et logicielles du serveur, et du poste d'administration (voir section1.3 à la page 7).

Un serveur Microsoft SQL ou MSDE (Microsoft Data Engine) sont utilisés pour stocker les informations sur le serveur d'administration. Par conséquent, si votre réseau d'entreprise ne possède ni SQL Server, ni MSDE, installez l'un d'eux avant d'installer le serveur d'administration. Pour installer MSDE, vous pouvez utiliser le paquet d'installation de Kaspersky Administration Kit.. Reportez-vous aux instructions ci-après pour installer MSDE à partir du CD d'installation de Kaspersky Administration Kit (voir section 3.1 à la page 36).

Pour installer Kaspersky Administration Kit sur un ordinateur, vous devez posséder des privilèges d'administrateur, à la fois sur l'ordinateur local et sur le domaine Windows de ce même ordinateur.

3.1. Installation de MSDE avec le paquet d'installation de Kaspersky Administration Kit

MSDE est installé en local à partir du paquet d'installation de Kaspersky Administration Kit.

Pour installer MSDE :

1. Insérez le CD de Kaspersky Administration Kit dans votre lecteur de CD-ROM et lancez le fichier **setup.exe** dans le dossier **MSDE2KSP3**. Ceci démarre un Assistant qui va vous guider au

cours des différentes étapes de l'installation. Vous allez pouvoir sélectionner la configuration et lancer l'installation. Suivez les instructions de l'Assistant.

2. Les premières étapes de l'installation couvrent la récupération et la recopie de fichiers sur votre disque dur, l'acceptation du contrat de licence, et la saisie des informations utilisateur.

3. Dans la boîte de dialogue **Sélectionnez l'emplacement cible**, indiquez ce qui suit :

   - Le dossier de destination des fichiers de MSDE (dans la zone **Fichiers de programme**). Le chemin par défaut est **Program Files\Microsoft SQL Server**. Si le dossier n'existe pas, le programme le créera.

   - Le dossier de stockage de la base du serveur MSDE (dans la zone **Fichiers de données**). Le chemin par défaut est **Program Files\Microsoft SQL Server**.

   Pour choisir une autre destination, cliquez sur **Parcourir...**

4. Dans la boîte de dialogue **Nom d'instance MSDE 2000** (voir Figure 2), choisissez un nom pour ce serveur MSDE.

   Le nom par défaut est **KAV_CS_Admi_Kit**. Cochez la case **Par défaut** si vous voulez utiliser le nom par défaut.

   Si vous voulez choisir un autre nom, annulez la coche **Par défaut** et saisissez le nouveau nom dans la zone **Nom d'instance**.

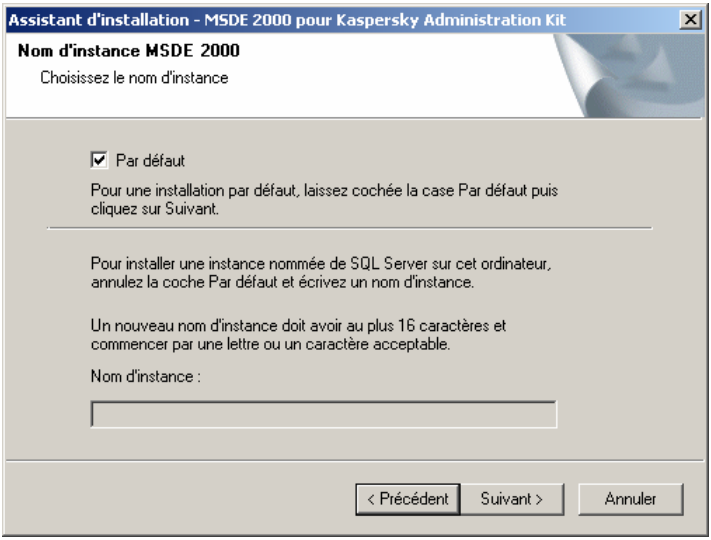

Figure 2. Installation de MSDE. Choix d'un nom d'instance.

Après avoir configuré les paramètres d'installation, vous pouvez les passer en revue et commencer l'installation. Ceci mettra fin à l'installation de MSDE, nécessaire pour le bon fonctionnement de Kaspersky Administration Kit.

L'installation de MSDE à partir du paquet d'installation de Kaspersky Administration Kit ne peut se faire qu'avec cette application.

3.2. Installation du serveur d'administration et de la console d'administration

Pour installer le serveur d'administration et/ou la console d'administration :

1. Lancez le fichier **Setup.exe** du CD de Kaspersky Antivirus pour démarrer l'Assistant d'installation. Vous allez pouvoir sélectionner la configuration et lancer l'installation. Suivez les instructions de l'Assistant.

2. Les premières étapes de l'installation couvrent la récupération et la recopie de fichiers sur votre disque dur, l'acceptation du contrat de licence, et la saisie des informations utilisateur.

3. Sélectionnez le dossier de destination. Le dossier par défaut est **Program Files\Kaspersky Lab\Kaspersky Administration Kit**. Si ce dossier n'existe pas, l'Assistant le créera automatiquement. Pour choisir un autre dossier, cliquez sur **Parcourir...**.

4. Sélectionnez les composants de Kaspersky Administration Kit que vous voulez installer (voir Figure 3): **Console d'administration Kaspersky** – Installe la console d'administration ou **Kaspersky Administration Serveur** – Installe le serveur d'administration.

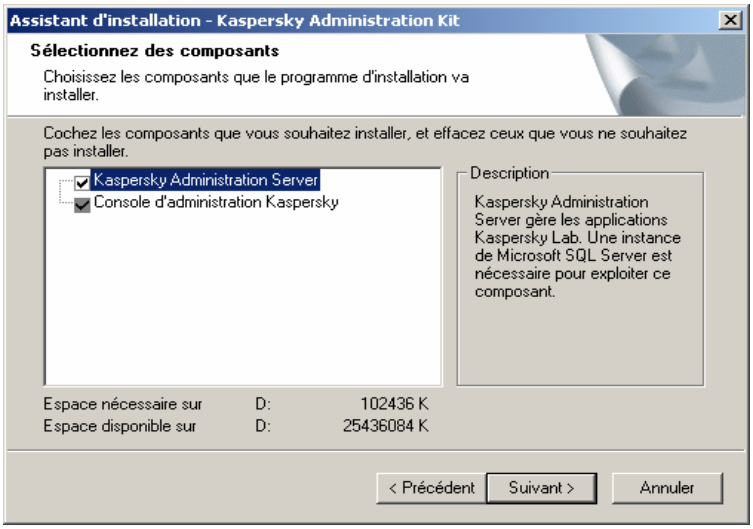

Figure 3. Choix des composants à installer.

Vous avez le choix entre l'installation des deux composants, ou seulement de la console d'administration. Vous ne pouvez pas choisir d'installer le serveur d'administration sans installer la console d'administration. Par défaut, les deux composants sont installés.

L'information de référence suivante est disponible dans la boîte de dialogue de l'Assistant :

- La zone **Description** sur le côté gauche affiche une description du composant choisi
- La zone **Espace nécessaire sur** affiche la quantité d'espace nécessaire pour les composants sélectionnés ;

- La zone **Espace disponible sur** affiche l'espace disponible sur le disque sélectionné pour installer les composants.

Si vous installez seulement la console d'administration, aucune autre étape n'est nécessaire. L'Assistant vous invite à vérifier les paramètres d'installation et à commencer l'installation.

5. Définissez le compte de service utilisé au démarrage par le serveur d'administration (voir Figure 4).

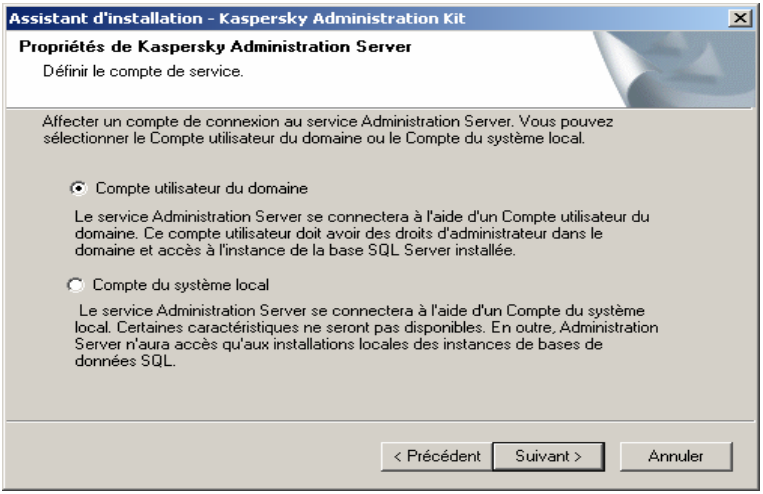

Figure 4. Installation de Kaspersky Administration Kit. Configuration du compte de service.

Vous pouvez choisir l'une des options suivantes :

- **Compte utilisateur du domaine** – Démarre le serveur d'administration sous un compte d'utilisateur de domaine. Le serveur d'administration effectuera toutes les opérations avec les droits d'accès affectés à ce compte. À l'étape suivante, vous devez indiquer le nom d'utilisateur de domaine, utilisé pour ouvrir une session dans le serveur.

Si votre réseau d'entreprise utilise une structure de domaine Windows, il est recommandé de choisir le compte d'administrateur de domaine pour ouvrir une session dans le serveur d'administration. Dans ce cas, le serveur d'administration aura accès à toutes les ressources administratives nécessaires.

- **Compte du système local** – Démarre le serveur d'administration en utilisant le compte **Système local**. Cette

variante est recommandée si votre réseau ne possède pas de structure de domaine Windows. Dans ce cas, vous sauterez l'étape de sélection d'un utilisateur pour passer directement à l'emplacement de la base de données du serveur de MSDE (voir étape 7 à la page 43).

Pour un fonctionnement correct de Kaspersky Administration Kit, le compte de service utilisé pour démarrer le serveur doit avoir des privilèges d'administrateur sur l'ordinateur hébergeant la base de données MSDE.

6. Si vous lancez le serveur d'administration sous un compte d'utilisateur de domaine, indiquez le nom d'utilisateur dans la boîte de dialogue suivante de l'Assistant.

   Dans la boîte de dialogue (voir Figure 5), spécifiez le nom d'utilisateur parmi ceux enregistrés dans le domaine. Pour ce faire, saisissez le nom souhaité dans la zone **Nom utilisateur** ou cliquez sur **Parcourir...** pour choisir un utilisateur.

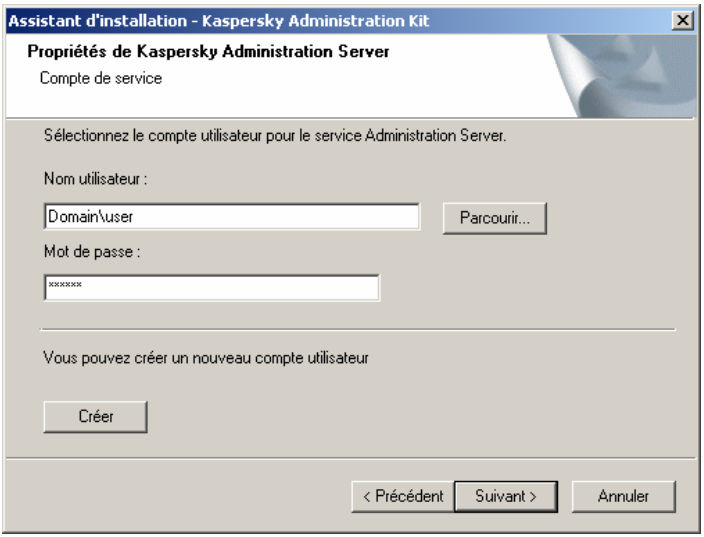

Figure 5. Installation de Kaspersky Administration Kit. Choix d'un utilisateur.

Si le compte d'utilisateur que vous avez indiqué ne possède aucun privilège d'administrateur de domaine, le serveur d'administration démarrera sous ce compte mais en limitant les fonctionnalités de Kaspersky Administration Kit. Par exemple, en raison des droits d'accès limités du compte choisi, une installation sur des ordinateurs distants à l'aide de scripts peut s'avérer impossible

(voir section 4.6.1.2 à la page 59), ou encore, certains domaines du réseau Windows ne pourront pas être parcourus. L'avertissement correspondant est affiché (Figure 6).

Pour exploiter les applications installées directement sur des clients distants, le compte d'utilisateur doit posséder le privilège **Ouverture de session en tant que service**. Pour démarrer des tâches d'installation à distance en utilisant des scénarios de démarrage, vous devez avoir le droit de modifier ces scénarios dans la base de données du contrôleur de domaine.

Dans la zone **Mot de passe**, saisissez le mot de passe d'utilisateur du compte d'utilisateur de domaine.

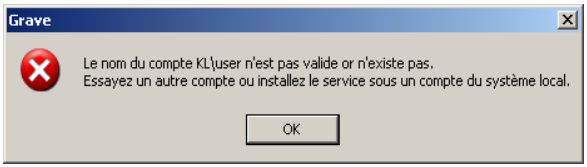

Figure 6. Installation de Kaspersky Administration Kit.
Message sur les fonctions limitées du serveur d'administration

Si le compte de domaine sélectionné possède des privilèges d'administrateur de domaine mais pas le droit d'**Ouverture de session en tant que service**, ce dernier sera automatiquement accordé au (voir Figure 7).

Figure 7. Installation de Kaspersky Administration Kit.
Message du privilège d'**Ouverture de session en tant que service** accordée à l'utilisateur

Avec des privilèges d'administrateur de domaine, vous pouvez créer un utilisateur spécial et ouvrir une session sous ce compte utilisateur dans le serveur d'administration. Les droits d'administrateur de domaine et le droit d'**Ouverture de session en tant que service** seront automatiquement accordés à ce compte d'utilisateur.

Pour créer un utilisateur spécial, cliquez sur le bouton **Nouvel utilisateur** et saisissez les informations suivantes dans la boîte de dialogue (voir Figure 8):

- Nom d'utilisateur dans la zone **Nom utilisateur** (obligatoire).

- Nom complet d'utilisateur dans la zone **Nom complet** (facultatif).
- Informations sur l'utilisateur dans la zone **Description**. La valeur par défaut est **Compte du composant Administration Server de Kaspersky**(facultatif).
- Mot de passe dans la zone **Mot de passe** (obligatoire).
- Confirmation du mot de passe dans la zone **Confirmez le mot de passe** (obligatoire).

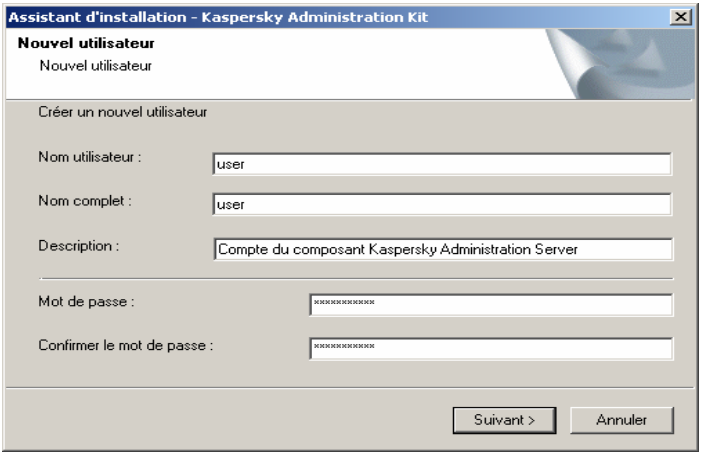

Figure 8. Installation de Kaspersky Administration Kit. Création d'un nouvel utilisateur

7. À l'étape suivante, vous devez définir la ressource (MSDE ou Microsoft SQL Server) chargée de stocker la base de données du serveur d'administration (voir Figure 9). Sans ce paramètre, vous ne pourrez pas poursuivre l'installation.

   Si un serveur MSDE ou MS SQL existe dans votre réseau d'entreprise et que vous souhaitez l'utiliser pour les besoins de Kaspersky Administration Kit, indiquez son nom dans la zone **Nom du serveur** ainsi que le nom de la base de données dans **Nom de la base de données**. **KAV** est le nom par défaut de la base de données.

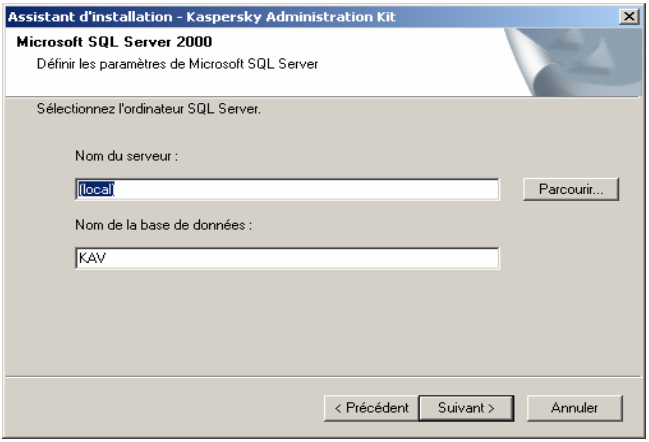

Figure 9. Installation de Kaspersky Administration Kit. Choix d'un serveur SQL

Cliquez sur **Parcourir...** pour afficher la liste de tous les serveurs Microsoft SQL du réseau. Si le serveur SQL se trouve sur l'ordinateur à partir duquel vous installez Kaspersky Administration Kit, la mention **local** est automatiquement indiquée dans la zone **Nom du serveur**.

Si votre réseau ne possède aucun serveur MS SQL ou que vous ne pouvez pas utiliser de serveur(s) existants, vous devrez alors en installer un (voir section 3.1 à la page 36).

Si voulez installer Microsoft SQL Server sur le même ordinateur où vous installez Kaspersky Administration Kit, alors annulez l'installation courante, installez le serveur SQL, puis recommencez l'installation.

Si vous voulez installer Microsoft SQL Server sur un ordinateur à distance, il n'est pas nécessaire d'annuler l'installation de Kaspersky Administration Kit. Vous pouvez installer Microsoft SQL Server et poursuivre l'installation de Kaspersky Administration Kit.

8. Au cours de cette étape vous devez déterminer la méthode d'authentification utilisée pour la connexion du serveur d'administration au serveur SQL. Vous avez le choix parmi les deux options suivantes :

   - **Mode d'authentification Microsoft Windows**- dans ce cas, votre compte est utilisé pour vérifier vos droits d'utilisation du Serveur d'administration;
   - **Mode d'authentification SQL Server**- dans ce cas, c'est le compte spécifié à la suite qui sera utilisé pour vérifier les droits.

Saisissez le mot de passe dans les champs **Compte**, **Mot de passe** et **Confirmation du mot de passe**.

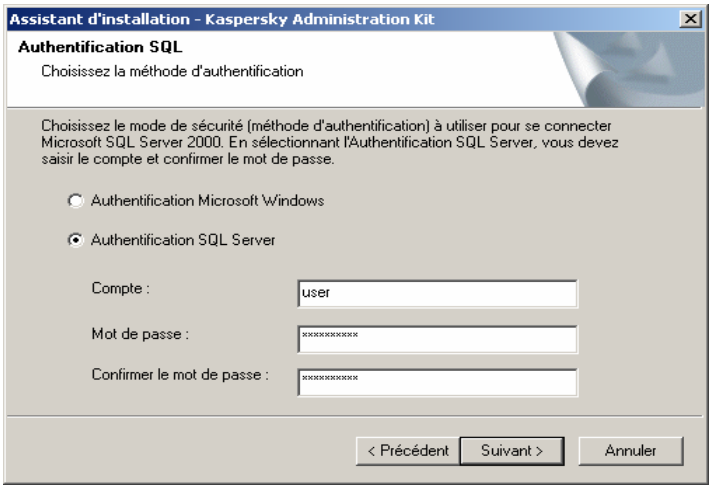

Figure 10 **Mode d'authentification SQL Server**

9. Si vous installez le serveur d'administration, définissez le chemin vers le dossier partagé (voir Figure 11) qui sera utilisé pour entreposer :

   - Les fichiers requis pour l'installation à distance d'applications Kaspersky Lab. Les fichiers sont recopiés dans le serveur d'administration lorsque vous créez les paquets d'installation.
   - Les mises à jour recopiées sur le serveur d'administration à partir de la source de mise à jour.

   Des droits de lecture sur ce dossier seront accordés à tous les utilisateurs.

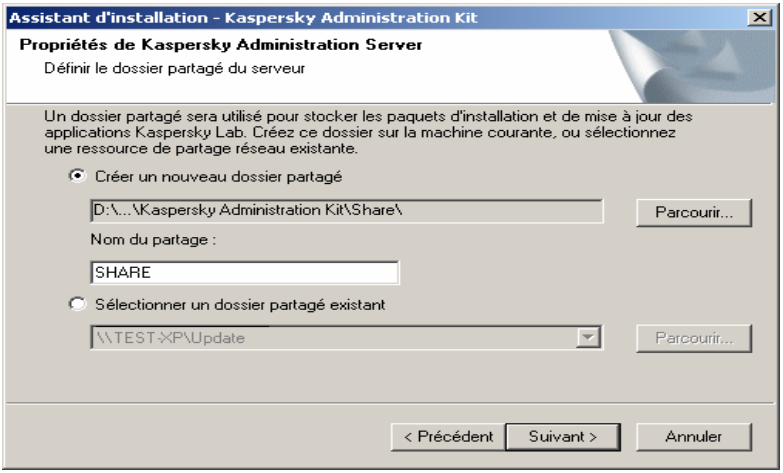

Figure 11. Installation de Kaspersky Administration Kit. Création d'un dossier partagé.

Vous pouvez choisir l'une des options suivantes :

- **Créer un nouveau dossier partagé** – Pour créer un nouveau dossier, entrez le chemin d'accès dans la zone inférieur et spécifiez le nom de dossier dans la zone **Nom du partage**.
- **Sélectionner un dossier partagé existant** – Sélectionne un dossier partagé parmi les dossiers existants.

Le dossier partagé peut se trouver sur n'importe quel ordinateur local o distant du réseau de l'entreprise.

Un dossier **SHARE** par défaut est créé dans le répertoire de Kaspersky Administration Kit.

10. Définissez les paramètres de port pour la connexion au serveur d'administration (voir Figure 12):

    - Le champ **Port du serveur** donne le numéro de port utilisé pour se connecter au serveur d'administration. Le port par défaut est **14000**. Modifiez ce numéro si ce port est déjà en service.
    - Le champ **Port SSL du serveur** donne le numéro de port utilisé pour une connexion SSL au serveur d'administration. Le port par défaut est **13000**.

Si le serveur d'administration est exploité sous Windows XP SP2, le pare-feu incorporé verrouillera les ports TCP 13000 et 14000. Vous devez donc ouvrir manuellement ces ports pour faciliter l'accès au serveur d'administration.

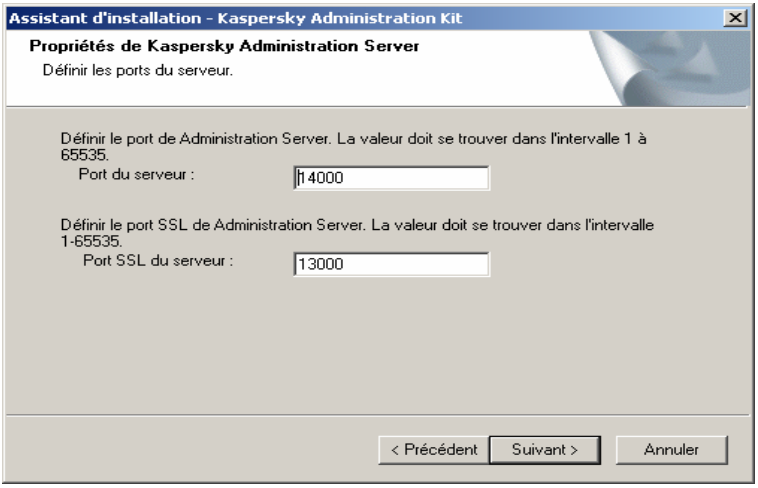

Figure 12. Installation de Kaspersky Administration Kit. Paramètres du port

Après avoir complété l'installation, le raccourci Kaspersky Administration Kit apparaît dans le menu Démarrer\Programmes\ Kaspersky Administration Kit**.**

Les paramètres d'installation par défaut du Serveur d'administration sur un ordinateur sont les suivants :

- Nom : **Serveur d'administration Kaspersky**;
- **Lancement automatique** au démarrage du système ;
- Compte : **Compte du système local** ou compte utilisateur (voir la page 46 et page 41).

Pour afficher les propriétés du service **Kaspersky Administration Server** et contrôler l'exploitation du programme, utilisez l'outil d'administration des **Services** Windows. Les comptes-rendus d'exploitation du service **Kaspersky Lab Administration Server** sont enregistrés dans le journal système Windows, sur le poste où se trouve installé le serveur d'administration.

Les groupes d'utilisateurs locaux **KLAdmins** et **KLOperators** sont créés sur le même ordinateur d'installation du serveur d'administration. Si le serveur d'administration est configuré pour fonctionner sous un compte d'utilisateur de domaine, les groupes **KLAdmins** et **KLOperators** sont ajoutés à la liste de groupes d'utilisateurs du domaine. Les groupes peuvent être modifiés à l'aide des outils standard d'administration de Windows.

3.3. Désinstallation des composants de Kaspersky Administration Kit

Pour désinstaller les composants de Kaspersky Administration Kit, utilisez les outils standard de Windows (**Démarrer→Panneau de contrôle→Ajout ou suppression de programme**). Le serveur d'administration et de la console d'administration seront supprimés.

3.4. Mise à jour vers une version plus récente de l'application

Pour passer de la version 4.x à la version 5.0 Kaspersky Administration Kit, supprimez la version précédente et installez la nouvelle en suivant les instructions données dans ce document.

Si vous faites une mise à jour de la version 5.0 vers une version plus récente, par exemple de Maintenance Pack 1 à Maintenance Pack 2, nous vous recomnandons de suivre la procédure suivante :

1. Créer une copie de sauvegarde des données du serveur d'administration à l'aide de l'outil ***klbackup.exe*** (voir section 4.14, page 72). Cet outil est fourni avec le paquet de distribution Kaspersky Administration Kit et se trouve dans le dossier racine d'installation du serveur d'administration. Notez que pour restaurer complètement les données du serveur d'administration, vous devez faire une copie de sauvegarde du certificat serveur.
2. Lancez l'installation de la version la plus récente de Kaspersky Administration Kit 5.0 sur l'ordinateur où se trouve installée la version antérieure du serveur d'administration. Mettez à jour le composant. Au cours de la mise à jour, toutes les données de la version précédente du serveur d'administration sont enregistrées et rendues disponibles dans la

nouvelle version. La compatibilité arrière est assurée avec les versions précédentes du serveur d'administration.

3. Afin de pouvoir mettre à niveau l'agent réseau installé sur les ordinateurs du réseau, créez un groupe ou une tâche d'installation globale de le nouvelle version du composant. Exécutez la tâche manuellement ou planifiée. Une fois la tâche terminée, l'agent réseau aura été mis à niveau avec la nouvelle version.

CHAPITRE 4. UTILISATION DE L'APPLICATION

Ce Guide contient une description générale de l'utilisation de Kaspersky Administration Kit. Les instructions pas à pas sont données dans le Guide de référence de Kaspersky Administration Kit. Les fonctions décrites dans le Guide de référence sont soulignées.

4.1. Lancement du programme et connexion au serveur d'administration

Pour lancer Kaspersky Administration Kit, sélectionnez **Kaspersky Lab Administration Kit** dans le groupe **Kaspersky Administration Kit** du menu **Démarrer\Programmes**. Ce groupe de programme est créé uniquement sur des postes administrateurs pendant l'installation de la console d'administration.

Vous ne pouvez utiliser Kaspersky Administration Kit que si le serveur d'administration est en cours d'exécution.

Après le démarrage, la fenêtre principale du programme affiche l'arborescence de console, avec l'espace de noms **Kaspersky Anti-Virus Control Base** 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. 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.

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 correspondants sur chacun des réseaux.

4.2. 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 administrateurs et aux opérateurs du réseau logique (voir section 2.6, page 20).

Vous pouvez accorder les droits pour opérer sur le réseau logique et certains groupes administratifs, à d'autres groupes d'utilisateurs et à des opérateurs enregistrés sur l'ordinateur où se trouve installée la Console d'administration.

Les privilèges suivants sont disponibles pour configurer les droits d'accès:

- **Lecture**:
    - connexion au serveur d'administration;
    - affichage de la structure du réseau logique (ou du groupe administratif);
    - Affichage des valeurs de configuration de stratégie, de tâches et d'application.
- **Exécution**: démarrage et arrêt des tâches de groupe et des tâches globales existantes.
- **Écriture**:
    - création d'un réseau logique, ajout de groupes et de postes clients au réseau (ou au groupe administratif);
    - installation du composant Agent Réseau sur les postes clients;
    - création et installation des paquets d'installation et des clés de licence nécessaires aux applications Kaspersky Lab sur les postes clients;
    - mise à jour des applications installées sur les postes clients ;
    - création de stratégies, de tâches pour des ordinateurs en groupe ou individuels, modification des paramètres d'application ;

- contrôle centralisé des applications, génération de rapports d'activité sur leur usage des services du serveur d'administration, de l'agent réseau et de la Console d'administration ;
- autorisation donnée aux utilisateurs et aux groupes d'utilisateurs des droits d'accès aux fonctions de Kaspersky Administration Kit.

L'administrateur peut suivre les actions de l'utilisateur d'après les événements d'activité du serveur d'administration enregistrées dans les registres d'événements. Ces événements sont affectés à des **messages de type information** et qui commencent par le mot **Audit**.

4.3. 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 :

- Un réseau logique avec une structure semblable à celle des domaines et des groupes d'utilisateurs du réseau Windows. En outre, vous pouvez importer la structure de réseau logique des versions précédentes de Kaspersky Administration Kit (versions 4.0 ou 4.5) (au choix de l'administrateur).

  

  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 de Kaspersky Antivirus 5.0 pour stations de travail Windows,

une tâche de mise à jour globale pour le serveur d'administration et la copie des données de sauvegarde.

Aucune stratégie n'est créée pour Kaspersky Antivirus 5.0 pour stations de travail Windows s'il en existait déjà une autre dans le dossier **Groupes**.

Si des tâches de groupe ont été déjà créées pour le groupe **Groupes**, et si la tâche de mise à jour globale existe déjà, avec leurs noms, ces tâches ne seront pas mises en place à ce moment.

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

La structure du réseau logique, sa hiérarchie la structure de ses groupes administratifs sont définis à l'étape de conception. La création du réseau logique dans le dossier **Groupes** du programme principal Kaspersky Administration Kit, se fait en créant une hiérarchie de groupes et en leur ajoutant des postes clients.

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 4.2 à la page 51).

Pour créer manuellement la structure du réseau logique :

1. Connectez-vous au serveur d'administration (voir section 0 à la page 50).
2. Organisez une hiérarchie de groupes en créant des groupes imbriqués
3. Ajoutez des postes clients aux 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.

Pour obtenir des informations sur un poste client spécifique ou sur un groupe d'ordinateurs, 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 assurer cette recherche et enregistrer les informations sur les ordinateurs dans un dossier séparé de l'arborescence de console, utilisez la fonction Nouvelle requête.

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 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 Agent Réseau.

- Ajouter des clients aux groupes.

  Votre serveur d'administration peut être configuré pour que les nouveaux ordinateurs détectés sur votre réseau local, soient ajoutés automatiquement à un groupe déterminé du réseau logique.

- Modifier la hiérarchie des objets du réseau logique, en déplaçant des clients et des groupes vers d'autres groupes.

  Le déplacement d'un groupe vers un autre groupe se fait avec tous les sous-groupes, les clients, les stratégies et les tâches de groupe qui en dépendent. Le groupe déplacé recevra de nouveaux paramètres en fonction de son nouvel emplacement dans la hiérarchie du réseau logique.

  Assurez-vous que le nom du groupe supprimé est unique dans ce nouvel emplacement. Vous pouvez éviter des conflits de nom en renommant le nom de groupe avant de le déplacer. Si le nom existe déjà dans un groupe, des suffixes **_1, _2, _...** seront automatiquement ajoutés à la fin du nouveau nom.

- Supprimer les groupes ou les postes clients du réseau logique.

Vous ne pouvez pas supprimer ni modifier le nom du dossier **Groupe**, car il s'agit d'un composant intégré dans la console d'administration.

Un groupe peut être supprimé du réseau logique s'il ne contient ni groupes, ni serveurs secondaire ni postes clients imbriqués. Pour supprimer le groupe

sélectionné, cliquez sur **Supprimer** dans le menu contextuel ou dans le menu **Action**.

- Déplacer les clients et les groupes avec leur contenu d'un réseau logique à l'autre.

  Si vous avez plusieurs réseaux logiques et plusieurs serveurs d'administration dans votre réseau d'entreprise, vous pouvez déplacer des clients d'un réseau logique à un autre en les réaffectant a un autre serveur d'administration.

  Créez et exécutez **Modification de Kaspersky Administration Server** pour réaffecter un client à un autre serveur d'administration. Vous pouvez réaffecter soit des clients individuels à l'aide d'une tâche globale, soit des groupes en créant une tâche de groupe. Au résultat, tous les clients indiqués seront déconnectés de l'ancien serveur d'administration, puis affectés au groupe **Non attribué** du nouveau serveur. Vous devez supprimer manuellement les clients dans les groupes de l'ancien réseau logique puis les ajouter aux groupes du nouveau réseau en utilisant l'option Console d'administration.

Vous pouvez connecter le poste client à un serveur d'administration différent localement depuis ce poste client.

Cette opération est effectuée en utilisant l'outil **klmover.exe** compris avec l'Agent Réseau. Après l'installation de l'agent réseau, cet outil se trouve placé à la racine du dossier d'installation du composant.

4.5. Hiérarchie des serveurs d'administration

De multiples serveurs d'administration peuvent former une hiérarchie « primaire--secondaire » (aussi appelée « maître -- esclave »). Le serveur d'administration primaire pourra inclure de nombreux serveurs secondaires à l'intérieur du réseau logique, et la structure de celui-ci inclura respectivement autant de réseaux logiques que de serveurs secondaires.

L'utilisation de serveurs secondaires permet au serveur maître d'effectuer les tâches suivantes :

- Créer des stratégies globales à la fois pour les serveurs d'administration secondaires et pour les postes clients qui y sont connectés.

- Créer des tâches à la fois pour les serveurs d'administration secondaires et pour les postes clients qui y sont connectés.

Les stratégies et les tâches provenant d'un serveur d'administration primaire ne peuvent pas être modifiées sur un serveur secondaire.

Les tâches récupérées sur un serveur d'administration primaire ne peuvent pas être lancées ou stoppées à partir d'un serveur secondaire.

- Déplacer des postes clients d'un serveur d'administration vers un autre.
- Créer des rapports récapitulatifs sur tous les serveurs d'administration secondaires (voir section.
- Déployer des mises à jour à partir du serveur d'administration primaire vers les serveurs secondaires.

Chaque poste client inclus dans une structure de réseau logique ne doit être connectée qu'à un seul et unique serveur d'administration.

L'administrateur doit contrôler les connexions des postes clients aux serveurs d'administration, a l'aide de l'option de recherche de postes dans les réseaux logiques des différents serveurs, à travers leurs propriétés réseau.

Pour ajouter un serveur d'administration secondaire vous devez ajouter un nouvel objet serveur à la structure du réseau logique puis configurer les paramètres pour connecter le serveur secondaire au serveur d'administration primaire.

Vous pouvez afficher la structure du réseau logique d'un serveur secondaire depuis la fenêtre principale Kaspersky Administration Kit sur un poste serveur primaire. Pour ce faire, vous devez vous connecter au serveur d'administration secondaire.

Pour afficher le réseau logique du serveur d'administration secondaire, vous devez successivement vous connecter au serveur d'administration primaire puis au serveur d'administration secondaire.

4.6. Installation et désinstallation d'applications sur des postes clients

Avant de procéder à l'installation, assurez-vous que les postes clients répondent aux spécifications matérielles et logicielles (voir section 1.3 à la page 7).

Kaspersky Administration Kit permet l'installation et la désinstallation d'applications Kaspersky Lab sur les postes clients du réseau logique par les procédés suivants :

- la méthode centralisée ou à distance à travers la console d'administration;
- l'installation locale, sur chaque poste client.

Le composant Agent Réseau assure la connectivité entre le serveur d'administration et les postes clients. Par conséquent, il faut l'installer sur chaque ordinateur connecté au système d'administration distant, avant même d'installer les applications antivirus.

Le composant Agent Réseau est installé de la même manière que les applications antivirus. Il peut être installé à distance ou localement. Pour une description détaillée du paquet d'installation de Agent Réseau, reportez-vous au Livre de Référence de Kaspersky Administration Kit.

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

- nom : **Kaspersky Network Agent**;
- lancement au démarrage du système d'exploitation ;
- avec le compte **Système local**.

Vous pouvez afficher en local les propriétés du service **Kaspersky Network Agent**, le lancer et l'arrêter, et surveiller son exécution en utilisant l'outil standard **Services/Gestion de l'ordinateur**.

Agent Réseau est un outil utilisé par toutes les applications Kaspersky Lab, son installation ne se fait qu'une seule fois sur un poste client.

Si le serveur d'administration ne peut pas se connecter au poste client, vérifiez la connexion entre les deux. Cette opération peut s'effectuer en local depuis le poste client en utilisant l'outil ***kinagchk.exe*** compris dans la 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.

Les plug-ins de console fournissent l'interface de gestion de Kaspersky Administration Kit. Pour utiliser cette interface de gestion, le plug-in correspondant doit être installé sur le poste administrateur. Lors du déploiement d'une application, le plug-in est installé automatiquement avec la création du premier paquet d'installation de l'application. En cas d'installation locale, le plug-in est installé manuellement par l'administrateur.

Le fichier d'installation de Agent Réseau (**klcfginst.exe**) se trouve dans le dossier **NetAgent** du paquet d'installation de Kaspersky Administration Kit.

4.6.1. Installation à distance (déploiement) et désinstallation du logiciel

L'installation et la désinstallation des applications antivirus sur des ordinateurs distants se réalise depuis la fenêtre principale de Kaspersky Administration Kit, sur le poste administrateur.

Vous ne pouvez installer ou désinstaller à distance que les applications Kaspersky Lab disposant d'un fichier spécial de définition de l'application, présent dans le CD d'installation des programmes. Ce fichier **.kpd** est utilisé pour créer et pour enregistrer un **paquet d'installation** sur le serveur d'administration.

Le paquet d'installation contient le fichier **setup.exe**, utilisé pour installer localement l'application en mode silencieux.

Pour installer des applications Kaspersky Lab sur des clients distants :

1. Créez un paquet d'installation pour les applications que vous souhaitez installer (voir section 4.6.1.1 à la page 59) (si ce paquet n'a pas été encore créé). Lors de la création de ce paquet d'installation, le plug-in de console correspondant à cette application est réinstallé sur le poste administrateur.
2. Créez une tâche de déploiement:

Pour installer l'application sur tous les ordinateurs du réseau logique ou de multiples groupes administratifs, ou sur des ordinateurs spécifiques appartenant à des groupes différents, créez une tâche de déploiement globale.

Pour installer une application sur tous les postes clients de n'importe quel groupe d'administration, créez une tâche de déploiement de groupe.

Vous pouvez utiliser l'Assistant de création de tâche de déploiement pour créer soit un groupe ou une tâche globale.

L'exécution de cette tâche sera planifiée aux heures indiquées. Les installations en arrière plan sont exécutées jusqu'à ce qu'elles soient complètement terminées sur tous les clients cibles ; le serveur d'administration doit être informé de l'installation réussie de ces applications sur tous les clients. L'application installée est lancée sur un ordinateur après la fin de son installation. Les paramètres d'application de chaque client sont définis conformément à la stratégie de groupe et aux paramètres par défaut.

Vous pouvez forcer la fin du processus d'installation.

Si l'installation à distance réussit sur un client, elle ne sera plus lancée sur cet ordinateur la fois suivante.

Si vous effacez par erreur le paquet d'installation de Agent Réseau, afin de le créer à nouveau, sélectionnez **klnagent.kpd** dans le dossier **NetAgent** du paquet d'installation de Kaspersky Administration Kit : c'est son fichier de définition.

4.6.1.1. Création de paquets d'installation

Tous les paquets d'installation créés pour le serveur d'administration sont placés sous l'entrée **Installation distante** de l'arborescence de console. Vous pouvez examiner les propriétés et changer le nom ou les paramètres du paquet d'installation .

Le même paquet d'installation peut être utilisé pour créer des tâches de déploiement d'application autant de fois que souhaitées.

Les paquets d'installation sont entreposés sur le serveur d'administration dans le dossier **Packages**, dans un dossier partagé spécifié.

Les paramètres par défaut du paquet d'installation de Agent Réseau garantissent le fonctionnement de base du programme. Vous pouvez

commencer à utiliser le composant avec les paramètres par défaut, aussitôt après l'installation du programme. Vous pouvez le modifier.

Quand Agent Réseau est réinstallé sur un client, les paramètres de connexion et le certificat du serveur d'administration sont automatiquement mis à jour.

Après l'installation de Agent Réseau, vous ne pourrez pas changer le nom du dossier contenant les nouveaux ordinateurs ajoutés au groupe **Non attribué**. Ce paramètre ne peut pas être modifié à l'aide de stratégies ou de paramètres d'application.

4.6.1.2. Création d'une tâche de déploiement d'application

Deux méthodes permettent d'effectuer le déploiement d'applications sur les postes clients : **l'installation par envoi** et **l'installation à l'aide d'un script de connexion**.

L'installation par envoi permet d'installer à distance des applications sur des postes clients spécifiques de votre réseau logique. Lors de l'exécution de la tâche de déploiement d'une application, le serveur d'administration en recopie ses fichiers d'installation depuis le dossier partagé vers les dossiers temporaires de chaque poste client, puis exécute le programme d'installation sur ces ordinateurs. Pour forcer l'installation d'une application, le serveur d'administration doit posséder les privilèges nécessaires pour lancer à distance les applications sur les clients du réseau logique. Cette méthode est recommandée pour l'installation d'applications sur 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 Agent Réseau est installé.

Si le serveur d'administration et un client communiquent entre eux par Internet, ou si la connexion est protégée par un pare-feu, il n'est pas possible d'utiliser de dossiers partagés pour transférer des données. Dans ce cas, l'agent réseau peut être utilisé pour l'installation des fichiers sur le client. L'agent réseau doit être installé en local sur ces ordinateurs.

L'installation avec un script de connexion vous permet de lancer le déploiement d'applications dès qu'un utilisateur spécifique ouvre une session sur le domaine (plusieurs utilisateurs). En fonction de la programmation de la tâche, la condition de lancement du programme d'installation est associée, dans le script de connexion, à certains utilisateurs spécifiques. Le programme d'installation d'application est entreposé dans le dossier partagé du serveur d'administration. Pour lancer une tâche de déploiement d'application, le serveur

d'administration doit posséder des privilèges de modification des scripts de connexion dans la base de données du contrôleur de domaine. Quand un utilisateur spécifié ouvre une session sur le domaine, l'installation démarre sur le poste client utilisé pour se connecter. Cette méthode est recommandée pour installer des applications Kaspersky Lab sur des ordinateurs sous MS Windows 95/98/Me.

Le compte utilisateur doit avoir des droits d'administrateur sur tous les postes clients sur lesquels vous prévoyez d'exécuter la tâche de déploiement d'application.

Si vous installez des applications sur des ordinateurs qui appartiennent à différents domaines, des relations d'approbation doivent être activées entre les domaines respectifs du poste client et du serveur d'administration.

Si vous installez des applications sur des postes clients qu n'appartiennent pas au domaine, vous devez exécuter une tâche de déploiement à partir du compte de l'utilisateur possédant des privilèges administrateur sur l'ordinateur en question.

Les tâches de déploiement global sont affichée dans l'arborescence sous l'entrée Tâches du premier niveau de la hiérarchie, les tâches de groupe sont affichée dans les dossiers **Tâches** des groupes administratifs correspondants.

Vous pouvez examiner et modifier les valeurs des paramètres de tâche.

Vous pouvez modifier les paramètres suivants dans le cas d'une tâche d'installation forcée.

- Modifier le compte pour démarrer cette tâche.
- Choisir de réinstaller une application existante sur un client.
- Indiquer comment les fichiers d'installation seront transmis aux clients.
- Déterminer le nombre de tentatives de démarrage de cette tâche (si la tâche est planifiée).

Si vous configurez une tâche d'installation par script de connexion, vous pouvez modifier dans l'onglet **Paramètres** la liste de comptes d'utilisateur auxquels les modifications seront applicables (voir

4.6.2. Assistant de déploiement d'application

Pour déployer des applications Kaspersky Lab à travers votre réseau logique, vous pouvez utiliser l'Assistant de déploiement d'application, capable d'installer des applications à distance par envoi, à partir de paquets d'installation préparés, ou directement, à partir d'un fichier d'installation.

Cet Assistant:

- Crée un paquet d'installation pour installer une application (si ce paquet n'a pas été créé auparavant). Le paquet est conservé dans l'entrée **Installation distante** sous le nom de l'application et son numéro de version.
- Crée et exécute la tâche d'installation à distance du groupe. La tâche est entreposée dans le groupe **Tâches** utilisé pour sa création. La tâche peut être exécutée par la suite. Le nom de tâche correspond au nom de l'application et à son numéro de version. Le nom de tâche correspond au nom du paquet d'installation.

4.6.3. Installation locale des applications

L'installation locale est effectuée séparément sur chaque ordinateur. Pour installer une application en local, vous devez posséder des privilèges d'administrateur sur l'ordinateur en local.

Vous pouvez effectuer une installation local sur le poste client via la Console d'administration en utilisant une connexion au bureau à distance.

La méthodologie d'installation en local des applications Kaspersky Lab pourrait être la suivante :

- Installez l'agent réseau et établissez la connexion entre le client et le serveur d'administration.
- Installez les applications requises sur les ordinateurs présents dans le système de protection antivirus, en suivant les instructions fournies par la documentation de ces applications.
- Installez le plug-in d'administration correspondant à chaque application installée sur le poste administrateur.

Kaspersky Administration Kit prend en charge l'installation locale des applications en mode silencieux, à partir des fichiers créés lors de la génération du paquet d'installation.

Si vous prévoyez d'utiliser le disque dur de l'ordinateur pour en déployer une image sur d'autres ordinateurs lors de l'installation de l'agent réseau, il faut créer cette image disque avant de lancer le service de l'agent réseau pour la première fois.

Une fois agent réseau a été lancé, ce composant ne peut pas être restauré correctement à partir d'une image du disque. Le serveur d'administration considèrera tous les ordinateurs comme un même ordinateur.

4.7. Gestion de stratégies

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

Lors de la création d'une 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.

Par la suite, vous pourrez modifier la stratégie, changer les valeurs des paramètres, imposer un restriction aux modifications de configuration dans les stratégies des groupes imbriqués et dans les paramètres d'application. Les paramètres gouvernés par la stratégie dont la modification est contrôlée (interdite) seront signalés par . Pour imposer une restriction, cliquez dessus. L'icône changera a .

Les paramètres locaux ont une priorité supérieure par rapports aux paramètres de stratégie. Pour activer la stratégie sur les ordinateurs locaux, vous devez verrouiller certains des paramètres concernés.

Après la création de la stratégie, celle-ci sera ajoutée au dossier **Stratégies** du groupe et de tous les groupes imbriqués correspondants, et affichée 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. Dans les paramètres de stratégie la case Stratégie active doit être cochée. La stratégie peut être activée automatiquement, déclenchée par un certain événement. Vous ne pouvez revenir à la stratégie précédente que manuellement.

Vous pouvez supprimer, copier, déplacer, exporter et importer des stratégies d'un groupe dans un autre.

La stratégie est déployée sur les postes clients, lors de la première synchronisation des postes clients avec le serveur après la création de la

stratégie. 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.

La stratégie est mise en place de la façon suivante. Si des tâches résidentes (protection en temps réel) fonctionnent sur un client, ces nouveaux paramètres de stratégie seront appliqués à ces tâches sans intervention supplémentaire. 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 anciens paramètres. Les nouveaux paramètres de stratégie seront appliqués 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.

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's dans les Guides des application. La configuration de stratégie du composant Agent Réseau est décrite dans le Livre de Référence de Kaspersky Administration Kit.

4.8. Administration de tâches

Les applications Kaspersky Lab installées sur les clients du réseau logique peuvent être contrôlées en créant et en démarrant des tâches. Vous pouvez attribuer et mettre en œuvre à distance les mêmes tâches que vous utilisez en local. Pour plus de détails sur les tâches de chaque application Kaspersky Lab, reportez-vous à la documentation correspondante.

Kaspersky Administration Kit dispose des tâches suivantes

- **Tâche de déploiement de produit**
- **Démarrage et arrêt de l'application**

- **Tâche de téléchargement des mises à jour par le serveur d'administration**
- **Tâche de modification de Kaspersky Administration Server**

Les types de tâches précédents sont différents selon que cela implique des tâches de création ou d'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 catégorie de tâche. La tâche de déploiement d'application peut être affectée à un groupe (tâche de groupe) ou à tous les ordinateurs (tâche globale). Le téléchargement des mises à jour par le serveur d'administration est le seul type pour lequel des tâches globales sont créées.

Les tâches affectées à un groupe sont conservées dans le dossier **Tâches** des groupes correspondants. Les tâches globales sont placées sous l'entrée **Tâches**, qui fonctionne comme un entrepôt spécialisé dans l'arborescence de console. Vous pouvez examiner la liste de tâches locales attribuées à un client dans sa boîte de dialogue de propriétés

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

Les paramètres des tâches exécutées sur des clients dépendent de la stratégie de groupe, des paramètres de tâche, et des paramètres de l'application sur le client (voir section 2.2 à la page 14).

Les tâches sont programmées pour démarrer à une certaine heure. Pour les ordinateurs qui sont désactivés à l'heure planifiée, le système d'exploitation peut être lancé automatiquement par la fonction Wake On Lan.

Le temps d'exécution de la tâche peut être contrôlé, et dans ce cas, interrompu après un délai d'attente spécifié dans les paramètres. Il existe la possibilité de désactiver l'exécution d'une tâche programmée. Dans ce cas, les tâches, sans être supprimées, ne sont pas démarrées.

Vous pouvez exécuter une tâche, interrompre son exécution, faire une pause ou la continuer manuellement, en utilisant les commandes du menu contextuel ou encore, depuis la fenêtre de configuration de la tâche.

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

Vous pouvez surveiller l'exécution d'une tâche ou afficher les résultats de l'exécution de la tâche dans la boîte de dialogue des paramètres de tâche.

L'historique des tâches est géré et enregistré conformément aux paramètres courants dans les registres d'événements de Windows ou de Kaspersky Administration Kit, de manière centralisée sur le serveur d'administration ou en local, sur chaque poste client. Il peut être enregistré de manière centralisée (sur le serveur d'administration) ou en local, sur chaque poste client. L'administrateur et les autres utilisateurs peuvent recevoir des notifications au sujet des comptes-rendus d'activité de tâche, en fonction des paramètres courants de tâche.

Pour afficher des comptes-rendus d'activité de tâche pour chaque client, ouvrez la boîte de dialogue **Propriétés de <Nom de poste>** à partir du bouton **Historique** de l'onglet **Tâches** (voir ci-dessous). Ceci affichera l'information entreposée sur le serveur d'administration.

Si l'historique des tâches est entreposé en local sur un poste de travail, utilisez la console d'administration installée sur cet ordinateur.

Quand vous opérez dans une structure hiérarchique, les serveurs d'administration secondaires récupèrent les tâches de groupe dans le serveur primaire puis les déploient sur les postes clients. La configuration du groupe de tâches n'est modifiable que sur le serveur d'administration primaire. Ensuite, les serveurs secondaires modifient et déploient conformément les tâches de groupe sur les postes clients.

Les résultats du déploiement de tâches sur les serveurs d'administration secondaires sont affichés sur la fenêtre **Historique** dans la fenêtre de propriétés de la tâche de groupe du serveur d'administration secondaire.

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.

4.9. Contrôle des paramètres d'application

Kaspersky Administration Kit permet de contrôler les applications installées sur des clients distants du réseau logique par le biais de la configuration des paramètres d'application. 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 paramètres autorisés par la stratégie de groupe de cette application.

L'ensemble des paramètres qui configurent le l'agent réseau est le même que celui spécifié pour la stratégie de cette application. Vous trouverez une description détaillée de la configuration de Agent Réseau dans le Livre de Référence de Kaspersky Administration Kit.

4.10. Mise à 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 entreposées sur le serveur d'administration dans un dossier public d'où elles seront redistribuées vers les clients en fonction de la tâche de mise à jour des applications. Les tâches de réception des mises à jour par les serveur d'administration secondaires peuvent être démarrées automatiquement immédiatement après que le serveur principal reçoive les mises à jour, indépendamment de la planification de la tâche.

Pour améliorer la sécurité antivirus, vous devez créer des tâches de mise à jour pour toutes les applications antivirus présentes dans le système de protection de votre réseau logique et dans tous les serveurs d'administration secondaires.

Pour plus d'informations sur la création des tâches de mise à jour, reportez-vous au guide de l'utilisateur de chaque application en particulier.

Vous pouvez afficher des informations sur les mises à jour téléchargées dans l'entrée **Mises à jour** de l'arborescence de console ; la liste de mises à jour est affichée dans le panneau de détails.

Grâce au système de contrôle à distance, vous pouvez déployer automatiquement des mises à jour récupérées par le serveur d'administration à travers tous les réseaux logiques. Nous vous recommandons de procéder au déploiement automatiquement des mises à jour, car cette solution permet de limiter le trafic Internet et de réduire le nombre de requêtes transmises par les clients au serveur. Le mode de déploiement automatique des mises à jour permet d'éviter des erreurs lors de la configuration des tâches d'un grand nombre de clients.

4.11. Travail avec la quarantaine

Les applications antivirus permettent de stocker des objets suspects dans des zones spéciales. Des zones de stockage individuelles sont fournies localement pour chaque ordinateur.

Les applications Kaspersky Administration Kit conservent de manière centralisée d'une liste d'objets en quarantaine par les applications Kaspersky Lab. Cette information est conservée dans la base de données du serveur d'administration. Vous pouvez (via la console d'administration) afficher les propriétés des objets conservés en quarantaine sur les ordinateurs locaux, démarrer l'analyse des zones de quarantaine et y supprimer des objets.

Vous pouvez examiner des objets placés dans les quarantaines des postes clients du réseau logique et gérer ces objets depuis le dossier **Quarantaine**.

Kaspersky Administration Kit ne possède pas de quarantaine centralisée. Tous les objets seront placés dans les espaces de quarantaine des postes clients.

Les objets seront restaurés dans l'ordinateur où la *console d'administration* est installée, dans le dossier spécifié par l'administrateur.

4.12. Registres d'événements, rapports et notifications

Kaspersky Administration Kit est un outil puissant permettant de surveiller constamment votre système de protection antivirus.

L'application est capable de gérer un historiques des événements sur l'activité du Serveur d'administration ainsi que de toutes les applications contrôlées au moyen de Kaspersky Administration Kit.

Le registre 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 sur 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 d'administration. Ces paramètres sont déterminés dans les stratégies de groupe de l'application. Leur configuration se fait depuis la fenêtre de configuration de la stratégie de groupe.

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

Les notifications peuvent se produire par l'envoi de messages de courrier électronique ou directement sur 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 entreposées sur le serveur d'administration (de manière centralisée) ou sur le poste client local. Des informations peuvent être enregistrées à la fois dans le journal d'événements **de Windows** et dans celui de Kaspersky Administration Kit.

Dans le premier cas, l'accès aux informations est assuré par l'outil standard **Observateur d'événements** de Windows. Les informations du Information journal d'événements de Kaspersky Administration Kit entreposé sur le Serveur d'administration peuvent être examinée dans le dossier **Événements** de l'arborescence de console.

Pour simplifier l'affichage et la recherche de données présentes dans le journal des événements, il est possible de créer des requêtes. Les requêtes permettent de rechercher et de structurer les informations sur les événements enregistrés et une fois la requête appliquée, seules les données qui satisfont les critères spécifiés sont disponibles. Ceci devient vite indispensable dès que les informations conservées dans le serveur d'administration atteignent un grand volume. La possibilité est prévue d'enregistrer les événements sous forme de fichier au format .txt ou .csv.

Les événements enregistrés peuvent être supprimés automatiquement après la période de stockage déterminée par la stratégie ou manuellement en utilisant l'option **Effacer** du menu contextuel. Vous pouvez sélectionner puis supprimer un événement isolé dans le panneau de résultats, tous les événements, ou seulement ceux satisfaisant certains critères.

Vous pouvez afficher la liste des événements enregistrés pendant l'activité de l'application pour chaque poste client, dans sa fenêtre de propriétés. Les informations reçues seront celles conservées dans le journal d'événements de Kaspersky Administration Kit du serveur d'administration.

Il est possible d'examiner le contenu local du journal d'événements de Kaspersky Administration Kit, utilisez la console d'administration installée sur le même poste.

Vous pouvez recevoir des rapports sur l'état courant de la protection antivirus, construits à partir des informations entreposées dans le serveur d'administration. Des rapports peuvent être créés pour

- l'ensemble du système de protection antivirus,

- des ordinateurs d'un même groupe, ou
- des ordinateurs de groupes administratifs différents.
- le système de protection antivirus des réseaux logiques des serveurs d'administration secondaires.

Vous pouvez afficher les types de rapports suivants :

- **Rapport d'activité antivirus** – Informations sur les résultats de l'analyse antivirus de tous les clients du réseau logique.
- **Rapport de protection antivirus** – Informations sur les clients mal protégés.
- **Rapport de version du logiciel** – Informations sur les versions des applications Kaspersky Lab installées sur les clients.
- **Rapport de version des bases antivirus** – Informations sur les versions de la base antivirus utilisée par les applications KL.
- **Rapport d'erreurs** – Enregistrement de données sur les erreurs générées par des applications fonctionnant sur des postes clients.
- **Rapport sur les postes les plus infectés** – Journal des postes clients qui ont renvoyé le plus grand nombre d'objets suspects ou infectés.
- **Rapport sur les licences** – Informations sur l'état courant des clés de licence utilisées par les applications KL, et si ces licences sont conformes aux termes des accords de licence (disponible uniquement pour le réseau logique complet).

Vous pouvez générer des rapports à partir de modèles prédéfinis. Les modèles de rapport sont conservés dans l'entrée **Rapports** de l'arborescence de console.

Il existe sept modèles standard qui correspondent à autant de types de rapports sur le système de protection antivirus :

- **Rapport sur les versions de la base antivirus**
- **Rapport d'erreurs**
- **Rapport sur les licences**
- **Rapport sur les postes les plus infectés**
- **Rapport sur le niveau de protection antivirus**
- **Rapport sur les versions des logiciels Kaspersky Lab installés**
- **Rapport d'activité antivirus**

Vous pouvez créer de nouveaux modèles, supprimer les modèles existants, et afficher et modifier les paramètres d'un modèle.

Le navigateur par défaut du système sera utilisé pour afficher les rapports.

Si vous utilisez la structure hiérarchique des serveurs d'administration, vous pouvez créer des rapports contenant des données sur les serveurs d'administration secondaires.

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

4.13. Gestion des clés de licence

L'accord de licence signé après votre achat d'une application Kaspersky Lab vous permet d'utiliser les applications de Kaspersky Anti-Virus pendant la période de licence.

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 téléphonique et par courrier électronique sur l'installation, la configuration et l'utilisation de l'application antivirus ;
- Envoyer les objets suspects ou infectés chez Kaspersky Lab pour une expertise.

Le programme vous avez installé 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 entreposées 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.

Vous pouvez configurer les paramètres de notification principaux de la clé de licence dans la boîte de dialogue des propriétés du serveur d'administration sur l'onglet **Traitement des événements**. 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 compteur d'ordinateurs** – Nombre maximum d'ordinateurs qui peuvent utiliser cette clef de licence
- **Période de licence** – Période d'expiration de la clé 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.

4.14. 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, et de restaurer les données à l'occasion d'une mise à jour vers une nouvelle version de Kaspersky Administration Kit.

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

- la base de données du serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le serveur d'Administration);
- données de configuration de la structure du réseau logique et des postes clients ;
- entrepôt des paquets de déploiement des applications (le contenu du dossier **Packages**);
- 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 la restauration postérieure peuvent être effectuées automatiquement par la tâche de sauvegarde ou manuellement, à l'aide de l'outil **klbackup** fourni avec le paquet de 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 est créée automatiquement par **Assistant Démarrage rapide** et se trouve sous le nom **Sauvegarde des données du serveur d'administration** 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.

ANNEXE A. FORUM AUX QUESTIONS

Ce chapitre est consacré aux questions les plus fréquemment posées par les utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Anti-Virus. Nous avons tenté d'y répondre de la manière la plus exhaustive possible.

Question : Est-il possible d'utiliser Kaspersky Antivirus en même temps qu'un logiciel antivirus d'un autre fabricant ?

Pour éviter les conflits, nous vous recommandons de désinstaller tout logiciel antivirus d'autres fabricants avant d'installer Kaspersky Antivirus.

Question : Pourquoi Kaspersky Anti-Virus entraîne-t-il une baisse des performances de mon ordinateur et surcharge le processeur ?

La détection des virus est avant tout une tâche mathématique liée à l'analyse de structures, de sommes de contrôle et de conversions de données mathématiques. Pour cette raison, la principale ressource utilisée par tout logiciel antivirus est le processeur et chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse. C'est le prix à payer pour garantir la fiabilité et la sécurité des données.

D'autres logiciels réduisent la durée de l'analyse en éliminant des bases antivirus les virus les plus complexes à identifier ou les plus rares (sur le lieu géographique du fournisseur), ainsi que les formats de fichiers les plus difficiles à analyser (comme les fichiers PDF).

En revanche, Kaspersky Lab considère que le rôle de tout antivirus est de garantir à ses utilisateurs une protection réelle et complète contre les virus. Il ne peut être question de protection partielle. Qui plus est, la " protection partielle " est pire que l'absence de protection (dans ce cas au moins, l'utilisateur adopte lui-même des mesures de prévention).

Kaspersky Anti-Virus confère à l'utilisateur un sentiment de protection totale. Bien entendu, Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer la vitesse de l'analyse au détriment du niveau global de sécurité grâce à l'exclusion de toute une série de différents fichiers.

Toutefois, nous ne vous conseillons pas d'agir ainsi si vous souhaitez vous sentir vraiment en sécurité. Signe de la protection maximale qu'il assure aux utilisateurs, Kaspersky Anti-Virus reconnaît plus de 700 formats de fichiers archivés ou compressés. Ceci est très important pour

la sécurité antivirus car du code exécutable malicieux peut se trouver dissimulé à l'intérieur de fichiers au format inconnu. Néanmoins, il convient de remarquer que chaque nouvelle version du logiciel est plus rapide que la précédente, malgré l'augmentation quotidienne du nombre de virus identifiés par Kaspersky Anti-Virus (plus de 30 nouveaux virus chaque jour) et l'augmentation constante des formats pris en charge. Tout ceci est rendu possible grâce aux nouvelles technologies développées par Kaspersky Lab comme i-Checker™ et i-Stream™. Ces technologies permettent de rechercher d'éventuels virus dans les fichiers une seule fois, lors de la première analyse. Si ce fichier n'a pas été modifié depuis la dernière analyse, il ne sera pas repris dans l'analyse suivante. Autrement dit, les performances s'améliorent considérablement la première analyse du fichier.

Question : Pour quoi faire, un fichier de clé ? Ma copie du logiciel antivirus peut-elle fonctionner sans ce fichier ?

Non, Kaspersky Anti-Virus ne peut pas fonctionner sans une clé de licence.

Si vous n'avez pas encore décidé d'acheter ou non Kaspersky Anti-Virus, nous pouvons vous fournir une clé d'évaluation (trial-key) qui fonctionnera deux semaines ou un mois. À l'expiration de ce délai, la clé restera bloquée.

Question : Mon application antivirus ne fonctionne pas.

Que dois-je faire ?

Avant tout, vérifiez si la solution de votre problème n'est pas décrite dans les pages de ce manuel et plus particulièrement dans cette rubrique ou dans notre site Web.

En outre, nous vous conseillons de souscrire le contrat de maintenance auprès du distributeur auquel vous avez acheté Kaspersky Anti-Virus, ou de vous adresser à notre service d'assistance technique (support@kaspersky.com) ou à l'adresse figurant dans les informations de la clé de licence.

Pour être sûr de recevoir une réponse rapidement, procédez de préférence comme ceci :

1. Indiquez dans le sujet du message la version du système d'exploitation installé sur votre ordinateur, le nom du logiciel de Kaspersky Lab que vous utilisez et le problème. Par exemple :
   MS Windows 2000, Kaspersky Antivirus 5.0 pour stations de travail sous Windows, la mise à jour des bases antivirus ne fonctionne pas.
2. Composez votre message au format texte.

3. Mentionnez au début de votre message la version exacte du système d'exploitation, la distribution de Kaspersky Anti-Virus et le numéro de votre licence.
4. Décrivez clairement et brièvement le problème. N'oubliez pas qu'au moment même où ils lisent vos explications, les membres du service technique ne savent encore rien de votre problème. Ils ne pourront vous aider qu'après l'avoir compris complètement et simulé.
5. Envoyez les données suivantes au service technique (créez un fichier compressé avant de les envoyer) :

   Fichier journal antivirus ;

   la clé de licence ;
6. Ne manquez pas d'indiquer également la présence de :

   un contrôleur SCSI ;

   un processeur très ancien ou récent, de plusieurs processeurs ;

   une mémoire inférieure à 64 Mo ou supérieure à 2 Go.
7. Spécifiez le niveau de trafic journalier et les moments de pointe de surcharge.

Question : J'utilise un serveur proxy et la mise à jour ne fonctionne pas. Que dois-je faire ?

L'impossibilité d'accéder aux mises à jour via un serveur proxy peut être causée par plusieurs facteurs :

- Mauvaise configuration du réseau :

  Il existe deux modes de configuration de connexion au réseau pour l'obtention des mises à jour: l'utilisation des paramètres de MS Internet Explorer ou l'utilisation de paramètres individuels. Le service de mise à jour n'utilise pas toujours correctement les paramètres de MS Internet Explorer. C'est le cas lorsque :

  Internet n'est pas configuré sur l'ordinateur;

  Les paramètres de MS Internet Explorer ne sont pas accessibles ou n'ont pas été saisis;

  Le serveur proxy requiert une autorisation.

  Dans tous ces cas, il convient de définir les paramètres du réseau directement dans les paramètres du service de mise à jour.

- Utilisation d'un type de serveur proxy qui n'est pas compatible avec le service de mise à jour de Kaspersky Anti-Virus.

  Le service de mise à jour ne fonctionne pas via Kerio WinRoute car WinRoute n'est pas entièrement compatible avec le protocole http 1.0. Il est recommandé dans ce cas d'utilise n'importe quel autre serveur proxy.

De même, le service de mise à jour ne fonctionne pas via le protocole ftp avec Microsoft ISA Server. Dans ce cas, il est recommandé de procéder à la mise à jour au départ des serveurs de mise à jour de Kaspersky Lab via le protocole http.

ANNEXE B. 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 (Agent Réseau) – 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 comprises dans Kaspersky Lab Business Optimal et Corporate Suite.

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.

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* utilisé comme "clef" 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 Agent Réseau 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 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. Dans le cas d'une installation par envoi, le serveur d'administration doit disposer des privilèges nécessaires pour exécuter les 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 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, entreposées pendant un certain temps, ainsi que les dernières modifications dans l'architecture de l'application.

N

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.

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.

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 du dossier Packages);
- Certificat du serveur d'administration

S

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

Sauvegarder – Créer une copie de sauvegarde d'un fichier dans un dossier de sauvegarde avant traitement (désinfection ou suppression). Par la suite, ce fichier peut être restauré à partir de sa sauvegarde, par exemple, pour son analyse postérieure à partir d'une base antivirus mise à jour.

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 – voir **Stratégie de groupe**

Stratégie de groupe – Ensemble des paramètres d'application d'un groupe administratif contrôlé par le 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.

T

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 a assure une vitesse maximum mais un degré moindre de sécurité.

ANNEXE C. 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 Bénélux, 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 3 heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

C.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Windows 98/ME, 2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (riskware). Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Le système unique d'analyse heuristique des données neutralise efficacement les virus inconnus. Le logiciel peut fonctionner dans l'un des modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :

- La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
- **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

Kaspersky Anti-Virus®Personal ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une **nette augmentation de la rapidité d'exécution de l'application**.

Le logiciel représente donc un obstacle de taille pour les virus qui tenteraient d'infecter l'ordinateur via le courrier électronique. Kaspersky Anti-Virus® Personal analyse et répare automatiquement tous les messages entrants et sortants via les protocoles POP3 et SMTP. Il décèle également avec efficacité les virus dans les bases de données de messagerie.

Le logiciel est compatible avec plus de 700 formats de fichiers archivés ou compressés et assure l'analyse antivirale automatique de leur contenu. Il peut également supprimer tout code malveillant des fichiers archivés au format **ZIP, CAB, RAR, ARJ**.

La simplicité de la configuration du logiciel est assurée grâce à l'existance de trois niveaux prédéfinis : **Sécurité maximale**, **Recommandé** et **Vitesse maximale**.

Les bases de données antivirus sont actualisées toutes les trois heures. Leur distribution est garantie même en cas de coupure ou de modification de la connexion.

Kaspersky Anti-Virus® Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Windows 98/ME, Windows 2000/NT, et Windows XP, ainsi que des applications MS Office. Kaspersky Anti-Virus® Personal Pro dispose d'un outil intégré de mise à jour pour le téléchargement des bases de données antivirus et des modules de programmes. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Ce système d'analyse heuristique de seconde génération parvient à neutraliser les virus inconnus. L'utilisateur peut facilement configurer l'application à travers une interface simple et facile.

Kaspersky Anti-Virus® Personal Pro possède les caractéristiques suivantes :

- **Analyse à la demande** des unités locales ;
- **Protection automatique en temps réel** de tous les fichiers, contre les virus;
- **Filtre de courrier** qui analyse et désinfecte automatiquement tout le trafic de messagerie entrant et sortant de n'importe quel client de messagerie utilisant les protocoles POP3 et SMTP et détecte efficacement les virus dans les bases de données de messagerie ;
- **Bloqueur de comportements** qui assure une protection maximale des applications MS Office contre les virus ;
- **Analyseur de fichier compressés –** Kaspersky Anti-Virus prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirale automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les fichiers au format **ZIP**, **CAB**, **RAR** ou **ARJ**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte

n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite est une suite logicielle conçue pour organiser la protection intégrée des ordinateurs personnels tournant sous Windows. Cette solution bloque l'intrusion des programmes malveillants et des riskwares via toutes les sources d'infection possible, vous protège contre l'accès non-autorisés à vos données et lutte contre le courrier indésirable

Kaspersky® Personal Security Suite possède les fonctions suivantes :

- Protection des données de votre ordinateur contre les virus.
- Protection des utilisateurs des clients de messagerie Microsoft Outlook et Microsoft Outlook Express contre le courrier indésirable.
- Protection de l'ordinateur contre l'accès non-autorisé aux données ainsi que contre les attaques de pirates informatiques réalisées depuis le réseau local ou Internet.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[3] intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- *Postes de travail* sous Windows 98/ME, Windows NT/2000/XP Workstation et Linux ;

[3] En fonction du type de livraison

- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition ;
- *Ordinateurs de poche* sous Windows CE et Palm OS et téléphones intelligents tournant sous Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

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 SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la

technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie.

C.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://www.kaspersky.com/supportinter.html E-mail : france@support.kaspersky.com

Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : sales@kaspersky.fr

ANNEXE D. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE (« LICENCE ») SUIVANT, À PROPOS DE CE LOGICIEL (« LOGICIEL ») FABRIQUÉ PAR KASPERSKY LAB. (« KASPERSKY LAB »).

L'ACQUISITION DE CE LOGICIEL VIA INTERNET A LA SUITE D'UN CLIC SUR LE BOUTON ACCEPTER SIGNIFIE QUE VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) 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 SOUS FORME PHYSIQUE, EN OUVRANT LE SCELLÉ DU BOÎTIER, VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. SI LE SCELLÉ EST DÉCHIRÉ OU LE BOÎTIER A ÉTÉ OUVERT, VOUS N'AUREZ PAS DROIT AU REMBOURSEMENT DU LOGICIEL. LES LOGICIELS POUR USAGE DOMESTIQUE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) ACHETÉS SOUS FORME DE TÉLÉCHARGEMENT PAR INTERNET PEUT ETRE RETOURNE, ET REMBOURSÉ INTEGRALEMENT DANS LES 14 JOURS APRÈS SON ACHAT, À KASPERSKY LAB, SES REVENDEURS ET DISTRIBUTEURS AGREES. AUTRES PRODUITS NON REMBOURSABLES. LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

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

1. Licence de droits. Sous réserve d'acceptation des termes de la présente Licence d'utilisation et du paiement du prix d'achat du logiciel, Kaspersky Lab vous autorise à utiliser une copie unique et non transférable de la version spécifiée de ce logiciel et de la documentation (la « Documentation ») selon les termes de ce Contrat uniquement pour un usage interne à l'entreprise. Vous pouvez installer une copie du logiciel sur votre système. Si la licence concerne une suite d'applications (plus d'un seul logiciel), cette licence s'applique à tous les logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée dans la liste de prix ou pour chaque paquet d'applications.

1.1 Utilisation. Ce logiciel ne peut être installé que sur un seul système (un seul ordinateur) par le client, et la licence d'utilisation n'est octroyée qu'à un utilisateur unique, sauf stipulation contraire dans cette Section.

1.1.1 Le Logiciel est dit « utilisé » sur un système client lorsqu'il est chargé dans la mémoire tampon (mémoire vive ou RAM) ou installé dans une mémoire permanente (par ex. disque dur, CD-ROM ou autre périphérique de stockage) de ce système client. La présente licence vous autorise à réaliser une copie unique du logiciel dans son intégralité à des fins de sauvegarde, à condition que les copies contiennent toutes les notices de propriété du Logiciel. Il vous incombe en outre de garder une trace de toute copie du logiciel et de sa documentation réalisée à des fins de sauvegarde et de prendre les précautions nécessaires pour qu'aucune autre copie et qu'aucune utilisation illégale ne soit effectuée.

1.1.2 Si vous cédez le Système Client 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 de l'ingénierie inverse, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, ni 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 pas d'ingénierie amont ou de décompilation hors les limites autorisées par la loi.

1.1.4 Il vous est interdit ainsi qu'à vos tiers de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, de produire des applications dérivées.

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

1.1.6 Vous ne pourrez pas utiliser ce Logiciel avec des outils automatiques, semi-automatiques ou manuels conçus pour créer des signatures de virus, des routines de détection de virus ou tout autre code de détection de code ou de données dangereuses.

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur (« Serveur ») dans un environnement multi-utilisateurs ou en réseau (« Mode-Serveur ») uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est nécessaire pour chaque Système Client ou « poste », sans tenir compte du fait que ces systèmes autorisés ou ces postes sont connectés simultanément ou réellement en train d'utiliser le logiciel. L'utilisation de logiciels ou de matériels permettant de réduire le nombre de dispositifs client ou de

postes utilisant le Logiciel (par exemple, par "multiplexage" ou "sondage" du logiciel ou du matériel) ne réduit pas le nombre de licences nécessaires : le nombre de licences requises égale le nombre d'entrées séparées gérées en interface par le programme ou matériel multiplexeur ou de sondage. Si le nombre de Systèmes Clients ou postes pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures raisonnables pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. La présente licence vous autorise à télécharger ou à effectuer autant de copies de la documentation que le réseau compte de Clients possédant une licence d'utilisation du logiciel, à condition que la documentation contienne toutes les mentions de propriété légale.

1.3 Licences par volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en œuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Ce permis vous autorise à tirer ou télécharger une copie de la documentation pour chaque copie additionnelle autorisée par le permis de volume, à condition que chaque une telle copie contienne toutes les notices de propriété industrielle du document.

2. Durée. Ce Contrat de Licence est valable pour la durée prévue par le fichier de clé (le fichier unique nécessaire pour activer complètement le Logiciel : reportez-vous au menu Aide/ À propos du logiciel ; pour la version Unix/Linux, consultez la note sur la date d'expiration du fichier de clé) à moins qu'il n'arrive à terme avant ce délai pour l'une des raisons prévues ci-après. Ce Contrat se terminera automatiquement si vous n'en respectez pas les termes, les limites ou les conditions décrites. Dans ce cas, il vous incombe de détruire toute copie du logiciel et de sa documentation que vous auriez réalisée. Vous pouvez mettre un terme à ce contrat à tout moment en détruisant les copies du logiciel et de sa documentation.

3. Support technique.

(i) Kaspersky Lab fournira une assistance technique (« Support ») comme décrit ci-dessous pour une période d'un an :

(a) le paiement des frais de l'assistance technique en cours ait été fait, et ;

(b) à la condition qu'ait été rempli le Formulaire d'inscription au Support Technique (Bon d'enregistrement) fourni avec le produit ou disponible sur le site Web de Kaspersky Lab, et qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Lab avec le présent Contrat de Licence. Il restera à l'entière discrétion

de Kaspersky Lab de juger si vous remplissez les conditions d'accès prévues aux services de support technique.

(ii) Le support technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Stratégie de Confidentialité de Kaspersky Lab jointe à ce Contrat, et vous consentez explicitement au transfert de données vers d'autres pays que le votre en accord avec les termes de la Stratégie de Confidentialité.

(iv) Le « service de support technique » comprend :

(a) Mises à jour quotidienne de la base antivirus ;

(b) Mises à jour logicielles gratuites, y compris les mises à niveau de la version ;

© Support technique avancé par courrier électronique et par téléphone, assuré par le revendeur ou le distributeur.

(d) Mises à jour de détection et d'éradication de virus par intervalles de 24 heures.

4. Droits de propriété. Le logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs conservent tous les droits de propriété applicables au logiciel. Le fait que vous en possédiez une copie et que vous l'ayez installée ne vous donne aucun droit de propriété intellectuelle sur le logiciel.

5. Confidentialité. Vous acceptez que le logiciel, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez pas et ne fournirez en aucun cas ces informations confidentielles sous quelque forme que ce soit à un tiers sans l'autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en œuvre des mesures de sécurité minimale visant à assurer que la confidentialité du Fichier Clé d'Identification est respectée, sans pour autant compromettre les conditions précédentes.

6. Limite de garantie

(i) Kaspersky Lab garantit que pour une durée de [90] jours suivant le téléchargement ou l'installation du logiciel, ce dernier fonctionnera correctement 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 sa documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions ou d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaîtra tous les virus connus ou n'affichera pas de message de détection erroné ;

(iv) La responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement au paragraphe (i), 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 représentant au cours de la période de garantie. Vous devrez fournir toutes les informations nécessaires au fournisseur pour 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 (v) 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).

7. Décharge de responsabilité

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (i) de non-satisfaction de l'utilisateur, (ii) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, (iii) de toute infraction aux obligations impliquées par la loi « s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 » ou (iv) de responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i), le Fournisseur 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) ;

© Perte de moyens de paiement ;

(d) Perte d'économies prévues ;

(e) Perte de marché ;

(f) Perte d'occasions commerciales ;

(g) Perte d'image ;

(h) Perte de réputation ;

(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 (suite au contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal au prix d'achat du Logiciel.

8. L'interprétation du présent Contrat de Licence sera effectuée en accord avec la législation locale. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Lab était autorisé en tant que requérant à entamer des poursuites auprès de n'importe quelle juridiction compétente.

9. (i) Le présent Contrat de Licence 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 ou l'un de ses représentants. En dehors des situations prévues dans les paragraphes (ii) - (iii), vous n'aurez aucune possibilité de recours contre Kaspersky Lab au cas où vous auriez fourni des informations erronées dans le cadre du présent Contrat de Licence. En dehors des situations prévues par les paragraphes (ii) – (iii), vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat (« Fausse Représentation ») et Kaspersky Lab ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé.

(ii) Rien dans ce Contrat ne pourra limiter ou exclure la responsabilité de Kaspersky Lab pour toute Fausse Représentation faite en connaissance de cause.

(iii) La responsabilité de Kaspersky Lab pour Fausse Déclaration portant sur une question fondamentale, y compris pour l'obligation du fabricant de respecter ses engagements au titre de ce Contrat, sera sujette à la décharge de responsabilité du paragraphe 7 (iii).