KASPERSKY LABS

Kaspersky® Administration Kit

GUIDE DE L'UTILISATEUR

KASPERSKY® ADMINISTRATION KIT

Guidede l'utilisateur

Visitez notre site Web : http ://www.kaspersky.com/fr/

Date d'édition : Août 2003

Table des matières

CHAPTER 1. PROGICIEL KASPERSKY® ADMINISTRATION KIT – GÉNÉRALITÉS

Le progiciel Kaspersky® Administration Kit s'adresse aux administrateurs des réseaux d'entreprise aussi bien qu'aux responsables des sociétés de la protection antivirus des ordinateurs. Il comprend un jeu d'outils à l'aide desquels l'administrateur réseau peut centraliser les opérations qu'il effectue sur tous les ordinateurs du réseau d'entreprise (*postes de travail*): installation des outils antivirus, leur configuration et mise à jour ainsi qu'une riposte efficace effectuée à temps contre les attaques des virus.

Le progiciel Kaspersky® Administration Kit offre à l'administrateur réseau les possibilités suivantes :

- gestion des paramètres de la protection antivirus sur les ordinateurs du réseau. La gestion des paramètres de la protection antivirus des ordinateurs du réseau d'entreprise permet à l'administrateur réseau de contrôler tous les ordinateurs de l'entreprise et ceci, sans quitter son poste de travail. Ce facteur est important surtout pour de grandes sociétés où le réseau d'entreprise peut comprendre plusieurs bâtiments ou locaux indépendants.

- *déploiement* des programmes antivirus sur les postes de travail. Cette possibilité facilite grandement la tâche de l'administrateur réseau touchant à la création d'un système de protection antivirus pour sa société. L'administrateur réseau n'a besoin de charger qu'une seule fois le pack de programmes antivirus Kaspersky Anti-Virus® sur son ordinateur (ou sur un *serveur* spécialement conçu à cet effet), après quoi, il ne lui reste plus qu'à le télécharger et l'installer à distance sur les ordinateurs du réseau.

- analyse des postes de travail à la demande de l'administrateur réseau ou à un horaire spécifié à l'avance. Celle-ci permet à l'administrateur réseau de lancer le processus de vérification et de dépannage des postes de travail et de déterminer les horaires du lancement automatique de cette vérification.

- mise à jour automatique des bases de données antivirus sur les postes de travail. La mise à jour peut s'effectuer d'une manière centralisée sans

que chaque poste de travail se connecte au serveur Internet de Kaspersky Labs. La mise à jour peut également se faire d'une manière automatique, selon un horaire spécifié par l'administrateur réseau.

- La réception du *rapport réseau*. Le rapport réseau fait état des événements relevés par les logiciels antivirus sur tous les postes de travail. Il est possible de recevoir des rapports analogues sur des postes de travail individuels également.

- système d'avertissement par messagerie. Ce système d'avertissement permet à l'administrateur réseau de créer une liste des événements à l'apparition desquels des avertissements par messagerie lui sont envoyés. Parmi ces événements on peut citer, par exemple, la détection de virus ou une interruption anormale de la procédure de mise à jour des bases de données antivirus sur un poste de travail.

- une **mise en quarantaine** qui est un stockage centralisé des fichiers suspects, leur codage et déplacement vers une **zone de quarantaine** *du serveur*. L'administrateur réseau peut ainsi créer un régime de protection maximal des ordinateurs contre les virus, car même en cas de suppression d'un fichier infecté il reste toujours la possibilité de le restaurer à partir de la **zone de quarantaine** .

- gestion exclusive des paramètres de protection des ordinateurs d'une société. Seul l'administrateur réseau possède un accès aux paramètres de protection. Cette possibilité accroît sensiblement l'efficacité de celle-ci.

- répartition des ordinateurs par sous-réseaux logiques et délégation des droits de gestion aux autres administrateurs réseau. Simplifie la gestion de la protection antivirus sur plusieurs postes de travail.

1.1. Nouveautés de la version 4.5

La version du progiciel Kaspersky® Administration Kit, décrite dans le présent guide, se distingue des versions antérieures par de nouvelles fonctionnalités :

- un programme d'installation unique pour les applications suivantes : Kaspersky® Network Control Centre, Kaspersky Anti-Virus® Server, Kaspersky® Anti-Virus Control Centre et Kaspersky Anti-Virus® Updater.

- une édition différée de la configuration des outils de protection contre les virus. Cette possibilité permet à l'administrateur réseau de ne pas se soucier de l'accessibilité des postes de travail dont il veut éditer la configuration. Les postes de travail peuvent, tout simplement, être déconnectés pendant l'édition. Les modifications sont portées dans la copie des configurations stockée sur le serveur principal et sont, de fait, transmises au poste de travail après sa reconnexion au réseau.

- une configuration simultané des objets du réseau logique. L'édition des paramètres de la protection antivirus peut désormais être effectuée simultanément pour plusieurs postes de travail, serveurs et sous-réseaux.
- une mise en **quarantaine** du réseau. Elle permet de conserver sur les serveurs les fichiers placés "en quarantaine ". De cette façon, la probabilité d'infection du réseau d'entreprise par des virus est réduite au minimum.
- une extension des possibilités de recherche et d'ajout d'ordinateurs au réseau logique. Des fonctions supplémentaires qui rendent plus faciles les opérations de recherche d'ordinateurs sur le réseau logique. L'ajout d'ordinateurs s'accompagne désormais de l'analyse du réseau Microsoft en plus du réseau logique Kaspersky AV.
- détection d'une attaque logique – il s'agit d'une infection simultanée de plusieurs ordinateurs du réseau. Configuration des paramètres de réaction à cet événement.
- rapport réseau. C'est la réception du rapport général de tous les événements enregistrés par les outils antivirus sur les objets du réseau logique aussi bien que l'information relative aux violations de l'intégrité du réseau.

1.2. Spécifications logicielles et matérielles

Les spécifications suivantes sont nécessaires pour le progiciel Kaspersky® Administration Kit :

- Un réseau qui maintient le protocole TCP/IP.
- Système d'exploitation MS Windows 95/98/Me/NT/2000/XP. Si vous utilisez un système equipé de MS Windows NT 4.0, Service Pack 6 doit avoir été installé.

Sur le poste de travail de l'administrateur pour le logiciel Kaspersky® Network Control Centre :

- 16 Mo de mémoire vive accessible (libre).
- 10 Mo d'espace de disque libre.

Pour le logiciel Kaspersky AV Server :

- MS Windows 2000/NT/XP.
- 5 Mo de mémoire vive accessible (libre).

- 1 Mo d'espace de disque libre et l'espace nécessaire pour le stockage des mises à jour des bases antivirales et des composants du paquet Kaspersky Anti-Virus®, aussi bien que des logiciels téléchargés au serveur.
- Pour envoyer par courrier électronique les alertes des tâches fonctionnant sur les postes de travail une possibilité doit exister sur le serveur d'envoyer les messages de poste ou en utilisant le client MAPI ou en suivant le protocole SMTP. Après l'installation du client MAPI il est nécessaire de configurer un profil du système de messagerie sur le serveur. Pour cela, choisissez dans le Barre de configuration MS Windows l'élément **Courrier** et générer la configuration du courrier.

Les exigences envers les programmes et le matériel informatiques des postes de travail sont décrites dans la documentation de Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur.

Kaspersky® Administration Kit 4.5 est préparé pour des réseaux locaux avec une structure de domaines.

1.3. Contenu de la distribution

Vous pouvez acquérir Kaspersky Anti-Virus® Personal chez un distribuiteur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, www.kaspersky.com/fr/, lien **Buy online** / Achat en ligne).

- Le paquet vendu en magasin contient: Une enveloppe fermée avec le CD d'installation, contenant les fichiers du produit logiciel ;
- Le Guide de l'utilisateur ;
- Une clé de license inscrite sur le CD d'installation ; une carte d'inscription avec le numéro de série du produit ;
- accord de licence.

Avant d'ouvrir l'enveloppe avec le CD, assurez-vous de lire soigneusement le contrat de licence..

Si vous achetez Kaspersky Anti-Virus® Personal en-ligne, le fichier d'installation du produit est téléchargé du site Web de Kaspersky Labs. Ce fichier d'installation inclut ce guide de l'utilisateur et la clé de licence. La clé de licence peut être également envoyée par courriel après réception de votre paiement.

1.3.1. Le contrat de licence.

Le contrat de licence (CL) est un contrat légal établi entre vous et le fabricant (Kaspersky Labs Ltd.), qui spécifie les conditions d'utilisation du produit antivirus que vous avez acheté.

Lisez soigneusement le contrat de licence !

Si vous n'acceptez pas les termes du CA, vous pouvez retourner le produit non utilisé à votre revendeur Kaspersky Anti-Virus® pour un remboursement complet, si l'enveloppe contenant le CD (ou les disquettes) est bien fermée.

Le fait d'ouvrir l'enveloppe signifie que vous acceptez toutes les clauses du CL.

1.3.2. Carte d'inscription

Remplissez le coupon détachable de la carte d'inscription avec votre nom, votre téléphone et votre adresse de courriel (si vous l'avez) et postez-le à l'adresse du revendeur qui vous a vendu le progiciel.

En cas de changement de votre adresse postale ou électronique, informez-en votre revendeur.

La carte d'inscription est un document qui atteste votre condition d'utilisateur au sein de votre société, et qui donne droit à un service d'assistance complet pendant la durée de souscription. Les utilisateurs enregistrés, qui sont abonnés au bulletin de Kaspersky Labs sont informés de la parution des nouveaux produits de Kaspersky Labs.

1.4. Assistance aux utilisateurs inscrits

Kaspersky Labs 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 un abonnement, vous recevrez les services suivants pour toute la période de votre inscription :

- nouvelles versions du logiciel, fournies gratuitement ;
- assistance téléphonique et par voie électronique sur l'installation, la configuration et l'utilisation de ce produit antivirus ;
- Informations sur les nouveaux produits et les nouveaux virus d'ordinateurs (pour les abonnés au bulletin de Kaspersky Labs).

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

1.5. Conventions

Cet ouvrage utilise certaines conventions afin de mettre en relief les différentes parties significatives de la documentation. Le tableau ci-après répertorie les conventions utilisées dans le guide de l'utilisateur.

Convention	Usage
Texte gras	Titres de menus, commandes, titres de fenêtres, éléments de boîtes de dialogue, etc.
 Note.	Information complémentaire, remarques
 Attention!	Informations essentielles
 *Pour ce faire,* 1. Etape 1. 2. …	Actions à suivre
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du produit.
 Solution	Une solution donnée au problème
[touche]— la fonction de la touche.	Touches 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 commandes.

CHAPTER 2. CONFIGURATION DE LA PROTECTION ANTIVIRUS

2.1. Réseau logique Kaspersky Anti-Virus®

On définira le *réseau logique Kaspersky Anti-Virus®* (dans la suite appelé *réseau logique*) comme étant l'ensemble des ordinateurs formant un réseau local sur lequel est utilisé pour la protection antivirus le progiciel Kaspersky Anti-Virus® géré par l'utilitaire Kaspersky® Administration Kit. Les ordinateurs peuvent participer au réseau logique en tant que :

poste de travail Kaspersky Anti-Virus® (ou simplement *poste de travail*[1]) – ordinateur à proprement parler, objet de la protection antivirus. Le progiciel Kaspersky Anti-Virus® de même que l'application Kaspersky AV Control Centre doivent être installés.

Le serveur Kaspersky Anti-Virus® (ou simplement *serveur*[2]) est un ordinateur où le programme Kaspersky AV Server est installé. Ses fonctions consistent à organiser les entrepôts des distributeurs de programmes, mettre à jour les bases de données antivirus et les éléments du programme, à détecter l'apparition d'attaques logiques (infection de plusieurs postes de travail) et à envoyer par courrier électronique les alertes générées par les *tâches* s'exécutant sur les postes de travail, ces tâches étant une composante comportant un nombre défini de paramètres du paquet Kaspersky Anti-Virus®. Ces alertes peuvent informer, par exemple, de la détection de virus sur un poste de travail. Plusieurs postes de travail peuvent être affectés à un seul serveur.

Un *groupe* est un ensemble concret de serveurs et de postes de travail qui sont affectés. Ces sous-réseaux peuvent être rassemblés en d'autres sous-réseaux formant un niveau de hiérarchie plus élevé etc. Un serveur au moins doit être inclus dans un groupe.

Les stations d'administration sont des ordinateurs équipés du composant d'administration Kaspersky® Network Control Centre. À partir de ces ordinateurs, les administrateurs réseau peuvent gérer la configuration de tout le logiciel Kaspersky Anti-Virus® installé sur les ordinateurs connectés au réseau local.

---

[1] On définira dans la suite par "poste de travail », un poste de travail de Kaspersky Anti-Virus®

[2] On définira toujours dans la suite par "serveur », un serveur de Kaspersky Anti-Virus®.

Par *objets du réseau logique* on désignera les postes de travail, les serveurs ainsi que les sous-réseaux de tout niveau.

La structure du réseau logique ou la configuration du réseau, c'est à dire, l'information sur les liens hiérarchiques entre les sous-réseaux, les serveurs et les postes de travail, est conservée sur l'un des serveurs. Ce type de serveur sera considéré comme étant le *serveur principal* du réseau logique.

Le même ordinateur peut servir de poste de travail, de serveur et de poste de travail de l'administrateur réseau. Les limites ne sont pas imposées sur la quantité des postes de travail, des serveurs et des postes de travail de l'administrateur réseau, mais le serveur principal du réseau logique doit être unique.

La station de travail et le serveur peuvent faire partie du réseau seulement uns de la fois. Si dans le réseau informatique on crée quelques réseaux logiques Kaspersky Anti-Virus®, l'ajout des éléments d'un réseau logique à l'autre n'est pas autorisée.

Un exemple de structure du réseau logique est reproduit dans l'Illustration 1.

Illustration 1. Un exemple de structure du réseau logique

2.2. Adresses des objets du réseau logique

Les objets du réseau logique (serveurs et postes de travail) sont adressés à l'aide des adresses réseau des ordinateurs sur lesquels les programmes appropriés sont installés. En qualité d'*adresse de l'objet du réseau logique* on peut avoir (selon la configuration du réseau):

- une adresse numérique IP statique ;
- un nom de domaine complet (FQDN);
- un nom d'ordinateur connecté au réseau Microsoft (nom NetBIOS).

La première n'est accessible que dans le cas où une adresse IP statique a été allouée à l'ordinateur mais elle est inaccessible dans le cas d'attribution dynamique d'adresses par un serveur DHCP.

La deuxième possibilité n'est accessible que dans le cas où il existe un service DNS et que les noms de domaine sont permanents et affectés aux ordinateurs.

La troisième possibilité est accessible si le service WINS est effectif.

Plus bas, tous les types d'adresses énumérés jusqu'ici seront identifiés en tant qu'*adresse d'objet*.

2.3. Création du réseau logique

La création du réseau logique suppose les étapes principales suivantes :

1. Élaboration du réseau logique : *l'administrateur du réseau logique* (dans la suite *administrateur réseau*) définit les ordinateurs sur lesquels seront installés les postes de travail des administrateurs réseau, le serveur principal, les serveurs et les postes de travail. La structure du réseau logique peut varier, mais il existe quelques recommandations principales à faire à ce sujet :

   - tous les ordinateurs où il est prévu d'installer Kaspersky Anti-Virus® doivent devenir des postes de travail.
   - dans chaque segment de réseau, au moins un serveur doit être présent (généralement, un seul serveur suffit). Tous les postes de travail de ce segment doivent être reliés à ce serveur.
   - le serveur principal doit être installé sur le même segment de réseau que le poste de travail de l'administrateur réseau (le même ordinateur, par exemple).
   - les serveurs auxquels les postes de travail sont reliés, devront être répartis par sous-réseaux si la taille et la complexité du réseau logique qui en résulte excèdent les capacités de gestion d'un seul administrateur réseau.
   - si cela est nécessaire, les administrateurs des sous-réseaux devront être désignés et le logiciel du poste de travail de l'administrateur réseau sera installé sur leurs ordinateurs.

2. L'installation du logiciel sur les ordinateurs comprend :

   - l'installation de Kaspersky® Network Control Centre sur le poste de travail de l'administrateur réseau (voir le paragraphe 3.1).

- l'installation de Kaspersky AV Server sur les ordinateurs du serveur principal et les serveurs du réseau logique (voir le paragraphe 3.1).
- l'installation du logiciel pour les postes de travail (voir le paragraphe 6.3).

3. Configuration du réseau logique :
   - intégration des serveurs au réseau logique (voir le paragraphe 6.2).
   - connexion des postes de travail aux serveurs (voir le paragraphe 6.3).
   - spécification des paramètres serveur (voir le paragraphe 7.3).
   - configuration des serveurs pour le traitement des alertes générées par les postes de travail (voir le Chapter 7).
   - spécification des paramètres de recherche et de traitement antivirus sur les postes de travail.
   - en cas de besoin, répartition des serveurs aussi bien que des postes de travail qui y sont associés, par sous-réseaux (voir le paragraphe 6.1).
4. L'attribution des privilèges d'accès aux autres utilisateurs :
   - Autorisation ou interdiction d'accès aux autres utilisateurs à la configuration du Kaspersky AV Control Centre sur les postes de travail (voir le paragraphe 8.1).
   - Le rôle des administrateurs des sous-réseaux (voir le paragraphe 8.2).

Exemple. Une société possède des bureaux dans plusieurs bâtiments éloignés les uns des autres. Tous les ordinateurs de la société sont intégrés au réseau, et l'administrateur réseau doit assurer la protection du réseau contre les virus. Il installe l'utilitaire Kaspersky® Administration Kit et le paquet de programmes Kaspersky Anti-Virus® sur les ordinateurs, forme le réseau logique et en définit les paramètres. Après quoi, l'administrateur réseau contrôle la sécurité antivirus des ordinateurs de toute la société sans quitter son poste de travail.

2.4. Administrateurs réseau du réseau logique. Privilèges d'accès

On désignera par *administrateur du réseau logique,* l'utilisateur qui a installé l'utilitaire Kaspersky® Administration Kit sur les ordinateurs connectés au réseau local. L'administrateur réseau peut contrôler tous les serveurs et postes de travail du réseau logique. On désignera par *administrateur réseau du groupe*, l'utilisateur ayant un droit d'accès aux serveurs et sur les postes de travail faisant partie d'un groupe. Ci-dessous on désignera l'administrateur du réseau logique de même que l'administrateur réseau de tout groupe par *administrateur réseau*, tout simplement. Pour commencer avec le logiciel Kaspersky® Network Control Centre, l'administrateur réseau définit l'adresse du serveur principal, son mot de passe pour l'accès à la configuration du réseau et son pseudo. A l'aide du logiciel Kaspersky® Network Control Centre l'administrateur réseau est capable de :

- construire le réseau logique, ajouter des sous-réseaux, serveurs et postes de travail (voir le chapitre 6);
- gérer les éléments du paquet Kaspersky Anti-Virus® installés sur les postes de travail ;
- gérer les privilèges d'accès des utilisateurs aux paramètres du progiciel Kaspersky Anti-Virus® (voir le paragraphe 8.1);
- assigner des administrateurs des groupes (voir le paragraphe 8.2).

Pour construire un réseau logique l'administrateur réseau doit connaître non seulement son nom et son mot de passe, mais aussi les *mots de passe de l'accès au réseau* des postes de travail et des serveurs qu'il va intégrer au réseau logique. *Les mots de passe pour autoriser l'accès sur les postes de travail du réseau* sont déterminés lors de l'installation du logiciel Kaspersky AV Control Centre (voir le paragraphe 6.3). Les *mots de passe pour autoriser l'accès aux serveurs du réseau* sont déterminés lors de l'installation du logiciel Kaspersky AV Server (voir le point 6.3).

Après avoir créé le réseau logique, l'administrateur réseau peut bloquer les privilèges d'accès des autres utilisateurs aux paramètres du progiciel Kaspersky Anti-Virus® pour les postes de travail (voir le paragraphe 8.1.1).

De plus, l'administrateur réseau peut changer la hierarchie des privilèges des administrateurs des sous-réseaux qui font partie de son groupe, sans se préoccuper de celui qui avait attribué ce privilège.

Tous les administrateurs réseau peuvent changer la structure du réseau logique tout en restant dans les limites de leurs attributions, ils ne peuvent, cependant, pas le faire simultanément. Si l'un des administrateurs réseau entre dans le logiciel Kaspersky® Network Control Centre en mode édition, les autres ne pourront pas le faire.

2.5. Maintenance du réseau logique

Après création et configuration du réseau logique nous recommandons aux administrateurs réseau d'effectuer régulièrement les opérations suivantes :

examiner tous les jours le rapport réseau et le rapport sur le fonctionnement des antivirus sur les postes de travail (voir le paragraphe 9.1). Pour chaque tâche, le rapport contient des statistiques sur les résultats de la dernière tâche. Par exemple, le rapport sur le travail du logiciel Kaspersky AV Scanner contient l'information sur le nombre de secteurs, de fichiers, de dossiers, d'archives examinés, de modules exécutables compactés, la quantité de virus trouvés, le nombre de signatures de virus, la quantité d'objets désinfectés, éliminés, suspects et endommagés ainsi que la durée de recherche des virus.

Si l'appel de l'administrateur réseau vers un poste de travail n'aboutit pas (un message apparaissant sur l'impossibilité d'établir une connexion avec ce poste de travail), alors que l'ordinateur est accessible par le réseau local, il faut vérifier si le paquet Kaspersky Anti-Virus® n'a pas été supprimé ou réinstallé par l'utilisateur. Ces actions sont décrites en détail au paragraphe 9.4.

consulter la boîte aux lettres et lire les alertes émises par les postes de travail (voir le paragraphe 9.6).

Une liste complète des avertissements générés par les tâches du paquet Kaspersky Anti-Virus® est jointe à la documentation pour l'utilisateur de ces tâches. Lors de la configuration du réseau logique à l'aide du logiciel Kaspersky® Network Control Centre, l'administrateur réseau peut activer ou désactiver l'envoi des alertes diverses en provenance d'un poste de travail (voir le document " Kaspersky Anti-Virus® pour les postes de travail / Kaspersky Anti-Virus® pour MS NT Serveur. Guide de l'utilisateur ").

si l'administrateur réseau constate sur l'un des postes de travail une situation demandant une intervention de sa part, il peut le faire sans quitter son poste de travail, d'où il procédera, par exemple, au traitement des fichiers infectés trouvés sur ce poste de travail (voir le paragraphe 9.7).

mettre à jour les bases de données antivirus du progiciel Kaspersky Anti-Virus® sur les postes de travail. Pour cela, il faut, après avoir installé le régime de mise à jour par serveur, utiliser la tâche de mise à jour comprise dans la liste des tâches exécutables régulièrement sur les postes de travail (voir le

paragraphe 7.4). Dans ce cas, les fichiers des bases de données antivirus seront copiés vers les postes de travail à partir de l'entrepôt des mises à jour du serveur. Nous recommandons de configurer une mise à jour automatique des entrepôts des serveurs à partir de l'entrepôt d'un des serveurs, lequel devrait être mis à jour automatiquement à partir de l'Internet.

2.6. Spécifications de sécurité. Organisation du travail en commun des administrateurs réseau

Pour maintenir la capacité du réseau à être contrôlé et pour le protéger des actions malveillantes ainsi que pour maintenir l'efficacité du travail en commun des administrateurs réseau, nous vous suggérons de suivre ces quelques recommandations.

Les administrateurs réseau devront garder secrets les mots de passe d'accès à la configuration du réseau.

Si un administrateur réseau a perdu son mot de passe, il pourra obtenir un nouveau mot de passe auprès de l'administrateur réseau qui l'a nommé.

Si le mot de passe de l'administrateur principal du réseau logique est perdu, l'accès à la configuration du réseau devient impossible. Dans ce cas, il faudra réitérer tout le processus de création et de configuration du réseau logique.

Afin d'éviter toute confusion nous ne recommandons pas aux administrateurs réseau de modifier la configuration du paquet des programmes Kaspersky Anti-Virus® installés sur les postes de travail gérés par les administrateurs des sous-réseaux. Dans le cas où cela s'avèrerait indispensable, il est conseillé de le communiquer aux administrateurs des sous-réseaux en personne

.

CHAPTER 3. INSTALLATION DU PROGICIEL

3.1. Installation du logiciel Kaspersky® Network Control Centre

Ci-dessous est décrite la procédure de l'installation des programmes de Kaspersky® Administration Kit sur les ordinateurs où les programmes de ce progiciel n'ont pas encore été installés. Les procédures d'installation complémentaire, de réinstallation et d'élimination des composants individuels sont décrites ci-dessous dans le paragraphe 3.2.

Le programme d'installation vous offrira d'installer Kaspersky® Network Control Centre et Kaspersky AV Server sur le même ordinateur. Cette installation est recommandée au début de la formation du réseau logique, et dans ce cas vous créer le poste de travail de l'administrateur et le serveur principal.

S'il est nécessaire d'installer seulement Kaspersky AV Server ou seulement Kaspersky® Network Control Centre quelques étapes de la procédure décrite doivent être omises. Les directives appropriées sont fournies dans la description de la procédure.

Avant d'installer les programmes Kaspersky® Network Control Centre et Kaspersky AV Server sur l'ordinateur il est préférable de fermer tous les programmes actifs de Kaspersky Anti-Virus®.

Pour installer Kaspersky® Network Control Centre, Kaspersky AV Server ou les deux programmes sur votre ordinateur :

1. Lancez le fichier exécutable **Setup.exe** qui se trouve sur le CDROM de la distribution. Une fenêtre d'informations du programme d'installation s'ouvrira pour vous notifier que l'installation de Kaspersky® Administration Kit est en train de progresser. Appuyez sur le bouton **Suivant** pour continuer l'installation ou cliquez sur **Annulation** pour interrompre l'installation du progiciel. Ci-dessous ces boutons ne sont pas décrits, aussi bien que le bouton **Précédent** permettant de retourner à l'étape précédente de la procédure d'installation.

2. Une fenêtre contenant le contrat de licence apparaît. Pour l'accepter et continuer l'installation cliquez sur **Oui**, sinon, si vous n'acceptez pas les termes du contrat, cliquez sur **Non** (en ce cas, l'installation sera interrompue).

3. Une boîte de dialogue de renseignements sur l'utilisateur apparaît. Remplissez les champs de saisie **Nom de l'utilisateur** et **Organisation** (assurez-vous de compléter les deux zones, sans quoi l'installation ne se poursuivra pas).

4. La boîte de sélection de dossier où le programme sera installé apparaît. Le dossier où le progiciel sera installé par défaut sera représenté dans le champ de destination intitulé **Répertoire de destination**. S'il est nécessaire de modifier ce dossier cliquez sur **Parcourir** et sélectionnez le dossier souhaité dans la boîte de dialogue standard de MS Windows.

5. La boîte de sélection de dossier (du logiciel) où l'icône du programme sera placé apparaît. Le nom par défaut est affiché dans le champ **Dossier des programmes**. Choisissez un des dossiers existants pour y placer l'icône de la liste **Dossiers existants** ou indiquez le nom d'un nouveau dossier dans le champ **Dossier des programmes**.

6. La boîte de sélection des composants à installer apparaît (voir : Illustration 2). Tous les composants sont sélectionnés ce qui correspond au mode d'installation des deux programmes.

   - Si vous installez seulement Kaspersky® Network Control Centre, cochez le champ près de Kaspersky® Network Control Centre et décochez-le près de Kaspersky Anti-Virus® Server (en ce cas la sélection des cases sera supprimée des noms des composants respectifs).

   - Si vous installez seulement Kaspersky AV Server, d' le champ près du nom de Kaspersky® Network Control Centre. En ce cas les champs seront cochés par défaut près des noms de Kaspersky Anti-Virus® Updater et de Kaspersky® Control Centre. Les composants respectifs sont nécessaires pour le fonctionnement correct du serveur, mais ils font partie de Kaspersky Anti-Virus® pour les postes de travail également, et s'ils sont déjà installés sur cet ordinateur, on peut décocher le champ près de leurs noms.

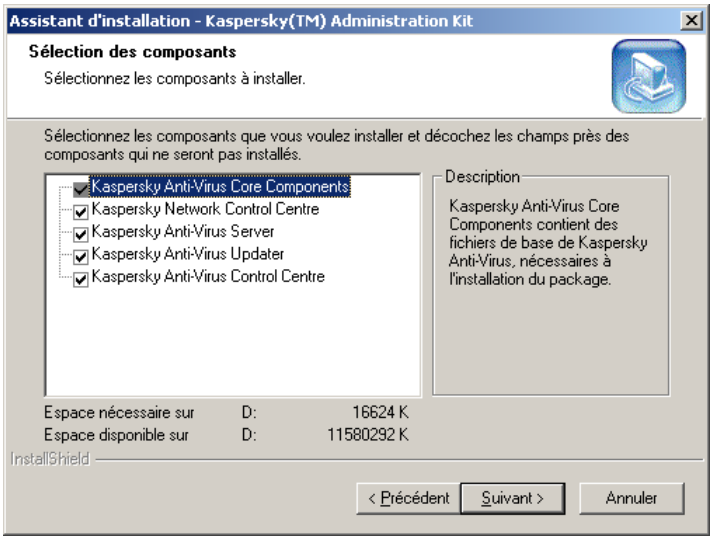

Illustration 2. Sélection des composants à installer

7. Une fenêtre d'informations apparaît intitulée **Démarrage de la copie des fichiers** (voir: Illustration 3), contenant le résumé des informations saisies à l'avance. Vérifiez attentivement ces informations avant de continuer l'installation. En cas de détection d'erreurs cliquez à besoin sur le bouton **Précédent**, retournez dans l'une des fenêtres décrites ci-dessus et corrigez un paramètre entré incorrectement.

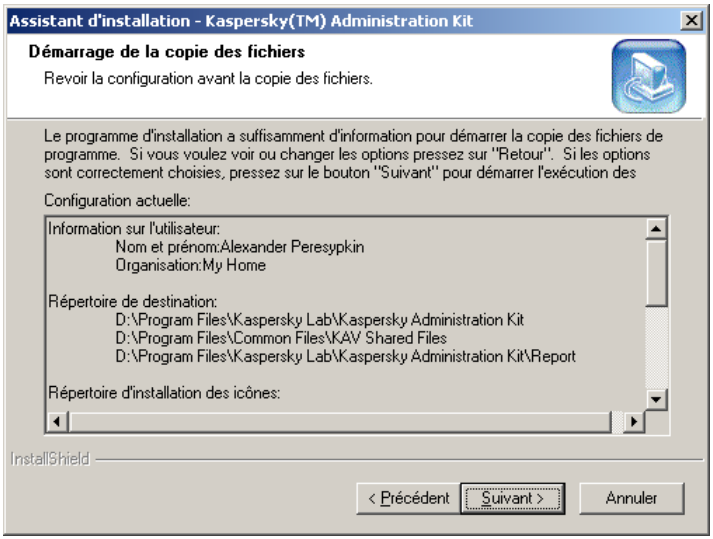

Illustration 3. Fenêtre **Démarrage de la copie des fichiers**

8. Une fenêtre de sélection de dossier apparaît (voir: Illustration 4). Dans la zone **Type de fichier de rapport** indiquez pour travailler avec quels fichiers ultérieurement il faudra toujours utiliser le programme Report Viewer : *.rep et/ou *.rpt. Le dossier où les rapports seront conservés par défaut sera représenté dans le champ d'information intitulé **Dossier de destination**. S'il est nécessaire de modifier ce dossier cliquez sur **Parcourir** et sélectionnez le dossier souhaité dans la boîte de dialogue standard de MS Windows.

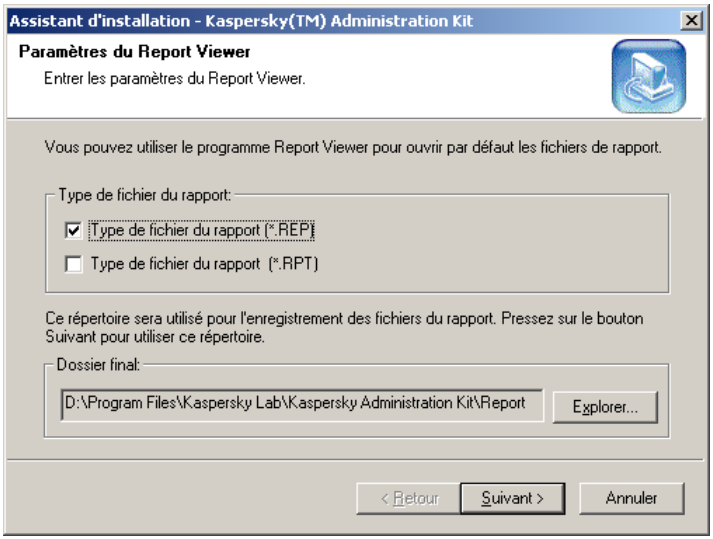

Illustration 4. Fenêtre **Configuration du Report Viewer**

9. Si Vous êtes en train d'installer Kaspersky AV Server, après la copie des fichiers une fenêtre apparaît proposant de saisir le mot de passe pour administration du réseau logique (voir: Illustration 5). Indiquez le mot de passe dans le champ **Nouveau mot de passe** entrez de nouveau le mot de passe dans le champ **Confirmation**.

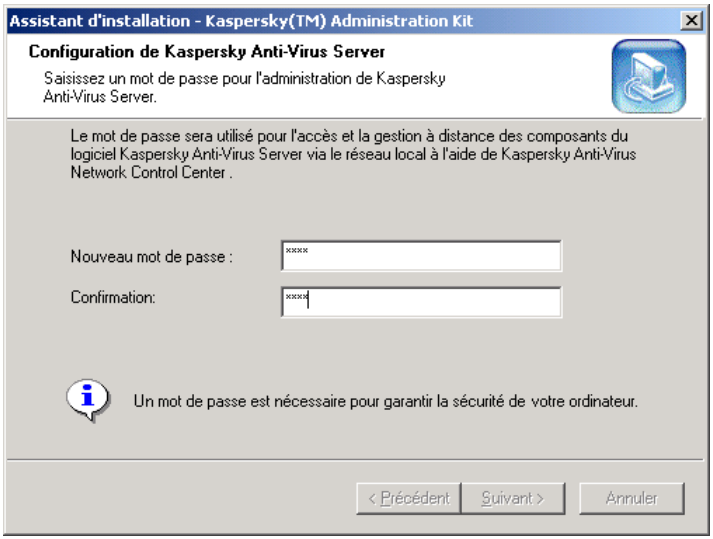

Illustration 5. Saisie du mot de passe de l'administration du serveur par réseau

10. Si Kaspersky AV Server est installé sous MS Windows NT/2000/XP, un champ de saisie apparaît vous proposant de saisir les paramètres du compte du système, sous lequel Kaspersky AV Server fonctionnera en tant que service (voir: Illustration 6).

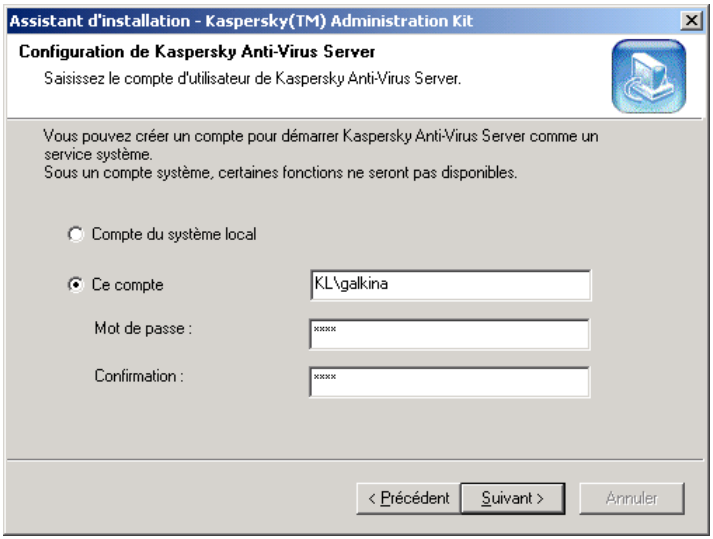

Illustration 6. Saisie des paramètres du compte du système

Sélectionnez dans le groupe d'options si le lancement et le fonctionnement du serveur auront lieu sous le compte du système local ou sous un compte ordinaire du système. Dans le dernier cas il est nécessaire de saisir également le compte de système, le mot de passe et la confirmation du mot de passe dans des champs de saisie correspondants. Nous recommandons de travailler sous le compte de système local (il faut se rendre compte qu'en ce cas il est impossible de renvoyer les messages via MAPI).

11. En cas d'installation de Kaspersky AV Server apparaît une fenêtre de saisie de dossiers pour les entrepôts organisées par le serveur (les dossiers d'entrepôts des mises à jour, des bases antivirales, des programmes et ceux pour placement de la quarantaine du serveur). Dans la plupart des cas, on pourra utiliser les valeurs proposées dans les champs informatiques respectifs par défaut (voir: Illustration 7). S'il est nécessaire de changer la place d'un dossier cliquez sur **Parcourir** près du champ en question et sélectionnez le nouvel emplacement dans la boîte de dialogue standard de MS Windows.

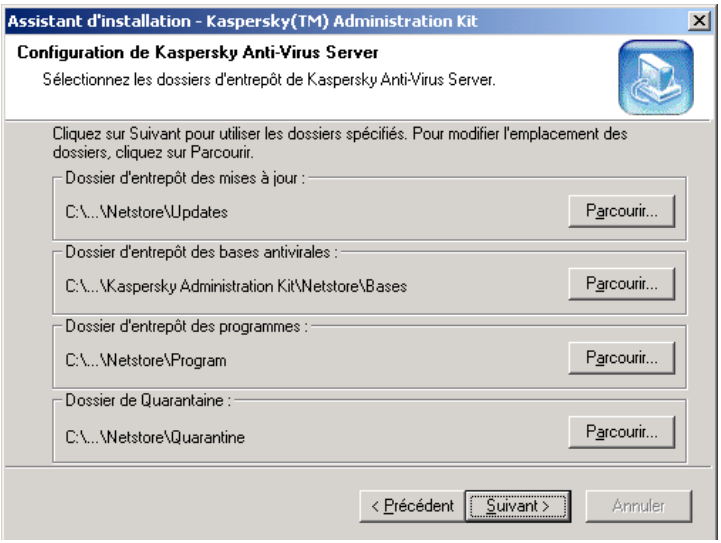

Illustration 7. Sélection du placement d'entrepôts

12. Si vous avez inclus Kaspersky AV Control Centre au nombre des composants à installer une fenêtre de saisie de mot de passe de l'accès du réseau à ce programme apparaît (voir: Illustration 8). Indiquez le mot de passe et la confirmation dans les champs de saisie correspondants.

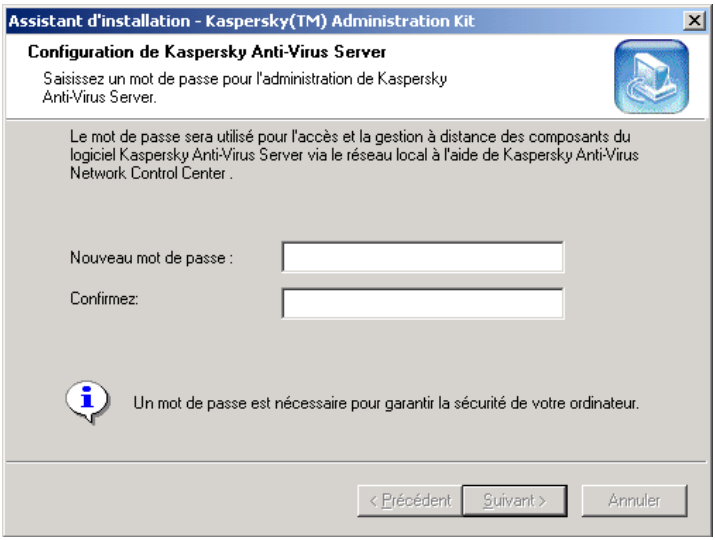

Illustration 8. saisie de mot de passe d'accès du réseau pour Kaspersky AV Control Centre

13. Après la copie des fichiers faisant partie des composants choisis une fenêtre de formation de la liste des fichiers des clés d'utilisateurs apparaît (voir: Illustration 9). Au début la fenêtre contient le nom du fichier (des fichiers) transmis à vous sur le CDROM de la distribution. Si vous possédez d'autres fichiers contenant les clés d'utilisateurs qui vous offrent des droits complémentaires vous pouvez ajouter ces fichiers à la liste. Pour cela faire, cliquez sur **Ajouter** et sélectionnez le fichier souhaité dans la fenêtre standard de MS Windows. Si certaines des clés représentées dans la liste ne sont plus nécessaires (à cause de licence expirée par exemple), sélectionnez ces fichiers dans la liste et cliquez sur **Supprimer**.

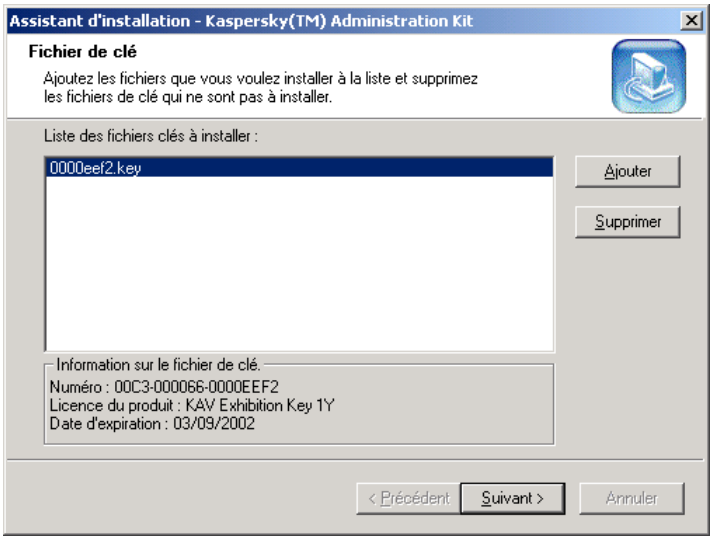

Illustration 9. Formation de la liste des clés

14. Une fenêtre de fin d'installation apparaît. Sélectionnez l'option **Oui, redémarrer l'ordinateur maintenant** pour le redémarrage immédiat de l'ordinateur ou, si vous voulez le redémarrer plus tard, choisissez **Non, je redémarrerai l'ordinateur plus tard**. Faites attention : pour terminer l'installation correctement, il faut redémarrer l'ordinateur.
15. Cliquez sur **Terminer**. L'installation est terminée.

3.2. Ajout, réinstallation et désinstallation des composants individuels

Pour ajouter, désinstaller ou réinstaller un composant de Kaspersky® Administration Kit sur un ordinateur où certains composants sont déjà installés veuillez lancer le programme d'installation comme cela est indiqué au paragraphe 3.1. En ce cas la procédure d'installation aura un nombre de différences par rapport à celle qu'on vient de décrire.

Après la fenêtre d'informations annonçant le début de l'installation la fenêtre de sélection du mode d'installation apparaît (voir: Illustration 10).

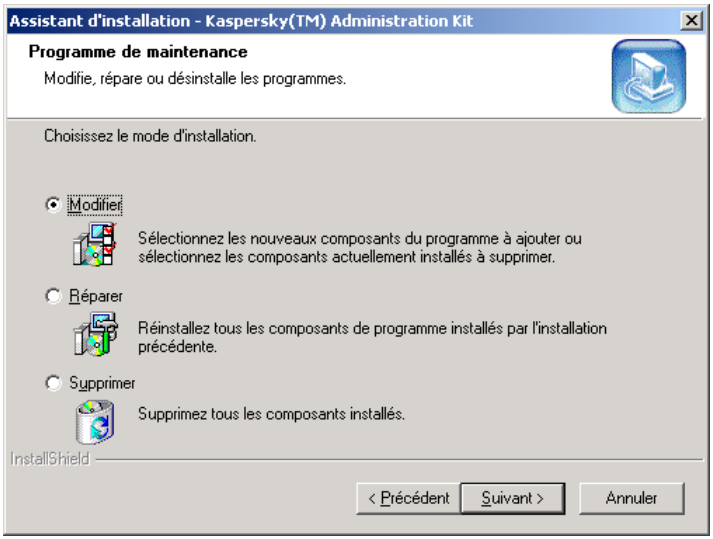

Illustration 10. Sélection du mode d'installation

Dans le groupe des boutons de sélection choisissez **Modifier**, si vous voulez ajouter ou supprimer certains composants, **Réparer**, si vous voulez réinstaller des composants déjà installés, et **Supprimer** pour complètement supprimer Kaspersky® Administration Kit.

Si vous avez choisi **Réparer**, la fenêtre de sélection des composants apparaît. Les composants que vous choisirez seront installés et tous les autres seront supprimés. L'installation qui suit est analogue à celle décrite précédemment.

Au cas où le CDROM de la distribution manque vous pouvez toujours lancer le programme d'installation pour supprimer comme a été décrit dessus des composants individuels (ou tous les composants installés). Pour ce faire, dans le Panneau de contrôle de MS Windows choisissez **Installation et suppression de programmes** et dans la liste des programmes qui se présentera choisissez Kaspersky® Administration Kit, après quoi cliquez sur **Ajouter/Supprimer**. L'assistant d'installation de Kaspersky® Administration Kit sera lancé.

CHAPTER 4. PREMIERS PAS.

Ce chapitre décrit les premières actions de l'utilisateur du progiciel après l'installation. On examine la création et l'introduction au fonctionnement du réseau logique le plus simple. On suppose que l'utilisateur est familier avec les principes de base de l'interface graphique de MS Windows.

Les chapitres qui suivent donnent la description détaillée de l'interface du programme de base du progiciel Kaspersky® Network Control Centre. En plus on fournira une explication successive de l'installation, de la modification et de configuration du réseau logique. Si la description qui suit dans ce chapitre semble trop brève consultez la description plus détaillée fournie par les chapitres suivants.

Ci-dessous on va supposer que le logiciel est déjà installé sur les ordinateurs, et en particulier, sur le poste de travail de l'administrateur le logiciel Kaspersky® Network Control Centre est installé, sur l'ordinateur qui sert du serveur sont installés les programmes Kaspersky AV Server, Kaspersky AV Control Centre et Kaspersky AV Updater, et sur l'un des ordinateurs est installé le logiciel pour les postes de travail Kaspersky Anti-Virus® (Kaspersky AV Control Centre y inclus). Pour vous familiariser avec le logiciel vous pouvez l'installer en totalité sur le même ordinateur.

Pour créer le plus simple réseau logique il vous faudra :

1. Lancer Kaspersky® Network Control Centre.
2. Indiquer le serveur principal et créer un réseau vide.
3. Ajouter le serveur au réseau logique.
4. Ajouter au réseau logique une poste de travail après l'avoir ajouté au serveur.

Après l'accomplissement de ces actions vous pouvez vous familiariser aux outils proposés par le logiciel pour la résolution des tâches antivirales.

Abordons donc l'exécution d'un simple exemple de création du réseau logique.

Lancer le logiciel Kaspersky® Network Control Centre. Pour ce faire :

1. Dans, la barre des tâches de MS Windows, cliquez sur **Démarrer**.
2. Sélectionnez dans le menu l'option **Programmes**.

3. Dans le menu suivant, sélectionnez d'abord **Kaspersky Anti-Virus®**, puis **Administration**.

4. Dans le menu suivant, sélectionnez l'option **Kaspersky® Network Control Centre**. Après cela, une boîte de dialogue **Connexion au Kaspersky® Network Control Centre** apparaît (voir: Illustration 11).

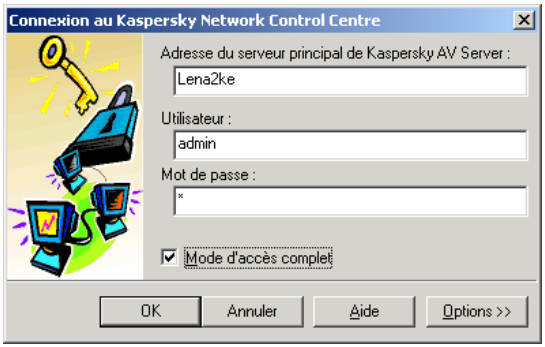

Illustration 11. Entrée dans Kaspersky® Network Control Centre

5. Dans le champ **Adresse du serveur principal de Kaspersky AV Server** indiquez l'adresse du serveur principal du réseau logique. Le logiciel Kaspersky AV Server installé à l'avance sur cet ordinateur doit être lancé.

6. Dans le champ **Utilisateur** indiquez le nom symbolique et dans le champ **Mot de passe** indiquez le mot de passe de l'administrateur du réseau logique.

Quand vous accédez Kaspersky® Network Control Centre pour la première fois, élaborez et entrez un nom symbolique et un mot de passe que vous utiliserez ultérieurement.

- Vous pourrez changer ultérieurement le nom et le mot de passe de l'administrateur du réseau (voir le paragraphe 10.1).

7. À la première entrée au programme aussi bien qu'ultérieurement si vous voulez changer la structure du réseau logique cochez la case **Régime d'accès complet** .

Deux administrateurs ne peuvent pas changer simultanément la structure du réseau logique. C'est pourquoi au cas où l'administrateur lance le programme et l'autre administrateur est déjà entré dans le réseau avec des privilèges d'accès complet, celui-là pourra accéder à la documentation au régime de "lecture seule ". En ce cas l'administrateur peut corriger les paramètres des objets, mais il ne peut pas ajouter ou supprimer les objets du réseau logique.

8. Cliquez sur **OK**. Après le lancement du programme d'installation la fenêtre **Nouvelle configuration du réseau** apparaît à l'écran, et il vous faudra indiquer les moyens de création de la structure du réseau logique (voir: Illustration 12):

   - **Créer la configuration initiale du réseau** créer un réseau logique vide. Choisissez ce point si vous commencez le travail avec le réseau logique pour la première fois.
   - **Importer la configuration du réseau depuis le fichier** – importer du fichier la structure du réseau logique. Choisissez ce point si vous avez déjà travaillé avec le réseau logique et si vous avez déjà exporté sa structure dans un fichier. Il faut indiquer le nom complet du fichier à l'aide de ce bouton  . Ce fichier est créé à l'aide de l'exportation de la configuration du réseau du serveur principal existant (voir le paragraphe 7.7.1).

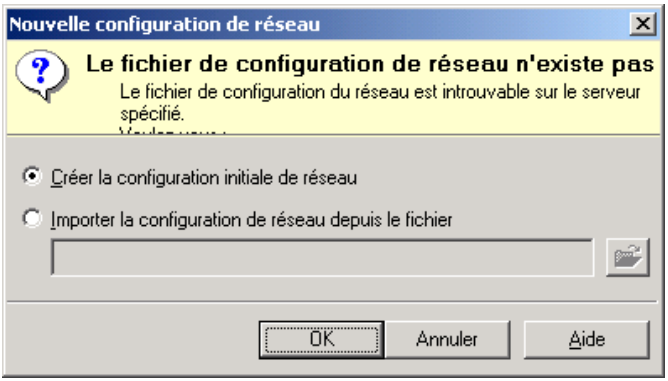

Illustration 12. Nouvelle configuration de réseau

9. Après la sélection du moyen de création de la structure du réseau logique cliquez sur **OK**. Une fenêtre principale du programme s'ouvrira sur l'écran (voir: Illustration 13).

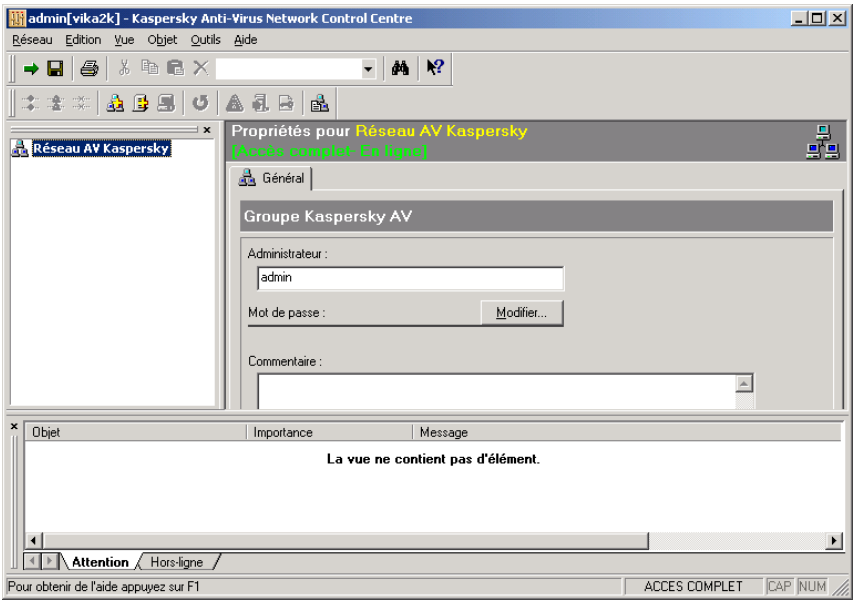

Illustration 13. La fenêtre principale du logiciel Kaspersky® Network Control Centre

Ajouter un serveur au réseau logique. Pour ce faire :

1. Cliquez sur l'icône **Réseau AV Kaspersky** dans la partie à gauche en haut de la fenêtre principale.

2. Dans le menu **Objet** cliquez sur  de la barre d'outils (d'actions). Après cela une boîte de dialogue **Ajouter un serveur** apparaît (voir: Illustration 14).

   `<Ctrl>+<E>`

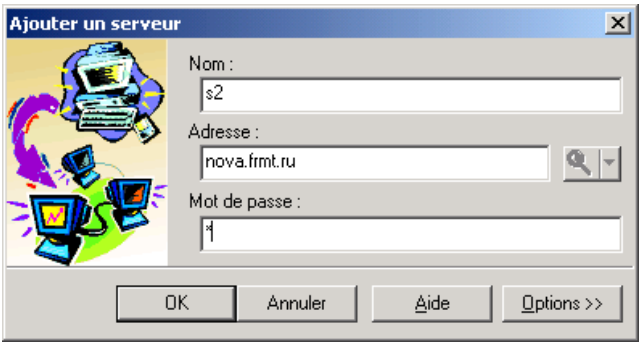

Illustration 14. Ajouter un serveur

3. Dans la zone **Adresse** indiquez l'adresse du serveur.
4. Si cela est nécessaire, dans la zone **Nom** indiquez le nom du serveur du réseau logique que vous venez d'ajouter.
5. Dans la zone **Mot de passe** indiquez le mot de passe d'accès au réseau du logiciel Kaspersky AV Server que vous aviez indiqué lors de l'installation du programme (voir paragraphe 3.1).
6. Cliquez sur **OK**.

Après cela le serveur sera ajouté au réseau.

Ajoutez un poste de travail. Pour ce faire :

1. Dans la liste des objets du réseau logique (qui se trouve dans la barre du réseau dans la partie gauche de la fenêtre principale) cliquez sur le nom ou l'icône du serveur.
2. Dans le menu **Objet** choisissez le point **Ajouter un poste de travail** ou cliquez sur  de la barre d'outils. Après cela une boîte de dialogue **Ajouter un poste de travail** apparaît (voir: Illustration 15).

   <Ctrl>+<W>

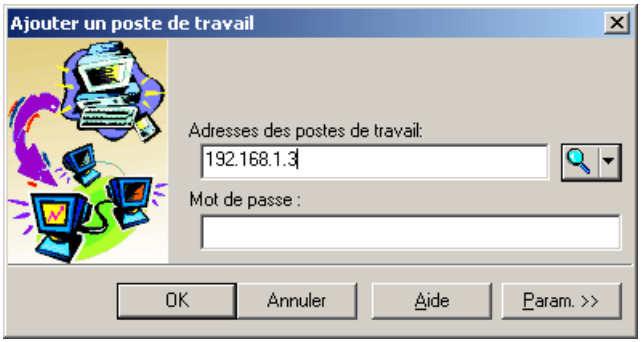

Illustration 15. Ajouter un poste de travail

3. Dans la zone **Adresses des postes de travail** indiquez une adresse d'un poste de travail.

Il est impossible d'ajouter un poste de travail sur un réseau logique si son nom NetBios est composé uniquement de chiffres (par exemple, 123). Nous vous conseillons d'ajouter ce type de station en utilisant son adresse IP.

4. Dans la zone **Mot de passe** entrez sur le poste de travail le mot de passe du contrôle du réseau du logiciel Kaspersky AV Control Centre indiqué lors de l'installation. Cliquez sur **OK**.

Vous pourrez choisir ultérieurement les postes de travail et les serveurs parmi les objets auxquels ils sont associés et régler les paramètres de la protection antivirale dans les onglets de la zone de description qui occupe la partie majeure de la fenêtre. Pour un exemple des paramètres d'un poste de travail, voir: Illustration 16.

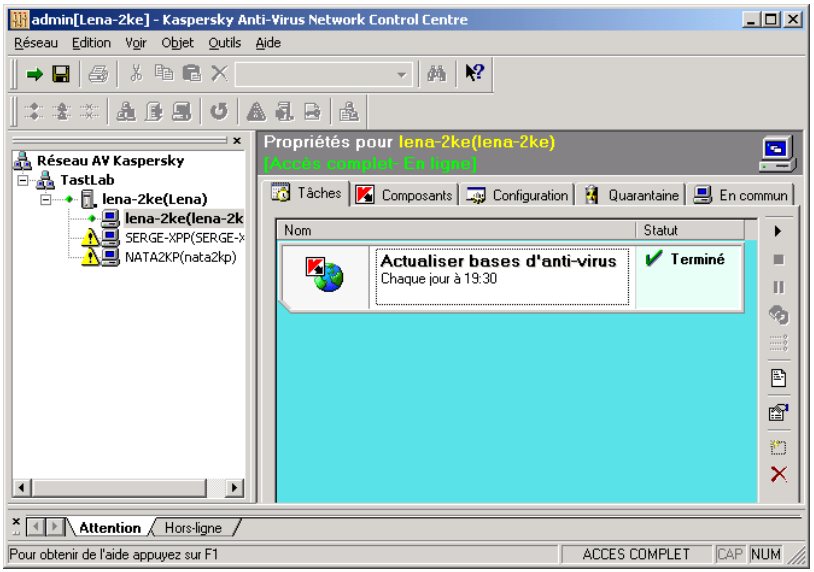

Illustration 16. Onglet **Tâches** d'un objet de type **poste de travail**

Sur l'illustration dessus la partie centrale de la fenêtre est occupée par la liste des tâches de Kaspersky Anti-Virus® pour un poste de travail. Vous pouvez choisir dans la liste toute tâche et régler à distance l'horaire de son lancement, la lancer immédiatement ou l'arrêter etc. Ces réglages sont décrits en détail dans les chapitres qui suivent.

CHAPTER 5. INTERFACE UTILISATEUR

5.1. Fenêtre principale

Dans la fenêtre principale du programme Kaspersky® **Network Control Centre** (voir: Illustration 17) sont disposés :

- le menu ;
- la barre d'outils ;
- la barre du réseau ;
- la zone de description des attributs de l'objet actuel du réseau logique ;
- la barre d'informations ;
- la barre d'état.

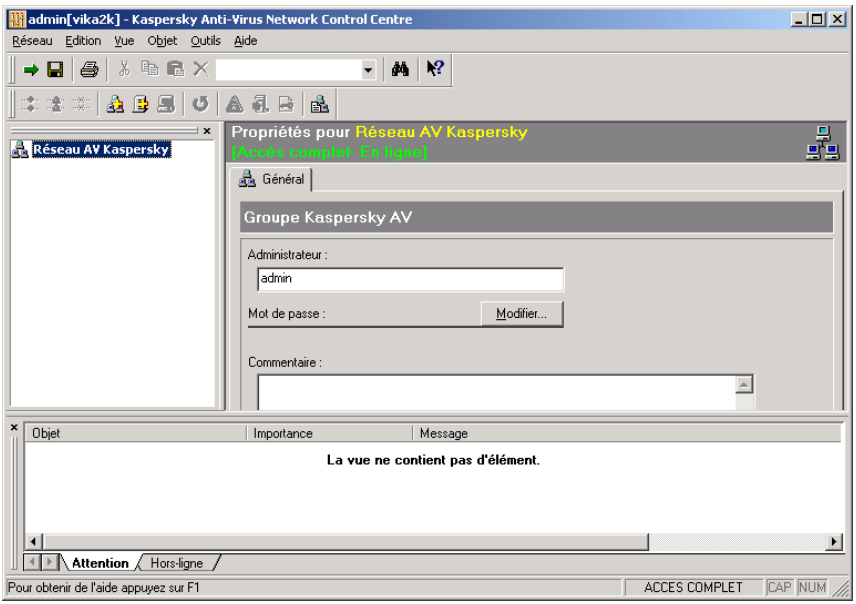

Illustration 17. Fenêtre principale du logiciel Kaspersky® Network Control Centre

5.2. Menus

Dans la partie supérieure de la fenêtre principale sont disposés les *menus*. Certaines commandes des menus sont doublées par des combinaisons de raccourcis clavier ou par des boutons des barres d'outils (voir paragraphe 5.3). Par exemple, au lieu de choisir l'option Connexion dans le menu **Réseau** vous pouvez cliquer sur le raccourci clavier <Ctrl>+<L> ou sur le bouton  dans les barres d'outils.

Les raccourcis clavier sont indiqués dans les menus à côté des options correspondantes. Un tableau regroupant toutes ces correspondances se trouve à l'Annexe A.

5.3. Barres d'outils

Un tableau regroupant toutes ces correspondances est reproduit dans l'Illustration 18.

Illustration 18. Barre d'outils

La ligne supérieure des boutons s'appelle une *barre standard d'outils*, et l'inférieure est la *barre d'actions*. Chaque bouton dans la barre d'outils correspond à une certaine option du menu. Le tableau des correspondances est donné dans l'Annexe B.

*Pour masquer une barre d'outils de l'écran choisissez dans le menu **Vue** l'option **Barres d'outils**, puis dans le sous-menu qui s'ouvre décochez le champ près de l'option **Standard** ou **Actions**, respectivement. Pour afficher la barre d'outils cocher le champ correspondant.*

5.4. Barre du réseau

Dans la partie gauche de la fenêtre principale du programme se trouve la barre du réseau (voir: Illustration 19) contenant une liste d'objets du réseau logique.

La structure de la liste des objets du réseau logique suit :

- Au premier niveau se trouve le nom du groupe radical du réseau logique **Réseau AV Kaspersky**.

- Peuvent suivre les noms des groupes, des groupes du deuxième niveau, des groupes du troisième niveau etc. Un groupe de tout niveau est marqué par l'icône .
- À l'avant-dernier niveau se trouvent les adresses des serveurs et leurs noms mis entre parenthèses. Le serveur est marqué par l'icône . Un seul groupe peut contenir plusieurs serveurs.
- Au dernier niveau se trouvent les adresses des postes de travail et leurs noms mis entre parenthèses. Un poste de travail est marqué par l'icône .

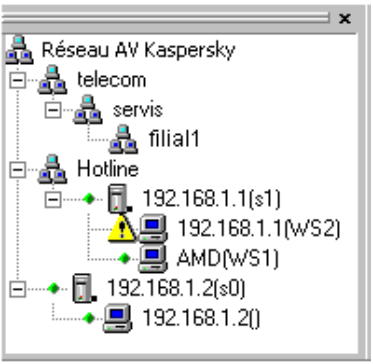

Illustration 19. Barre du réseau

Un *objet actuel* du réseau logique est celui qui est fléché dans l'arborescence des objets.

À la gauche des icônes correspondant aux objets du type **groupe** et **serveur** se trouve un carreau en cliquant sur lequel du bouton gauche de la souris vous pouvez développer/réduire le contenu du groupe ou du serveur. Si le contenu est développé le signe ⊟ apparaît dans le carreau, si le contenu est réduit, cela est indiqué par le signe ⊞.

Vous pouvez déplacer la barre d'outils à l'intérieur de la fenêtre principale aussi bien que modifier sa largeur et son hauteur.

Pour masquer ou afficher la barre du réseau de l'écran choisissez dans le menu ***Vue*** *l'option* ***Barre du réseau*** *. On peut masquer la barre en cliquant sur* ✕ *à l'intérieur de la barre.*

5.5. Menu contextuel

Les objets représentés dans la liste des objets du réseau logique aussi bien que les onglets associés aux objets peuvent avoir un menu contextuel permettant d'exécuter des opérations et les appliquer précisément à ces objets.

Pour appeler le menu contextuel d'un objet

1. Pointez avec la souris sur l'objet dont le menu contextuel vous voudriez appeler.
2. Cliquez avec le bouton droit de la souris. Cette opération déclenche l'apparition du menu contextuel de l'objet (voir: Illustration 20).

Illustration 20. Le menu contextuel de l'objet de type **groupe**

5.6. Zone de description des attributs de l'objet actuel du réseau logique

Dans la partie droite de la fenêtre principale est disposée la zone de description des attributs de l'objet actuel du réseau logique. Les éléments suivants en font partie :

- nom d'objet ;
- icône correspondant à son type :  pour le réseau logique,  pour un serveur ou un groupe et  pour un poste de travail ;
- information concernant les privilèges d'accès à l'objet actuel (**Accès complet** – accès complet à l'objet, **Accès interdit** – accès à l'objet est limité, **Accès complet – mode hors-ligne – les derniers réglages connus** - erreur de connexion avec l'objet, où les derniers réglages connus sont représentés (voir les détails au paragraphe 7.1.2), **Lecture seule** – l'objet n'est accessible qu'à la lecture);
- les onglets indiquant les attributs de l'objet actuel.

En fonction du type de l'objet actuel (groupe, serveur ou poste de travail) la quantité et le contenu des onglets changent.

Les objets de chaque de ces trois types possèdent un onglet **Général** où sont déterminés les privilèges d'accès de l'objet actuel.

5.6.1. Onglets groupe

Pour les objets du type **groupe** les paramètres suivants sont indiqués pour l'onglet **Général** (voir: Illustration 21) nom et mot de passe de l'administrateur ayant accès à ce groupe. A l'aide des champs de ce onglet on peut créer une structure à plusieurs niveaux pour l'administration du réseau logique.

Pour changer le nom symbolique de l'administrateur du groupe entrez le nouveau nom dans le champ **Administrateur**.

Pour changer le mot de passe de l'administrateur du groupe cliquez sur **Modifier** dans la zone **Mot de passe**. Une fenêtre d'entrée du nouveau mot de passe apparaît où il faudra le nouveau mot de passe et sa confirmation dans les champs correspondants.

Vous pouvez aussi entrer un texte que vous voulez dans la zone de saisie **Commentaire** (par exemple une description détaillée du groupe).

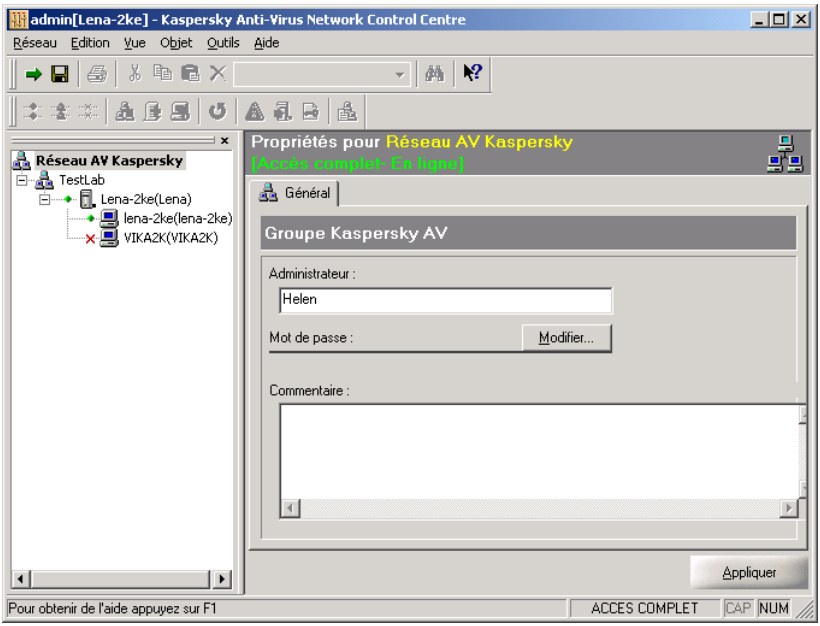

Illustration 21. Onglet **Général** de l'objet de type **groupe**

5.6.2. Onglet serveur

Pour travailler avec un objet de type **serveur** quatre onglets sont prévus : **Entrepôts**, **Options**, **Déploiement**, **Général**.

L'onglet **Entrepôts** (Illustration 22) contient les éléments suivants :

- Le contenu des répertoires où sont stockés les bases de données anti-virus et les mises à jour du logiciel utilisé par les postes de travail connectés au.
- Le contenu des répertoires du serveur où sont stockés les fichiers suspects, détectés par les logiciel antivirus (également appelé la quarantaine serveur. Pour plus de détails sur les types de quarantaine, reportez-vous au sous-chapitre 7.5 à la page 91).

Cet onglet permet également à l'utilisateur de gérer des objets individuels placés dans ces répertoires.

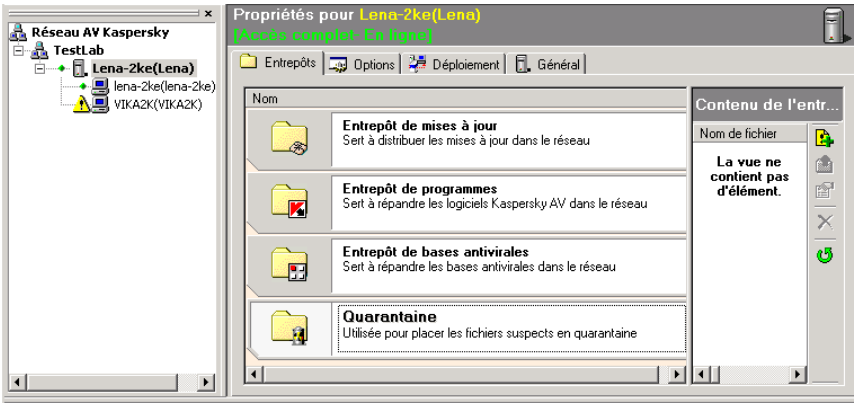

Illustration 22. Onglet **Entrepôts** des objets du type **serveur**

Dans l'onglet **Configuration** (voir: Illustration 23) se trouvent les paramètres de gestion du serveur à distance (voir le paragraphe 7.3), aussi bien que les paramètres d'envoi des alertes des tâches lancées sur les postes de travail associés à ce serveur (voir le paragraphe 7.2). Dans le même onglet est configurée la réaction simultanée du système à l'attaque virale sur plusieurs ordinateurs du réseau protégé (voir le paragraphe 7.2.4).

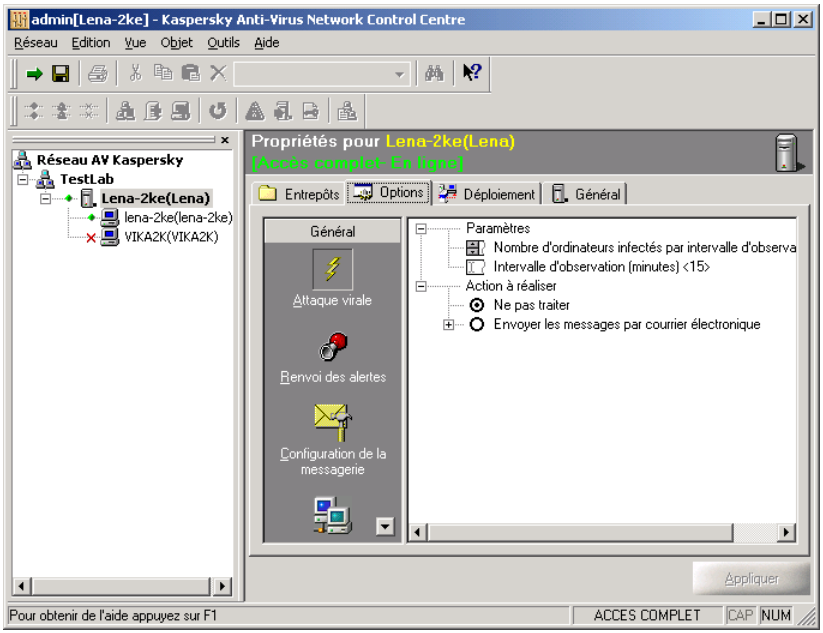

Illustration 23. Onglet **Configuration** de l'objet de type **serveur**

Onglet **Déploiement** est destiné au déploiement des programmes sur les postes de travail (voir le paragraphe 6.3).

Dans l'onglet **Général** est modifié le mot de passe d'accès du réseau au serveur (voir la description détaillée de sa fonction au paragraphe 2.2, sur sa modification voir le paragraphe 10.2).

5.6.3. Onglets poste de travail

Cinq onglets sont utilisés pour travail avec les objet de type **poste de travail**.

Les onglets **Tâches**, **Composants** et **Configuration** sont destinés à gestion de réseau du progiciel Kaspersky Anti-Virus® à l'aide du logiciel Kaspersky AV Control Centre, installé sur un poste de travail. Sur l'onglet **Composants** on peut voir les informations sur les composants du progiciel Kaspersky Anti-Virus® installés sur les postes de travail. L'onglet **Tâches** (voir: Illustration 24) est destiné à la configuration du lancement automatique des tâches, au lancement manuel des tâches sur les postes de travail, aussi bien qu'au rappel des résultats de l'exécution des tâches. Gestion des paramètres antiviraux à l'aide de ces onglets est étudiée en détail dans la description du logiciel Kaspersky AV Control Centre, qui fait partie de la documentation de " Kaspersky Anti-Virus®

pour les postes de travail / Kaspersky Anti-Virus® pour MS NT Serveur. Guide de l'utilisateur".

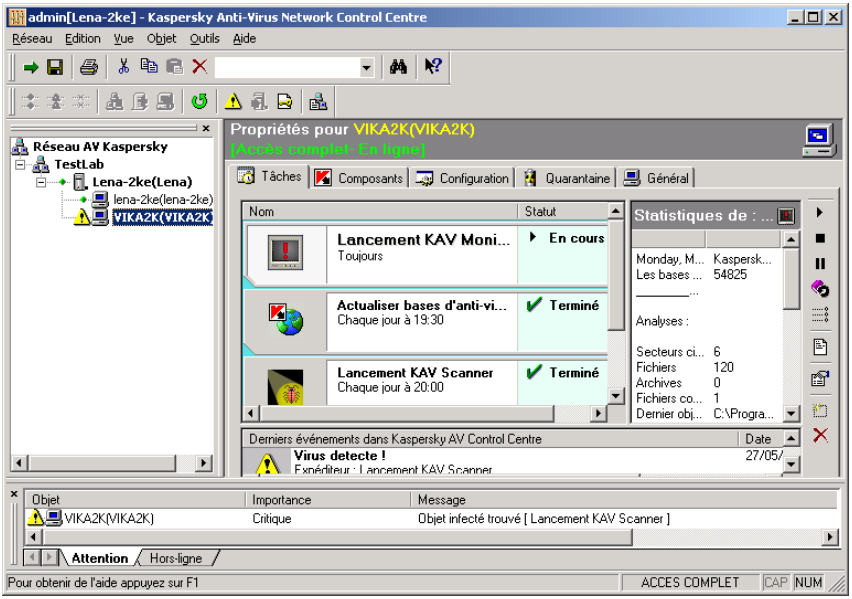

Illustration 24. Onglet **Tâches** d'un objet de type **poste de travail**

Dans l'onglet **Configuration** (voir: Illustration 25) sont indiqués les paramètres de Kaspersky AV Control Centre, qui définissent la possibilité et les moyens de gestion de poste de travail par le réseau (voir Chapter 7, paragraphe 8.1.1, ainsi que la description du logiciel Kaspersky AV Control Centre).

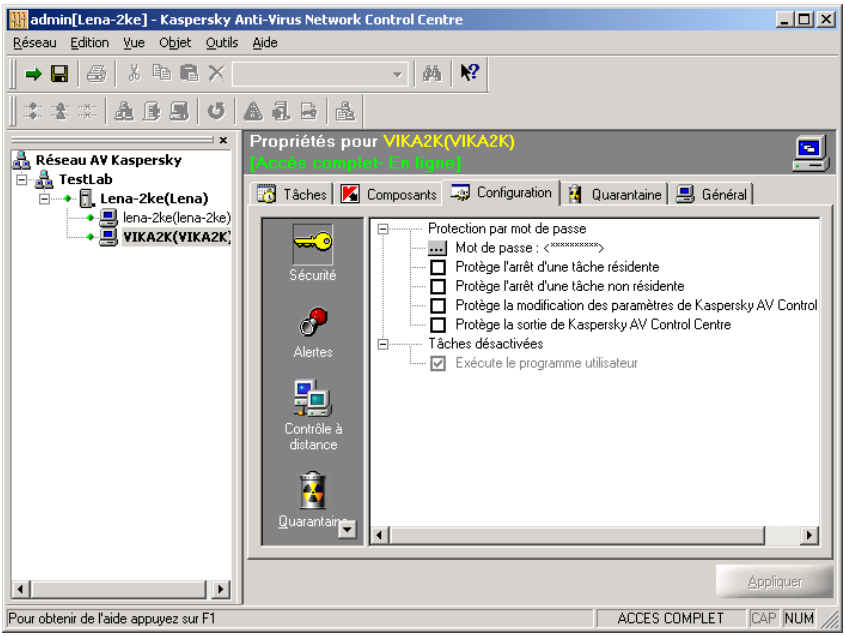

Illustration 25. Onglet **Configuration** d'un objet de type **poste de travail**

Dans l'onglet **Général** est modifié le mot de passe d'accès du réseau au poste de travail (voir la description détaillée de sa fonction au paragraphe 2.4, sur sa modification voir le paragraphe 10.2).

L'onglet **Quarantaine** fournit une liste des fichiers détectés par les programmes antiviraux et mis en quarantaine sur un poste de travail. Sur ce onglet vous pouvez extraire un fichier mis en quarantaine, le mette en quarantaine ou supprimer le fichier définitivement. Voir les détails sur la quarantaine au paragraphe 7.5.

L'onglet **Quarantaine** n'apparaît qu'au cas où le progiciel Kaspersky Anti-Virus® 3.5.5.x ou supérieur est installé sur le poste de travail. En cas de la configuration depuis le réseau du poste de travail avec le progiciel installé version 3.5 l'onglet **Quarantaine** ne sera pas affiché.

5.7. Barre d'informations

La barre d'informations contient deux onglets : **Attention** et **Hors-ligne**.

Dans l'onglet **Attention** (voir: Illustration 26) se trouve une liste d'objets ayant le statut **Attention**: la section **Objet** contient le nom d'objet et l'icône correspondant

au type de l'objet, dans la colonne **importance** est indiqué le niveau d'importance du dernier avertissement de ce niveau issu par l'objet, la colonne **Message** contient le texte de l'avertissement, et les colonnes **Date** et **Heure** – indiquent, respectivement, la date et l'heure quand l'avertissement a été reçu.

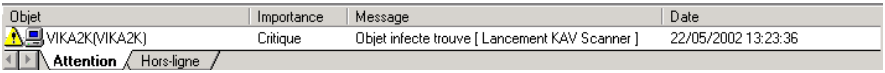

Illustration 26. Barre d'informations, onglet **Attention**

L'onglet **Hors-ligne** (voir: Illustration 27) contient la liste des objets auxquels le programme n'a pas réussi d'accéder : la colonne **Objet** contient le nom d'objet et l'icône correspondant au type de l'objet, et les colonnes **Date** et **Heure** indiquent, respectivement, la date et l'heure de la première tentative infructueuse de connexion.

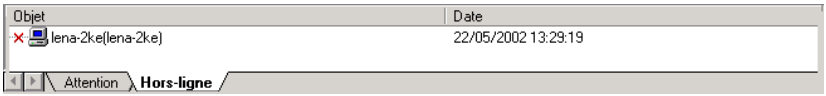

Illustration 27. Barre d'informations, onglet **Hors-ligne**

Vous pouvez trier les lignes des tables tant par ordre de croissance que de suppression du contenu de toute colonne. Pour ce faire cliquez sur le titre de la colonne souhaité : une fois pour trier par croissance et deux fois pour trier par suppression.

La barre d'information possède son propre menu contextuel.

*Pour masquer ou afficher la barre d'informations de l'écran choisissez dans le menu **Vue** l'option **Barre d'informations**. On peut masquer la barre en cliquant sur*  *à l'intérieur de la barre.*

5.8. Barre d'état

Dans la partie inférieure de la fenêtre principale se trouve la *barre d'état* (voir: Illustration 28).

Celle-ci affiche les informations suivantes :

- aide contextuelle ;
- informations sur privilèges d'accès au réseau logique ;
- indicateur du mode **CAPS LOCK** ;
- indicateur du mode **NUM LOCK** .

Illustration 28. Barre d'état

*Pour masquer (ou masquer) la barre d'état de l'écran choisissez dans le menu **Vue** l'option **Barre d'état**.*

5.9. Système d'aide

En travaillant avec le logiciel Kaspersky® Network Control Centre, vous pouvez utiliser son *système d'aide*.

*Pour appeler le système d'aide, sélectionnez dans le menu **Aide** l'option **Contenu** .*

`<F1>`

*Ayant appuyé sur **Renseignement** dans tout boîte de dialogue on peut obtenir des informations détaillées sur celui-ci.*

`<Shift>+<F1>`

Ayant appuyé sur le bouton  *(après quoi un signe d'interrogation apparaît à la droite du curseur) et par cliquant avec la souris sur un des éléments du logiciel Kaspersky® Network Control Centre, on peut obtenir des information sur cet élément.*

`<Shift>+<F1>`

CHAPTER 6. CREATION ET MODIFICATION DE LA STRUCTURE DU RESEAU LOGIQUE

D'habitude, la création du réseau logique suppose les étapes suivantes :

- création des groupes (voir le paragraphe 6.1);
- ajout des serveurs (voir le paragraphe 6.2);
- installation des produits de Kaspersky Anti-Virus® sur les postes de travail (voir le paragraphe 6.3);
- connexion des postes de travail aux serveurs (voir le paragraphe 6.3);
- indication du mode du traitement des alertes issus par les tâches opérationnelles sur les postes de travail (voir le paragraphe 7.2.1);
- Configuration de l'administration à distance des serveurs et des postes de travail (voir le paragraphe 7.2.2, ainsi que la description de Kaspersky AV Control Centre);
- Configuration pour chaque poste de travail du progiciel Kaspersky Anti-Virus® qui y est installé (voir le paragraphe 7.3).

6.1. Création de groupes

Tout nombre de groupes de tout niveau peut être crée à l'intérieur du réseau logique.

Pour créer un groupe

1. Si vous voulez placer un nouveau groupe au niveau supérieur du réseau logique choisissez la ligne **Réseau AV Kaspersky** dans la liste des objets du réseau logique. Si vous voulez inclure un groupe que vous êtes en train de créer dans un autre groupe, choisissez le nom de celui-ci dans la liste des objets.
2. Dans le menu **Objet** sélectionnez **Ajouter un groupe** ou cliquez sur  dans la barre d'outils (d'actions). Vous pouvez choisir

également l'option **Ajouter un groupe** dans le menu contextuel de la liste des objets du réseau logique. Après cela une boîte de dialogue **Ajouter un groupe** apparaît (voir: Illustration 29).

<Ctrl>+<G>

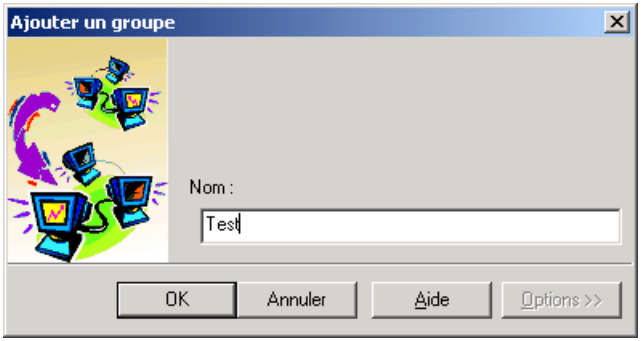

Illustration 29. Ajouter un groupe

3. Dans la zone **Nom** indiquez le nom du groupe que vous êtes en train de créer.
4. Cliquez sur **OK**.

6.2. Ajout des serveurs

On peut ajouter les serveurs directement au réseau logique aussi bien qu'aux groupes de tout niveau. Chaque groupe doit inclure au moins un serveur.

Pour ajouter un serveur

1. Si vous voulez ajouter un serveur directement au réseau logique choisissez dans la liste des objets la ligne **Réseau AV Kaspersky**. Si vous voulez inclure un serveur dans un groupe, choisissez le nom de celui-ci dans la liste des objets.
2. Dans le menu **Objet** sélectionnez **Ajouter un serveur** ou cliquez sur dans la barre d'outils (d'actions). Vous pouvez choisir également l'option **Ajouter un serveur** dans le menu contextuel de la liste des objets du réseau logique. Après cela une boîte de dialogue **Ajouter un serveur** apparaît (voir: Illustration 30).

   <Ctrl>+<E>

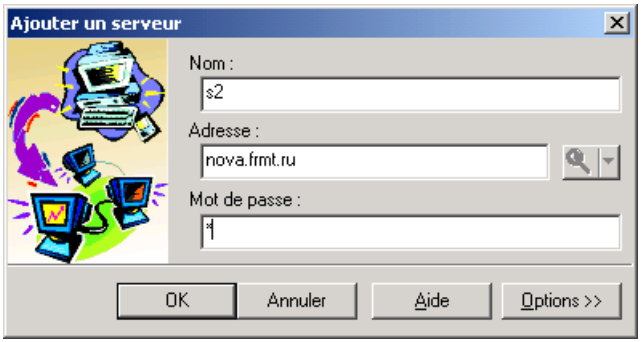

Illustration 30. Ajouter un serveur

3. Dans la zone **Adresse** indiquez l'adresse du serveur.
4. Si cela est nécessaire, dans la zone **Nom** indiquez le nom du serveur du réseau logique que vous venez d'ajouter.
5. Si le serveur possède un mot de passe d'accès au réseau (voir le paragraphe. 2.4), saisissez-le dans la zone **Mot de passe**.
6. Cliquez sur **OK**.
7. Si le serveur possède un mot de passe d'accès au réseau et vous ne l'avez pas indiqué une boîte de dialogue **Mot de passe pour accès réseau à l'objet** apparaît(voir: Illustration 31).

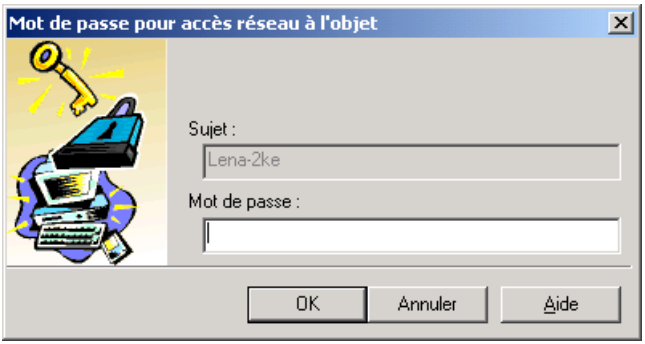

Illustration 31. Saisie de mot de passe pour accéder au réseau

8. Dans la zone **Mot de passe** indiquez le mot de passe pour l'accès de réseau au serveur.

Après cela le serveur sera ajouté au réseau.

Il ne faut pas ajouter le serveur au réseau logique deux fois comme cela peut aboutir à la conduite incorrecte du programme.

6.3. Ajout des postes de travail

Tout nombre de postes de travail peut être ajouté aux serveurs. Vers le moment de connexion il faut installer tout le logiciel nécessaire sur les postes de travail. Ci-dessous on considère une situation où le logiciel a été déjà installé sur l'ordinateur. Pourtant à l'aide de Kaspersky® Administration Kit l'administrateur peut installer le logiciel de Kaspersky Anti-Virus® sur les postes de travail (les ordinateurs qui auront ce rôle y inclus) sans quitter son poste de travail. Cette procédure est décrite dessous au paragraphe 6.4.

Pour ajouter un poste de travail

1. Dans la liste des objets du réseau logique choisissez le nom du serveur auquel vous voudriez ajouter le poste de travail que vous êtes en train d'associer.
2. Dans le menu **Objet** choisissez le point **Ajouter un poste de travail** ou cliquez sur  dans la barre d'outils. Vous pouvez choisir également l'option **Ajouter un poste de travail** dans le menu contextuel de la liste des objets du réseau logique. Après cela une boîte de dialogue **Ajouter un poste de travail** apparaît (voir: Illustration 32).

   <Ctrl>+<W>

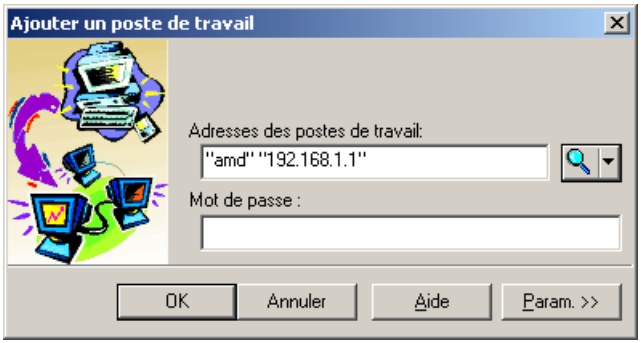

Illustration 32. Ajouter un poste de travail

3. Dans la zone **Adresses des postes de travail** entrez les adresses des postes de travail.

- Choisissez les postes de travail dans la liste des ordinateurs qui font partie du même segment que le serveur auquel vous êtes en train d'ajouter le poste de travail. Pour ce faire cliquez sur  . Après cela une boîte de dialogue **Rechercher un poste de travail** apparaît (voir: Illustration 33) et celle-ci aura une liste des adresses des postes de travail où le logiciel Kaspersky AV Control Centre est installé. Faites attention : les postes de travail n'apparaissent pas dans la liste immédiatement après que le progiciel Kaspersky Anti-Virus® y est installé, mais après un délai court de trois minutes à peu près. Vous pouvez exclure de la liste les adresses qui sont déjà inclues au réseau logique. Pour cela cochez la case ☑ **Exclure les adresses déjà ajoutées au réseau Kaspersky AV**. Si vous voulez ajouter les postes de travail selon leurs adresses IP numériques, cochez la case ☑ **Ajouter selon adresse IP**. Ensuite choisissez dans la liste le poste de travail souhaité (ou plusieurs postes de travail) et cliquez sur **"??".**

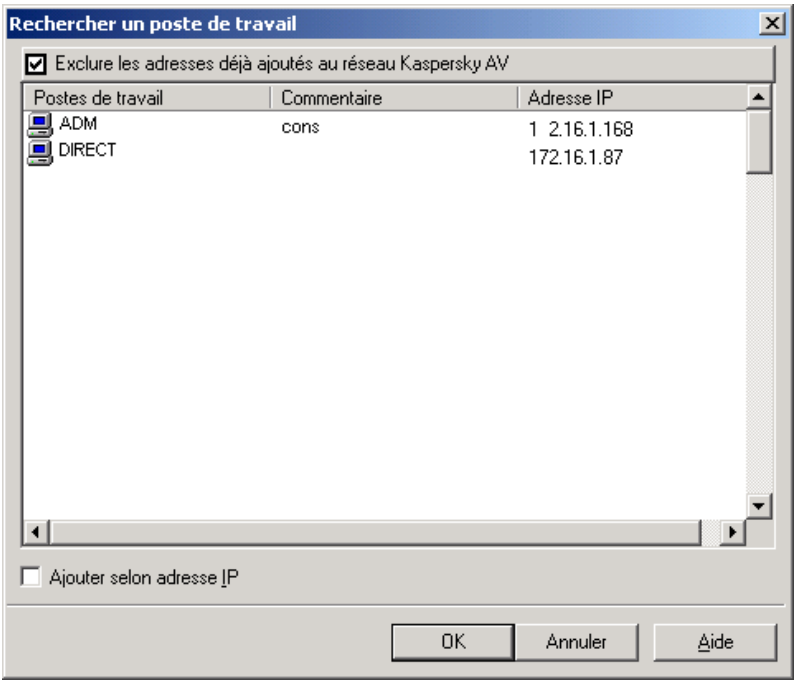

Illustration 33. Sélection de poste de travail

- Pour obtenir une liste complète de tous les postes de travail du segment du réseau local, auquel appartient le poste de travail de l'administrateur, cliquez sur la flèche dans la partie à droite du bouton  . Le menu contenant deux options s'ouvrira, sélectionnez **Browse Microsoft network**. En ce cas la fenêtre **Rechercher un poste de travail** décrite précédemment s'ouvrira qui contient une liste de tous les ordinateurs du réseau Microsoft.

- Si vous voulez ajouter un poste de travail ne faisant pas partie de la liste, entrez dans la zone **Adresses des postes de travail** l'adresse du poste de travail.

Dans la zone **Adresses des postes de travail** vous pouvez entrer les adresses de plusieurs postes de travail, en les énumérant entre guillemets séparées par l'espace (par exemple, **"andrey " "roma " "alex "**). En ce cas tous les postes de travail énumérés seront ajoutés au serveur choisi.

Il est impossible d'ajouter un poste de travail sur un réseau logique si son nom NetBios est composé uniquement de chiffres (par exemple, 123). Nous vous conseillons d'ajouter ce type de station en utilisant son adresse IP.

4. Si le poste de travail qu'on est en train d'ajouter possède un mot de passe d'accès au réseau, entrez-le dans le champ **Mot de passe**. Si vous êtes en train d'ajouter plusieurs postes on essaie de distribuer ce mot de passe à tous les postes (Vous pouvez également indiquer un mot de passe, entre autres l'individualiser pour chaque poste de travail que vous ajoutez, pendant l'étape suivante de la procédure décrite – voir les détails dessous). Cliquez sur **OK**.

5. Si un poste de travail possède un mot de passe pour accéder au réseau (voir le paragraphe 6.3), qui diffère de celui que vous avez indiqué, une boîte de dialogue **Mot de passe pour accès réseau à l'objet** s'ouvrira.

6. Dans la zone **Mot de passe** indiquez le mot de passe pour l'accès de réseau au poste de travail choisi.

7. Cliquez sur **OK**.

8. Les trois pas précédents se répètent pour chaque poste de travail qu'on ajoute pour lequel le mot de passe n'a pas été indiqué ou bien a été indiqué incorrectement.

Il ne faut pas ajouter le poste de travail au réseau logique deux fois comme cela peut aboutir à la conduite incorrecte du programme.

6.4. Déploiement de Kaspersky Anti-Virus® sur les postes de travail

Pour déployer le logiciel Kaspersky Anti-Virus® sur les postes de travail à partir du poste de travail de l'administrateur il est nécessaire de :

- ajouter au moins un serveur au réseau logique (voir le paragraphe 6.2);
- placer dans l'entrepôt des programmes du serveur (le paragraphe 6.4.1) le logiciel qu'il est nécessaire d'installer sur les postes de travail (à l'aide de la procédure décrite le logiciel Kaspersky Anti-Virus® peut être installé si l'installation est accompagnée du support de travail au réseau);
- régler pour le logiciel Kaspersky AV Control Centre qu'on est en train d'installer le mot de passe d'accès du réseau et les autres paramètres (voir le paragraphe 6.4.2);
- lancer le déploiement du logiciel et le transmettre du serveur sur les postes de travail (paragraphe 6.4.2 et paragraphe 6.4.3).

Avant le déploiement du progiciel Kaspersky Anti-Virus® version 3.5.5.x ou supérieure sur l'ordinateur où la version du progiciel 3.5 ou 3.0 est déjà installée ; il faut supprimer manuellement la version ancienne du progiciel. Sinon la nouvelle version sera installée au-dessus de l'ancienne sans la suppression correcte du progiciel ce qui aboutira au fonctionnement incorrect du progiciel.

6.4.1. Transfert du logiciel dans l'entrepôt des programmes du serveur. Configuration des paramètres des programmes à déployer

Le logiciel Kaspersky AV Server utilise un dossier spécial, ou *l'entrepôt des programmes* pour la sauvegarde des copies des distributifs du logiciel qui est à installer à distance sur les postes de travail. L'emplacement de cet entrepôt sur le serveur est réglé lors de l'installation de Kaspersky AV Server (voir le paragraphe 3.1).

Pour placer le logiciel Kaspersky Anti-Virus® dans l'entrepôt des programmes du serveur et le régler pour le déploiement il faut :

1. Choisir dans la liste des objets du réseau logique le serveur à partir duquel l'installation sera accomplie.

2. Dans la zone des attributs d'objet ouvrez l'onglet **Entrepôt** et cliquez sur **Entrepôt de programmes** (voir: Illustration 34).

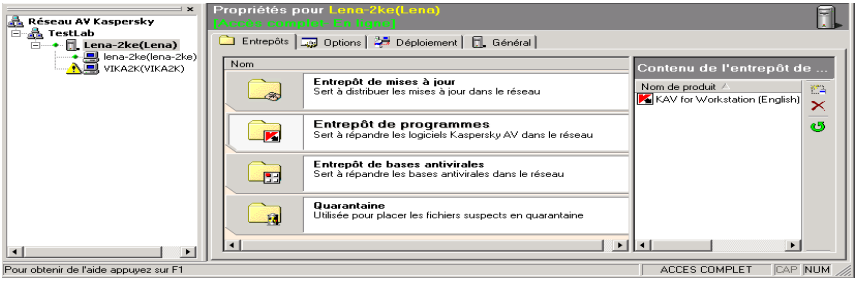

Illustration 34. Travail avec l'entrepôt des programmes

3. Cliquez sur  , qui se trouve dans la fenêtre à droite, ou sélectionnez **Ajouter** dans le menu contextuel. Ceci aura pour effet d'activer l'assistant de transfert du produit au serveur (voir: Illustration 35).

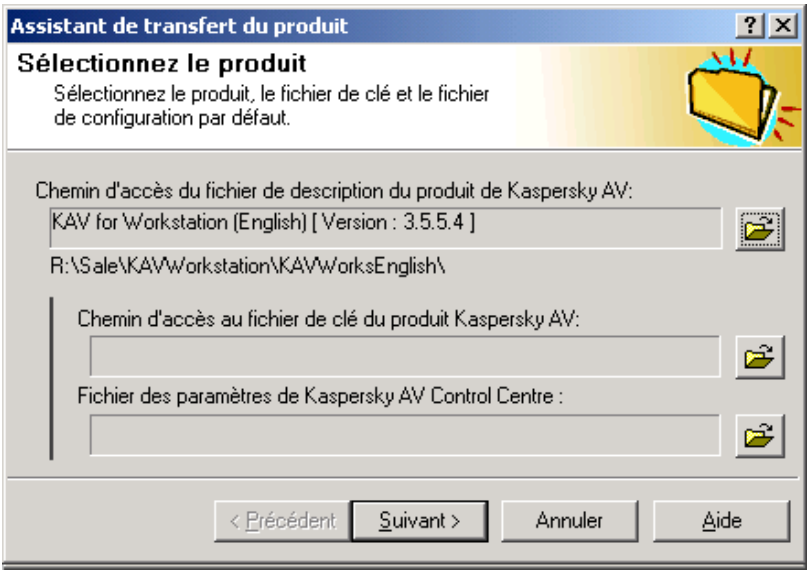

Illustration 35. Assistant de transfert du produit sur KasperskyAV serveur

4. Un fichier spécial de description du produit doit faire partie du progiciel qui est à télécharger sur le serveur (ce fichier ayant

l'extension **.kpd**). Cliquez sur  qui se trouve dans à droite du champ **Chemin d'accès du fichier de description du produit Kaspersky AV** et dans la boîte de dialogue standard MS Windows et choisissez ce fichier.

5. Cliquez sur  qui se trouve à droite du champ **Chemin d'accès au fichier de clé** et dans la boîte de dialogue standard MS Windows qui vient de se présenter choisissez ce fichier (ce fichier ayant l'extension **.key)**.

6. Pour le logiciel Kaspersky AV Control Centre, qui est installé à l'aide de la procédure décrite précédemment, on peut spécifier les paramètres à l'avance (tells que liste du lancement des tâches etc.) Si cela n'est pas fait le programme sera installé et aura les paramètres par défaut. Les réglages qu'on vient de mentionner peuvent être copiés de toute installation de Kaspersky AV Control Centre. Pour cela il faut exporter les paramètres du programme déjà installé au fichier **policy.dat**. Pour la description détaillée de la procédure d'exportation des paramètres voir la description de Kaspersky AV Control Centre dans la documentation " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur ", on peut se servir également de l'exportation des paramètres d'un poste de travail à l'aide de Kaspersky® Network Control Centre (voir le paragraphe 7.7.2). Si un fichier de ce type a été créé à l'avance cliquez sur  qui se trouve à droite du champ **Fichier des paramètres de Kaspersky AV Control Centre** et dans la boîte de dialogue standard MS Windows qui se présente choisissez ce fichier.

7. Cliquez sur **Suivant**. La copie des fichiers du progiciel commencera.

8. À la fin de la copie une fenêtre s'ouvrira contenant un message vous avertissant de la fin de copie du produit. Pour se familiariser avec le rapport détaillé sur le processus de copie cliquez sur **Détails**. Pour terminer la procédure de copie cliquez sur **Terminer**.

Le nom du produit placé dans l'entrepôt apparaît dans la liste **Contenu de l'entrepôt** (voir: Illustration 36).

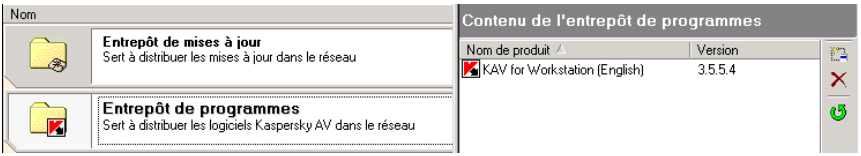

Illustration 36. Contenu de l'entrepôt des programmes après l'ajout d'un produit

Pour supprimer un des produits se trouvant dans l'entrepôt, sélectionnez-le dans la liste et cliquez sur  ou sélectionnez **Supprimer** dans le menu contextuel.

Pour rafraîchir une liste (si par exemple les modifications y ont été ajoutées par un autre programme) cliquez sur  .

6.4.2. Configuration du déploiement. Lancement du déploiement à partir du script de connexion

Pour régler un déploiement du logiciel : se trouvant dans l'entrepôt des programmes du serveur ouvrez l'onglet **Déploiement** (voir: Illustration 37).

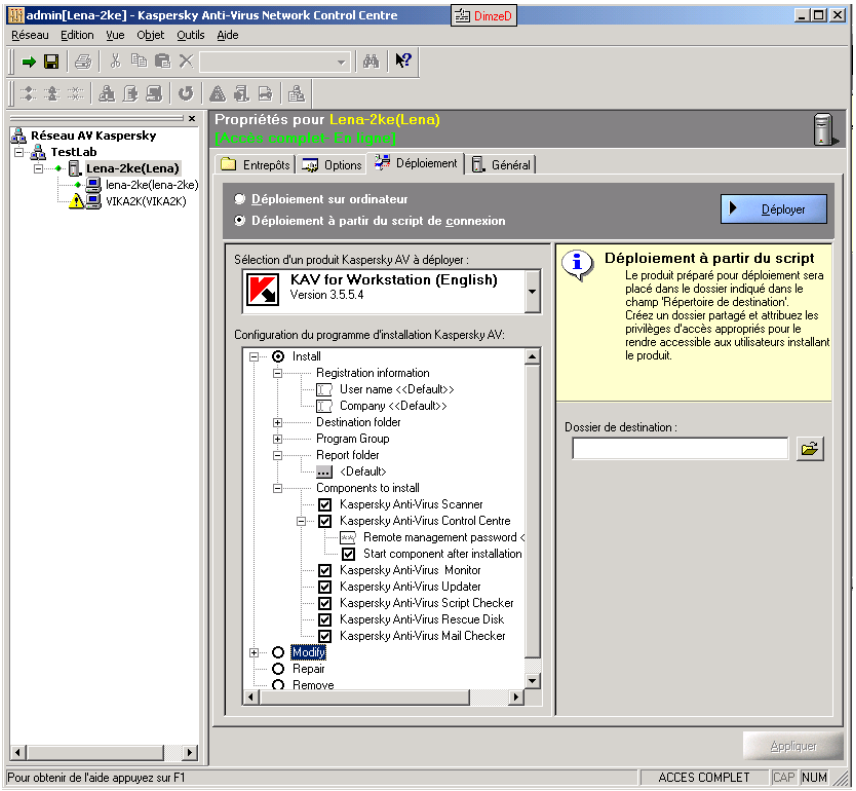

Illustration 37. Configuration d'un déploiement

Il faut choisir, avant tout, une des méthodes de déploiement :

- Déploiement sur ordinateur.
- Déploiement à partir du script de connexion.

La première méthode accorde à l'administrateur plus de possibilités, mais n'est acceptable qu'au cas où le serveur et le poste de travail où est effectuée l'installation fonctionnent avec les systèmes d'exploitation MS Windows NT/2000/XP.

La deuxième méthode est plus universelle, et au cas où est elle est appliquée les ordinateurs peuvent également fonctionner sous MS Windows 95/98/Me. Il est nécessaire qu'un serveur du domaine Windows NT soit présent sur le réseau local et que la connexion sur le poste de travail où l'installation est en train de se produire soit effectuée parallèlement à l'entrée au domaine. Outre cela, tant que

les nouvelles versions de Kaspersky Anti-Virus® soient émises ce mécanisme permet de conduire la mise à jour centralisée des versions. Cette méthode de déploiement est décrite en détail ci-dessous et les particularités d'installation type **ordinateur à ordinateur** sont décrites au paragraphe suivant.

Pour effectuer l'installation par la méthode du script de connexion :

1. Dans le groupe d'options se trouvant dans la partie supérieure de l'onglet **Déploiement** choisissez la méthode **Déploiement à partir du script de connexion**.
2. La signification des paramètres définis est similaire à celle des paramètres d'installation ordinaire des produits de Kaspersky Anti-Virus®. Dans le groupe d'options composant le premier niveau de l'arborescence choisissez le mode d'installation (**Installer**, **Modifier**, **Corriger** ou **Supprimer**; voir la description détaillée des modes d'installation au paragraphe 3.2).
3. Si vous avez choisi les modes **Installer** ou **Modifier** il faut développer la ramification correspondante. Agrandissez également la ramification **Composants à installer** et cochez le champ près des noms des composants que vous voulez installer (en ce cas les composants dont les champs ne sont pas cochés, lors de l'installation dans le mode **Installer** ne seront pas installés, et lors de l'installation dans le mode **Modifier** seront supprimés du poste de travail).
4. Si vous avez choisi d'installer un des composants de Kaspersky Anti-Virus® Control Centre, développez la ramification correspondante et cliquez sur l'option **Mot de passe pour l'administration** (voir: Illustration 38).

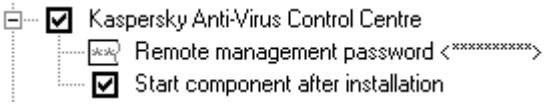

Illustration 38. Configuration de Kaspersky AV Control Centre

5. Indiquez le mot de passe pour l'administration réseau du poste de travail dans le champ qui se présente et pressez sur la touche <Enter>.
6. Si cela est nécessaire décochez la case **Lancement après l'installation**.
7. Si vous avez choisi le mode d'installation **Installer**, développez, si ce la est nécessaire, la ramification **Renseignements sur**

l'utilisateur, **Fichier destinataire**, **Fichier aux raccourcis** et **Fichier aux rapports**, cliquez sur le nom du paramètre correspondant et corrigez dans le champ qui se présente. Si l'on ne change pas ces valeurs l'installation sera effectuée avec les paramètres indiqués par défaut.

8. Indiquez le nom du fichier auquel vous avez l'accès du réseau dans le champ **Fichier destinataire**. Le produit à installer sera mis dans ce fichier. Pour choisir un fichier on peut se servir du bouton  , en ce cas la fenêtre standard MS Windows se présentera.

9. Cliquez sur **Déployer**. Une fenêtre avec la demande de confirmation **Commencer l'installation automatique ?** apparaît. Cliquez sur **Oui** pour placer le produit dans le fichier destinataire.

10. La boîte de sélection de la langue du progiciel à installer apparaît (voir: Illustration 39). Choisissez dans la liste qui se présente le langue du produit et cliquez sur **OK**.

Illustration 39. Sélection de la langue du produit

11. À la fin de la copie une fenêtre d'informations s'ouvrira décrivant les actions suivantes de l'administrateur. Cliquez sur **OK** pour fermer cette fenêtre.

Dans le fichier destinataire le sous-fichier **PRODUCT.AVP** est créé, où l'on place le distributif du produit choisi aussi bien que le programme **avpdtup.exe**, et ce programme gère la procédure d'installation pour les postes de travail. Au lancement du programme il détecte si le produit est présent et vérifie si l'installation de cette version du produit n'a pas déjà été effectuée. Si le produit a déjà été installé aucune action n'est plus nécessaire, sinon la procédure d'installation sur le poste de travail est lancée (l'installation est alors effectuée en mode de traitement parallèle des données, aucuns messages n'apparaissent sur l'écran et aucune réaction n'est requis de l'utilisateur).

Si un redémarrage est nécessaire après une installation distante du correctif, le message correspondant est affiché sur l'ordinateur distant.

Pour garantir le lancement de **avpdtup.exe** accompagné par l'installation du produit sur un poste de travail lors de la première connexion d'un utilisateur concret, l'administrateur doit placer dans le script de connexion de cet utilisateur la ligne suivante

start \\ordinateur\nom_du_fichier_destinataire\PRODUCT.AVP\avpdtup.exe

Les action nécessaires au lancement dépendent de l'architecture du réseau. Si donc le dossier système du premier contrôleur du domaine est intitulé **WinNT**, alors il faut créer un fichier de type bat, contenant la ligne décrite précédemment et le placer au dossier **Winnt\System32\Repl\Import\Scripts**. Plus tard à l'aide de User Manager pour Domaines il faut désigner ce fichier en tant que login-script.

À la première connexion de l'utilisateur auquel ce script de connexion a été affecté le déploiement sera accomplie. Les connexions ultérieures des utilisateurs seront accompagnées par le lancement vite du programme **avpdtup.exe** mais la réinstallation ne sera pas effectuée, c'est pourquoi il n'est pas nécessaire de supprimer cette ligne du script de connexion.

6.4.3. Lancement du déploiement à l'aide du mode ordinateur à ordinateur

Pour effectuer le déploiement à l'aide du mode **ordinateur à ordinateur** sélectionnez correspondante dans le groupe d'options dans la partie supérieure de l'onglet **Déploiement**. L'onglet **Déploiement** prendra l'aspect représenté par l'Illustration 40.

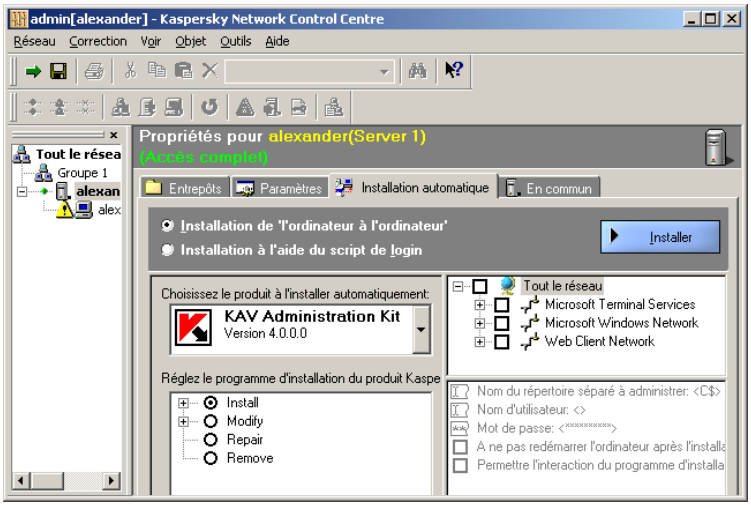

Illustration 40. Déploiement sur ordinateur

Cette méthode d'installation est permise seulement quand le serveur, le poste de travail et le poste de travail de l'administrateur fonctionnent avec les systèmes d'exploitation MS Windows NT: Windows NT 4 Server, Windows NT 4 Workstation, Windows 2000 Server ou Windows 2000 Professional, Windows XP. Si le poste de travail de l'administrateur est géré par un autre système de Windows ce bouton de choix sera inaccessible.

Le déploiement effectué par la méthode **ordinateur à ordinateur** diffère de l'installation à partir du script de connexion décrite précédemment.

En cas d'installation par la méthode ***de l'ordinateur à l'ordinateur*** *:*

1. Dans l'arborescence du réseau (se trouvant à droite dans l'onglet) où sont reflétés tous les ordinateurs du réseau local donné, cochez le champ près des ordinateurs où l'installation sera effectuée (si parmi les ordinateurs choisis il y en aura ceux qui fonctionnent sous MS Windows 95/98/Me, l'installation sera omise pour ces ordinateurs).
2. Au cas où l'ordinateur souhaité n'est pas présent dans l'arborescence, y ajoutez-le manuellement. Pour ce faire choisissez dans le menu contextuel de l'objet **Microsoft Windows Network** l'option **Ajouter un ordinateur** (voir: Illustration 41) et indiquez le

nom de l'ordinateur à ajouter dans le champ de la fenêtre qui se présente.

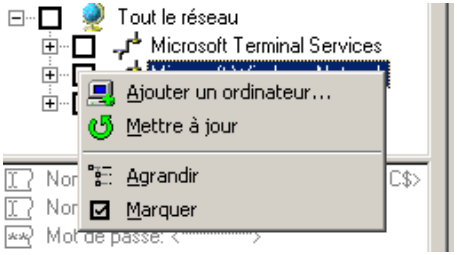

Illustration 41. Ajouter un ordinateur à l'arborescence du réseau

3. Si cela est nécessaire on peut connaître la composition des produits de Kaspersky Anti-Virus® et de leurs composants individuels qui sont déjà installés sur un ordinateur, mais il faut avoir le droit de l'administrateur pour l'ordinateur indiqué. Pour ce faire, dans le menu contextuel de cet ordinateur sélectionnez **Détails**. Une fenêtre s'ouvrira contenant la liste des produits installés dans la partie supérieure et la liste des composants installés dans la partie inférieure (voir: Illustration 42).

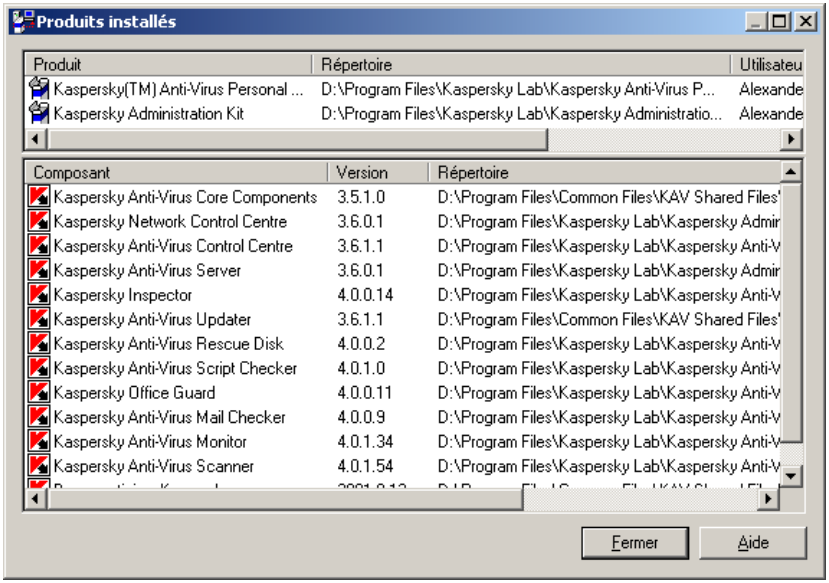

Illustration 42. Information sur produits et composants installés

4. Dans la barre qui se trouve sous l'arborescence du réseau indiquez les paramètres d'installation pour les ordinateurs :

   - **Nom du partage disque administrateur** une ressource séparable de l'ordinateur où le distributif du produit-programme sera copié pour son installation ultérieure. La ressource séparable dissimulée **C$** est utilisée par défaut.

   - **Nom d'utilisateur** et **Mot de passe** – nom de l'utilisateur ayant les droits de l'administrateur sur l'ordinateur et son mot de passe. Si ces paramètres ne sont pas indiqués le nom et le mot de passe sous lesquels vous avez entré le système seront utilisés.

L'accès à la ressource dissimulée C$ du système n'est autorisé qu'aux membres du groupe **Administrateurs**. Si vous ne possédez pas de droits pareils sur l'ordinateur où est effectuée l'installation la procédure n'aura pas de succès.

   - **Ne pas redémarrer l'ordinateur après l'installation** est un paramètre permettant d'activer ou de désactiver le mode du démarrage de l'ordinateur après que le produit-programme y soit installé. Le logiciel installé ne fonctionnera correctement qu'après le redémarrage.

   - **Permettre l'interaction du programme d'installation avec le Bureau** - le champ est coché la procédure d'installation va interagir avec le Bureau de l'ordinateur où l'installation est en train de se produire.

5. Indiquez les paramètres du programme installateur (ils sont analogues de ceux décrits dessus). L'onglet prendra l'aspect représenté par l'Illustration 43.

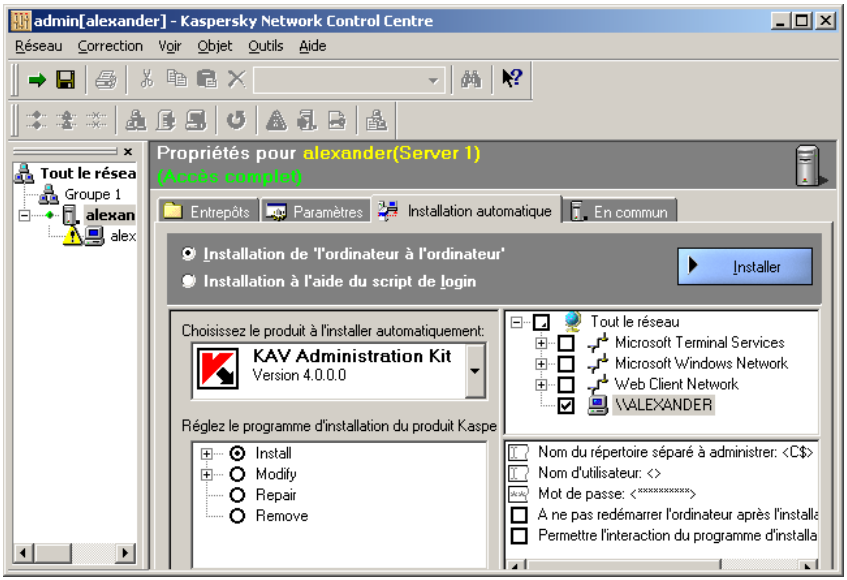

Illustration 43. Réglages de l'utilitaire de déploiement

6. Cliquez sur **Déployer**.

7. La boîte de sélection de la langue du progiciel à installer apparaît (voir: Illustration 44). Choisissez dans la liste qui se présente le langue du produit et cliquez sur **OK**.

Illustration 44. Sélection du langage du produit

8. La procédure d'installation du produit sur les postes de travail choisis commence. Les étapes de cette procédure sont représentées dans la fenêtre spéciale (voir: Illustration 45).

Si un redémarrage est nécessaire après une installation distante du correctif, le message correspondant est affiché sur l'ordinateur distant.

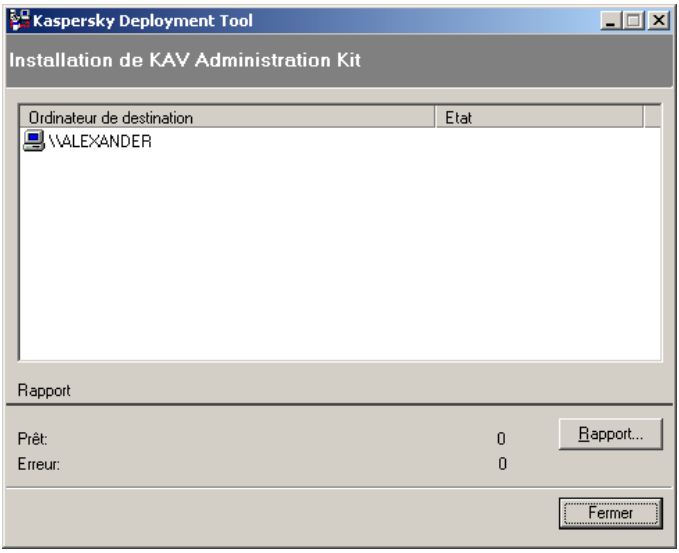

Illustration 45. Étapes de déploiement

9. À la fin de l'installation vous pouvez vous familiariser avec le rapport détaillé des étapes de l'installation. Pour ce faire, cliquez sur **Détails**. La fenêtre du rapport s'ouvrira (voir: Illustration 46).

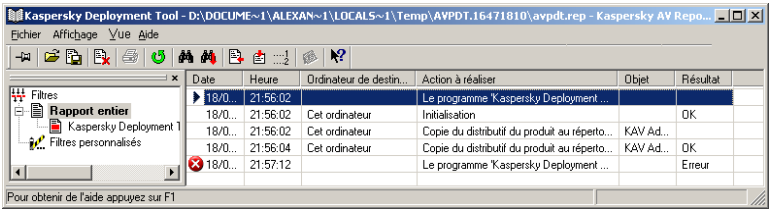

Illustration 46. Rapport de déploiement

6.5. Ajout de nouveaux objets au réseau logique

L'ajout de nouveaux objets au réseau logique est effectué selon les mêmes principes que la création du réseau logique :

- Ajout des groupes est décrit au paragraphe 6.1.
- Ajout des serveurs est décrit au paragraphe 6.2.
- Ajout des postes de travail est décrit au paragraphe 6.3. Le logiciel Kaspersky Anti-Virus® peut être installé sur les postes de travail qui sont à ajouter au réseau, à l'aide des programmes d'installation de ce logiciel ou par déploiement (voir le paragraphe 6.3).

6.6. Déplacement et suppression des objets du réseau logique

Vous pouvez déplacer et supprimer les serveurs, les postes de travail et les groupes du réseau logique.

Pour ce faire on peut utiliser le clavier, le menu, les boutons dans la barre d'outils et la souris. Pour déplacer les objets du réseau logique adhérez aux principes qui suivent :

- tout serveur peut être déplacé dans tout groupe ;
- tout poste de travail peut être déplacé et ajouté à tout serveur ;
- tout groupe peut être déplacé dans tout groupe à l'exception des groupes faisant partie du groupe qui est en train d'être déplacé ;
- si un objet est déplacé ou supprimé, ceci est de même pour tous les objets qui en font partie. Par exemple, si vous êtes en train de déplacer un serveur auquel des postes de travail sont ajoutés il sera déplacé avec tous ses postes de travail.

Pour déplacer un serveur (un poste de travail, un groupe)

1. Dans la liste des objets du réseau sélectionnez le serveur (le poste de travail, le groupe) que vous voulez déplacer.
2. Dans le menu **Edition** sélectionnez **Couper** ou cliquez sur  dans la barre (standard) d'outils.

   `<Ctrl>+<X>`
3. Dans la liste des objets du réseau sélectionnez le groupe (serveur, groupe) où vous avez l'intention de déplacer l'objet choisi.
4. Dans le menu **Edition** sélectionnez **Coller** ou cliquez sur  dans la barre (standard) d'outils.

<Ctrl>+<V>

Pour supprimer un objet du réseau logique

1. Dans la liste des objets du réseau sélectionnez celui que vous voulez supprimer.
2. Dans le menu **Edition** sélectionnez **Supprimer** ou cliquez sur  dans la barre (standard) d'outils.

   <Del>

L'opération de copie (option **Copier** du menu **Edition**, bouton  de la barre standard d'outils, ou le raccourci clavier **<Ctrl>+<C>**) sert à copier les paramètres du progiciel Kaspersky Anti-Virus® d'un poste de travail à l'autre (voir le paragraphe 7.1.1).

6.7. Recherche et changement de noms des objets du réseau logique

Pour trouver un objet du réseau logique

1. Dans le menu **Edition** sélectionnez **Rechercher** ou cliquez sur  dans la barre (standard) d'outils.

   <Ctrl>+<F>
2. Dans la fenêtre **Rechercher un objet réseau** qui s'ouvre (Illustration 47) dans le groupe des boutons de choix indiquez le type de l'objet qu'il faut trouver: **Tous**, **Groupe**, **Serveur**, **Poste de Travail**.
3. Dans la zone **Nom d'objet** entrez la ligne qui est présente dans le nom de l'objet à trouver.
4. Si cela est nécessaire dans la zone **Adresse d'objet** entrez la ligne qui est présente dans l'adresse de l'objet recherché. Si le champ du nom et le champ de l'adresse de l'objet sont tous les deux remplis le masque finale de recherche sera obtenue par la multiplication logique.
5. Cliquez sur **Suivant**.

Illustration 47. Rechercher un objet réseau

Après cela dans la liste des objets du réseau logique le premier objet trouvé qui puisse satisfaire les paramètres de la recherche sera identifié comme objet actuel. Pour passer à l'objet suivant cliquez encore une fois sur le bouton **Suivant**. Pour fermer la fenêtre **Rechercher un objet réseau**, cliquez sur **Annuler**.

Pour la recherche rapide de l'objet par son nom utilisez la liste déroulante dans la barre d'outils. Entrez la ligne faisant partie du nom de l'objet recherché dans la liste déroulante et cliquez sur **<ENTREE>**.

Pour renommer un objet du réseau logique

1. Dans la liste des objets du réseau sélectionnez celui que vous voulez renommer.
2. Dans le menu **Edition** ou bien dans le menu contextuel de l'objet sélectionnez **Renommer**.

CHAPTER 7. CONFIGURATION DU RESEAU LOGIQUE

7.1. Propriétés générales de configuration des postes de travail

7.1.1. Copie des paramètres du progiciel Kaspersky Anti-Virus® d'un poste de travail à l'autre

On peut copier les paramètres du progiciel Kaspersky Anti-Virus® d'un poste de travail à l'autre.

Pour copier les paramètres du progiciel Kaspersky Anti-Virus® d'un poste de travail à l'autre

1. Dans la liste des objets du réseau sélectionnez le poste de travail dont les paramètres vous voulez copier.
2. Dans le menu **Edition** sélectionnez **Copier** ou cliquez sur  dans la barre d'outils.

   `<Ctrl>+<?>`
3. Dans la liste des objets du réseau sélectionnez le poste de travail dont les paramètres vous voulez indiquer lors de la procédure de copie.
4. Dans le menu **Edition** sélectionnez **Coller** ou cliquez sur  dans la barre d'outils.

   `<Ctrl>+<V>`

Ensuite les paramètres du progiciel Kaspersky Anti-Virus® du poste de travail-source seront copiés sur le poste de travail-récepteur.

*Pour enregistrer les modifications cliquez sur **Appliquer** dans la zone de description des propriétés du poste de travail-récepteur.*

7.1.2. Mode hors-ligne. Configuration différée

Les réglages du poste de travail au réseau du Kaspersky Anti-Virus® sont sauvegardés sur le poste de travail aussi bien qu'au serveur auquel ce poste de travail est affecté. Normalement ces exemples des paramètres sont les mêmes. Pourtant les intervalles de temps se trouvent possibles où un poste de travail est inaccessible pour l'administrateur (désactivé par exemple, exclu du réseau local, appartient au segment qui est temporairement non relié au réseau local ou Kaspersky AV Control Centre est incapable de fonctionner sur le poste de travail). En de cas pareils on dit que le poste de travail se trouve en *mode hors-ligne*.En ce cas il est possible de voir les paramètres et de les éditer mais les modifications réelles sont saisies dans la copie des paramètres sauvegardée au serveur auquel le poste de travail est associé.

Si le poste de travail fonctionne toujours, alors les programmes du progiciel Kaspersky Anti-Virus® continuent à utiliser les paramètres anciens sauvegardés sur le poste même.

Quand le poste de travail redevient accessible (c'est à dire, au premier redémarrage de Kaspersky AV Control Centre sur le poste de travail, qui est accompagné de la connexion entre le serveur et le poste de travail), l'entrée réelle des modifications aux réglages utilisés par ce poste de travail aura lieu.

Sur l'Illustration 48 est choisi un poste de travail, qui se trouve en mode hors-ligne ; et le message **Mode hors-ligne – Paramètres différés** nous en avertit dans le domaine des propriétés de l'objet.

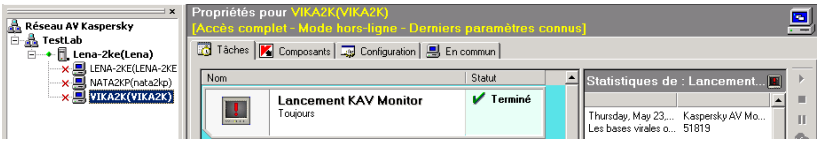

Illustration 48. Paramètres différés d'un poste de travail

7.2. Configuration d'envoi des alertes et des messages électroniques issus des postes de travail et des serveurs

7.2.1. Alertes émises par les postes de travail et leur importance

Après l'ajout d'un serveur au réseau logique nous recommandons d'indiquer le moyen de traitement des alertes. Les alertes sont émises par des tâches fonctionnant sur les postes de travail associés au serveur3. La tâche du type **Kaspersky AV Scanner** par exemple générera l'avertissement **Objet infecté trouvé** à la détection de virus sur un poste de travail, et la tâche du type **Kaspersky AV Updater** en cas de tentative infructueuse de mise à jour des bases antivirales générera l'alerte **Une erreur a eu lieu pendant la procédure de mise à jour**. Les tâches de Kaspersky Anti-Virus® qui sont à accomplir sur les postes de travail renvoient les alertes au serveur, qui à son tour les renvoie aux adresses électroniques qui lui sont indiquées.

Vous devez activer le mode d'envoi des alertes via le serveur à tous les postes de travail se trouvant sous votre gestion. Pour cela il faut indiquer le mode d'envoi des alertes via le serveur parmi les paramètres pour le poste de travail (voir le paragraphe 7.2.2).

Une liste complète d'alertes qui sont envoyées par les composants du paquet Kaspersky Anti-Virus® est jointe à la documentation pour l'utilisateur de ces composants. Lors de configuration du réseau logique, à l'aide du logiciel Kaspersky AV Control Centre, l'administrateur peut activer ou désactiver le renvoi des alertes diverses d'un poste de travail (voir la documentation de " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur ").

Par exemple, Kaspersky AV Scanner est un composant du progiciel de Kaspersky Anti-Virus® et il est capable d'envoyer sept types d'alertes (voir: Illustration 49).

3 Dans cette version chaque composant du package Kaspersky Anti-Virus® peut envoyer seulement un nombre prédéterminé d'alertes.

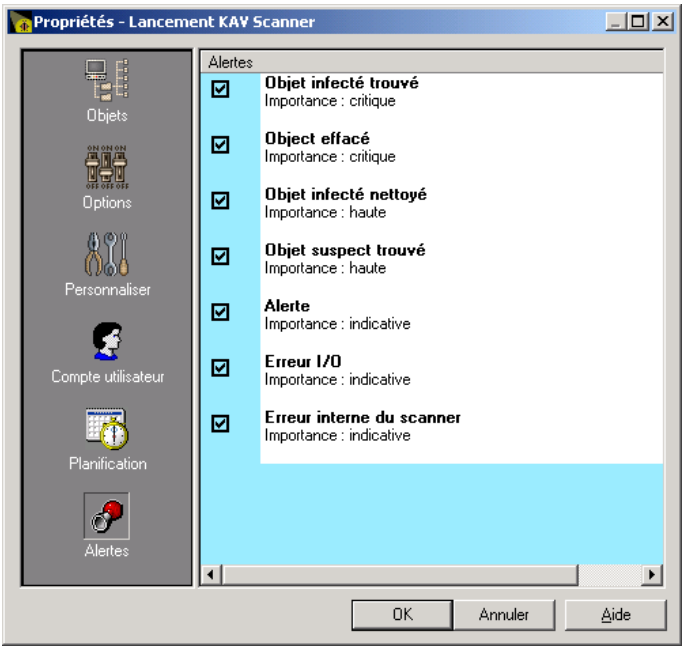

Illustration 49. Alertes envoyées par le logiciel Kaspersky AV Scanner

Le serveur regroupe les alertes reçues selon leur *importance* et il les envoie également, si cela est indiqué par les paramètres, des alertes de plusieurs niveaux d'importance aux adresses électroniques différentes. Sont prévus les niveaux d'importance suivants pour les alertes envoyées au serveur par les tâches de Kaspersky Anti-Virus® : **indicative** – les alertes visant à informer, **bas** – alertes importantes, **haut –** alertes plus importantes, **critique** – alertes les plus importantes. Ainsi, les alertes **Objet infecté trouvé** et **Objet effacé** générées par le logiciel Kaspersky AV Scanner ont le niveau d'importance **critique** .

7.2.2. Activation du mode d'envoi des alertes par un poste de travail via le serveur

Pour activer le mode d'envoi des alertes par un poste de travail via le serveur :

1. Choisissez ce poste de travail dans la liste des objets du réseau logique.

2. Dans la zone d'édition des attributs d'objet ouvrez l'onglet **Configuration** et cliquez sur **Alertes**.

3. Dans l'arborescence des paramètres qui apparaît (voir: Illustration 50) choisissez **Traiter les alertes via Kaspersky AV Server** dans le groupe d'options.

4. S'il est nécessaire de limiter le nombre des alertes émises par une seule tâche cochez la case **Maximum d'alertes pour une simple tâche** et indiquez le nombre imposant cette limite dans le champ qui apparaît.

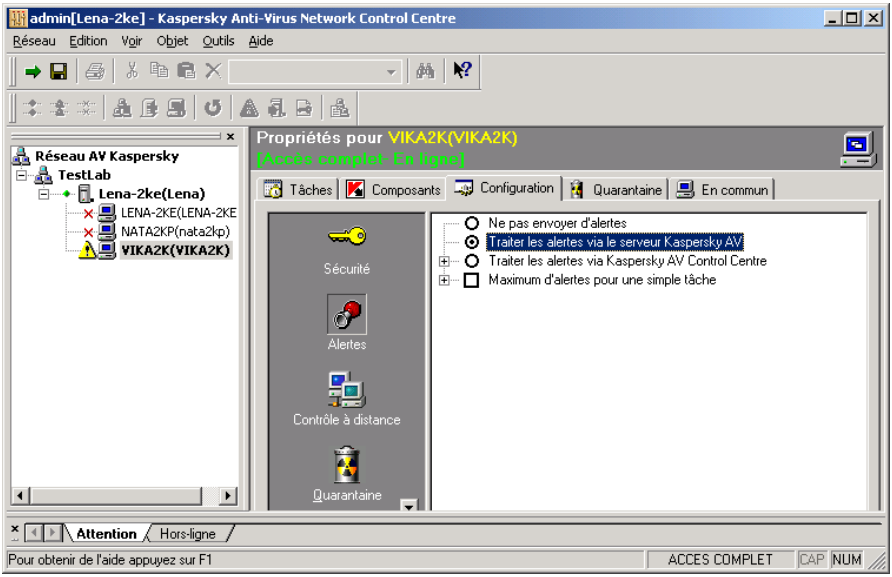

Illustration 50. Autorisation d'envoi des alertes via le serveur

7.2.3. Envoi d'alertes en accord avec leur importance

Le traitement ultérieur des alertes et en particulier leur renvoi, selon le niveau d'importance, aux plusieurs adresses, est la responsabilité du serveur du réseau logique auquel les postes de travail correspondant sont associés.

Pour définir les paramètres d'envoi des alertes par courrier électronique

1. Dans la liste des objets du réseau logique choisissez le serveur qu'on est en train de régler.
2. Dans la zone d'édition des attributs du serveur ouvrez dans l'onglet **Options** et cliquez sur **Renvoi des alertes**. Une arborescence des paramètres d'envoi des alertes en fonction de leur importance s'ouvrira (voir: Illustration 51).

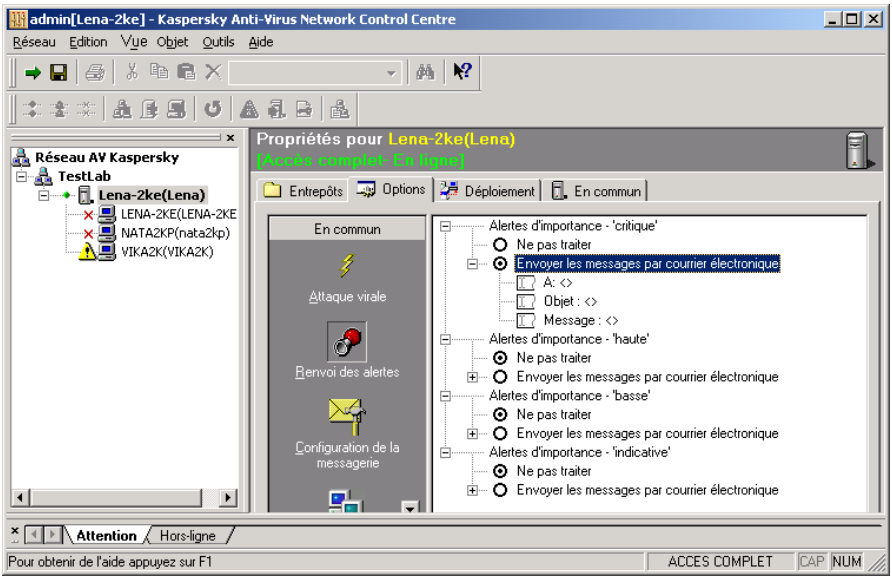

Illustration 51. Définition des paramètres d'envoi des alertes par courrier électronique

L'arborescence de classification des alertes en fonction de leur importance occupe la partie principale de l'onglet, et pour chaque niveau le moyen de traitement des alertes est spécifié (voir: Illustration 52).

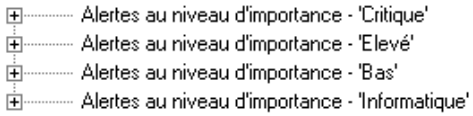

Illustration 52. Arborescence de classification des alertes, les sections correspondant aux niveaux d'importance sont réduites

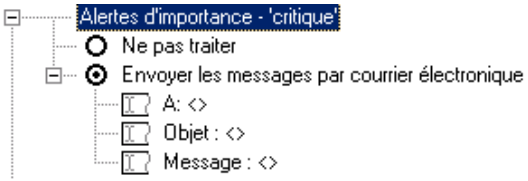

Illustration 53. Section **Alertes au importance…**

Dans chaque section intitulée **Alertes d'importance...** le moyen de traitement des alertes ayant le niveau correspondant d'importance est spécifié (voir: Illustration 53).

Vous pouvez choisir un des deux moyens suivants de traitement des alertes :

Ne pas traiter	Ne pas traiter les alertes au importance choisi.
Envoyer les messages par courrier électronique	Envoyer les alertes au importance choisi par courrier électronique. Si vous avez choisi ce moyen de traitement veuillez indiquer les paramètres suivants :
A:	Adresse de courrier électronique du destinataire des alertes.
Objet :	Objet du message électronique.
Message :	Texte du message électronique.

7.2.4. Envoi des messages en cas d'attaque virale

La détection des virus ayant lieu pendant une période temporelle courte sur plusieurs ordinateurs du réseau local témoigne, avec une grande probabilité, d'un type spécifique d'infection virale - une *attaque virale visant au réseau* (autrement dit, on peut supposer que le virus est en train de se répandre actuellement dans le réseau).

Ce type d'infection demande une réaction immédiate de l'administrateur en vue de quoi une procédure spéciale d'alerte d'infection est prévue.

Pour régler la réaction à une attaque virale visant au réseau (infection pendant une période temporelle courte sur plusieurs ordinateurs associés à un seul serveur):

1. Dans la liste des objets du réseau logique choisissez le serveur souhaité.
2. Dans la zone d'édition des attributs d'objet ouvrez l'onglet **Options** et cliquez sur **Attaque virale**.
3. Dans l'arborescence qui apparaît (voir: Illustration 54) réglez les critères qui vous permettront de considérer cette situation en tant qu'attaque virale visant au réseau (voir le paragraphe 7.2.4.1) et réglez également la façon d'y réagir (voir le paragraphe 7.2.4.2).

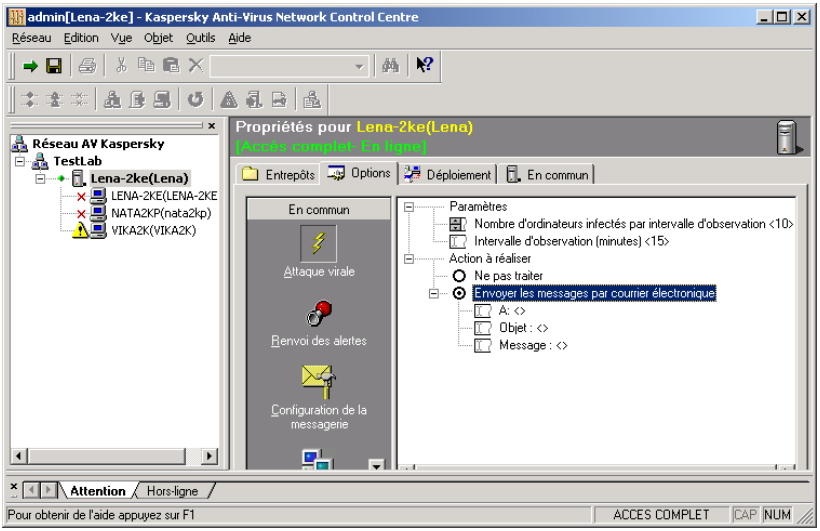

Illustration 54. Configuration de réaction à l'attaque virale

7.2.4.1. Configuration des critères de détection de l'attaque virale

Agrandissez si vous en avez besoin la ramification **Paramètres** (voir: Illustration 54). La situation de l'attaque virale visant au réseau est vue comme atteinte (excès) d'un certain nombre d'ordinateurs infectés détectés pour une période temporelle définie.

Pour définir une période temporelle cliquez sur l'élément **Intervalle d'observation** puis entrez dans le champ qui apparaît une valeur de longueur d'une période (15 minutes par défaut).

Pour définir un nombre d'ordinateurs infectés cliquez sur l'élément **Nombre d'ordinateurs infectés pour intervalle d'observation** puis entrez dans le champ qui apparaît le nombre nécessaire (10 par défaut).

7.2.4.2. Configuration d'alerte de l'attaque virale

Si vous ne supposez pas envoyer les messages sur l'attaque virale visant au réseau, choisissez la réaction **Ne pas traiter** dans le groupe d'options **Action** (voir: Illustration 54). Sinon choisissez la réaction **Envoyer les messages par courrier électronique**.

Au dernier cas il est également nécessaire de régler les paramètres des messages à envoyer. Pour ce faire cliquez sur les éléments de la ramification portant le même nom (les ayant développés si nécessaire) et indiquez l'adresse à laquelle il faut envoyer le message dans le champ **A:** qui apparaît. Si cela est nécessaire entrez l'objet du message dans le champ **Objet :** et entrez le message dans le champ **Message :** (si l'on laisse vides ces champs ils seront remplis par défaut ; dans la plupart des cas cette variante est préférable).

7.2.5. Configuration du service de messagerie

Pour régler les paramètres du courrier (indication du destinataire du message, la sélection du type et de configuration du service choisi) pour les messages issus du serveur, choisissez le serveur dans la liste des objets du réseau logique, cliquez sur **Paramètres du courrier** dans l'onglet **Paramètres**. Une arborescence des paramètres du courrier s'ouvrira contenant le paramètre **Du** et la section **Services du courrier** où il faudra indiquer les paramètres du système de messagerie reliés à la façon d'envoi des avertissements (voir: Illustration 55).

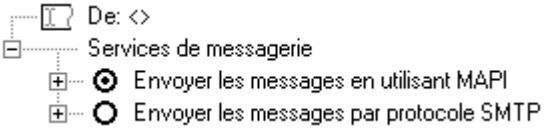

Illustration 55. Configuration des paramètres du courrier

Il existe deux procédés d'envoi des messages électroniques :

- avec utilisation de MAPI (voir le paragraphe 7.2.5.1 pour les détails),
- avec utilisation de SMTP (voir le paragraphe 7.2.5.2 pour les détails).

De : La ligne qui s'affichera dans le champ **De** du message électronique. Ce paramètre est obligatoire lors du travail avec certains serveurs SMTP et est utilisé pour identifier l'utilisateur.

Voir les détails sur les types de messages électroniques issus du serveur au paragraphe 9.6.

7.2.5.1. Paramètres d'envoi des messages avec MAPI

Le logiciel Kaspersky AV Server permet de régler l'envoi des messages avec MAPI, si Windows 9x est installé sur l'ordinateur (voir: Illustration 56).

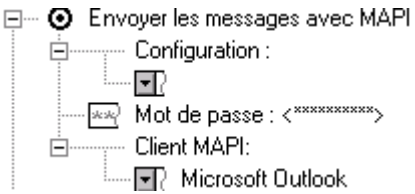

Illustration 56. Paramètres de configuration de MAPI

Pour régler les paramètres du protocole MAPI, sélectionnez l'option **Envoyer un e-mail avec MAPI**, entrez ensuite les valeurs des paramètres suivants :

Configuration nom du profil (du fichier de réglages) du client MAPI;

Mot de passe mot de passe pour l'accès au profil ;

Client MAPI nom du client MAPI qui sera utilisé pour l'envoi des messages d'information.

Tous les clients MAPI n'utilisent pas de profils c'est pourquoi pour certains d'entre eux les champs **Configuration** et **Mot de passe de configuration** doivent rester vides.

7.2.5.2. Paramètres d'envoi des messages avec SMTP

Pour l'envoi des messages d'information par SMTP, il est nécessaire d'activer le bouton **Envoyer un e-mail en utilisant le protocole SMTP** et de saisir ensuite les paramètres de configuration de SMTP (voir: Illustration 57).

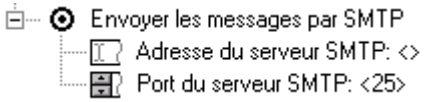

Illustration 57. Paramètres de configuration de SMTP

Adresse du serveur SMTP Adresse du serveur de type SMTP. Il est possible d'utiliser sinon une adresse IP numérique (par exemple 125.5.29.1), sinon un nom de domaine complètement défini (test.mail.ru par exemple), sinon le nom d'ordinateur au réseau Microsoft (par exemple test).

Port du serveur SMTP Numéro du serveur de type SMTP. La valeur par défaut est égale à 25.

7.3. Configuration de gestion à distance pour les serveurs et les postes de travail

7.3.1. Paramètres d'administration à distance

Vous pouvez spécifier pour chaque serveur et chaque poste de travail les paramètres d'administration à distance : les paramètres de sécurité du programme, les numéros des ports utilisés et les paramètres de questionnement des postes de travail. Dessous est décrit la configuration de ces paramètres pour les serveurs, certaines différences pour les postes de travail sont fournies au paragraphe 7.3.4.

Pour spécifier les paramètres d'administration à distance

1. Dans la liste des objets du réseau logique choisissez le serveur qu'on est en train de régler.
2. Dans la zone d'édition des attributs du serveur ouvrez dans l'onglet **Options** et cliquez sur **Contrôle à distance**. La fenêtre d'arborescence s'ouvrira (voir: Illustration 58).

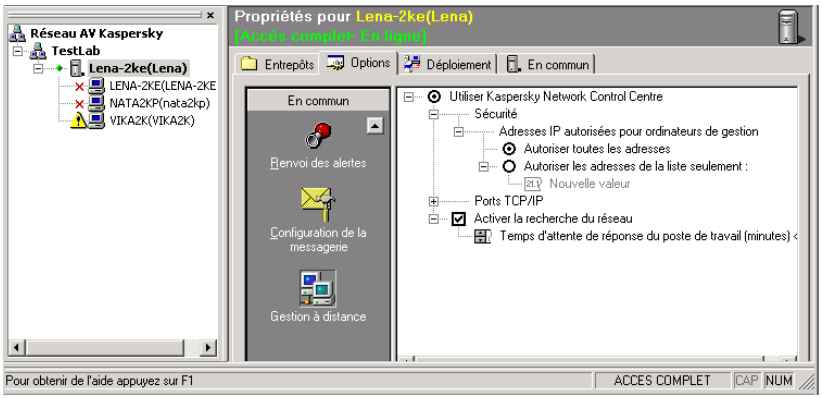

Illustration 58. Paramètres d'administration du serveur à distance

Dans l'arborescence de l'onglet **Options** dans la zone des attributs du serveur se trouvent les sections suivantes :

Sécurité — Configuration de sécurité du travail au réseau en cas de gestion à distance du progiciel Kaspersky Anti-Virus® (voir les détails au paragraphe 7.3.2);

Ports TCP/IP — entrée des numéros des ports (TCP et UDP), utilisés pour gestion des composants du progiciel (voir les détails au 7.2.2);

Activer la recherche du réseau — Configuration des paramètres de questionnement des postes de travail (voir les détails au paragraphe 7.3.3).

7.3.2. Configuration de sécurité en cas d'administration à distance

La configuration de sécurité en cas d'administration à distance permet de limiter le nombre d'ordinateurs ayant l'accès au serveur.

Illustration 59. Configuration de sécurité pour la connexion à distance

La ramification de l'arborescence **Sécurité** (voir: Illustration 59) contient les options qui suivent :

Autoriser toutes les adresses — autoriser tous les ordinateurs du réseau d'effectuer la gestion du serveur à distance ;

Autoriser les adresses de la liste seulement — autoriser la gestion à distance seulement aux ordinateurs dont les adresses IP numériques sont énumérées dessous (la présence des adresses IP permanentes pour les ordinateurs est requise).

Nous recommandons d'autoriser la gestion à distance effectuée uniquement des ordinateurs des administrateurs. Pour ce faire il est nécessaire d'inclure l'option

Autoriser les adresses de la liste seulement et d'ajouter ensuite à la liste les adresses IP des ordinateurs des administrateurs.

7.3.3. Configuration de la recherche du réseau

Les paramètres de la recherche du réseau par le serveur se trouvent dans la section **Activer la recherche du réseau** (voir: Illustration 60). Ces paramètres définissent si le serveur va montrer au clic sur le bouton  la liste des postes de travail où fonctionne le logiciel Kaspersky AV Control Centre en cas d'ajout des postes de travail dans la boîte de dialogue **Ajouter un poste de travail** (voir le paragraphe 6.3).

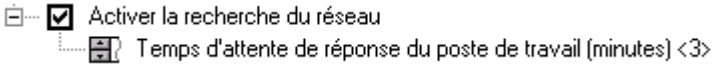

Illustration 60. Configuration des paramètres de la recherche du réseau

Activer la recherche du réseau	Rechercher le réseau pour former la liste des postes de travail.
Temps d'attente de réponse du poste de travail (minutes).	Le temps pendant lequel le serveur doit attendre la réponse des postes de travail.

7.3.4. Particularités de la configuration du contrôle à distance pour les postes de travail

Les paramètres de gestion à distance pour les postes de travail sont réglés dans l'onglet **Configuration** dans la zone des attributs de l'objet. En cliquant sur **Contrôle à distance** s'ouvre une arborescence des paramètres (voir: Illustration 61), qui est pareille à celle du serveur décrite précédemment.

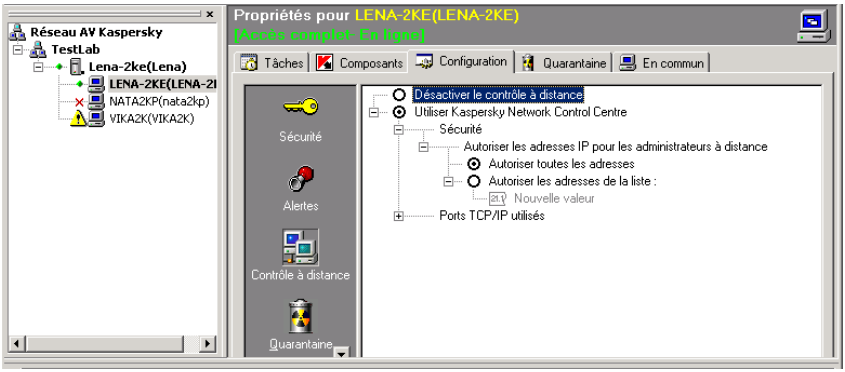

Illustration 61. Configuration de gestion à distance pour les postes de travail

Pourtant, la configuration de gestion à distance pour les postes de travail a de certaines particularités :

- Au niveau supérieur de l'arborescence une possibilité est fournie de sélectionner l'option **Désactiver le contrôle à distance**. En ce cas toute la responsabilité pour la gestion du poste de travail est placée sur l'utilisateur. Il faut en user avec de grandes précautions.
- La ramification **Activer la recherche du réseau** est absente (cette fonction est spécifique au serveur).

7.4. Configuration de la mise à jour automatique des bases antivirales sur les postes de travail

Nous recommandons de mettre à jour régulièrement les bases antivirales du progiciel Kaspersky Anti-Virus® sur les postes de travail. Le moyen optimal de ce type est *la mise à jour automatique* des bases antivirales de l'entrepôt des mises à jour du serveur. Cette procédure permet d'éliminer le risque d'affaiblissement de la protection antivirale causé par la mise à jour tardée des bases sur un poste de travail. En cas de création du réseau logique l'administrateur doit régler la procédure de mise à jour automatique des bases et programmes antiviraux de Kaspersky Anti-Virus® sur les postes de travail de l'entrepôt des bases antivirales et du celui des mises à jour des serveurs. Cette procédure est décrite en détail au paragraphe 7.4.1.

Les entrepôts des serveurs peuvent être mis à jour via l'Internet ou via l'entrepôt d'un autre serveur qui est mis à jour via l'Internet, en fonction de la complexité du réseau logique (voir le paragraphe 7.4.2).

7.4.1. La mise à jour des bases antivirales sur les postes de travail via Kaspersky AV Server

Pour régler la mise à jour automatique des bases antivirales sur les postes de travail via le serveur il faut :

1. Inclure la tâche de mise à jour automatique dans la liste des tâches du poste de travail. Pour ce faire choisissez le poste de travail souhaité dans la liste des objets du réseau logique, dans la zone d'édition des attributs d'objet ouvrez l'onglet **Tâches** et cliquez sur  se trouvant à droite dans l'onglet. Une fenêtre d'assistant de la création d'une nouvelle tâche s'ouvrira (voir: Illustration 62).

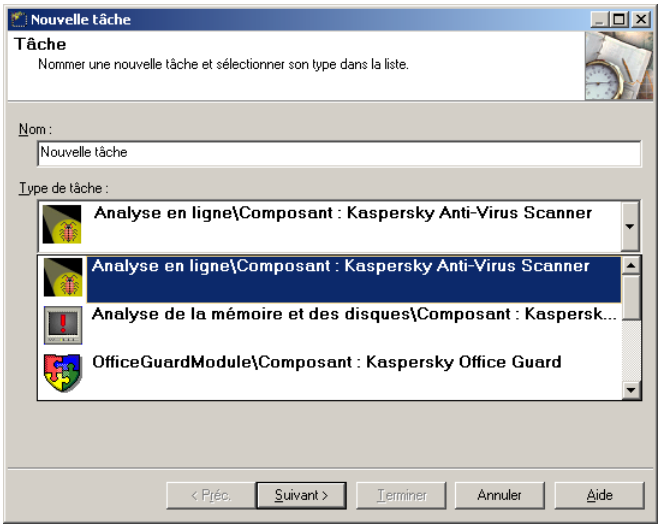

Illustration 62. Assistant de la création d'une nouvelle tâche

2. Dans la zone **Nom** indiquez le nom de la tâche de mise à jour automatique et choisissez cette tâche dans liste déroutante **Type de tâche** et cliquez ensuite sur le bouton **Suivant**.

3. Dans la zone **Horaire** (voir: Illustration 63) réglez l'horaire du lancement automatique de la tâche.

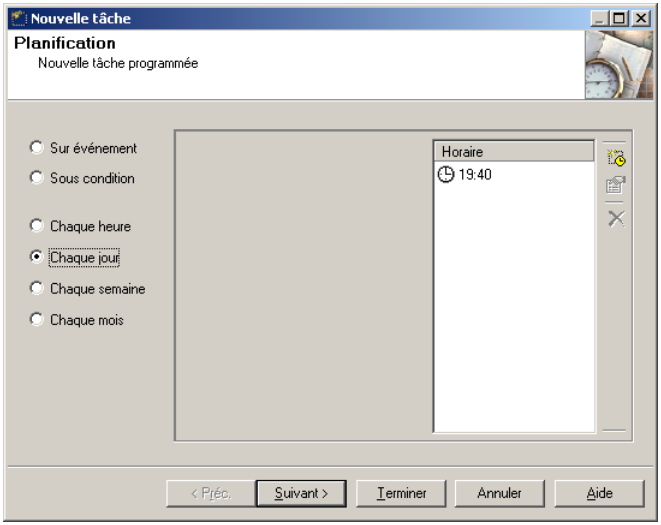

Illustration 63. Planification, Nouvelle tâche

Nous recommandons les paramètres suivants pour la tâche de mise à jour automatique : sélectionnez l'option **Chaque jour**, puis cliquez sur le bouton  dans la partie droite de la fenêtre. La fenêtre **Ajouter un horaire** s'ouvrira (voir: Illustration 64).

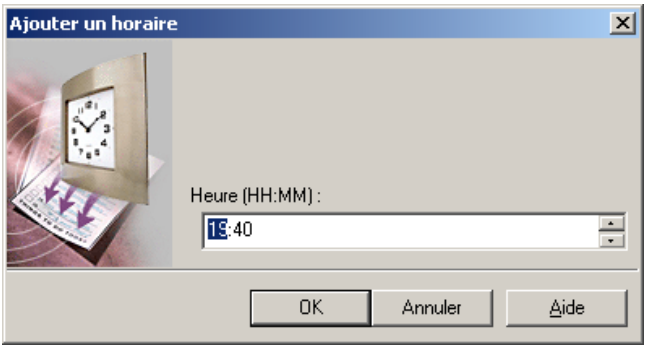

Illustration 64. Ajouter un horaire

Entrez l'heure du lancement quotidien de la tâche dans la zone de saisie **Heure**.

De retour dans la fenêtre **Horaire** cliquez sur **Suivant** (la configuration de l'horaire du lancement automatique est décrite en détail au paragraphe 7.6).

4. La fenêtre **Avertissement** où sont réglés les avertissements issus d'une tâche. Conservez les paramètres par défaut et cliquez sur **Suivant**.

5. La fenêtre **Connexion** s'ouvrira (voir: Illustration 65). Sélectionnez l'option **Mise à jour de Kaspersky® via Internet** et cochez les cases **Mise à jour des bases antivirales** et **Mise à jour des exécutables**.

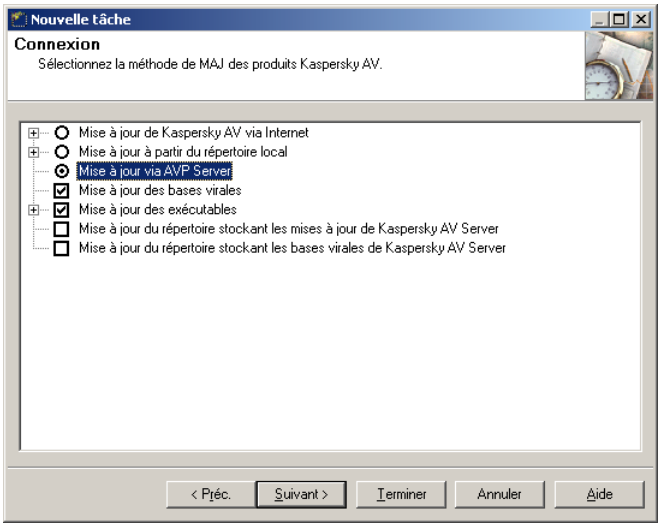

Illustration 65. Sélectionnez la méthode de MAJ des produits Kaspersky AV

Cliquez sur **Terminer** pour terminer la procédure de configuration ou bien sur **Suivant** pour régler les paramètres du rapport créé par le programme dans la fenêtre suivante.

La description détaillée d'ajout et de configuration d'une nouvelle tâche est fournie par la description du logiciel Kaspersky AV Control Centre dans la documentation de " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur".

Si la tâche de mise à jour est déjà installée sur un poste de travail, choisissez-la dans la liste des tâches dans l'onglet **Tâches** et cliquez sur  se trouvant à droite dans l'onglet (ou bien sélectionnez **Propriétés** dans le menu contextuel des tâches). Une fenêtre **Propriétés…** s'ouvrira dont les onglets correspondent

aux fenêtres d'assistant d'installation portant les mêmes noms qui ont été décrites dessus. Ouvrez l'onglet **Connexion** de cette fenêtre (voir: Illustration 67) et sélectionnez **Mise à jour via AVP serveur** dans le groupe d'options.

7.4.2. Mise à jour du contenu d'entrepôt des bases antivirales du serveur via un autre serveur du réseau logique

Aux cas où plusieurs serveurs font partie du réseau logique il est utile de régler la réception automatique des mises à jour des bases antivirales issue d'un seul serveur. Une installation pareille simplifie l'administration du réseau et élimine le risque de ne pas mettre à jour en temps les entrepôts d'un des serveurs.

Il faut que les entrepôts du serveur **S0** soient mis à jour par l'Internet et que les serveurs **S1**, **S2** etc. soient mis à jour automatiquement via le serveur **S0**. Les réglages nécessaires sont décrits dessous.

Pour régler la réception des mises à jour du serveur S1 via le serveur S0:

1. Sur l'ordinateur où se trouve le serveur **S1**, installez le logiciel pour un poste de travail (pour cela il suffit d'installer les composants Kaspersky AV Control Centre et Kaspersky AV Updater, qui font partie du progiciel Kaspersky® Administration Kit) et assignez ce poste de travail au serveur **S0**, comme cela est décrit au paragraphe 6.3. Un exemple de construction pareille de réseau est reproduit dans l'Illustration 66(poste de travail ayant l'adresse **192.168.1.1**, qui se trouve sur le même ordinateur que le serveur **S1**, est affecté au serveur **S0**.

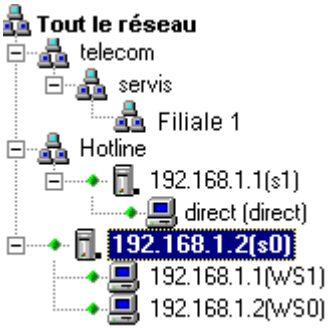

Illustration 66. Configuration du réseau pour mettre à jour les entrepôts du serveur

2. Sélectionnez ce poste de travail et comme cela a été décrit dessus au paragraphe 7.4.1, dans la fenêtre d'édition de la tâche de mise à jour automatique passez au feuillet **Connexion** (voir: Illustration 67).

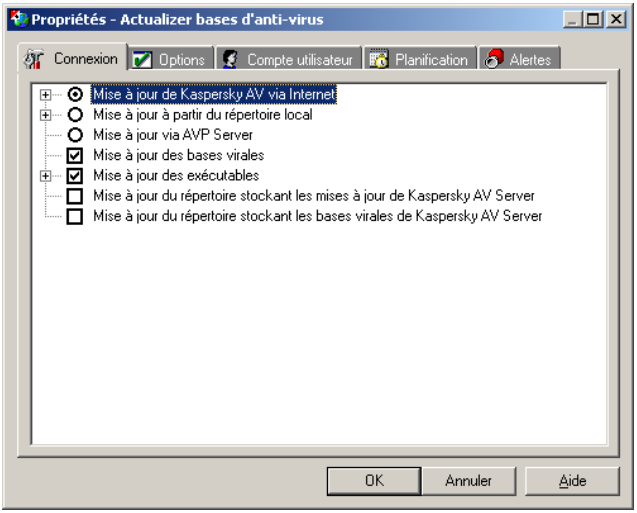

Illustration 67. Configuration de la mise à jour des entrepôts du serveur

3. Dans l'onglet indiqué cochez les cases **Mise à jour du répertoire stockant les mises à jour de Kaspersky AV serveur** et **Mise à jour du répertoire stockant les bases antivirales de Kaspersky AV Server**.

4. Sélectionnez l'option **Mise à jour via AVP serveur**.

Il est utile de régler l'horaire de la réception des mises à jour par le serveur d'une façon que l'accomplissement de la tâche de la réception des mises à jour pareilles finisse avant la réception des mises à jour par les postes de travail du serveur, en accord avec leur horaire.

Accomplissez les actions décrites dessus pour tous les serveurs recevant les mises à jour via le serveur **S0**.

Pour régler la réception des mises à jour par le serveur S0 via l'Internet :

1. Sur l'ordinateur où se trouve le serveur **S0**, le logiciel Kaspersky AV Control Centre doit être installé (pendant l'installation de Kaspersky AV Server celui-là est installé par défaut). Ajoutez-le au réseau et assignez-le au serveur **S0** (voir le paragraphe 6.4), si cela n'était

pas fait à l'avance (voir: Illustration 66, représentant la structure du réseau logique, là, c'est le poste de travail **WS0**).

2. Sélectionnez ce poste de travail et comme cela a été décrit dessus au paragraphe 7.4.1, dans la fenêtre d'édition de la tâche de mise à jour automatique passez au feuillet **Connexion** (voir: Illustration 68).

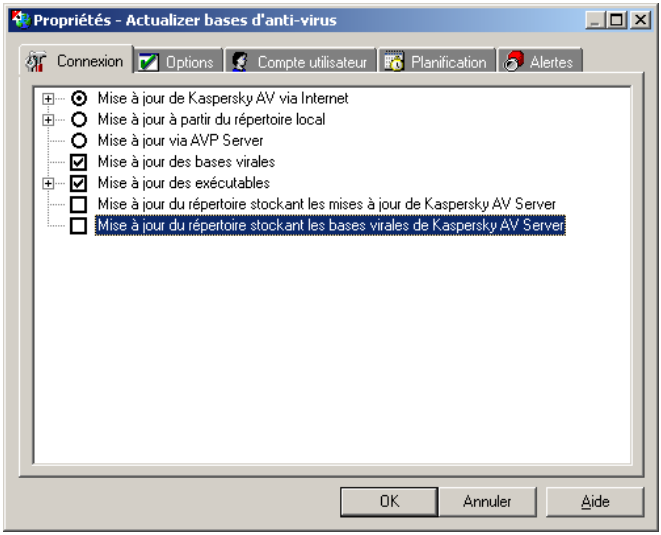

Illustration 68. Configuration de la mise à jour des entrepôts via l'Internet

3. Dans l'onglet indiqué cochez les cases **Mise à jour du répertoire stockant les mises à jour de Kaspersky AV Server** et **Mise à jour du répertoire stockant les bases virales de Kaspersky serveur AV Server**.

4. Sélectionnez l'option **Mise à jour de Kaspersky AV via l'Internet**.

7.5. Configuration et travail avec la quarantaine

7.5.1. Types de quarantaine

En tant qu'une possibilité de réaction possible les programmes antiviraux du progiciel Kaspersky Anti-Virus® permettent de mettre les fichiers en *quarantaine*

là où des fichiers infectés ont été détectés (voir les détails sur la quarantaine dans " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur ").

Pour que Kaspersky Anti-Virus® Scanner et Kaspersky Anti-Virus® Monitor puissent stocker un fichier dans cet entrepôt spécial, il est indispensable, dans l'onglet **Paramètres** de la boîte de dialogue des propriétés, de cocher la case **Utiliser la quarantaine**. Dans ce mode de travail le programme met les fichiers infectés en quarantaine, sans les supprimer du dossier où ils se trouvaient initialement. La suppression des fichiers infectés de l'ordinateur est effectuée par le programme si, en qualité d'actions sur les fichiers infectés, vous avez sélectionné dans les paramètres de Kaspersky Anti-Virus® Scanner et Kaspersky Anti-Virus® Monitor l'option **Supprimer**.

Les fichiers mis en quarantaine sont stockés sous une forme codée, ce qui garantit :

- l'absence de risque d'infection (le code exécutable ne peut être lancé sans son décryptage);
- l'économie du temps de travail des programmes anti-virus (les fichiers au format de quarantaine ne sont pas définis comme des fichiers infectés).

Ultérieurement, les fichiers mis en quarantaine peuvent être étudiés après et soit restaurés sous leur forme d'origine, soit supprimés.

Kaspersky® Network Control Centre offre une possibilité de travailler avec les fichiers de quarantaine depuis le poste de travail de l'administrateur.

Les fichiers mis en quarantaine peuvent être sauvegardés sur le poste de travail (*quarantaine locale*) aussi bien qu'au serveur auquel ce poste de travail est affecté (*quarantaine de serveur*). La quarantaine de serveur exclue la possibilité de réparation non-sanctionnée des fichiers mis en quarantaine par l'utilisateur du poste de travail. Nous recommandons d'utiliser ce type de quarantaine.

7.5.2. Choix de type de quarantaine

Choix de type de quarantaine (locale ou celle de serveur) est effectué séparément pour chaque poste de travail.

Pour choisir le type de quarantaine pour un poste de travail :

1. Choisissez le poste de travail souhaité dans la liste des objets du réseau logique.
2. Dans la zone des propriétés d'objet ouvrez l'onglet **Configuration**.
3. Cliquez sur **Quarantaine**.
4. Dans le groupe d'options dans la partie droite des propriétés choisissez le type de quarantaine (voir: Illustration 69).

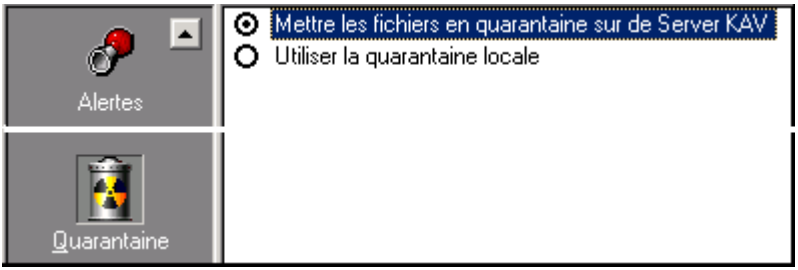

Illustration 69. Choix de type de quarantaine

7.5.3. Travail avec les fichiers mis en quarantaine

7.5.3.1. Travail avec la quarantaine de serveur

Vous pouvez voir la liste complète des fichiers mis en quarantaine de serveur sur le serveur donné et y mettre également tout fichier manuellement, extraire un fichier mis en quarantaine ou bien le supprimer.

Pour la liste des fichiers se trouvant en quarantaine de serveur :

1. Dans la liste des objets du réseau logique choisissez le serveur souhaité.
2. Dans la zone d'édition des propriétés d'objet ouvrez l'onglet **Entrepôts**.
3. Cliquez sur **Quarantaine**.

Dans la partie droite de la zone une fenêtre s'ouvrira contenant une liste des fichiers et les boutons permettant d'accomplir de différentes opération sur la quarantaine (voir: Illustration 70).

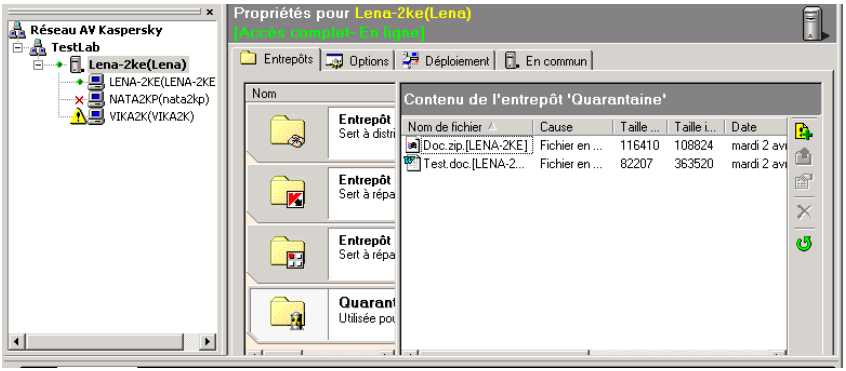

Illustration 70. Contenu de l'entrepôt **Quarantaine**

Pour extraire un fichier mis en quarantaine

1. Choisissez son nom dans la fenêtre et cliquez sur dans la partie droite de la fenêtre ou choisissez l'option **Extraire le fichier mis en quarantaine** dans le menu contextuel de l'élément de la liste.
2. Dans la fenêtre ouverte d'assistant d'extraction des fichiers mis en quarantaine (voir: Illustration 71) choisissez un dossier de destination où le fichier extrait sera placé et pour ce faire cliquez sur .

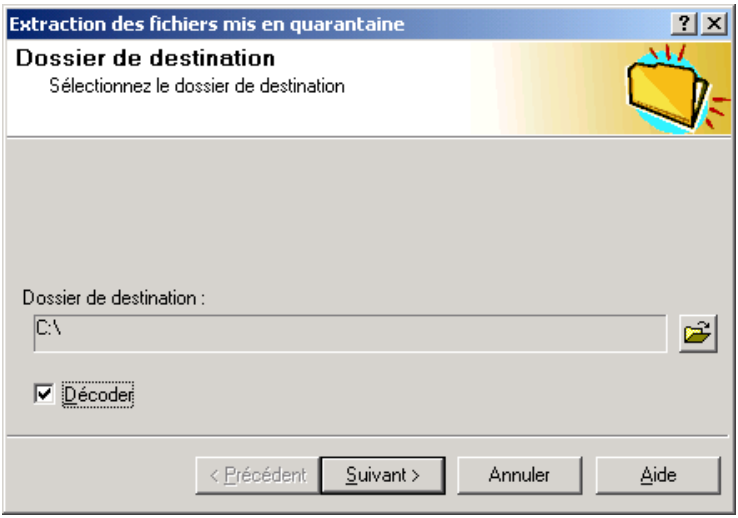

Illustration 71. Extraction des fichiers mis en quarantaine

3. Cochez la case **Décoder**.
4. Cliquez sur **Suivant>**.
5. Une fenêtre d'informations s'ouvrira dans laquelle s'affichera le déroulement de l'opération. À la fin de l'opération, cliquez sur **Terminer**.

Pour supprimer un fichier mis en quarantaine

1. Sélectionnez son nom et cliquez sur ou sélectionnez dans le menu contextuel du fichier l'option **Supprimer**.
2. Une fenêtre avec la demande de confirmer de l'opération de la suppression apparaît. Cliquez sur **Oui**.

Le programme ne supprimera le fichier que de la quarantaine, pas du dossier où il se trouvait initialement. Le programme ne supprimera définitivement un fichier infecté de l'ordinateur uniquement si en qualité d'actions sur les fichiers infectés vous avez choisi **Supprimer**.

Pour mettre à jour la liste des fichiers mis en quarantaine, cliquez sur ou bien choisissez dans le menu contextuel l'option **Mise à jour**.

Pour voir les propriétés du fichier

1. Sélectionnez son nom et cliquez sur ou sélectionnez dans le menu contextuel du fichier l'option **Propriétés**.
2. La fenêtre d'informations sur le fichier s'ouvrira (le volume d'informations correspond au volume mis dans le tableau, cependant les informations sont disposées de façon plus commode (voir: Illustration 72).

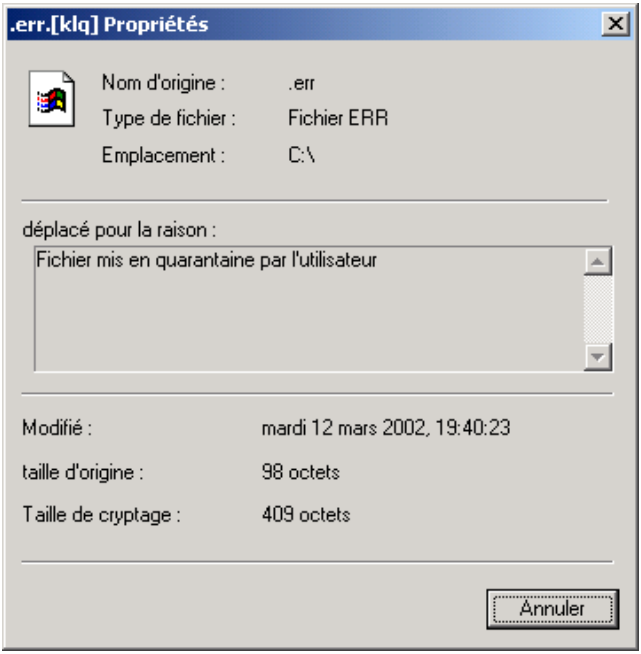

Illustration 72. Information sur un fichier mis en quarantaine

Pour ajouter un fichier à la quarantaine :

1. Cliquez sur ou choisissez dans le menu contextuel l'option **Mettre le fichier en quarantaine**.
2. Dans la fenêtre ouverte **Assistant de mise du fichier en quarantaine** (voir: Illustration 73) sélectionnez le fichier, et pour ce

faire cliquez sur  et choisissez le fichier dans la boîte de dialogue standard MS Windows).

3. Cliquez sur **Suivant** et attendez la fin du travail de l'Assistant.

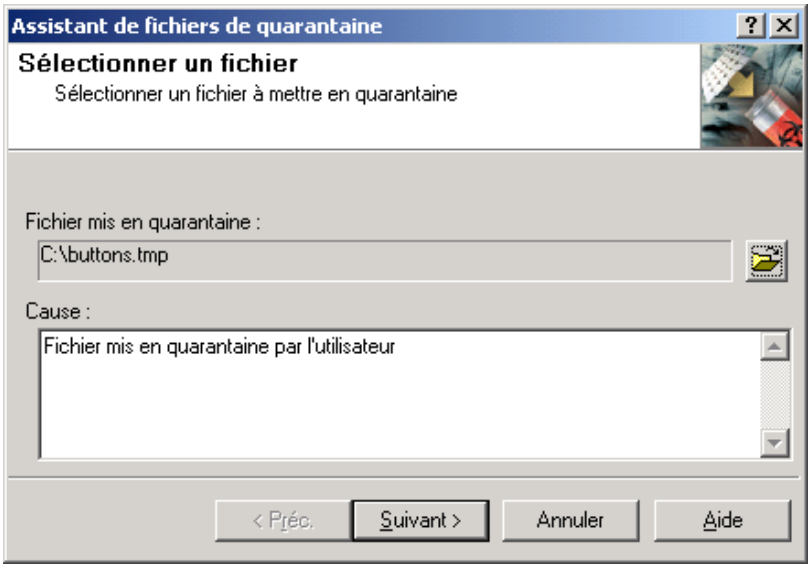

Illustration 73. Assistant de mise du fichier en quarantaine

7.5.3.2. Travail avec la quarantaine locale

Pour voir la liste des fichiers se trouvant en quarantaine locale :

1. Choisissez le poste de travail souhaité dans la liste des objets du réseau logique.
2. Dans la zone d'édition des propriétés d'objet ouvrez l'onglet **Quarantaine**. Une fenêtre s'ouvrira contenant l'information en forme de tableau sur les fichiers mis en quarantaine locale (voir: Illustration 74).

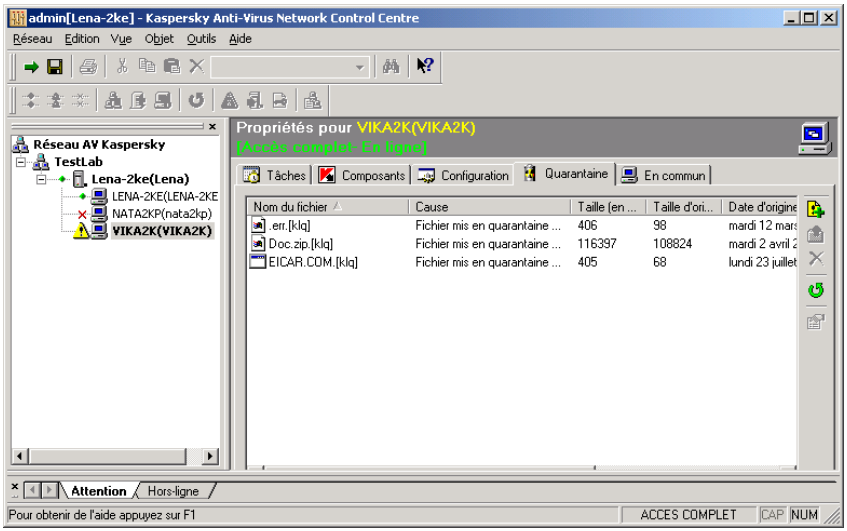

Illustration 74. Liste des fichiers en quarantaine locale

Les possibilités offertes par le système pour travail avec la quarantaine locale sont analogiques à celles décrites dessus pour la quarantaine de serveur. Description détaillée de ces possibilités est fournie par la documentation du logiciel Kaspersky AV Control Centre.

7.6. Configuration de lancement automatique des composants de Kaspersky Anti-Virus® sur les postes de travail

On entend par tâche, un programme possédant une sélection de paramètres et de réglages définis et un horaire de lancement à un moment précis du temps soit lors de la survenue d'un événement déterminé, soit sur indication directe de l'utilisateur. L'utilisateur peut créer, régler, supprimer et lancer les tâches sur les postes de travail. Pour régler l'horaire de lancement choisissez le poste de travail souhaité dans la liste des objets du réseau logique et ouvrez l'onglet **Tâches** dans la zone d'édition des propriétés d'objet (voir: Illustration 75).

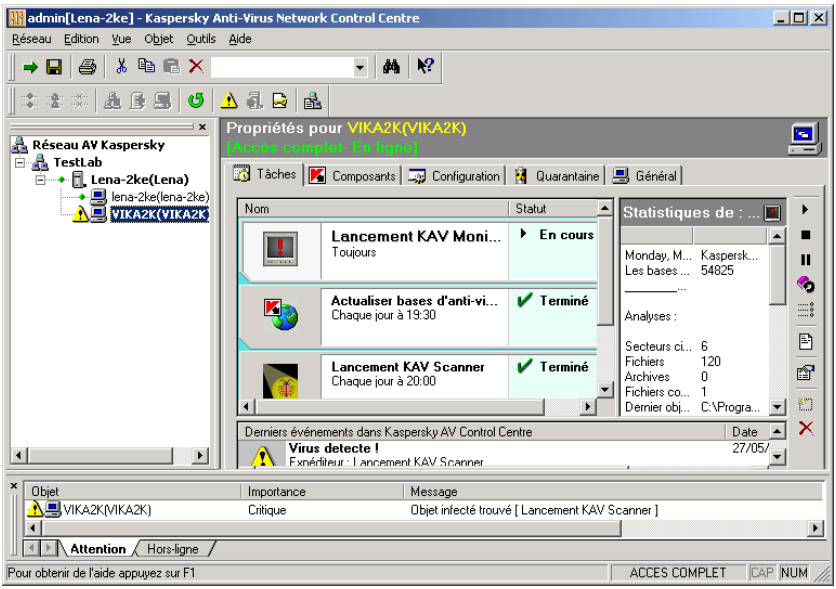

Illustration 75. Gestion des tâches

Pour régler l'horaire du lancement automatique d'un des composants installés du progiciel Kaspersky Anti-Virus®

1. Sélectionnez le composant approprié dans la liste des tâches et cliquez sur dans la partie droite de l'onglet (ou sélectionnez **Propriétés** dans le menu contextuel de la tâche).
2. Une fenêtre d'édition des propriétés de la tâche s'ouvrira. Ouvrez l'onglet **Planification** (Illustration 76).

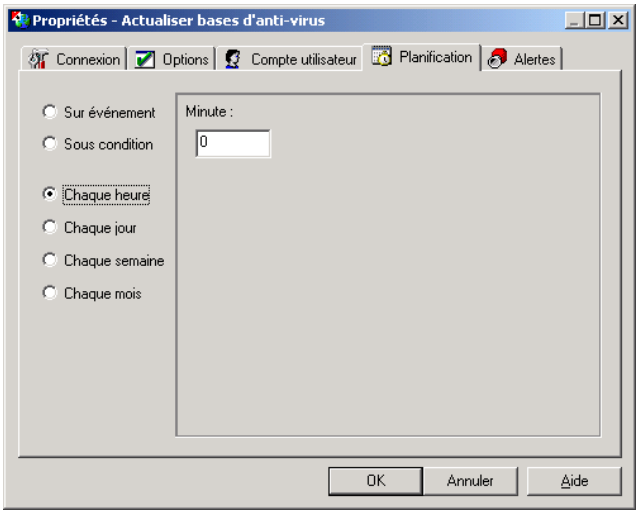

Illustration 76. Planification de l'horaire

3. Sélectionnez dans le groupe d'options une condition de lancement de la tâche. En ce cas dans le champ principal de l'onglet les éléments d'interface s'ouvriront à l'aide desquels sont réglés les paramètres complémentaires de l'horaire (voir dessous).

4. Réglez les paramètres complémentaires de l'horaire et cliquez sur **OK**.

Si vous avez choisi la condition de lancement **Sur événement** (voir: Illustration 77), choisissez dans la liste déroulante **Démarrer la tâche** le nom d'événement nécessaire au lancement de la tâche (hors cela, la liste inclut l'élément **Manuellement**, dont la sélection annule le lancement automatique). Si nécessaire, cochez la case **Une fois par jour** (en ce cas la tâche sera lancée à la première occasion d'un événement donné).

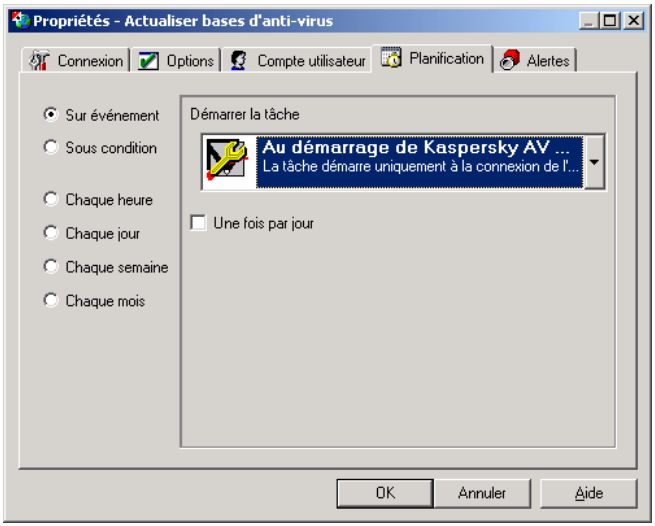

Illustration 77. Planification de l'horaire sur événement

Si vous avez choisi la condition de lancement **Sous condition** (voir: Illustration 78), choisissez dans la liste déroulante **Si la tâche…** le nom d'une des tâches installées de Kaspersky Anti-Virus® et dans la liste déroulante **s'est terminée avec le code 'sortie'** la description du code de la terminaison de la tâche.

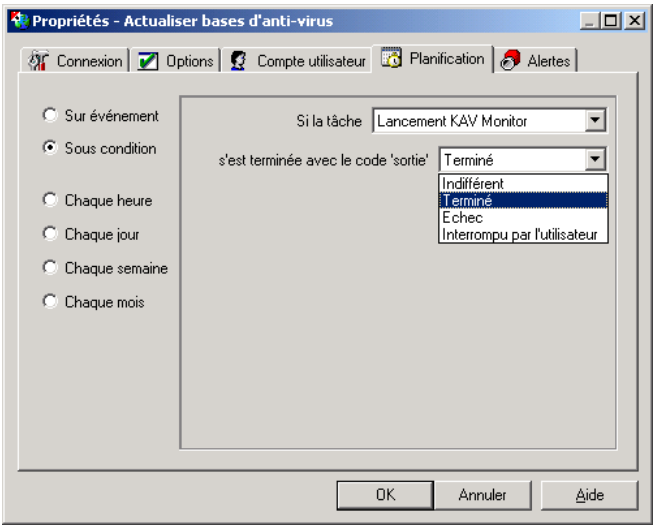

Illustration 78. Planification de l'horaire sur condition

Si vous avez choisi la condition de lancement **Chaque heure**, entrez dans le champ **Minute** un nombre entier de 0 à 59 - minute de chaque heure pendant laquelle le lancement de la tâche aura lieu.

Si vous avez choisi la condition de lancement **Chaque jour** (voir: Illustration 79), formez une Dossier exstants **Heure** contenant une liste des moments de la journée quand le lancement de la tâche aura lieu.

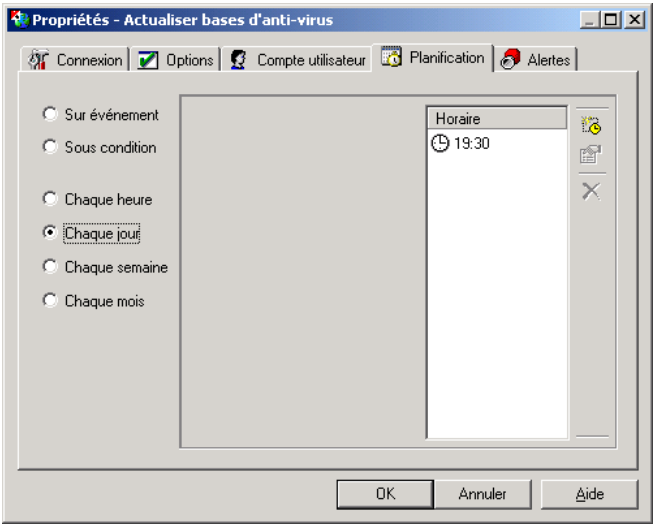

Illustration 79. Planification de l'horaire pour un démarrage tous les jours

Pour ajouter un moment à la liste cliquez sur le bouton  dans la partie droite de la fenêtre. La fenêtre **Ajouter un horaire** s'ouvrira (voir: Illustration 80).

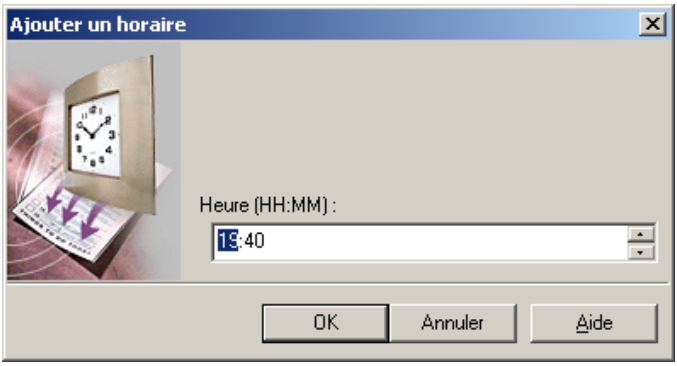

Illustration 80. Ajouter un horaire

Saisissez dans le champ **Heure…** le moment du temps au format **HH:MM** et cliquez sur **OK**.

Pour supprimer un moment de temps de la liste, sélectionnez-le dans la liste et cliquez sur  .

Pour éditer un des éléments de la liste des horaires, sélectionnez-le dans la liste et cliquez sur  . La fenêtre **Modifier l'heure** s'ouvrira, complètement identique à **Ajouter un horaire** décrite précédemment.

Choix de condition de lancement **Chaque semaine** (voir: Illustration 81) permet d'indiquer le lancement de la tâche pendant les jours déterminés de la semaine aux moments déterminés du temps (les mêmes chaque journée).

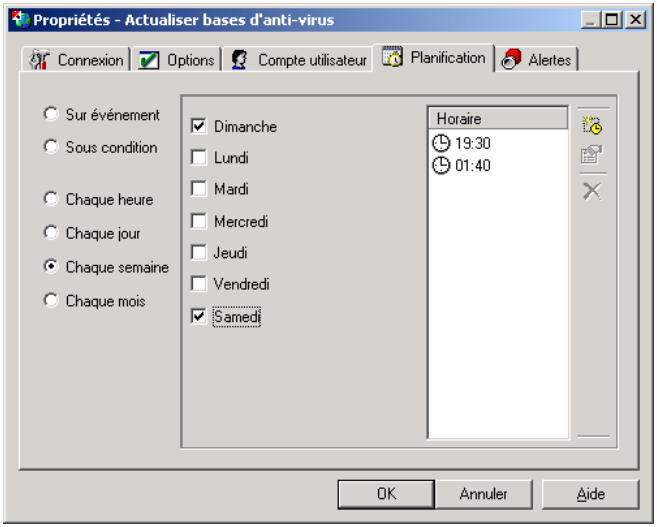

Illustration 81. Planification de l'horaire pour un démarrage chaque semaine

Cochez les cases près des noms des jours de semaine quand le lancement doit avoir lieu et complétez la liste des horaires (cette action est analogue à celle décrite pour le lancement ayant lieu chaque jour).

Dans le scénario de l'illustration la tâche sera lancée quatre fois par semaine à 19:30 et à 1:40 chaque dimanche et les mêmes temps chaque samedi.

Choix de condition de lancement **Chaque mois** (voir: Illustration 82) permet d'indiquer le lancement de la tâche pendant les dates déterminés de chaque mois aux moments déterminés du temps (les mêmes jours chaque mois).

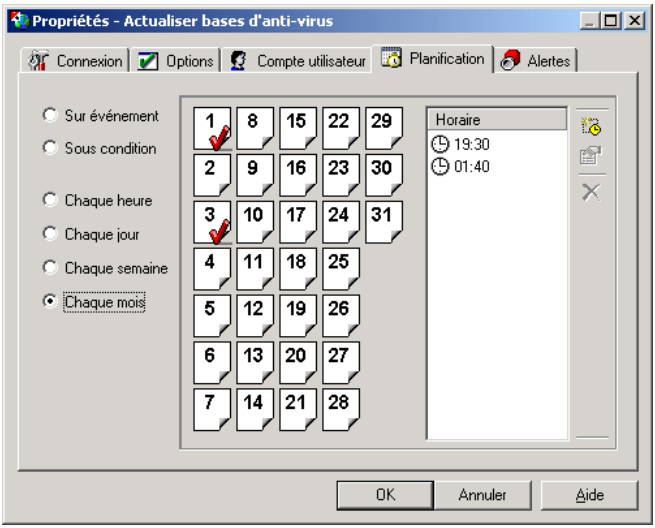

Illustration 82. Planification de l'horaire pour un démarrage tous les mois

Cochez les cases correspondant aux dates de lancement et complétez la liste des horaires (cette action est analogue à celle décrite pour le lancement ayant lieu chaque jour).

Dans le scénario de l'illustration la tâche sera lancée six fois par mois à 19:30 et à 1:40 les premier, onzième et vingt-deuxième jours de mois.

*Pour enregistrer les modifications du progiciel Kaspersky Anti-Virus® installés sur les postes de travail cliquez sur **Appliquer** dans la zone de description des propriétés du poste de travail.*

Les renseignements détaillés sur la gestion des tâches sont fournies dans la documentation " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur".

7.7. Importation et exportation de la configuration des objets du réseau logique

7.7.1. Exportation et impression de la structure du réseau logique

Vous pouvez imprimer la structure du réseau logique et conserver également sa description sous forme de fichier textuel ou fichier spécial de configuration de réseau. Pour ce faire :

1. Dans la liste des objets du réseau logique choisissez l'élément radical **Réseau AV Kaspersky**.
2. Dans le menu **Réseau** choisissez une des options suivantes :
   - **Exporter** – pour enregistrer la description du réseau logique dans un fichier. Le sous-menu contenant deux options s'ouvrira : **Comme texte…** et **Comme fichier de configuration du réseau**. Sélectionnez l'option nécessaire. En ce cas la fenêtre standard MS Windows pour la configuration de l'emplacement et de la nomination du fichier s'ouvrira. Le fichier de configuration de réseau qu'on vient de créer peut être utilisé à définir la configuration du réseau logique lors de sa création sur un autre réseau local.
   - **Imprimer** pour imprimer l'image de la structure du réseau en tant qu'arborescence des objets (la vue de la barre du réseau est reproduite complètement sur l'écran). Pour imprimer la structure on peut également cliquer sur le bouton  dans la barre d'outils (standard).
   - **Consultation préalable** pour voir l'aspect de document à imprimer sur l'écran.

7.7.2. Exportation et importation de la configuration des serveurs et des postes de travail

Vous pouvez enregistrer (exporter) les paramètres actuels de tout serveur ou poste de travail dans le fichier de format spécial à l'extension **.dat**. Pour ce faire, dans le menu contextuel de l'objet sélectionnez **Exporter la configuration…** Une fenêtre standard MS Windows s'ouvrira vous proposant de enregistrer le fichier.

Le fichier correspondant créé lors de l'exportation des paramètres du poste de travail peut être utilisé pendant le déploiement d'un nouveau poste de travail, du même type que le poste de travail donné du point de vue des tâches antivirales qu'on peut résoudre (voir le paragraphe 6.4.1) pour importer les paramètres sur un nouveau poste de travail.

CHAPTER 8. AFFECTATION DES PRIVILEGES D'ACCES AUX AUTRES UTILISATEURS

L'administrateur peut ouvrir ou fermer aux autres utilisateurs l'accès aux paramètres du progiciel Kaspersky Anti-Virus® pour les postes de travail (voir le paragraphe 8.1) et désigner les administrateurs secondaires des groupes (voir le paragraphe 8.2).

8.1. Protection des paramètres du progiciel Kaspersky Anti-Virus® des postes de travail

Le logiciel Kaspersky® Network Control Centre assure à l'administrateur la possibilité de protéger les paramètres du progiciel Kaspersky Anti-Virus® des modifications issues par des utilisateurs.

8.1.1. Interdiction d'accès aux paramètres du progiciel Kaspersky Anti-Virus® depuis un poste de travail

Pour interdire l'accès aux paramètres du progiciel Kaspersky Anti-Virus® depuis un poste de travail où le progiciel est installé

1. Choisissez le poste de travail souhaité dans la liste des objets du réseau logique.
2. Dans la zone d'édition des propriétés du poste de travail ouvrez l'onglet **Configuration** (voir: Illustration 83).
3. Cliquez sur **Sécurité**.

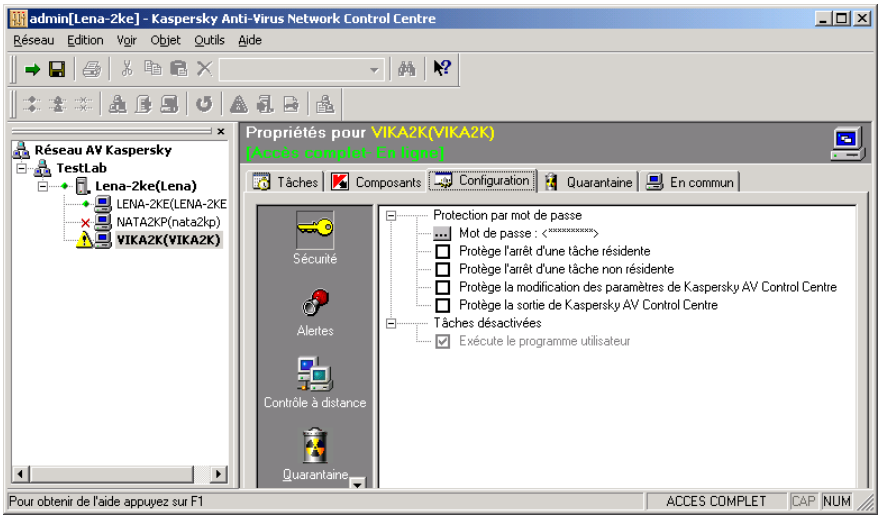

Illustration 83. Onglet **Configuration** de la zone d'édition des propriétés du poste de travail

Mot de passe

Mot de passe pour l'accès aux réglages du poste de travail. Pour modifier le mot de passe, cliquez sur [...]. Après cela une boîte de dialogue **Changer le mot de passe** apparaît (voir: Illustration 84).

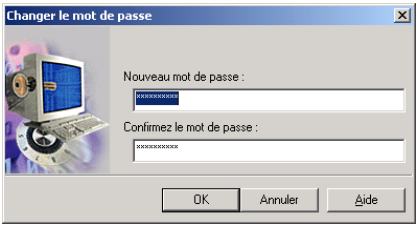

Illustration 84. Changer le mot de passe

1. Dans la zone **Nouveau mot de passe** saisissez le mot de passe pour accéder au réseau.
2. Dans la zone **Confirmez le mot de passe** entrez de nouveau le mot de passe.
3. Cliquez sur **OK**.

Arrêt des tâches résidentes

Activer le mode de demande d'un mot de passe en cas de tentative d'arrêter l'exécution des tâches résidentes sur un poste de travail.

Arrêt des tâches non-résidentes	Activer le mode de demande d'un mot de passe en cas de tentative d'arrêter l'exécution des tâches non-résidentes sur un poste de travail.
Modification des paramètres de Kaspersky AV Control Centre	Activer le mode de demande d'un mot de passe en cas de tentative les paramètres du progiciel Kaspersky Anti-Virus® sur un poste de travail
Fin du travail de Kaspersky AV Control Centre	Activer le mode de demande d'un mot de passe en cas de tentative de décharger le logiciel Kaspersky AV Control Centre sur un poste de travail.

8.1.2. Synchronisation des modifications des paramètres du progiciel Kaspersky Anti-Virus® par les administrateurs et l'utilisateur

Si l'administrateur travaille avec les paramètres du progiciel Kaspersky Anti-Virus®, installé sur un poste de travail, et en ce moment l'utilisateur essaie d'y lancer le logiciel Kaspersky AV Control Centre, celui-ci produira un message suivant : **Kaspersky AV Control Centre est verrouillé par l'administrateur du réseau**. Si au moment quand l'administrateur s'est adressé aux paramètres du progiciel Kaspersky Anti-Virus®, installé sur un poste de travail, une des fenêtres des propriétés du logiciel Kaspersky AV Control Centre y est déjà ouverte, celle-ci fermera après avoir produit le même message : **La station de travail est verrouillée** (voir: Illustration 85). En ce cas les paramètres non enregistrés seront perdus.

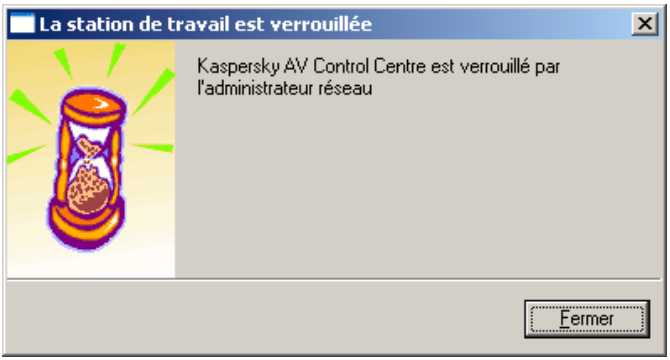

Illustration 85. Message sur le verrouillage du logiciel Kaspersky AV Control Centre

Si l'administrateur adresse le poste de travail avec les paramètres duquel un autre administrateur travaille le logiciel Kaspersky® Network Control Centre produira une alerte suivante (voir: Illustration 86).

Illustration 86. Message sur le verrouillage des paramètres du poste de travail

8.2. Désignation d'administrateur du groupe

L'administrateur peut transmettre une part de ses droits aux administrateurs des groupes. Après avoir lancé le logiciel Kaspersky® Network Control Centre et avoir entré ses nom et mot de passe, l'administrateur du groupe obtient l'accès uniquement aux certains groupes des postes de travail. Cet administrateur peut désigner également quelques administrateurs lui inférieurs.

Pour désigner un administrateur du groupe

1. Entrez au logiciel Kaspersky® Network Control Centre avec privilèges d'accès complet.

2. Dans la liste des objets du réseau logique choisissez un groupe pour lequel vous voudriez designer un administrateur ou sélectionnez plusieurs groupes (pour ajouter un objet non-sélectionné à la multitude des ceux qui ont été sélectionnés ou pour exclure un objet de cette multitude cliquez sur celui-ci en maintenant appuyée la touche **<CTRL>**).

3. Sur l'onglet unique **Général** dans la zone **Administrateur** saisissez le nom du nouvel administrateur du groupe.

4. Dans la zone **Mot de passe** cliquez sur **Modifier** (voir: Illustration 87).

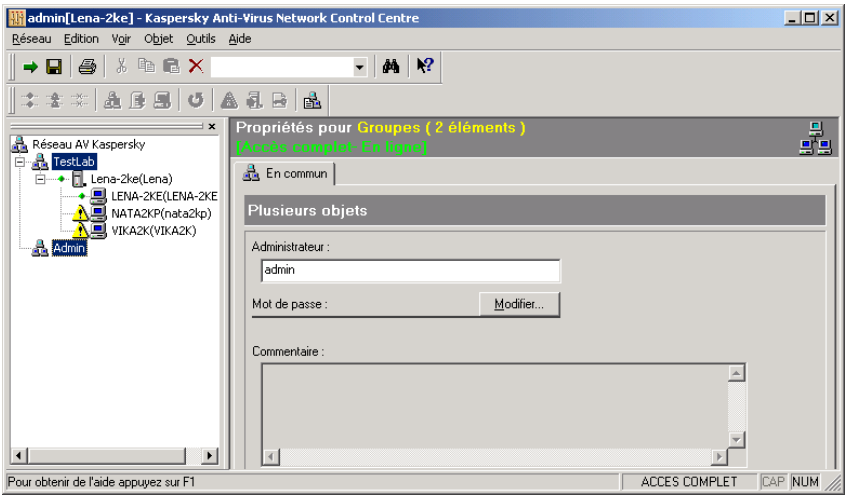

Illustration 87. Désignation d'administrateur des groupes

5. Boîte de dialogue **Changer le mot de passe** s'ouvrira. Entrez un nouveau mot de passe de l'administrateur et sa confirmation dans les champs de saisie correspondants (voir: Illustration 88).

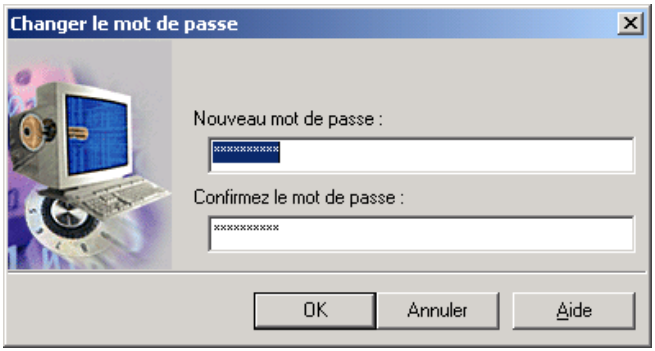

Illustration 88. Changer le mot de passe

6. Cliquez sur **Ok**.
7. Dans la fenêtre principale dans l'onglet **Général** saisissez (éditez) si nécessaire un texte libre explicatif dans la zone **Commentaire** (ce champ est accessible si un seul groupe est choisi).
8. Cliquez sur **Appliquer**.

Après cela informez le nouvel administrateur du groupe de son nom et de son mot de passe pour accéder au réseau logique à l'aide de Kaspersky® Network Control Centre. Après avoir saisi son nom et son mot de passe le nouvel administrateur obtiendra accès au groupe dont il a été désigné comme administrateur.

Après avoir choisi le groupe racine dans la liste des objets du réseau logique l'administrateur verra la ligne **Accès interdit** parce que uniquement une partie du réseau logique lui est accessible.

Vous pouvez vérifier quels privilèges d'accès a reçu un administrateur de groupe qui vous est subordonné. Pour ce faire, sélectionnez dans le menu **Réseau** l'option **Saisie de mot de passe d'accès** ou cliquez sur dans la barre d'outils ou pressez sur le raccourci clavier <Ctrl>+<L>. Après cela, une boîte de dialogue **Entrer Kaspersky® Network Control Centre** apparaît et il faudra y saisir le nom et le mot de passe de l'administrateur secondaire et cliquer sur le bouton **Ok** à la fin (voir: Illustration 89).

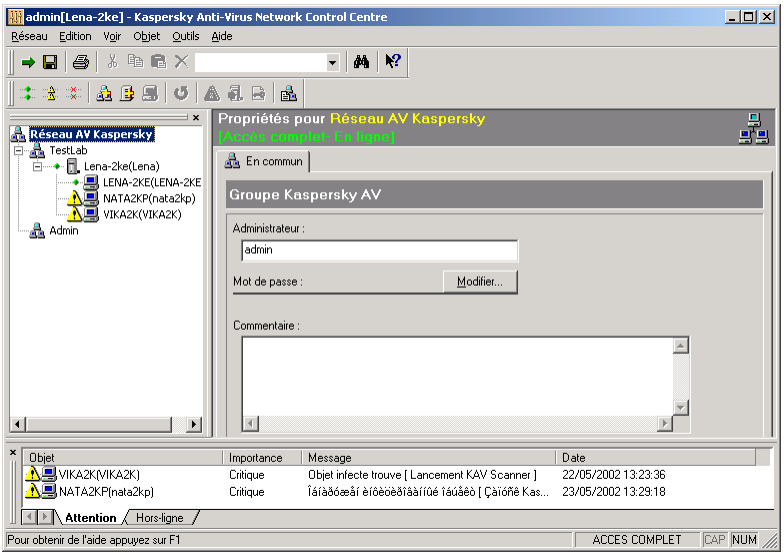

Illustration 89. Fenêtre principale en cas d'entrée comme administrateur de groupe

Après avoir choisi la ligne supérieure dans la liste des objets du réseau logique dans la zone d'édition des propriétés du réseau, l'utilisateur entré au programme comme administrateur du tout le réseau logique verra la ligne **Accès complet**.

CHAPTER 9. MAINTENANCE DU RESEAU LOGIQUE

9.1. Rapport du réseau

Le rapport du réseau est un moyen effectif d'enregistrer tous les événements ayant lieu aux objets du réseau logique.

Pour obtenir un rapport sur tous les événements liés à la détection des virus, aux pannes du fonctionnement du mécanisme de mise à jour des bases antivirales ou à l'absence de connexion avec un des objets choisissez dans le menu **Vue** l'option **Rapport du réseau**. La fenêtre du rapport s'ouvrira présentée à l'aide de l'outil Kaspersky® Report Viewer (voir: Illustration 90).

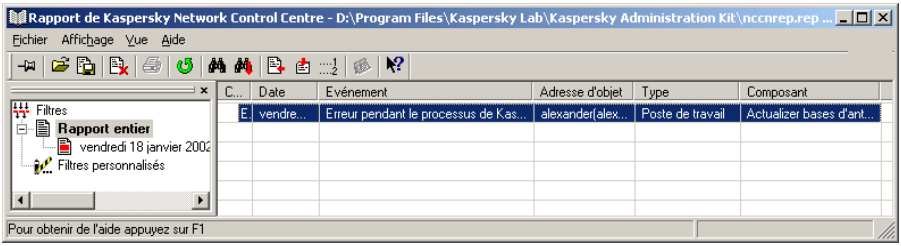

Illustration 90. Rapport de Kaspersky® Network Control Centre

La majeure partie de la fenêtre est occupée de la liste des événements organisée sous forme de tableau. La fenêtre possède un système de menus et une barre d'outils procurant une vue plus commode du rapport surtout en cas de sa grandeur.

La fenêtre du rapport du réseau consiste à deux parties :

- à gauche est la liste des sessions dans le fichier courant de rapport (un seul fichier de rapport peut être ouvert à la fois !);
- à droite est le rapport de session.

Pour consulter un rapport de session, sélectionnez-le dans la partie gauche de la fenêtre, après quoi dans la partie droite s'affichera le rapport approprié.

Le rapport consiste à des sections suivantes :

- **Catégorie** - catégorie d'importance d'un événement ;
- **Date** - la date et l'heure d'un événement ;

- **Événement** - description d'un événement ;
- **Adresse d'objet** - l'adresse de réseau de l'objet auquel l'événement est relié (où la tâche ayant issu le message était accomplie ou avec lequel la connexion est perdue);
- **Type** - type d'objet du réseau (poste de travail ou serveur);
- **Composant** - tâche de Kaspersky Anti-Virus® qui a délivré le message.

Au-dessus du rapport se trouve la barre d'outils contenant les boutons pour l'accomplissement des opérations principales. Les boutons sont assortis de bulles d'aide apparaissant au passage de la souris et affichant une petite fenêtre contenant une information très brève.

Dans la première ligne supérieure est disposé le menu principal. Vous pouvez noter que les boutons dans la barre d'outils et certaines commandes du menu ont la même fonction.

Pour la description détaillée des boutons et des menus du programme Report Viewer voir " Kaspersky Anti-Virus® pour les postes de travail / Kaspersky Anti-Virus® pour NT Server. Guide de l'utilisateur".

Pour obtenir des informations plus détaillées sur les événements reflétés dans le rapport du réseau et ayant à faire avec le fonctionnement des tâches sur les postes de travail choisissez le poste souhaité dans la liste des objets du réseau logique et ouvrez l'onglet **Tâches** (pour détails, voir le paragraphe 9.3).

Pour les informations plus détaillées sur les événements ayant à faire avec la perte de connexion avec les objets utilisez les moyens décrits au paragraphe 9.4.

9.2. Choix des objets du réseau logique pour consultation

Le logiciel Kaspersky® Network Control Centre vous offre une possibilité de sélectionner dans la liste des objets du réseau logique plusieurs postes de travail ou autres objets selon un critère pour consultation et édition de leurs propriétés.

Au début de l'opération de sélection un objet est sélectionné de la liste des objets du réseau logique et la sélection est conduite parmi les objets du niveau inférieur (ceci peut être un groupe ou un serveur).

Si un groupe est choisi, alors on peut conduire la sélection parmi les objets du niveau inférieur en utilisant deux critères simultanément (sont choisis les objets satisfaisant les deux critères). Le premier critère - type d'objet (groupe, serveur ou poste de travail), le deuxième - activité d'objet

(poste de travail ou serveur sont en ligne, hors-ligne, cochés **attention**). Le groupe est considéré satisfaisant le deuxième critère en tout cas.

Pour conduire une sélection pareille, sélectionnez dans le menu **Edition** l'option **Choisir**. Un sous-menu s'ouvrira (voir: Illustration 91).

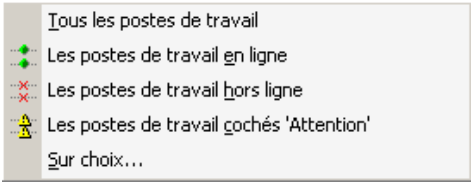

Illustration 91. Sous-menu de choix d'objets

Sélectionnez dans ce sous-menu l'option **Sur choix…**. La fenêtre **Choix d'objets** s'ouvrira (voir: Illustration 92).

Illustration 92. Configuration des critères de choix

Cochez le champ **Objets** avec des cases près des noms des types d'objets à sélectionner et dans la partie inférieure de la fenêtre cochez les cases de description de l'activité des objets après quoi cliquez sur **OK**.

Il faut se rendre compte du fait qu'en cas de sélection d'objets hétérogènes dans la zone d'édition des propriétés d'objet trop peu d'information sera représenté, et l'édition des paramètres sera impossible. Ainsi, dans l'exemple susmentionné (refléter les serveurs et les postes de travail en état connecté) les objets correspondants seront marqués d'une manière évidente, pourtant dans la zone d'édition des propriétés le bouton **Modifier** seul sera accessible dans la zone **Mot de passe** (voir: Illustration 93), et toute autre information ne sera pas présente.

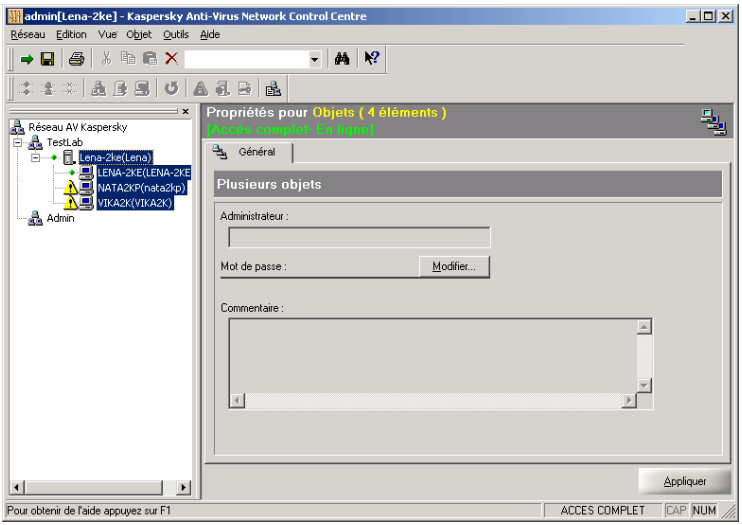

Illustration 93. Les serveurs et les postes de travail en ligne sont choisis

En cas particulier, quand il faut choisir les postes de travail seulement et en plus du même type d'activité (en ligne seulement, hors-ligne seulement, ou coché **attention** seulement) ou tous les postes à la fois, choisissez dans le menu **Edition** l'option **Sélectionner** et dans le sous-menu qui s'ouvre (voir: Illustration 91) choisissez une des options correspondantes. Dans la partie gauche du sous-menu les boutons sont fournis qu'un peut également utiliser pour sélectionner les postes de travail (les boutons eux-mêmes sont placés sur la barre d'outils).

Si vous sélectionnez plus d'un objet du même type, les propriétés du premier sont présentées dans la zone d'édition des propriétés ((voir: Illustration 94). Après avoir introduit vos modifications ou annulé la sélection d'objets, un fenêtre est affichée pour demander si la configuration du premier ordinateur doit être appliquée à l'ensemble du groupe sélectionné.

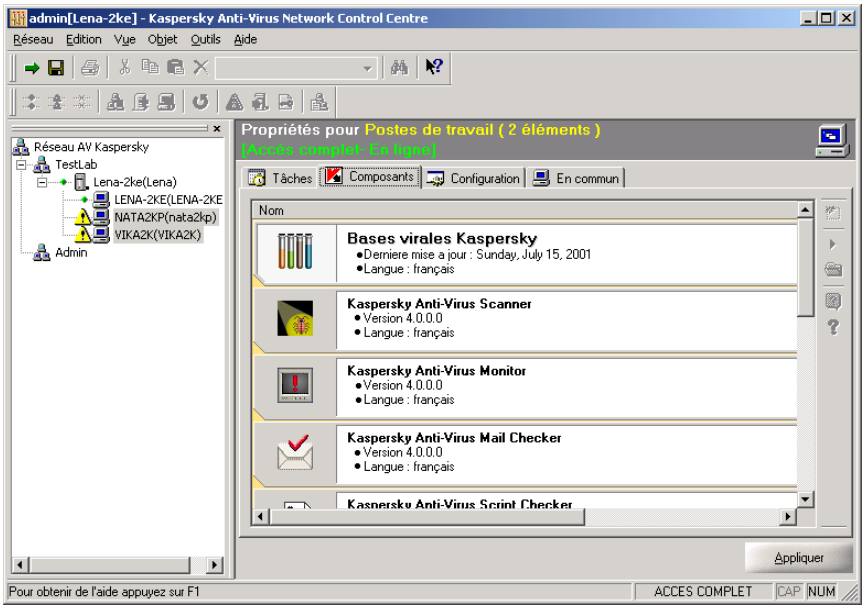

Illustration 94. Les objets homogènes sont choisis

9.3. Consultation des résultats de l'accomplissement des tâches

On peut voir les résultats de l'accomplissement des tâches automatiquement réalisées sur les postes de travail dans l'onglet **Tâches** dans la zone d'édition des propriétés du poste de travail. Dans le rapport de chaque tâche, figurent les statistiques sur les résultats de sa dernière exécution (voir: Illustration 95).

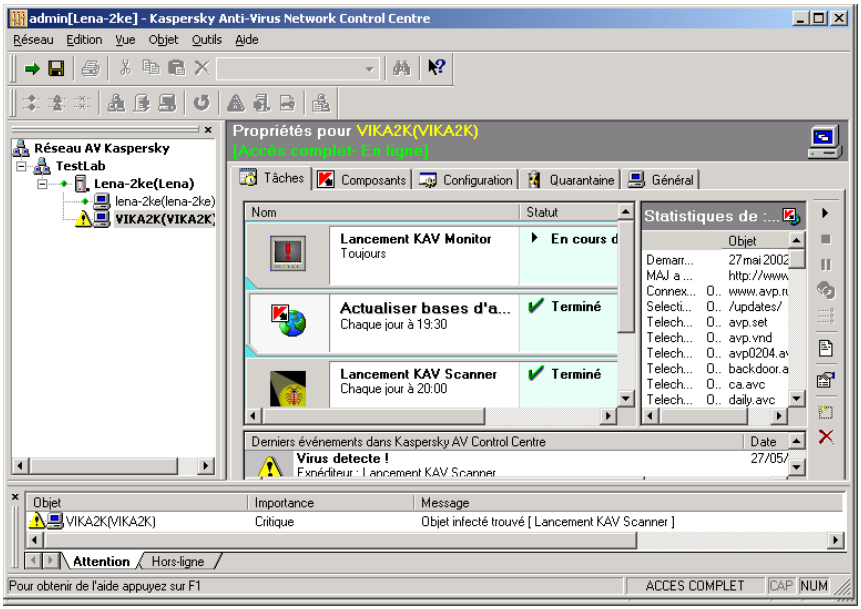

Illustration 95. Consultation des résultats de l'accomplissement de la tâche

Si l'administrateur choisit dans la liste des objets du réseau logique un poste de travail qui est désactivé ou inaccessible pour le moment, l'information sur les résultats de l'exécution des tâches sur ce poste copiée au serveur à l'avance (quand le poste était toujours accessible) sera reflétée dans l'onglet **Tâches**. Au titre de la zone d'édition des propriétés d'objet une ligne **Mode hors-ligne** sera présente (voir le paragraphe 7.1.2).

L'administrateur doit détecter les causes de l'inaccessibilité des postes de travail (voir le paragraphe 9.4).

9.4. Contrôle de l'accessibilité des postes de travail et des serveurs

En cas d'inactivité d'un poste de travail celui-ci est représenté dans la liste des objets du réseau logique par une icône spéciale . Le mode hors-ligne des postes de travail est également représenté dans le rapport du réseau (voir le paragraphe 9.1).

Le mode hors-ligne des objets du réseau logique est automatiquement détecté par le logiciel Kaspersky® Network Control Centre. Vous pouvez spécifier une temporisation du sondage réseau et définir le délai maximum utilisé pour tenter d'établir une connexion avec un objet sélectionné dans la liste.

Pour régler le temps d'attente de réponse d'un poste de travail ou d'un serveur :

1. Sélectionnez dans le menu **Outils** l'option **Configuration**.
2. Dans la fenêtre **Configuration** qui s'ouvre développez la ramification **Périodes d'attente** (voir: Illustration 96).

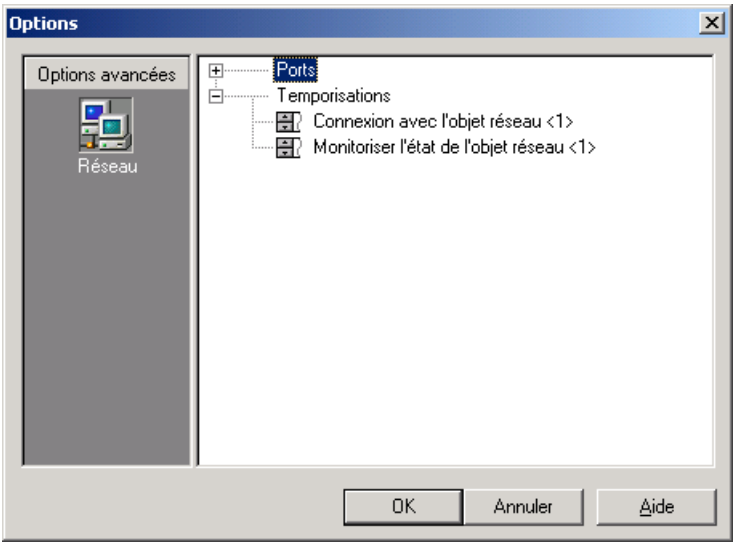

Illustration 96. Configuration des périodes d'attente

3. Saisissez dans la zone **Connexion avec l'objet réseau** le temps d'attente de réponse des objets en cas de sélection d'un objet dans la liste, et dans le champ **Monitoriser l'état de l'objet réseau** saisissez le temps d'attente de réponse sous monitorage du réseau (les valeurs sont indiquées en secondes).

L'administrateur doit distinguer les situations où le poste de travail est désactivé (ou non-relié au segment du réseau où se trouve le serveur) des situations où Kaspersky AV Control Centre ne fonctionne plus sur cet ordinateur (ou quand sa configuration est sérieusement endommagé). Au dernier cas il est nécessaire de restaurer la capacité opérationnelle du programme (la réinstaller, par exemple - voir le paragraphe 6.3).

Pour pouvoir distinguer ces situations nous recommandons de tester la connexion avec le poste de travail en utilisant les moyens du SO, tels que la commande **Ping**, par exemple. Si ce teste démontre que l'ordinateur a conservé la connexion au réseau on peut croire avoir constaté l'endommagement de Kaspersky AV Control Centre.

Pour lancer la commande Ping depuis le logiciel Kaspersky® Network Control Centre choisissez dans le menu **Outils** l'option **Ping ordinateur…** et saisissez ensuite dans le champ qui se présente l'adresse IP numérique celle de domaine de l'ordinateur.

La commande **Ping** peut également être lancée depuis la barre d'informations. Pour ce faire ouvrez l'onglet **Hors-ligne**, choisissez l'ordinateur que vous êtes en train de tester, dans la liste, et ensuite sélectionnez **Ping** dans le menu contextuel.

9.5. Réception d'alertes émises par les postes de travail avec indicateur 'Attention'

Lors de la génération d'une alerte par une tâche sur tout poste de travail le programme :

- place l'alerte dans la barre d'informations dans l'onglet **Attention**,
- assigne le poste de travail où l'alerte a été formée avec le statut **Attention**. Dans la liste des objets du réseau logique une signe d'exclamation est placée à gauche de l'icône de ce poste de travail  .

Pour voir des informations plus détaillée à propos du poste de travail où l'alerte a été formée

1. Dans la barre d'informations, choisissez dans l'onglet **Attention** l'alerte de laquelle vous voulez obtenir des renseignements plus détaillés.
2. Dans le menu contextuel de l'alerte sélectionnez l'option **Choisir l'objet**. Après cela dans la liste des objets du réseau logique le poste de travail où l'alerte a été formée sera identifié comme objet actuel.
    - Dans l'onglet **Tâches** dansla zone d'édition des propriétés du poste de travail vous pouvez voir tous les événements qui ont eu lieu sur ce poste de travail (voir: Illustration 97). Pour obtenir les renseignements détaillés sur un d'eux, cliquez dessus. Dans

la liste des tâches celle sera focalisée qui avait formé un message choisi sur l'événement. Dans le champ des statistiques à droite l'information détaillée sur les résultats de la dernière exécution de la tâche sera présentée.

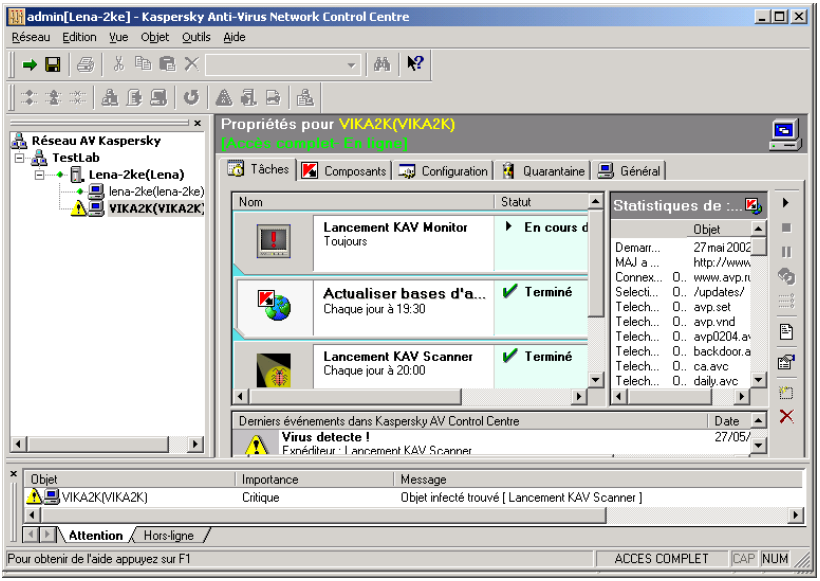

Illustration 97. Consultation des résultats de la dernière exécution de la tâche

*Pour éliminer l'indicateur **Attention** d'un poste de travail décochez l'indicateur **Attention** dans le menu **Objet** ou cliquez sur dans la barre d'outils.*

9.6. Réception du courrier électronique depuis les postes de travail

Nous recommandons à l'administrateur de consulter régulièrement sa boîte aux lettres et lire les alertes lui renvoyées par les serveurs et issues des tâches du progiciel Kaspersky Anti-Virus® fonctionnant sur les postes de travail.

Les messages contenant le texte des alertes sont envoyés par le serveur aux adresses indiquées dans ses réglages. En qualité d'objet de message et

l'adresse de retour figurent les paramètres indiqués dans les paramètres du serveur. Le texte du message est composé de l'alerte, du nom de la tâche qui l'avait généré, le nom du poste de travail où la tâche a été lancée etc. En outre, le texte prédéfini par les paramètres du serveur est mis à la tête du message.

Le format du message est le suivant :

```
<TEXTE_DU_MESSAGE>
Alerte <ALERTE> (envoyée <DATE> <HEURE>)
```

```
Tache <NOM_DE_TACHE>,
lancé par le composant <NOM_DE_COMPOSANT>
du poste de travail <NOM_DE_POSTE_DE_TRAVAIL>,
a généré le message avec le niveau d'importance <NIVEAU>.
Le message été envoyé <NOM_DE_PROGRAMME>
<NOM_D'_ORDINATEUR>
```

où <TEXTE_DU_MESSAGE> texte du message indiqué dans les paramètres du serveur,
<ALERTE> – texte d'alerte;
<DATE>, <HEURE> – date et heure, respectivement, quand la tâche a généré l'alerte;
<NOM_DE_TACHE> - nom de la tâche qui a généré l'alerte;
<NOM_DE_COMPOSANT> - nom du composant dont la tâche a le type <NOM_DE_TACHE>;
<NOM_DE_POSTE_DE_TRAVAIL> - est le nom du type de composant auquel se rapporte au <NOM_DE_TACHE>;
<NIVEAU> - niveau d'importance de l'alerte;
<NOM_DE_PROGRAMME> – nom du programme qui a envoyé le message électronique: ''Kaspersky AV Control Centre' ou 'Kaspersky AV Server';
<NOM_D'_ORDINATEUR> – nom de l'ordinateur d'où le message électronique a été envoyé.

9.7. Lancement des tâches sur les postes de travail

Si sur l'un des postes de travail une situation est constatée où l'administrateur croit nécessaire d'intervenir, il peut le faire sans quitter son poste de travail, d'où il conduira, par exemple, le traitement des fichiers infectés existant sur ce poste de travail.

Pour ce faire :

1. Choisissez le poste de travail souhaité dans la liste des objets du réseau logique et ouvrez l'onglet **Tâches** dans la zone d'édition des propriétés d'objet.
2. Dans le menu contextuel de la tâche nécessaire sélectionnez **Lancer**.

Les renseignements détaillés sur lancement manuel des tâches sont fournis dans la description de Kaspersky AV Control Centre dans la documentation de " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur".

9.8. Contrôle des mises à jour des bases antivirales

La configuration de la procédure de mise à jour automatique des bases antivirales sur les postes de travail depuis les entrepôts des serveurs aussi bien que du chargement automatique des mises à jour dans les entrepôts des serveurs depuis un des serveurs du réseau logique et sa mise à jour via Internet sont décrits au paragraphe 7.4.

L'administrateur doit détecter et analyser les situation liées à la perte de connexion entre les postes et les serveurs aussi bien que les pannes d'exécution de la tâche de mise à jour. A cette cause sont destinés des moyens comme rapport du réseau (voir le paragraphe 9.1) et la barre d'informations (voir les paragraphes 5.7 et 9.5). En de cas individuels il peut être nécessaire de mise à jour des bases antivirales manuellement (voir le paragraphe 9.7).

9.9. Installation du fichier de clé d'utilisateur sur un poste de travail

En cas d'extension de la licence d'utilisation de Kaspersky Anti-Virus® ou de modification des conditions de la licence active, les droits nouveaux ou prolongés à l'utilisation du progiciel sont confirmés à l'aide du fichier de clé d'utilisateur (voir les détails sur les clés d'utilisateurs dans " Kaspersky Anti-Virus® pour les postes de travail. Guide de l'utilisateur ").

Le nouveau fichier de clé de l'utilisateur peut être installé sur un poste de travail à distance à l'aide du logiciel Kaspersky® Network Control Centre par l'administrateur ayant le droit d'accès à ce poste de travail.

Pour installer le fichier de clé d'utilisateur sur un poste de travail

1. Choisissez le poste de travail ou plusieurs postes souhaités dans la liste des objets du réseau logique.
2. Dans le menu **Objet** sélectionnez **Distribuer le fichier de clé de Kaspersky AV** ou cliquez sur dans la barre d'outils (d'actions).
3. Dans la fenêtre ouverte **de l'assistant de distribution du fichier de clé** (voir: Illustration 98), cliquez sur et sélectionnez le fichier dans la boîte de dialogue standard MS Windows (le fichier a l'extension **.key**).

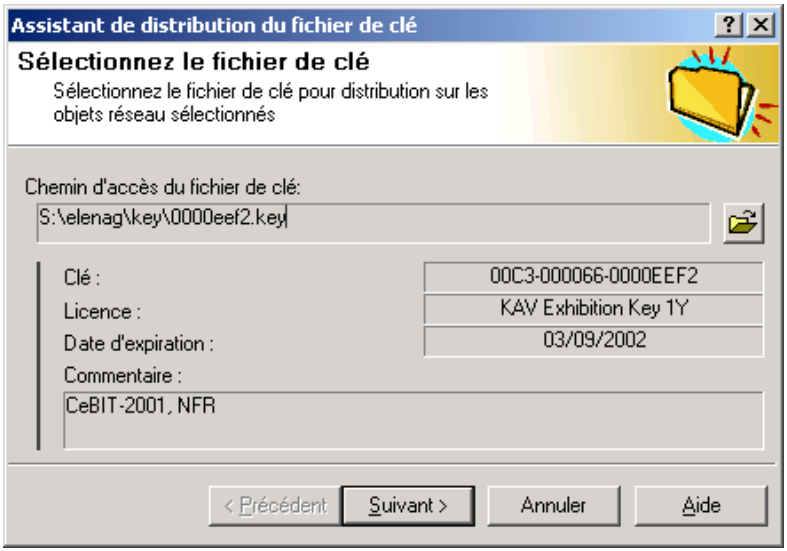

Illustration 98. Assistant de distribution du fichier de clé

4. Examinez les zones d'information **Licence**, **Date d'expiration** et **Commentaire** pour vérifier que la clé que vous êtes en train d'installer correspond à votre licence. Si par erreur vous avez choisi un fichier dont vous n'avez pas besoin cliquez de nouveau sur le

bouton  ou cliquez sur **Annulation** pour interrompre l'installation.

5. Cliquez sur **Suivant** pour continuer l'installation du fichier clé.
6. Une fenêtre annonçant la fin d'installation de la clé apparaît. Cliquez sur **Terminer** pour terminer l'installation.

CHAPTER 10. ORGANISATION DU TRAVAIL EN COMMUN DES ADMINISTRATEURS

10.1. Modification des noms et des mots de passe des administrateurs

Les administrateurs doivent tenir au secret des mots de passe d'accès à la configuration du réseau.

Si le mot de passe de l'administrateur est perdu, l'administrateur pourra obtenir un nouveau mot de passe de l'administrateur qui l'avait désigné.

Si le mot de passe de l'administrateur du réseau logique est perdu, il faudra réinstaller le logiciel Kaspersky® Network Control Centre et recréer le réseau logique.

La procédure de modification du nom et/ou du mot de passe de l'administrateur d'un seul ou de plusieurs groupes est identique à celle de l'installation de ces paramètres pour l'administrateur nouvellement affecté décrite en détail au paragraphe 8.2.

10.2. Modification des mots de passe pour l'accès sur les postes de travail et aux serveurs

Les administrateurs doivent tenir au secret des mots de passe d'accès au réseau pour les ordinateurs dont ils sont responsables. Nous recommandons également de changer ces mots de passé régulièrement.

Si les mots de passé d'accès au réseau deviennent connus à l'utilisateur externe celui-ci, ayant obtenu l'accès à l'ordinateur de l'administrateur pourra modifier tous les paramètres sur les postes de travail et les serveurs.

Vous pouvez changer le mot de passe d'accès au réseau pour tout poste de travail, serveur ou plusieurs objets (postes de travail et serveurs) simultanément. Pour ce faire choisissez l'objet nécessaire dans la liste des objets du réseau logique ou sélectionnez plusieurs objets (pour ajouter un objet non-sélectionné à la multitude des ceux qui ont été sélectionnés ou pour exclure un objet de cette multitude cliquez sur celui-ci en maintenant appuyée la touche <**CTRL**>).

La vue de la fenêtre principale et les onglets **Général** dans la zone d'édition des propriétés d'objet auront des différences en fonction des objets choisis :

Si un seul objet est choisi, sa vue va correspondre à celle décrite pour ce type d'objets au paragraphe 5.6.

Si plusieurs objets hétérogènes sont choisis seul l'onglet **Général** sera accessible.

Si plusieurs objets (hétérogènes ou homogènes) sont choisis le champ **Commentaire** de l'onglet **Général** sera inaccessible.

A l'Illustration 99 l'aspect de la fenêtre principale est fourni (onglet **Général**) quand plusieurs postes de travail sont choisis pour édition.

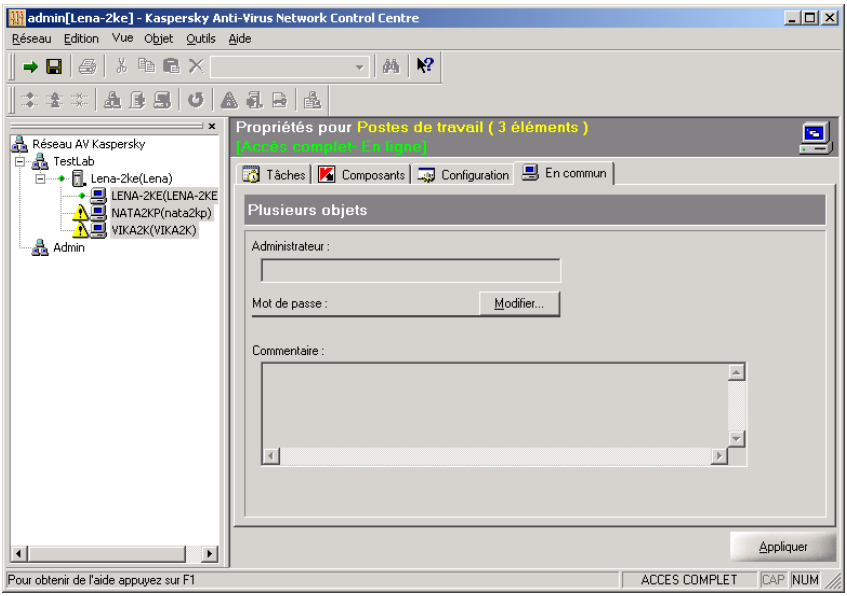

Illustration 99. Trois postes de travail sont choisis. Onglet **Général**

*Ouvrez l'onglet **Général** et indiquez le mot de passe pour l'accès de réseau au serveur. Pour ce faire :*

1. Dans la zone **Mot de passe** cliquez sur **Modifier**.
2. Une boîte de dialogue **Modifier le mot de passe** apparaît (voir: Illustration 100). Indiquez le mot de passe d'accès au réseau et sa confirmation dans les champs de saisie correspondants.

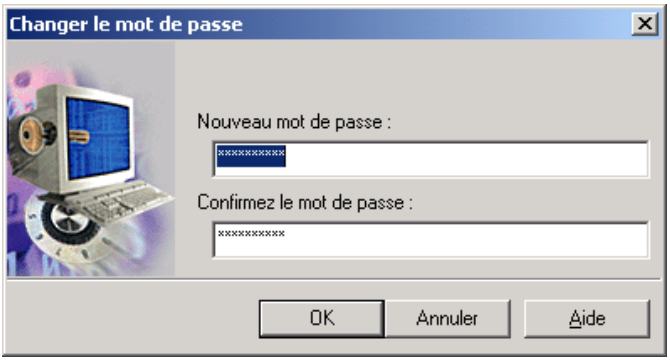

Illustration 100. Changer le mot de passe

3. Cliquez sur **Ok**.
4. Si un seul objet a été choisi pour édition vous pouvez si nécessaire éditer le texte dans la zone **Commentaire** de l'onglet **Général** dans la fenêtre principale...
5. Cliquez sur **Appliquer**.

APPENDIX A. AIDE DES MENUS DU PROGRAMME

A.1. Menu Réseau

Commande	Raccourci clavier	Bouton dans la barre d'outils	Commentaire
Saisie de mot de passe d'accès	<Ctrl>+<L>		Accès au programme (voir paragraphe 8.2).
Enregistrer la configuration du réseau	<Ctrl>+<S>		Sauvegarder la structure du réseau logique sur le disque du serveur principal (voir le paragraphe 7.7.1).
Exporter la configuration du réseau	–	–	Exporter la structure du réseau logique dans un fichier de texte (voir le paragraphe 7.7.1).
Impression	<Ctrl>+<P>		Imprimer la structure du réseau logique (voir le paragraphe 7.7.1).
Consultation préalable	–	–	Montrer la fenêtre de la consultation préalable de la structure du réseau logique avant l'impression.
Configuration d'impression	–	–	Afficher le dialogue de configuration des paramètres d'impression.
Quitter	–	–	Quitter le programme.

A.2. Menu Édition

Commande	Raccourci clavier	Bouton dans la barre d'outils	Commentaire
Couper	<Ctrl>+<X>		Copier et supprimer un objet du réseau logique.
Copier	<Ctrl>+<C>		Copier les paramètres d'un poste de travail (voir le paragraphe 7.7.1).
Coller	<Ctrl>+<V>		Insérer un objet du réseau logique ou les paramètres du poste de travail (voir le paragraphe 7.7.1).
Supprimer	<Del>		Supprimer un objet du réseau logique.
Renommer	–	–	Renommer un objet du réseau logique.
Développer tous les sous-niveaux			Afficher les éléments de la ramification du réseau logique commençant avec un objet donné.
Sélectionner			Choisir dans la liste d'objets les objets correspondants aux règles certains (??. ?. 9.1).
Rechercher	<Ctrl>+<F>		Rechercher un objet réseau logique (voir le paragraphe 6.7).

A.3. Menu Vue

Commande	**Raccourci clavier**	**Bouton dans la barre d'outils**	**Commentaire**
Rapport du réseau			Afficher le rapport du réseau (voir le paragraphe 9.1).
Barre d'outils	–	–	Sous-menu pour supprimer les barres d'outils de l'écran (ou bien pour les rentrer - voir le paragraphe 5.3).
Barre d'état	–	–	Afficher (ou masquer) la barre d'état de l'écran (voir paragraphe 5.8).
Barre d'informations	–	–	Afficher (ou masquer) la barre d'informations de l'écran (voir le paragraphe 5.7).
Barre du réseau	–	–	Afficher (ou masquer) la liste des objets du réseau logique de l'écran (voir le paragraphe 5.4).

A.4. Menu Objet

Commande	**Raccourci clavier**	**Bouton dans la barre d'outils**	**Commentaire**
Recharger les paramètres d'objet	<F5>		Mettre à jour les propriétés d'un objet du réseau logique.

Commande	Raccourci clavier	Bouton dans la barre d'outils	Commentaire
Annuler l'indicateur 'Attention'	–		Eliminer le statut **Attention** du poste de travail (voir le paragraphe 9.5).
Ajouter un groupe	<Ctrl>+<G>		Ajouter un groupe au réseau logique (voir le paragraphe 6.1).
Ajouter un serveur	<Ctrl>+<E>		Ajouter un serveur au réseau logique (voir le paragraphe 6.2).
Ajouter un poste de travail	<Ctrl>+<W>		Ajouter un poste de travail au réseau logique (voir le paragraphe 6.3).
Transférer les produits sur Kaspersky AV Server	–		Charger les produits de Kaspersky Anti-Virus® dans l'entrepôt du serveur Kaspersky AV (voir le paragraphe 6.4.1).
Distribuer le fichier de clé de Kaspersky AV			Installer le fichier de clé de l'utilisateur sur un poste de travail (voir le paragraphe 9.9).
Exporter la configuration	–	–	Exporter les paramètres d'un poste de travail ou d'un serveur dans un fichier (voir le paragraphe 7.7.2).

A.5. Menu Outils

Commande	Raccourci clavier	Bouton dans la barre d'outils	Commentaire
Ping ordinateur	–	–	Exécuter la commande de système Ping (voir le paragraphe 9.4).
Options			Régler les périodes d'attente du réseau logique (voir le paragraphe 9.4).

A.6. Menu Aide

Commande	Raccourci clavier	Bouton dans la barre d'outils	Commentaire
Sommaire	–	–	Appeler le système d'aide (voir le paragraphe 5.9).
Qu'est-ce que c'est ?	<Shift>+<F1>		Appeler l'aide contextuelle.
Recherche	–	–	Appeler une boîte de dialogue de recherche du sommaire du fichier d'aide.
Glossaire	–	–	Appeler le glossaire.
À propos de Kaspersky® Network Control Centre	–	–	Afficher les renseignements sur le logiciel Kaspersky® Network Control Centre.

APPENDIX B. SOMMAIRE DES BARRES D'OUTILS

B.1. Barre d'outils standard

Bouton	Menus	Raccourci clavier	Commentaire
	Réseau | Saisie de mot de passe d'accès	<Ctrl>+<L>	Entrer le programme (voir le paragraphe 8.2)..
	Réseau | Sauvegarder la configuration du réseau	<Ctrl>+<S>	Sauvegarder la structure du réseau logique sur le disque du serveur principal.
	Fichier | Impression	<Ctrl>+<P>	Imprimer la structure du réseau logique.
	Edition | Couper	<Ctrl>+<X>	Copier et supprimer un objet du réseau logique.
	Edition | Copier	<Ctrl>+<C>	Copier les paramètres d'un poste de travail (voir le paragraphe 7.1.1).
	Edition | Coller	<Ctrl>+<V>	Insérer un objet du réseau logique (voir le paragraphe 6.5) ou les paramètres du poste de travail.
	Edition | Supprimer	<Del>	Supprimer un objet du réseau logique.

Bouton	Menus	Raccourci clavier	Commentaire
admin	–	–	Rechercher un objet réseau logique par son nom (voir le paragraphe 6.7).
	Edition | Rechercher	<Ctrl>+<F>	Rechercher un objet réseau logique (voir le paragraphe 6.7).
	Aide | Sommaire	<Shift>+<F1>	Appeler l'aide contextuelle (voir le paragraphe 5.9).

B.2. Barre d'actions

Bouton	Menus	Raccourci clavier	Commentaire
	Edition | Sélectionner | Les postes de travail en ligne		Sélectionner tous les postes de travail en ligne dans la liste des objets du réseau logique (voir le paragraphe 9.1).
	Edition | Sélectionner | Postes de travail avec indicateur **Attention**		Sélectionner tous les postes de travail cochés **Attention** dans la liste des objets du réseau logique (voir le paragraphe 9.1).
	Edition | Sélectionner | Postes de travail hors-ligne		Sélectionner tous les postes de travail hors-ligne dans la liste des objets du réseau logique (voir le paragraphe 9.1).

Bouton	Menus	Raccourci clavier	Commentaire
	Objet | Ajouter un groupe	–	Ajouter un groupe au réseau logique (voir le paragraphe 6.1).
	Objet | Ajouter un serveur	–	Ajouter un serveur au réseau logique (voir le paragraphe 6.2).
	Objet | Ajouter un poste de travail	–	Ajouter un poste de travail au réseau logique (voir le paragraphe 6.3).
	Objet | Annuler l'indicateur 'Attention'	–	Eliminer le statut **Attention** du poste de travail (voir le paragraphe 9.5).
	Objet | Recharger les paramètres d'objet	<F5>	Mettre à jour les paramètres d'un objet du réseau logique.
	Objet | Transférer les produits sur Kaspersky AV Server	–	Charger les produits de Kaspersky Anti-Virus® dans l'entrepôt des programmes du serveur Kaspersky AV (voir le paragraphe 6.4.1).
	Objet | Distribuer le fichier de clé		Installer le fichier de clé de l'utilisateur sur un poste de travail (voir le paragraphe 9.9).
	Vue | Rapport du réseau		Appeler de la vue du rapport du réseau (voir le paragraphe 9.1).

APPENDIX C. GLOSSAIRE

Administrateur du groupe - l'utilisateur commandant les *serveurs* et *postes de travail* qui font partie d'un certain *groupe*.

Administrateur du réseau logique - l'utilisateur qui a créé *la configuration initiale de réseau*. L'administrateur du réseau logique définit son *nom symbolique* et le *mot de passe de l'administrateur* au premier lancement du programme *Kaspersky® Network Control Centre*.

Administrateur - *l'administrateurs du réseau logique* ou *l'administrateur du groupe*. L'administrateur peut désigner les administrateurs pour son groupe et pour les groupes qui en font partie à tout niveau de la hiérarchie. De l'autre côté, l'administrateur peut changer les droits des administrateurs des groupes faisant partie de son groupe, sans considérer qui avait affecté ce droit.

Kaspersky Anti-Virus® - sous ce nom général nous supposons le progiciel de la société Kaspersky Labs, destiné aussi bien pour les utilisateurs individuels que pour les réseaux corporatifs. Les composants du progiciel sont gérés par le programme d'administration *Kaspersky Anti-Virus® Control Centre*.

Attaque virale – une situation de l'infection simultanée (ou plutôt celle qui a lieu pendant une courte période de temps) de plusieurs ordinateurs du réseau. Les critères de l'attaque virale (période d'observation et nombre critique de cas d'infection) et le moyen d'en avertir sont indiqués parmi les paramètres du *serveur*.

Serveur principal du réseau logique - l'ordinateur où est enregistrée *la configuration du réseau*. Pour l'accomplissement de ces fonctions le logiciel *Kaspersky Anti-Virus® Server* doit être installé et lancé sur cet ordinateur.

Groupe - un ensemble des *serveurs* et des *postes de travail* y associés. Les groupes peuvent être unis en groupes formant un niveau de la hiérarchie plus élevé etc. Le regroupement des serveurs et des postes de travail par groupes et des groupes par groupes du niveau suivant n'est pas obligatoire - c'est une des possibilités du service qui peut être utile quand on travaille avec de grands réseaux dans les organisations à une structure compliquée parce qu'elle améliore la capacité du réseau logique d'être observé, et en outre de cela un administrateur à part peut être affecté à chaque groupe (*administrateur du groupe*). Le *réseau logique* en principe forme un groupe également (un groupe radical).

Arborescence des paramètres – élément de l'interface dans lequel toutes les données sont présentées sous la forme d'une arborescence, dont les nœuds sont les éléments standard de gestion (boutons, listes, commutateurs, etc.). Cela permet de cumuler les avantages de l'arborescence de l'information et les possibilités des éléments standards de gestion.

Quarantaine - un dossier pour enregistrer les fichiers infectés ou suspects en forme cryptée qui exclue l'activation du virus et l'analyse reprise. Lors du fonctionnement de Kaspersky Anti-Virus® sous *Kaspersky® Administration Kit* une possibilité existe de choisir entre le mode de quarantaine locale (sur le poste de travail) et celui de quarantaine du serveur, étant un des *entrepôts du serveur*.

Réseau logique - ensemble d'ordinateurs unis par un réseau soutenant le protocole TCP/IP, où pour la protection antivirale est utilisé le progiciel *Kaspersky Anti-Virus®* géré par le progiciel *Kaspersky® Administration Kit*. Sous "réseau " on supposera le réseau local ou plusieurs réseaux locaux unis à l'aide du protocole TCP/IP. Le réseau logique possède une structure hiérarchique qui comprend un seul *serveur principal*, un nombre libre de *serveurs* et de *postes de travail* y associés. Certains serveurs avec les postes de travail y associés peuvent être unis par des *groupes*.

La mise à jour des bases antivirales et des programmes du progiciel -une procédure de copie du contenu des *entrepôts du serveur* correspondants, à l'aide du composant *Kaspersky Anti-Virus® Updater*, depuis un poste de travail à un autre. Le contenu des entrepôts du serveur est mis à jour via Internet ou un autre serveur à l'aide du même programme.

Objets du réseau logique - les *postes de travail*, les *serveurs* et les *groupes* de tout niveau.

Package Kaspersky Anti-Virus® - voir *Kaspersky Anti-Virus®*.

Mot de passe de l'administrateur - un mot de passe protégeant la *configuration du réseau* des modifications non-sanctionnées. *L'administrateur du réseau logique définit* un mot de passe de ce type (avec son *nom symbolique*) à la première entrée au programme *Kaspersky® Network Control Centre*, et pour les autres administrateurs le mot de passe et le nom symbolique sont définis par l'administrateur qui les avait désignés. L'administrateur entre le nom symbolique et le mot de passe à chaque entrée au programme.

Mot de passe pour la protection des paramètres du poste de travail - mot de passe défini par l'*administrateur* pour limiter aux utilisateurs du *poste de travail* l'accès aux paramètres du progiciel *Kaspersky Anti-Virus®* sur le poste de travail (réglages de *Kaspersky Anti-Virus® Control Centre*) et pour pouvoir arrêter les tâches résidentes et non-résidentes.

Mot de passe pour l'accès de réseau au poste de travail un mot de passe qui protège le *poste de travail* de son association non-sanctionnée avec le *réseau logique*. Un mot de passe de ce type est défini par l'*administrateur* lors de l'installation du programme *Kaspersky Anti-Virus® Control Centre* sur le poste de travail.

Mot de passe pour l'accès de réseau au serveur - un mot de passe qui protège le *serveur* de son association non-sanctionnée avec le *réseau logique*.

Un mot de passe de ce type est défini lors de l'installation du programme *Kaspersky Anti-Virus® Server* sur le serveur.

Programme Kaspersky Anti-Virus® Control Centre est un programme permettant de superviser tous les logiciels du progiciel *Kaspersky Anti-Virus®*. Assure la connexion du progiciel *Kaspersky® Administration Kit* avec les composants du progiciel *Kaspersky Anti-Virus®*. Le programme peut également être installé sur le *serveur du réseau logique* pour gestion du processus de réception des mises à jour via le serveur.

Programme Kaspersky Anti-Virus® Server - composant du progiciel *Kaspersky® Administration Kit*. Est installé sur les *serveurs du réseau logique*.

Programme Kaspersky Anti-Virus® Updater – composant de *Kaspersky Anti-Virus®* responsable de la réception des mises à jour des bases antivirales et des programmes du progiciel. Ce programme est installé sur le serveur en tant que partie du progiciel *Kaspersky® Administration Kit* et sert à mettre à jour l'*entrepôt* du serveur correspondant, en ce cas il fonctionne sous gestion du programme *Kaspersky Anti-Virus® Control Centre*.

Programme Kaspersky® Network Control Centre - programme d'administration, faisant partie du progiciel *Kaspersky® Administration Kit*. Ce programme est installé sur les ordinateurs des *administrateurs*.

L'utilitaire Kaspersky® Administration Kit - un logiciel qui sert à l'organisation de la protection du réseau local des virus informatiques à l'aide de *Kaspersky Anti-Virus®*. L'utilitaire Kaspersky® Administration Kit permet à l'administrateur de gérer la progiciel de Kaspersky Anti-Virus® installé sur les ordinateurs associés au réseau local sans quitter son poste de travail. Le progiciel inclue un composant d'administration - le programme *Kaspersky® Network Control Centre* et le composant de service - le programme *Kaspersky Anti-Virus® Server*. La connexion du progiciel avec les applications de Kaspersky Anti-Virus® est assurée par le logiciel client - le programme *Kaspersky Anti-Virus® Control Centre* - qui est installé sur les ordinateurs des utilisateurs avec le progiciel Kaspersky Anti-Virus®.

Poste de travail - un ordinateur qui est l'objet de la protection antivirale. Le progiciel *Kaspersky Anti-Virus®* aussi bien que le programme *Kaspersky Anti-Virus® Control Centre* doivent y être installés. L'ordinateur peut être associé au *réseau logique* en qualité de poste de travail une fois seulement. Chaque poste de travail est associé au *serveur*.

Serveur -un ordinateur où le programme *Kaspersky Anti-Virus® Server* est installé. Ses fonctions consistent à l'enregistrement des *mises à jour* des bases antivirales et des programmes du progiciel Kaspersky Anti-Virus® pour les postes de travail, du logiciel installé à distance (voir *déploiement*), à l'envoi par courrier électronique des *alertes* issues par les composants du progiciel Kaspersky Anti-Virus® installés sur les *postes de travail* (les alertes sur la détection des virus par exemple), la détection de l'*attaque virale* et l'envoi d'une alerte portant sur ce

sujet. Plusieurs postes de travail peuvent être associées à un seul serveur. Voir *entrepôts du serveur*, *serveur principal*.

Configuration du réseau - fichier de renseignements sur la configuration du *réseau logique* et sur les paramètres des *objets du réseau logique*. Enregistrée sur le *serveur principal* du réseau logique. L'accès à la configuration du réseau n'est accordé qu'aux *administrateurs* après la saisie du *nom symbolique* et du *mot de passe de l'administrateur*.

Nom symbolique de l'administrateur est un nom indiqué par l'*administrateur* à l'entrée au programme *Kaspersky AV Network Control Centre*. Il est nécessaire d'accompagner le nom symbolique par un *mot de passe de l'administrateur*.

Alertes - messages diagnostiques générés par les tâches fonctionnant sur les postes de travail en cas d'occurrence de certains événements. La tâche du type " Kaspersky Anti-Virus® Scanner " par exemple formulera l'alerte "Un objet infecté a été détecté " à la détection de virus sur un poste de travail, et la tâche du type " Kaspersky Anti-Virus® Updater " en cas de tentative infructueuse de mise à jour des bases antivirales formulera l'alerte "Une erreur a eu lieu pendant la procédure de mise à jour ". Les alertes peuvent être envoyées depuis les *postes de travail* à l'administrateur directement d'un poste de travail (en ce cas une service de messagerie doit être formée sur le poste de travail) ou via le *serveur* (ce mode est préférable). Le programme *Kaspersky Anti-Virus® Server* permet de régler les paramètres personnalisés d'envoi des alertes pour les alertes de tout *niveau d'importance*.

Déploiement des composants de Kaspersky Anti-Virus® sur un poste de travail une procédure permettant à l'*administrateur* d'installer les programmes de Kaspersky Anti-Virus® sur les ordinateurs du réseau local sans quitter son poste de travail. En ce cas les composants nécessaires sont placés dans un des entrepôts du serveur (entrepôt des programmes) et ultérieurement sont copiés sur les ordinateurs de destination. Après l'installation du logiciel sur un *poste de travail* celui-ci peut être associé au serveur donné ou à un autre *serveur* et ensuite inclue au *réseau logique*.

Importance d'une alerte - une caractéristique selon laquelle le *serveur* forme des *alertes* qu'il reçoit des postes de travail depuis les tâches. Le serveur envoie les alertes aux niveaux d'importance divers aux différentes adresses de courrier électronique. Sont prévus les niveaux d'importance suivants pour les avertissements envoyés au serveur par les tâches de Kaspersky Anti-Virus® : "indicative " – les avertissements visant à informer, "bas " – avertissements importants, "haut " **–** avertissements plus importants, "critique " – avertissements les plus importants. Ainsi, les avertissements "Objet infecté trouvé " et "Objet effacé " générés par le composant Kaspersky Anti-Virus® Scanner ont le niveau d'importance "critique ".

Entrepôts du serveur - dossiers de réseau pour enregistrement des *mises à jour* des bases et programmes antiviraux, des composants du progiciel

Kaspersky Anti-Virus® pour ***déploiement*** et pour les fichiers mis en ***quarantaine*** par les programmes antiviraux su progiciel. Itinéraire aux entrepôts est enregistré dans les paramètres du ***serveur***.

APPENDIX D. ANNEXE D. LISTE DES QUESTIONS FREQUEMMENT POSES

Question. Quels produits de Kaspersky Labs fonctionnent avec Kaspersky® Administration Kit ?

Réponse. Kaspersky Anti-Virus® for Workstation, Kaspersky Anti-Virus® for MS NT Server, Kaspersky Anti-Virus® for Firewall, Kaspersky® Inspector, Kaspersky® WEB Inspector.

Question. Quels composants de Kaspersky Anti-Virus® peuvent être gérés par le programme d'administration Kaspersky® Network Control Centre ?

Réponse. Kaspersky AV Control Centre, Kaspersky AV Updater, Kaspersky AV Scanner, Kaspersky AV Monitor, Kaspersky AV pour Firewall

Question. Décrivez la procédure suggérée de transition des versions précédentes de Kaspersky® Network Control Centre à Kaspersky® Administration Kit.

Réponse. Nous recommandons la désinstallation complète de la version précédente du logiciel Kaspersky® Network Control Centre et l'installation ultérieure de la nouvelle version.

Avant la désinstallation de la version précédente il faut enregistrer la configuration du réseau logique dans un fichier. Au premier lancement de la nouvelle version du programme depuis ce fichier il est nécessaire d'exécuter l'importation de la configuration du réseau.

Question. Quels produits informatiques peuvent être installés à l'aide de la fonction de déploiement (Kaspersky® Deployment Tool)?

Réponses. Kaspersky Anti-Virus® for Workstation, Kaspersky Anti-Virus® for MS NT Server, Kaspersky® Inspector, Kaspersky® Administration Kit, Kaspersky® Virus Encyclopaedia.

Question. Le tampon d'échange ne fonctionne pas pour plus qu'un objet.

Réponse. Cette possibilité n'est pas réalisée dans la version actuelle de NCC.

Question. Le transfert d'objets ne fonctionne pas.

Réponse. Le transfert d'objets est désactivé dans la version actuelle de NCC.

Question. Décrivez les différences de gestion des paramètres des tâches Kaspersky AV Scanner et Kaspersky AV Monitor via Kaspersky AV Control Centre et Kaspersky® Network Control Centre.

Réponse. Lors de configuration des tâches de Kaspersky AV Scanner et Kaspersky AV Monitor via Kaspersky® Network Control Centre un nombre de possibilité est absent.

1) Une possibilité de travailler avec les paramètres des tâches du scanner et du moniteur est absente en mode **Expert**.

2) Impossible de voir le disque local de la machine éloignée via la liste des objets aussi bien que via le clic du bouton **Observer** pendant la modification des paramètres (là où ce bouton est présent). L'ajout des disques et des dossiers à analyser est effectué via l'option **Ajouter un dossier** du menu contextuel. Dans la boîte de dialogue au même nom qui se présente lors de la sélection de cette option indiquez l'itinéraire complet du disque ou dossier à ajouter.

3) Une possibilité est absente de modifier l'autorisation/interdiction de lancement des programmes de l'utilisateur (le paramètre de la protection antivirale **Lancement du programme utilisateur** de la section **Tâches interdites**). Ce mode peut être défini lors du déploiement du progiciel Kaspersky Anti-Virus® sur les postes de travail pour quoi il faut indiquer le fichier contenant les paramètres nécessaires dans la zone **Fichier des paramètres de Kaspersky AV Control Centre.**

APPENDIX E. KASPERSKY LABS LTD.

Fondée en 1997, Kaspersky Labs Ltd. est actuellement la société de développement de logiciels de sécurité informatique la plus connue en Russie. Son large éventail de solutions comprend vous protège contre les virus informatiques, le courrier non sollicité et les intrusions de pirates informatiques.

Kaspersky Labs est une société internationale. Le siège social se situe en Russie et la société dispose de représentations commerciales au Royaume-Uni, en France, en Allemagne, au Japon, au Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Le Centre européen d'études des virus, le dernier-né des départements de la société, a vu le jour en France. Notre réseau de partenaires réunit plus de 500 sociétés dans le monde entier.

La compagnie est constituée actuellement de plus de 250 spécialistes hautement qualifiés dont 10 sont titulaires d'un MBA (diplôme d'administration d'entreprises), 15 possèdent un doctorat et 2 sont membres de l'éminente organisation informatique de recherche antivirus (CARO).

La valeur essentielle de la société – c'est le savoir et l'expérience uniques accumulés par ses collaborateurs au cours de 14 années d'une lutte impitoyable contre les virus informatiques. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Labs. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Labs a été une des premières sociétés à développer plusieurs normes modernes pour les logiciels antivirus. Kaspersky Anti-Virus®, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : postes de travail, serveurs de fichiers, serveurs Web, serveurs de courrier électronique, pare-feu et ordinateurs de poche. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux éditeurs de logiciels étrangers utilisent dans leurs produits le noyau de Kaspersky Anti-Virus®. Citons par exemple : Nokia ICG (Etats-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Labs bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la

moindre de leurs attentes. Nous élaborons, mettons en oeuvre et accompagnons les dispositifs de protection antivirale pour entreprise. Notre base antivirus est mise à jour toutes les douze heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

E.1. Autres produits antivirus

Kaspersky Anti-Virus® Lite

Le logiciel antivirus le plus facile à utiliser de Kaspersky Labs est conçu pour protéger les ordinateurs à usage personnel sous Windows 98/Me, Windows 2000/NT Workstation et Windows XP.

Kaspersky Anti-Virus® Lite comprend :

- **Un analyseur antivirus** qui vérifie de manière exhaustive le contenu de tous les disques locaux et partagés à la demande de l'utilisateur ;
- **Un moniteur antivirus** qui vérifie automatiquement et en temps réel tous les fichiers utilisés ;
- **Un analyseur de bases de données de courrier** MS Outlook Express, capable de détecter des virus à la demande.

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Windows 98/ME, Windows 2000/NT et Windows XP contre tous les types de virus connus, y compris les chevaux de Troie, les vers Internet, les virus de script, les ActiveX et les applets Java dangereux, etc. Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Kaspersky Anti-Virus® Personal comprend un module de mise à jour quotidienne via Internet. Le système unique d'analyse heuristique des données de deuxième génération neutralise efficacement les virus inconnus. L'interface utilisateur conviviale permet de modifier rapidement la configuration et facilite au maximum l'utilisation du logiciel.

Kaspersky Anti-Virus® Personal permet :

- **L'analyse antivirale à la demande** des disques locaux ;
- **L'analyse antivirale automatique en temps réel** de tous les fichiers utilisés ;
- **Le filtrage du courrier** pour analyser en arrière-plan les messages entrants et sortants.

Kaspersky Anti-Virus® Personal 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.

Kaspersky Anti-Virus® Personal Pro

Ce logiciel a été conçu pour la protection antivirale globale des ordinateurs personnels qui tournent sous Windows 95/98/ME, Windows 2000/NT et Windows XP avec les applications de la suite MS Office 2000. Kaspersky Anti-Virus® Personal Pro renferme un programme qui assure le téléchargement quotidien des mises à jour des bases antivirus ou des modules du logiciel. Le système unique d'analyse heuristique des données de deuxième génération neutralise efficacement les virus inconnus. L'interface utilisateur, simple et conviviale, permet de modifier rapidement la configuration et facilite au maximum l'utilisation du logiciel.

En plus de l'analyse automatique de tous les fichiers en temps réel ou à la demande, Kaspersky Anti-Virus® Personal Pro propose également un filtre de courrier électronique ainsi qu'un **inhibiteur de comportement** qui garantit une protection totale contre les virus de macro.

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® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable contre les virus les données conservées dans un PDA sous système d'exploitation Palm OS ou Windows CE, ainsi que toute information transférée à partir d'un PC ou une carte mémoire, les fichiers ROM et les bases de données. 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 sur le PDA 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[4] intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail.

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

[4] En fonction du type de livraison

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 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- Flux de données qui passent par les pare-feu ;
- Ordinateurs de poche.

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.

E.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Labs Ltd. (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
Informations générales	WWW : http://www.kaspersky.com http://www.viruslist.com E-mail : sales@kaspersky.com

APPENDIX F. CONTRAT DE LICENCE

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

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

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN OUVRANT LE BOÎTIER DU CD, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. VOUS DEVEZ RETOURNER CE LOGICIEL POUR UN REMOOURSEMENT TOTAL. VOTRE DROIT AU RETOUR ET AU REMOOURSEMENT EXPIRE 30 JOURS APRES L'ACHAT CHEZ UN DISTRIBUTEUR OU REVENDEUR AGREE PAR KASPERSKY LABS. LE DROIT AU RETOUR ET AU REMOOURSEMENT 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 du logiciel ("Fichier Clé d'Identification ") qui vous sera fournie par Kaspersky Labs comme faisant partie du Logiciel.

1. Octroi de la Licence. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Labs vous offre le droit non-exclusif et non-transférable d'utiliser une copie de cette version du Logiciel et de la documentation jointe (la "Documentation ") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer une copie du Logiciel sur un ordinateur, poste de travail, assistant digital personnel, ou tout autre appareil électronique pour lequel le Logiciel a été conçu (un "Système Client "). Si le Logiciel est inscrit en tant que suite ou paquet avec 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 sur le tarif en vigueur ou l'emballage du produit qui concerne chacun de ces Logiciels.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul ; il ne peut être utilisé sur plus d'un Système Client ou par plus d'un utilisateur à la fois, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation " sur un Système Client lorsqu'il est chargé dans la mémoire tampon (random-access memory ou RAM) ou installé dans la mémoire permanente (par exemple, disque dur, CDROM, ou autre périphérique de stockage) de ce Système Client. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

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

1.1.4 Il est interdit de copier (au-delà de ce qui est permis exappuyément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

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

1.2 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 exigée pour chaque Système Client ou "siège " pouvant se connecter au Serveur à tout moment, indifféremment du fait que de tels Systèmes Clients inscrits ou sièges sont connectés en même temps au Logiciel, y accèdent ou l'utilisent. L'utilisation d'un logiciel ou de matériel réduisant le nombre de Systèmes Clients ou sièges qui accèdent au Logiciel ou l'utilisent directement (par exemple, un logiciel ou matériel de "multiplexage " ou de "regroupement ") ne réduit pas le nombre de licences exigées (le nombre requis de licences égalerait le nombre d'entrées distinctes au logiciel ou matériel de multiplexage ou de regroupement

frontal). Si le nombre de Systèmes Clients ou sièges pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. Cette licence vous permet d'effectuer ou de télécharger autant de copies de la Documentation que le réseau compte de Systèmes Clients ou sièges possédant une licence d'utilisation du Logiciel, et pourvu que chaque copie contienne les notes de propriété de la Documentation.

1.3 Licences de 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 oeuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous permet d'effectuer ou de télécharger une copie de la Documentation pour chaque copie additionnelle autorisée par la licence de volume, pourvu que chaque copie contienne toutes les notes de propriété de la Documentation.

2. Durée. Ce Contrat est valable pour [un (1)] an à moins qu'il n'arrive à terme avant ce délai pour l'une des raisons notées ci-après. Ce contrat se terminera automatiquement si vous n'en respectez les termes, limites ou conditions décrites. Au-delà du terme ou expiration de ce Contrat, vous devez immédiatement détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez mettre un terme à ce Contrat à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. Assistance technique.

(i) Kaspersky Labs vous fournira une assistance technique ("Assistance Technique ") comme décrit ci-dessous pour une période d'un an à condition que :

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

(b) le Formulaire d'Inscription à l'Assistance Technique fourni avec ce Contrat ou disponible sur le site web de Kaspersky Labs ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Labs avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Labs de juger si vous remplissez les conditions nécessaires pour un accès aux services d'Assistance Technique.

(ii) L'Assistance 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 Politique de Confidentialité de Kaspersky Labs 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 Politique de Confidentialité.

(iv) "Assistance Technique " signifie

(a) Mises à jour hebdomadaires des bases de données antivirales ;

(b) Mises à jour gratuites du logiciel, incluant des mises à niveau de versions ;

(c) Assistance Technique étendue par E-mail et assistance téléphonique fournie par votre Vendeur et/ou Distributeur ;

(d) Mises à jour de détection et désinfection de virus sous 24 heures.

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

5. Confidentialité. Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Labs reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Labs. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

6. Limites de Garantie

(i) Kaspersky Labs 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 Labs ne garantit pas que le Logiciel et/ou la Documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions et d'erreurs ;

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

(iv) L'entière responsabilité de Kaspersky Labs ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Labs de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Labs ou à un ayant-droit au cours

de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel ;

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Labs, (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 Labs 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. Limites de Responsabilité

(i) (i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Labs 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);

(c) Perte de moyens de paiement ;

(d) Perte d'économies prévues ;

(e) Perte de marché ;

(f) Perte d'occasions commerciales ;

(g) Perte de clientèle ;

(h) Atteinte à l'image ;

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

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

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

8. Le sens et l'interprétation de ce Contrat devront être déterminés en accord avec les lois d'Angleterre et du Pays de Galles. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Labs était autorisé en tant que requérant à entamer des procédures dans n'importe quelle juridiction compétente.

9. (i) Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Labs, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet. En dehors des situations prévues dans les termes des 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 Labs ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé exappuyément dans ce Contrat.

(ii) Rien dans ce Contrat n'engagera la responsabilité de Kaspersky Labs pour toute Fausse Représentation faite en connaissance de cause.

(iii) La responsabilité de Kaspersky Labs pour Fausse Déclaration quant à une question fondamentale pour la capacité du créateur à exécuter ses engagements envers ce Contrat, sera sujette à la limitation de responsabilité décrite dans le paragraphe 7 (iii).