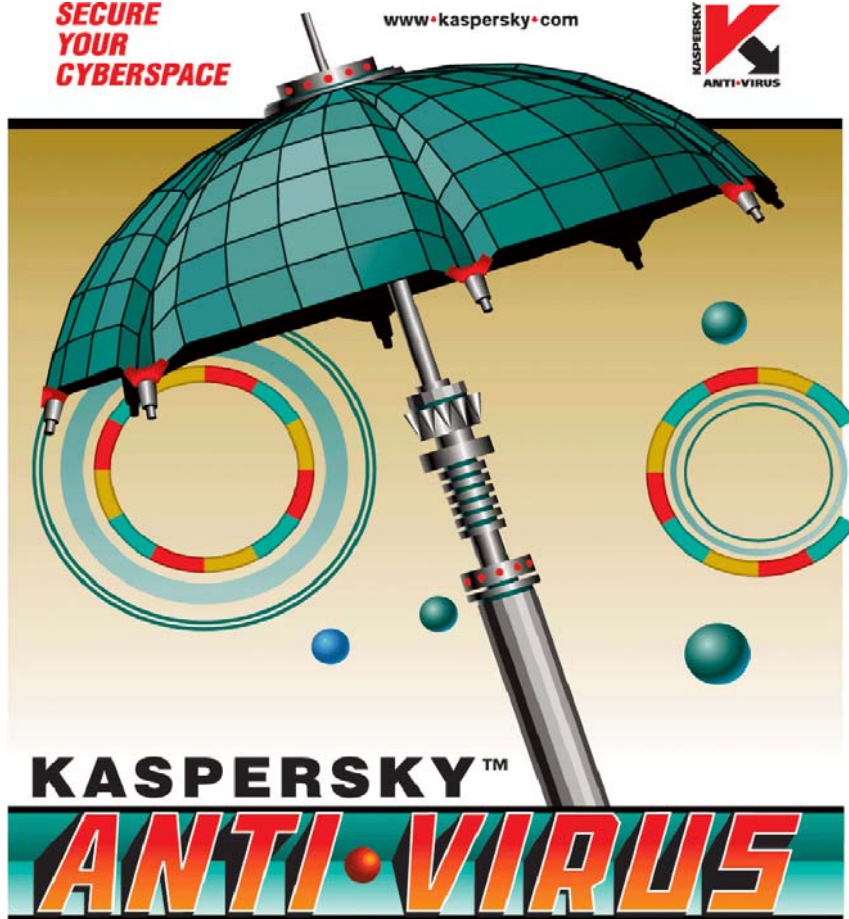


KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky® Administration Kit
version 5.0**

Livre de référence

KASPERSKY® ADMINISTRATION KIT
VERSION 5.0

Livre de référence

© Kaspersky Lab
Consultez notre site Web : <http://www.kaspersky.com/>

Date de révision : Décembre, 2005

Sommaire

CHAPITRE 1. KASPERSKY® ADMINISTRATION KIT.....	6
1.1. Objectif du document	8
1.2. Conventions utilisées dans cet ouvrage	8
CHAPITRE 2. PREMIERS PAS	10
2.1. Lancement du programme et connexion au serveur d'administration	10
2.2. Affectation de droits aux utilisateurs	14
2.3. Affichage des informations des sous-réseaux IP du réseau d'ordinateurs	18
2.4. Assistant Démarrage rapide	22
CHAPITRE 3. AFFICHAGE, CREATION ET CONFIGURATION D'UN RESEAU LOGIQUE	28
3.1. Affichage de la structure du réseau logique	28
3.2. Recherche d'un poste sur le réseau logique	36
3.3. Requêtes d'ordinateurs	41
3.4. Création, modification et suppression des groupes du réseau logique.....	46
3.5. Ajout, déplacement et suppression d'un ordinateur d'un réseau logique.....	49
3.6. Déplacement d'un client vers un autre réseau logique	51
3.7. Connexion locale du poste client au serveur d'administration	54
3.8. Vérification de la connexion du poste client au serveur d'administration	56
CHAPITRE 4. HIÉRARCHIE DES SERVEURS D'ADMINISTRATION.....	58
4.1. Connexion d'un serveur secondaire à un serveur primaire	58
4.2. Examen du réseau logique d'un serveur d'administration secondaire.....	60
CHAPITRE 5. INSTALLATION ET DESINSTALLATION D'APPLICATIONS SUR DES CLIENTS	61
5.1. Affichage des paramètres du paquet d'installation.....	61
5.2. Création de paquets d'installation	66
5.3. Configuration des paramètres du paquet d'installation de Network Agent	69
5.4. Création d'une tâche de déploiement d'application.....	70
5.5. Configuration de la tâche d'installation à distance	79
5.6. Désinstallation à distance du logiciel	81

5.7. Assistant de déploiement d'application	82
5.8. Installation locale de l'agent réseau	85
5.9. Installation locale du plug-in de console de Network Agent	90
5.10. Installation d'applications en mode silencieux	90
CHAPITRE 6. GESTION DE STRATEGIES	91
6.1. Création d'une stratégie pour une application	91
6.2. Affichage et modification d'une stratégie	94
6.3. Activation d'une stratégie	104
6.4. Création d'une stratégie pour Network Agent	105
6.5. Exportation et importation de stratégies	107
CHAPITRE 7. ADMINISTRATION DE TACHES	109
7.1. Création d'une tâche de groupe	109
7.2. Création d'une tâche globale	118
7.3. Création d'une tâche locale	119
7.4. Affichage et modification des paramètres de tâche	120
7.5. Tâche de démarrage / d'arrêt de l'application	128
7.6. Exportation et importation de tâches	129
7.7. Démarrage et arrêt des tâches	130
7.8. Suivi et affichage des comptes-rendus d'activité des tâches	131
7.9. Déploiement de tâches de groupe sur des serveurs d'administration secondaires	138
CHAPITRE 8. CONTROLE DES PARAMETRES D'APPLICATION	139
8.1. Affichage des paramètres d'application	139
8.2. Paramètres du serveur d'administration	143
8.3. Configuration de Network Agent	153
CHAPITRE 9. MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES DE PROGRAMME	154
9.1. Création de la tâche de mise à jour	154
9.2. Configuration de la tâche de mise à jour	157
9.3. Affichage de la liste de mise à jour	159
9.4. Déploiement de mises à jour automatiques	160
CHAPITRE 10. OPERATIONS SUR LA QUARANTAINE	162
CHAPITRE 11. ÉVÉNEMENTS, RAPPORTS ET NOTIFICATIONS	164

11.1. Enregistrement et affichage des événements et réception des notifications	164
11.2. Affichage et modification des modèles de rapport	172
11.3. Création d'un modèle de rapport	174
11.4. Génération et affichage de rapports	177
11.5. Génération de rapports récapitulatifs sur des serveurs d'administration secondaires.....	178
CHAPITRE 12. GESTION DES CLES DE LICENCE	180
12.1. Afficher des informations sur les clés de licence.....	180
12.2. Ajout d'une nouvelle clé de licence.....	182
12.3. Création et affichage de rapports sur les clés de licence	184
CHAPITRE 13. COPIE DE SAUVEGARDE ET RESTAURATION DES DONNEES DU SERVEUR D'ADMINISTRATION.....	186
13.1. Tâche de copie de sauvegarde	186
13.2. Utilitaire de copie de sauvegarde.....	189
ANNEXE A. QUESTIONS FREQUENTES	192
ANNEXE B. GLOSSAIRE	196
ANNEXE C. KASPERSKY LAB	203
C.1. Autres produits Kaspersky Lab	204
C.2. Comment nous contacter	209
ANNEXE D. CONTRAT DE LICENCE	211

CHAPITRE 1. KASPERSKY® ADMINISTRATION KIT

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

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

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

- Déployer des applications à travers le réseau sur des ordinateurs distants sous Windows. Cette fonction permet à l'administrateur de copier les distributions d'applications Kaspersky Lab nécessaires dans un ordinateur prédéfini puis de les déployer sur d'autres à travers le réseau.
- Contrôle des licences. Cette fonction permet d'installer des clés de licence pour toutes les applications Kaspersky Lab de manière centralisée, de surveiller la bonne application du Contrat de licence (c'est à dire, que le nombre de licences est en accord avec le nombre d'applications en cours d'exécution sur le réseau) ainsi que leur date de péremption.
- Gérer à distance des applications Kaspersky Lab à travers un réseau permettant de connecter des ordinateurs Windows. L'administrateur peut créer un système de protection antivirus à plusieurs niveaux et gérer toutes les applications à partir d'un même poste de travail administratif. Cette particularité est particulièrement importante dans le cas de sociétés de grande taille utilisant un réseau local avec de nombreux postes répartis sur plusieurs édifices ou bureaux séparés. Cette caractéristique permet à l'administrateur de :
 - Grouper les postes en tant que *groupes administratifs*, en fonction de leurs prestations et du nombre d'applications qui y sont installées ;
 - Configurer les applications de manière centralisée en créant et en appliquant des *stratégies de groupe*.
 - Configurer des paramètres isolés de l'application dans le cas de postes séparés, à l'aide des *Paramètres d'application*.

- Gérer l'activité des applications de manière centralisée en créant et en exécutant des *tâches locales ou de groupe*.
- Créer des modèles individualisés de fonctionnement d'une application, avec la création et l'exécution de tâches sur plusieurs postes appartenant à différents groupes administratifs.
- Mettre à jour automatiquement la base antivirus et les modules de programme sur les ordinateurs. Cette fonction permet d'assurer une mise à jour centralisée de la base antivirus de toutes les applications Kaspersky Lab installées, sans avoir à se connecter au serveur de mises à jour de Kaspersky Lab's sur Internet pour faire les mises à jour mise individuelles. La mise à jour peut s'effectuer automatiquement conformément à la planification définie par l'administrateur. L'administrateur peut surveiller l'installation des mises à jour sur les postes client.
- Recevoir des rapports à l'aide d'un poste dédié. Cette fonction permet de récupérer de manière centralisée des données statistiques sur toutes les applications Kaspersky Lab installées, de surveiller leur bon fonctionnement et de créer des rapports d'après les informations obtenues. L'administrateur peut créer un rapport sur l'activité d'une application, récapitulatif pour l'ensemble du réseau, ou pour chaque poste où l'application est installée.
- Utiliser le système de notification d'événements. Système d'envoi de notifications par messagerie. Cette fonction permet à l'administrateur de créer une liste des événements liés à l'activité des applications, sur lesquels il souhaite être informé. La liste de ces événements peut, par exemple, correspondre à la détection d'un nouveau virus, d'une erreur apparue en essayant de mettre à jour la base antivirus sur un ordinateur, ou d'un nouvel ordinateur sur le réseau.

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

- **Le serveur d'administration (Administration Server)** est un entrepôt centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau local de la société et un outil efficace de gestion de ces applications.
- **L'agent réseau (Réseau Agent)** coordonne les interactions entre le serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant prend en charge toutes les applications présentes dans Kaspersky Lab Business Optimal et Kaspersky Corporate Suite.

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



1.1. Objectif du document




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

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

1.2. Conventions utilisées dans cet ouvrage

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

Mise en forme	Signification / Usage
Gras	Titres de menus et de fenêtres, commandes, éléments de boîte de dialogue, etc.
 Note.	Information complémentaire, remarques
 Attention !	Informations nécessitant une attention particulière

Mise en forme	Signification / Usage
 <i>Pour exécuter...,</i> 1. Étape 1. 2. ...	Description de la succession des étapes que l'utilisateur doit suivre et des actions possibles.
 Tâche ou exemple	Définition d'un problème, exemple ou démonstration des possibilités de l'application
 Solution	Implémentation de la tâche
[option] – nom du paramètre	Paramètre de ligne de commande.
Texte des messages d'information et de la ligne de commande	Texte des fichiers de configuration, des messages d'information et de la ligne de commande.

CHAPITRE 2. PREMIERS PAS

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



Pour démarrer l'application,

Sélectionnez **Kaspersky Administration Kit** dans le groupe **Kaspersky Administration Kit** du menu standard **Démarrer\Programmes**. Ce groupe de programme est créé uniquement sur les postes administrateurs pendant l'installation de la console d'administration.



Pour vous connecter à un serveur d'administration :

sélectionnez l'entrée **Kaspersky Lab Administration Server (<Nom du serveur>)** dans l'arborescence de console.

Après ceci, l'application essaye de se connecter au serveur d'administration. S'il existe plusieurs serveurs d'administration sur votre réseau, le programme se connectera au dernier serveur utilisé lors d'une session précédente de Kaspersky Administration Kit. Lors du premier démarrage, l'application suppose que le serveur d'administration et la console d'administration se trouvent sur le même ordinateur. Par conséquent, le programme essaiera de détecter le serveur d'administration sur le poste utilisé.

Si le serveur est introuvable, il faut indiquer le nom de serveur manuellement dans la boîte de dialogue **Connexion au serveur** (voir Figure 1). Dans la zone **Adresse du serveur** indiquez l'adresse du serveur. Vous pouvez indiquer l'adresse IP ou le nom NetBIOS (nom du poste sur le réseau MS Windows). Les communications entre le serveur d'administration et la console d'administration sont sécurisées par SSL. Si vous voulez désactiver le protocole SSL, annulez la coche **Utiliser connexion SSL**. Cependant, ceci pourrait compromettre la sécurité des informations et l'intégrité de données.



Pour vous connecter au Serveur d'administration à travers un port différent du port par défaut, indiquez le <Nom du serveur>:<Numéro de port> dans le champ Adresse du serveur.

Cliquez sur **Options** pour afficher ou masquer les paramètres avancés suivants :

- **Utiliser connexion SSL.** Cochez cette case pour échanger des données entre le serveur d'administration et la console d'administration par SSL. Enlevez la coche si vous ne voulez pas communiquer par SSL. Cependant, ceci pourrait compromettre la sécurité et l'intégrité de données transmises.
- **Utiliser serveur proxy.** Cochez cette case pour vous connecter au serveur d'administration à travers un proxy. Indiquez l'adresse de connexion au serveur proxy dans le champ **Adresse du serveur proxy**. Complétez les champs **Utilisateur** et **Mot de passe** si une autorisation est nécessaire sur ce serveur proxy.

The screenshot shows a window titled "Connexion" with a close button in the top right corner. Inside the window, there is a label "Adresse du serveur :" followed by a text box containing "localhost". Below this are two checkboxes: "Utiliser connexion SSL" which is checked, and "Utiliser serveur proxy" which is unchecked. Under the second checkbox is a label "Adresse du serveur proxy :" followed by an empty text box. Below that are two more empty text boxes, one labeled "Utilisateur :" and the other "Mot de passe :". At the bottom of the window are three buttons: "OK", "Annuler", and "Options <<".

Figure 1. Connexion au serveur d'administration

Ensuite, la console d'administration vérifie les droits de connexion de l'utilisateur au serveur d'administration. Si le mode de connexion SSL est activé, la console d'administration authentifie le serveur d'administration avant de contrôler les droits utilisateur.

Si vous vous reliez au serveur pour la première fois ou si le certificat du serveur dans cette session diffère de votre copie locale, le programme affiche une demande de connexion au serveur et de réception d'un

nouveau certificat (voir Figure 2). Sélectionnez l'une des options suivantes :

- **Je veux me connecter au serveur et télécharger le certificat** – Sélectionnez cette option pour vous connecter au serveur d'administration et recevoir un nouveau certificat.
- **Je veux spécifier l'emplacement du fichier de certification** – Sélectionnez cette option pour indiquer l'emplacement du fichier de certification. Cliquez sur **Parcourir...** pour retrouver le fichier de certification. Le fichier possède une extension **.cer** et se trouve placé dans le dossier **Cert** du répertoire de Kaspersky Administration Kit sur le serveur d'administration. La console essaiera d'authentifier le serveur en utilisant le certificat que vous avez indiqué.



Vous pouvez copier le fichier de certification dans un dossier partagé ou une disquette. Cette copie peut être utilisée pour configurer des paramètres d'accès.

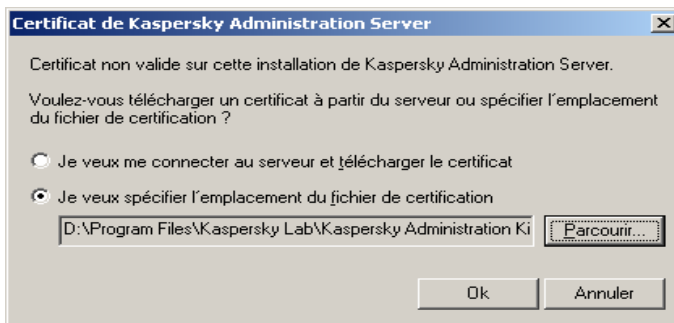


Figure 2. Demande de connexion au serveur d'administration.

Les droits des utilisateurs sont vérifiés en utilisant le procédé d'authentification d'utilisateur de Windows. Si l'utilisateur n'est pas autorisé à accéder au serveur d'administration, autrement dit, s'il ne dispose pas de privilèges d'opérateur (**KLOperators**) ou d'administrateur (**KLAdmins**) sur le réseau logique, essayez d'ouvrir la session sous un autre compte (voir Figure 3). Dans le format approprié, indiquez le compte d'utilisateur (nom et mot de passe) disposant de privilèges d'opérateur ou d'administrateur de réseau logique.

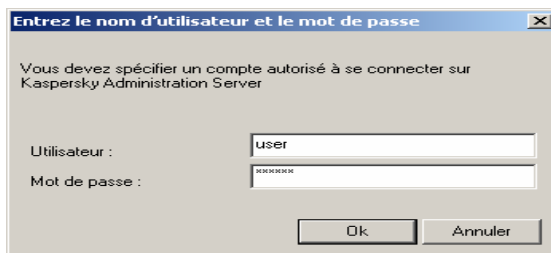


Figure 3. Enregistrement d'un utilisateur pour accéder au serveur d'administration

En cas de connexion réussie, la structure et les paramètres du réseau logique sont affichés dans l'arborescence de console.



Pour se déconnecter du serveur d'administration

sélectionnez l'entrée **Kaspersky Administration Server (<Nom du serveur>)** dans l'arborescence de console et cliquez sur **Déconnecter du serveur d'administration** dans le menu contextuel, ou utilisez son équivalent dans le menu **Action**).



Pour se connecter à un autre serveur d'administration :

Sélectionnez **Kaspersky Administration Server (<Nom du serveur>)** dans l'arborescence de console de la fenêtre principale de Kaspersky Administration Kit et cliquez sur l'option **Connexion au serveur** dans le menu contextuel ou dans le menu **Action**. Dans la boîte de dialogue **Connexion** (voir Figure 1), écrivez le nom du serveur (voir ci-dessus) et, au besoin, cochez la case **Utiliser connexion SSL** pour permettre une connexion sécurisée.



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

Si la connexion au serveur réussit, le contenu de l'entrée **Kaspersky Administration Server (<Nom du serveur>)** est mis à jour.



Pour ajouter un nouveau serveur d'administration à l'arborescence de console :

Sélectionnez l'entrée **Kaspersky Administration Server** dans la fenêtre principale de Kaspersky Administration Kit, ouvrez le menu contextuel, et

cliquez sur **Nouveau/Serveur KAV** (ou choisissez cette commande à partir du menu **Action**).

Une nouvelle entrée appelée **Kaspersky Administration Server (<Non connecté>)** apparaîtra dans l'arborescence de console. Utilisez cette entrée pour la connecter à un nouveau serveur installé sur votre réseau Windows.

2.2. Affectation de droits aux utilisateurs



Pour accorder aux utilisateurs des droits pour travailler sur le réseau logique du serveur d'administration:

1. sélectionnez l'entrée correspondant au serveur d'administration souhaité dans la fenêtre principale de Kaspersky Administration Kit, ouvrez le menu contextuel et choisissez **Propriétés**, ou utilisez son équivalent dans le menu **Action**.
2. Sélectionnez l'onglet **Sécurité** dans la fenêtre **Propriétés: <Nom du serveur>** ouverte (voir Figure 4).

La partie supérieure de l'onglet contient la liste des utilisateurs enregistrés sur le poste où la console d'administration est installée. La partie inférieure contient la liste des autorisations possibles :

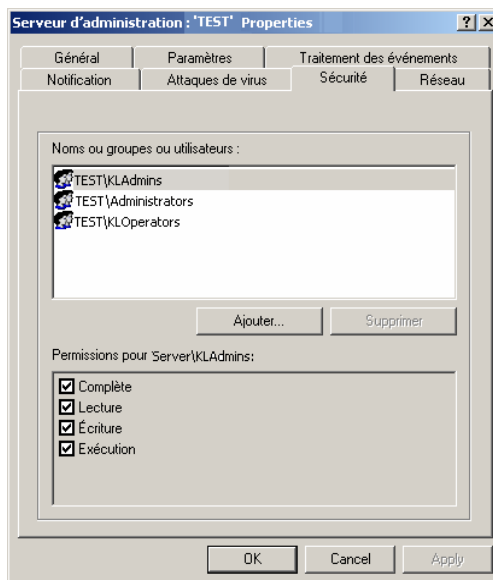


Figure 4. Affectation de droits d'accès au serveur d'administration

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

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

Pour attribuer des droits, sélectionnez le groupe d'utilisateurs souhaité et cochez les cases correspondant aux droits que vous voulez accorder. Si vous souhaitez cocher toutes les cases, cochez la case **Complète**.

Pour ajouter un nouveau groupe ou un nouvel utilisateur, cliquez sur **Ajouter**. Vous ne pouvez ajouter que des utilisateurs ou des groupes d'utilisateurs enregistrés sur l'ordinateur de la console d'administration.

3. Quand vous aurez terminé la configuration, cliquez sur **Appliquer** ou sur **Ok**.



Pour accorder des droits pour travailler sur un groupe administratif:

1. Sélectionnez le groupe administratif souhaité dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez **Propriétés** ou son équivalent dans le menu **Action**.
2. Sélectionnez l'onglet **Sécurité** dans la fenêtre **Propriétés: <Nom du serveur>** ouverte (voir Figure 5). Cet onglet est semblable à l'onglet **Sécurité** de la fenêtre de configuration des paramètres du serveur d'administration.

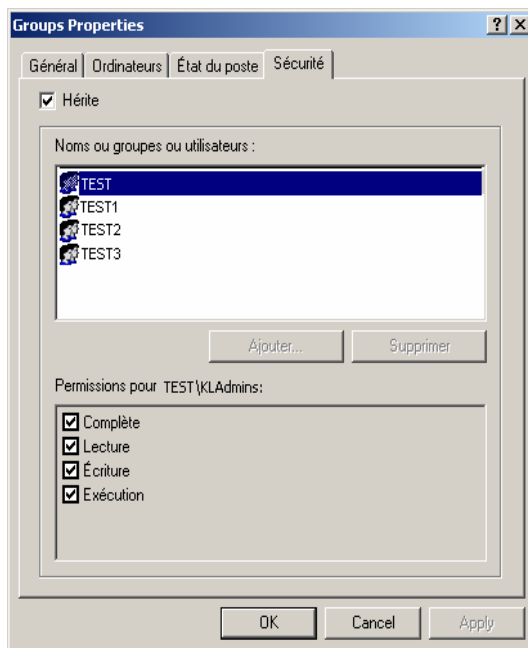


Figure 5. Attribution de droits à un groupe administratif

Les droits pour travailler sur le réseau logique et sur tous les objets compris dans sa structure sont configurés dans le réseau du serveur d'administration.

Pour configurer des droits d'accès séparés à un groupe administratif différent de celui spécifié dans les paramètres du serveur d'administration, décochez la case **Hérite**.

3. Après avoir configuré les droits d'accès, vous devrez autoriser les utilisateurs et les groupes d'utilisateurs de la listes. Les droits sont attribués de la même manière que pour le serveur d'administration.
4. Quand vous aurez terminé la configuration, cliquez sur **Appliquer** ou sur **Ok**.

2.3. Affichage des informations des sous-réseaux IP du réseau d'ordinateurs



Pour afficher les informations du réseau d'ordinateurs, que le Serveur d'administration récupère pendant un sondage périodique :

Sélectionnez **Réseau** dans l'arborescence de console.



*Pour sélectionner le format de présentation du réseau d'ordinateurs utilisé pour afficher le dossier **Réseau** ,*

sélectionnez le poste Réseau dans l'arborescence de console et choisissez une commande du groupe **Vue** dans le menu contextuel:

- **Domaines**– Affiche la structure du réseau d'ordinateurs comme une hiérarchie de dossiers reproduisant la la structure de domaines et de groupes de travail du réseau corporatif Windows. Au dernier niveau de chacun des dossiers, se trouve la liste de postes appartenant au domaine ou groupe de travail, mais qui n'appartiennent pas à la structure du réseau logique.
- **Active Directory**– Affiche la hiérarchie des dossiers correspondants à la structure Active Directory.
- **Sous-réseaux IP** – Affichage du réseau d'ordinateurs en tant que sous-réseaux IP.



Pour créer un nouveau sous-réseau IP :

1. Sélectionnez **Réseau** dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez la commande **Nouveau/Sous-réseau IP**, ou utilisez son équivalent dans le menu **Action**.



*La commande **Nouveau sous-réseau IP** est disponible uniquement si le dossier **Réseau** est présenté en tant que sous-réseaux IP.*

2. Dans la fenêtre **Nouveau sous-réseau IP** ouverte (voir Figure 6) spécifiez les valeurs des paramètres suivants :
 - Nom du sous-réseau ;

- Méthode de description du sous-réseau et valeurs des paramètres pour la méthode sélectionnée ;

Sélectionnez l'une des options suivantes :

- **Spécifiez le sous-réseau IP d'après en utilisant le masque d'adresse et de sous-réseau**; dans ce cas vous devez indiquer le **Masque de sous-réseau** et l'**Adresse de sous-réseau** dans les champs de saisie correspondants.
- **Sous-réseau IP d'après des adresses IP de début et de fin**; ensuite, indiquez les adresses IP de début et de fin.

Les valeurs des paramètres sont indiqués en notation décimale.

- un intervalle de temps après lequel les données d'un ordinateur inactif seront supprimées de la base de données du serveur d'administration - dans la **Durée de vie de l'adresse IP (heures)**.

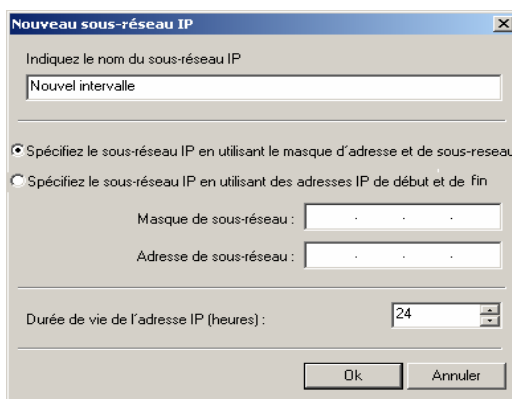


Figure 6. Création d'un nouveau sous-réseau IP

3. Quand vous aurez terminé la configuration, cliquez sur **Ok**.



Pour modifier les Paramètres de sous-réseau IP:

sélectionnez l'entrée correspondant au sous-réseau souhaité dans le dossier **Réseau**, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**, ou utilisez son équivalent dans le menu **Action**.

Ceci ouvrira la boîte de dialogue **Propriétés: <Nom du sous-réseau>** contenant les onglets **Général** et **Intervalles IP**.

Sur l'onglet **Général**, vous avez les possibilités suivantes (voir Figure 7):

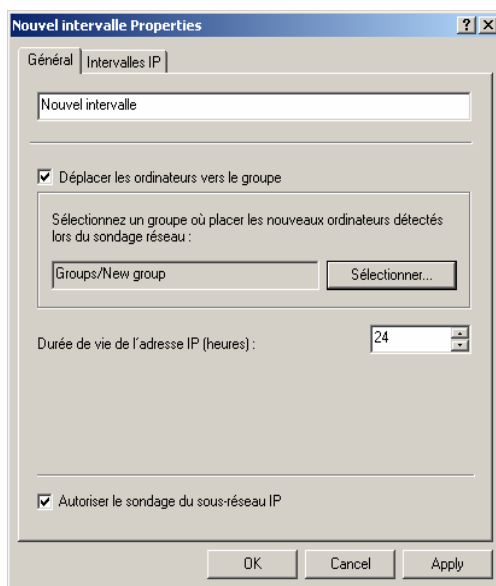


Figure 7. Affichage des paramètres du de sous-réseau IP
L'onglet **Général**

- Renommer le sous-réseau;
- Déterminer si le serveur d'administration déplacera automatiquement les nouveaux ordinateurs ajoutés au sous-réseau afin de les inclure dans la structure du réseau logique. Pour ce faire, cochez la case **Déplacer les ordinateurs vers le groupe** et sélectionnez le groupe administratif requis à l'aide de **Sélectionner**.
- Modifier la valeur de l'intervalle de temps après lequel les données d'un ordinateur inactif seront supprimées de la base de données du serveur d'administration - dans la **Durée de vie de l'adresse IP (heures)**.
- Autoriser ou annuler le sondage par le Serveur d'administration des ordinateurs du sous-réseau lorsqu'il effectue un sondage normal du réseau d'ordinateurs. Si vous ne souhaitez pas que le serveur d'administration sonde les ordinateurs lors du sondage suivant, décochez la case **Autoriser le sondage du sous-réseau IP**.

Vous pouvez ajouter ou supprimer des intervalles IP qui définissent le sous-réseau et modifier leurs paramètres dans l'onglet **Intervalles IP** (voir Figure 8).

- adresses IP de début et de fin de l'intervalle;
- masque de sous-réseau et adresse.

Pour ajouter un intervalle IP définissant le sous-réseau, cliquez sur **Ajouter**. Dans la fenêtre **Intervalle IP** ouverte (voir figure xx) spécifiez la méthode de description des intervalles puis saisissez les valeurs en fonction de la méthode choisie. Sélectionnez l'une des options suivantes :

- **Sous-réseau IP d'après l'adresse et le masque de sous-réseau**; dans ce cas vous devez indiquer le **Masque de sous-réseau** et l'**Adresse de sous-réseau** dans les champs de saisie correspondants.
- **Sous-réseau IP d'après des adresses IP de début et de fin**; ensuite, indiquez les adresses IP de début et de fin.

Les valeurs des paramètres sont indiquées en notation décimale.

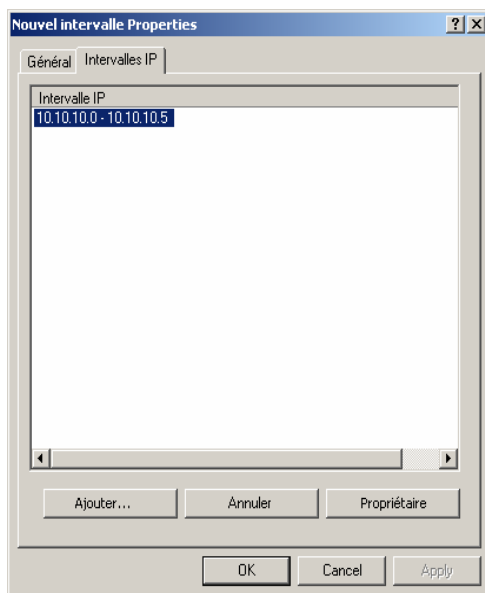


Figure 8. Affichage des paramètres du sous-réseau IP
L'onglet **Intervalles IP**

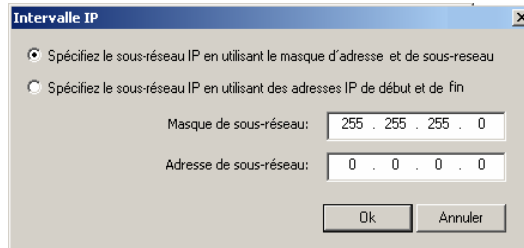


Figure 9. Ajout d'un Intervalle IP

2.4. Assistant Démarrage rapide



Pour créer un système de gestion centralisée de la protection antivirus :

1. Dans l'arborescence de console de la fenêtre principale de Kaspersky Administration Kit, sélectionnez **Kaspersky Lab Administration Server (<Nom de serveur>)** et ouvrez le menu contextuel correspondant à cette entrée. Cliquez sur **Assistant Démarrage rapide** dans le menu contextuel ou dans le menu **Action**.
2. C'est pendant cette première étape qu'intervient le sondage du réseau et l'indentification des ordinateurs (voir Figure 10). En fonction des résultats du sondage, un groupe de services Réseau et la structure du dossier Réseau sont mis en place. Les informations récupérées seront utilisées pour la création automatique du réseau logique. Pour afficher la structure du réseau d'ordinateurs, utilisez le lien **Afficher les résultats du sondage réseau**.

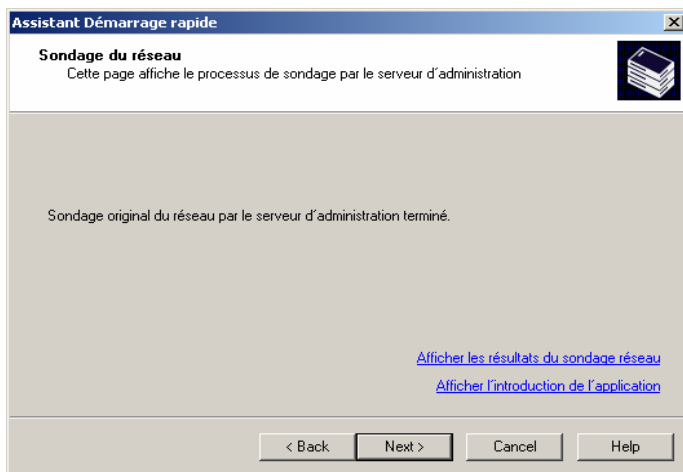


Figure 10. Sondage du réseau d'ordinateurs

3. Au cours de cette étape, vous devez spécifier la méthode de création d'un réseau logique (voir Figure 11). Vous avez le choix parmi les options suivantes :

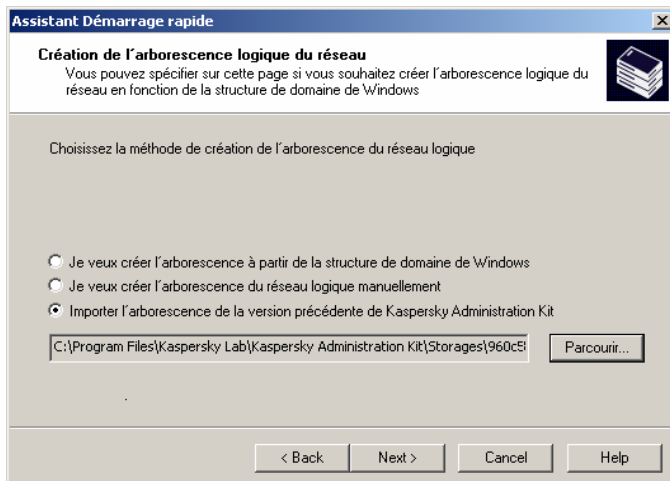


Figure 11. Assistant Démarrage rapide.
Choix de la méthode de création d'un réseau logique

- **Je veux créer l'arborescence à partir de la structure de domaine de Windows** – Crée un réseau logique

automatiquement, à partir de la structure des domaines de Windows et des groupes d'utilisateurs présents dans le dossier du groupe **Non attribué**.



Si un ordinateur en mode **Non attribué** n'est pas disponible quand vous créez un réseau logique (isolé ou déconnecté du réseau), l'Assistant n'ajoutera pas cet ordinateur au réseau logique. Vous pouvez ajouter cet ordinateur plus tard, au moment où vous configurez manuellement le réseau logique (voir section 3.5 à la page 49).



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

- **Je veux créer l'arborescence du réseau logique manuellement** – Crée un réseau logique plus tard.
- **Importer l'arborescence de la version précédente de Kaspersky Administration Kit** – Utilise la structure du réseau logique telle qu'elle existait dans les versions précédentes de Kaspersky Administration Kit. La structure sera reconstituée de la manière suivante : les serveurs et les groupes administratifs seront importés en tant que groupes administratifs ; les stations de travail affectées à chaque serveur seront ajoutées en tant que membres du groupe administratif correspondant.

Pour restaurer et importer la structure du réseau logique précédent, l'application utilise les données du fichier **ncd.dat** conservées dans le serveur principal. Ce fichier se trouve dans le dossier **NCD** du dossier d'installation de **Kaspersky Anti-Virus Server**. Le fichier de configuration sera automatiquement retrouvé si le serveur d'administration est installé sur le même ordinateur que le serveur principal précédent. Si le serveur d'administration ne retrouve pas le fichier **ncd.dat**, sélectionnez-le manuellement à l'aide du bouton **Parcourir**.

4. Dans la boîte de dialogue suivante de l'Assistant (voir Figure 12), configurez les paramètres d'envoi des alertes de messagerie et NET SEND générées par les applications Kaspersky Lab, et indiquez le modèle utilisé pour les alertes de messages (pour plus de détails, voir section 6.2 à la page 94). Ces paramètres seront

utilisés comme paramètres par défaut pour les stratégies d'application.

5. À l'étape suivante, vous devez configurer le système de protection antivirus (voir Figure 13).

Assistant Démarrage rapide

Paramètres de notification globale
Vous pouvez spécifier sur cette page les paramètres de par défaut pour les notifications administratives

Serveur SMTP pour envoi de notifications email :

Compte :
user@global.com

Adresse du serveur SMTP :
10.10.10.3

Port du serveur SMTP :
25

Ordinateurs pour notification NET SEND :
10.10.10.1

Texte du message...

< Back Next > Cancel Help

Figure 12. Configuration des paramètres de renvoi des notifications

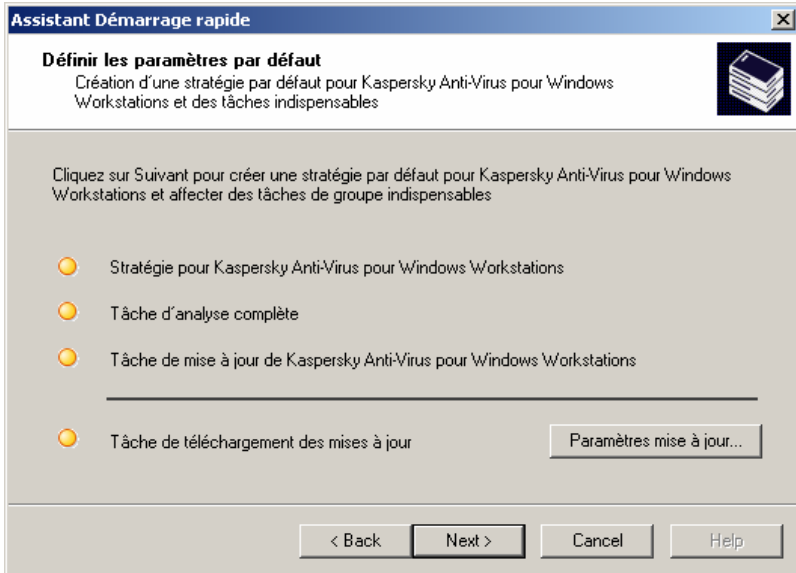


Figure 13. Assistant Démarrage rapide.
Configuration du système de protection antivirus

L'Assistant Démarrage rapide construit un système de protection antivirus pour les clients du réseau logique qui utilisent Kaspersky Antivirus 5.0 pour Windows Workstations. Dans ce cas, le serveur d'administration crée une stratégie et définit un ensemble minimum de tâches pour le niveau supérieur de la hiérarchie de Kaspersky Antivirus 5.0 pour Windows Workstations. Il configure également une tâche globale pour récupérer les mises à jour du serveur d'administration.

Lors de la mise en place un système de protection antivirus pour clients du réseau logique utilisant Kaspersky Antivirus 5.0 pour Windows Workstations, le serveur d'administration crée ce qui suit :

- Dans le dossier **Stratégies** du groupe **Groupes**, il crée une stratégie pour Kaspersky Antivirus 5.0 pour Windows Workstations. La stratégie est intitulée **Stratégie pour Kaspersky Anti-Virus pour Windows Workstations** et utilise une configuration par défaut.
- Dans l'entrée **Tâches globales** de l'arborescence de console, il existe une tâche globale pour mettre à jour le serveur d'administration. La stratégie s'appelle **Tâche de téléchargement des mises à jour** et utilise une configuration par défaut.

- La tâche de copie des données de sauvegarde du **Serveur d'administration** sous l'entrée **Tâches globales** de l'arborescence de console - avec le nom **Copie de sauvegarde des données du serveur d'administration** avec une configuration par défaut.
- Dans le dossier **Tâches** de la tâche **Groupe**, la tâche de mise à jour pour Kaspersky Antivirus 5.0 pour Windows Workstations est créée. La stratégie est intitulée **Stratégie pour Kaspersky Anti-Virus pour Windows Workstations** et utilise une configuration par défaut.
- Dans le dossier **Tâches** du groupe **Groupe**, la tâche d'analyse à la demande est créée pour Kaspersky Antivirus 5.0 pour Windows Workstations. La tâche est appelée **Tâche d'analyse complète** et utilise une configuration par défaut.



Aucune stratégie n'est créée pour Kaspersky Antivirus 5.0 pour Windows Workstations s'il en existait déjà une autre dans le dossier **Groupe**.

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

Au besoin, vous pouvez personnaliser les options de mise à jour. Pour ce faire, cliquez sur le bouton **Paramètres mise à jour...** et indiquez les valeurs requises dans la boîte de dialogue qui apparaît sur l'écran (pour plus de détails, voir section 9.2 à la page 157).

Cliquez sur **Suivant**. La fenêtre de l'Assistant montre la progression de la création des tâches et des stratégies. Un message d'erreur vous informe des éventuelles erreurs.

6. Dans la fenêtre finale, l'Assistant propose de lancer **L'assistant de déploiement**. Vous pouvez utiliser cet assistant pour installer l'agent réseau. Si vous ne souhaitez pas installer l'application immédiatement après la fin de l'Assistant Démarrage rapide, décochez la case **Lancer l'Assistant de déploiement d'application**.

CHAPITRE 3. AFFICHAGE, CREATION ET CONFIGURATION D'UN RESEAU LOGIQUE

3.1. Affichage de la structure du réseau logique



Pour afficher des informations sur un groupe qui fait partie du groupe de réseau logique :

Sélectionnez le dossier de groupe souhaité dans le dossier **Groupes**. La liste des objets présents dans ce groupe est affichée dans le panneau de détails (vous pouvez également développer la branche correspondante dans l'arborescence de console).

- Pour afficher le contenu des stratégies de groupe, sélectionnez le dossier **Stratégies**. Si des stratégies sont appliquées au groupe sélectionné, elles seront affichées dans le panneau de détails ; autrement le panneau de détails reste vide.
- Pour afficher le contenu des tâches de groupe, sélectionnez le dossier **Tâches**. Si des tâches ont été définies pour le groupe sélectionné, elles seront affichées dans le panneau de détails ; autrement le panneau de détails reste vide.
- Pour travailler avec le réseau logique du serveur d'administration secondaire, sélectionnez le dossier **Serveurs**.
- La liste des clients présents dans le groupe sélectionné est affichée dans le panneau de détails.



Pour afficher les paramètres du groupe et les paramètres d'interaction du serveur d'administration avec les postes clients qui font partie du groupe :

sélectionnez un dossier avec le nom du groupe souhaité dans le dossier **Groupes** puis utilisez la commande **Propriétés** dans le menu contextuel

ou dans le menu **Action**. La boîte de dialogue **Propriétés de <Nom de groupe>** s'affiche avec deux onglets : **Général** et **Ordinateurs**.

L'onglet **Général** (voir Figure 14) affiche les informations suivantes :

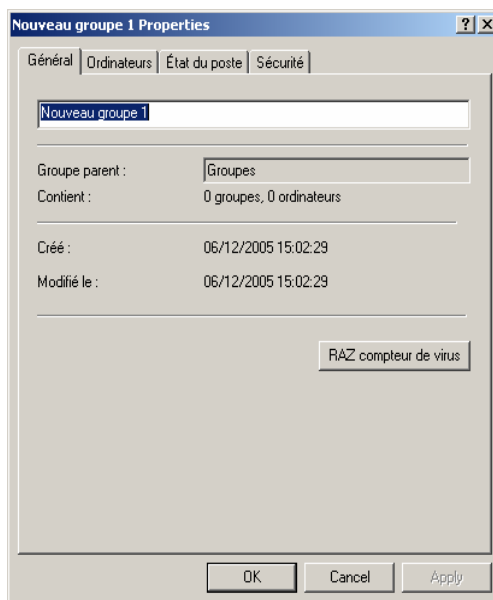


Figure 14. Affichage des propriétés du groupe. L'onglet **Général**

- Nom de groupe
- Nom du groupe parent (s'il n'y a aucun groupe parent pour ce groupe, la valeur est **Groupes**)
- Informations statistiques sur les structures de groupe – nombre de groupes imbriqués et le nombre total de clients, y compris des clients dans les groupes imbriqués.
- Date de création
- Date de dernière modification du nom ou des attributs du groupe (si le nom de groupe n'a pas changé, la valeur est **Inconnu>**)

Cliquez sur **RAZ compteur de virus** pour remettre à zéro le compteur de détection de virus pour tous les clients du groupe.

L'onglet **Ordinateurs** (voir Figure 15) affiche les informations suivantes :

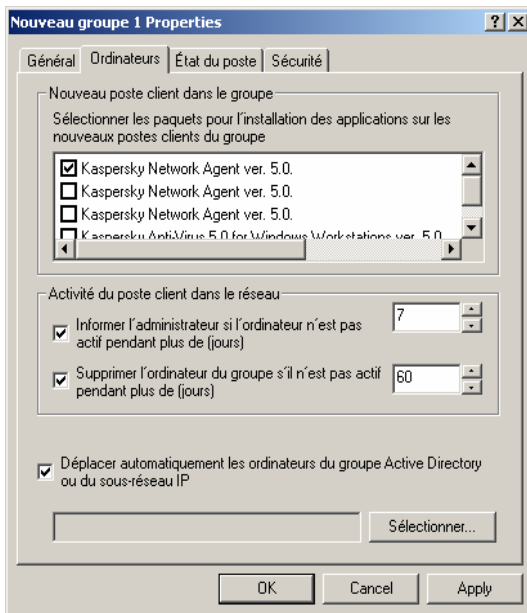


Figure 15. Affichage des propriétés du groupe. L'onglet **Ordinateurs**

- La section **Nouveau poste client dans le groupe** affiche les paquets d'installation employés pour l'installation à distance des applications Kaspersky Lab sur les nouveaux postes clients qui ont été ajoutés au groupe.

Pour les propriétés du groupe **Non attribué** (voir Figure 32), la section **Nouveau poste client dans le groupe** contient une case à cocher **Ajout d'ordinateur au groupe**. Si la case est cochée, les nouveaux ordinateurs du réseau Windows seront ajoutés automatiquement au groupe de réseau logique spécifié dans la zone de texte inférieure.

- La section **Activité du poste client dans le réseau** affiche les actions qui sont exécutées sur les clients qui ne répondent pas pendant un certain intervalle de temps (par exemple, en notifiant les administrateurs du réseau logique, ou en retirant ces clients du groupe).

L'onglet **État du poste** définit les critères de diagnostic de l'état des postes clients, en fonction de leur état de protection antivirus et des données concernant leur activité réseau. D'après ces critères, le poste client se verra affecter l'un des états suivants : **Critique** ou **Avertissement**. Si le

poste client ne vérifie aucune des conditions précédentes, alors son état est **Ok**.

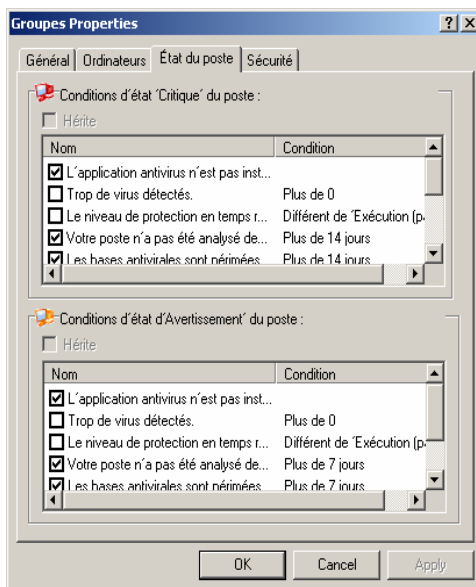


Figure 16. L'onglet **État du poste**

Il est possible de modifier les valeurs de seuil de certaines conditions. Pour ce faire, sélectionnez la condition requise dans la colonne Condition et double-cliquez sur elle pour ouvrir la fenêtre de modification (voir Figure 17).

Par exemple, vous pouvez établir le nombre maximum de jours pendant lesquels le client ne se sera pas connecté pas au serveur d'administration. À la fin de cette période de temps, l'ordinateur reçoit l'état **Critique**.

Si l'état de l'ordinateur est **Ok**, l'icône verte - est affichée. Si l'état de l'ordinateur est **Avertissement**, une icône jaune - sera affichée. Si l'état de l'ordinateur est **Critique**, une icône rouge - sera affichée.

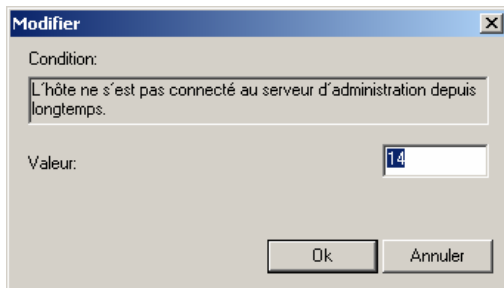


Figure 17. L'onglet Modifier l'État du poste

Les critères permettant de déterminer l'état du poste client sont définis dans les paramètres du groupe du niveau hiérarchique supérieur, et sont hérités par tous les groupes du réseau logique. Pour configurer des critères individuels pour un groupe, décochez la case Hérité(e) et configurez les paramètres.

- L'onglet **Sécurité** (voir Figure 5) est conçu pour configurer les droits d'accès au groupe administratif (voir section 2.2 à la page 14).



Pour afficher des informations sur un client de réseau logique :

Sélectionnez le groupe dans le dossier **Groupes** contenant le client souhaité. La liste des clients appartenant à ce groupe sera affichée dans le panneau de détails (vous pouvez également développer la branche correspondante dans l'arborescence de console). Sélectionnez le client et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. La boîte de dialogue **Propriétés de <Nom de poste>** s'affiche avec plusieurs onglets (voir Figure 18).



Pour retrouver le poste client recherché, utilisez la fonction **Rechercher** (voir section 3.2 à la page 36).

Sur l'onglet **Général** (voir Figure 18), vous avez les possibilités suivantes :

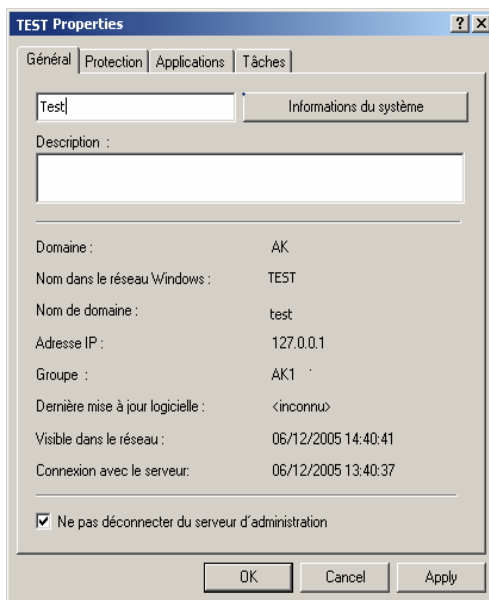


Figure 18. Affichage des propriétés du client. L'onglet **Général**

- Afficher les propriétés réseau de ce client.
- Afficher des informations sur la configuration client en cliquant sur **Infos système** (Figure 19).
- Modifier le nom d'hôte (le nom d'hôte est généralement attribué par le serveur d'administration ; il correspond au nom de l'ordinateur sur le réseau MS Windows (voir section
- Définir les paramètres de connexion avec le serveur d'administration en utilisant la case **Ne pas déconnecter du serveur d'administration**. Si la case est cochée, la connexion client-serveur est permanente. Par défaut, la connexion client-serveur est établie régulièrement afin de synchroniser ou de transmettre des données.



Notez qu'une connexion permanente ne devrait être attribuée qu'aux clients les plus importants, parce que le nombre total de connexions simultanées admises par le serveur d'administration est limité à quelques centaines.

L'information reflète les données reçues pendant la dernière session de synchronisation.

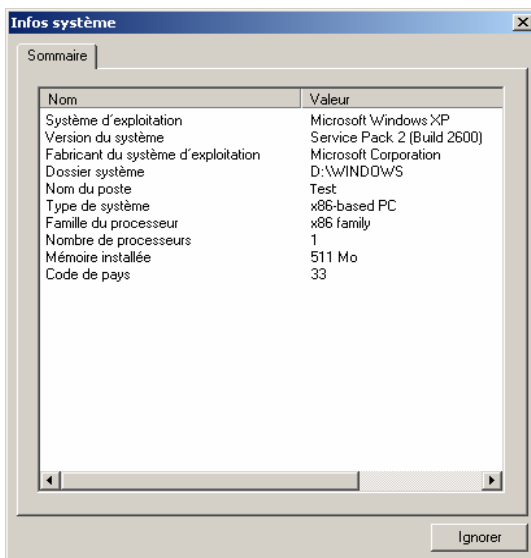


Figure 19. Affichage des caractéristiques du système d'un poste client

L'onglet **Protection** (voir Figure 20) affiche l'état actuel de la protection antivirus sur un poste client. Vous pouvez afficher les données suivantes :

- **Protection en temps réel**– Situation actuelle de la protection antivirus du client.
- **Dernière analyse complète** – Date et heure de la dernière analyse antivirus.
- **Virus trouvés** – Nombre de virus de virus détectés de la première analyse jusqu'à la remise à zéro du compteur. Pour remettre à zéro le compteur, cliquez sur **RAZ compteur de virus** dans le menu contextuel ou dans le menu **Action**.

- **État de protection** - Indicateur d'état du poste, d'après les critères de diagnostic de la protection antivirus et de l'activité réseau du poste, tels que déterminés par l'administrateur. Le champ **Description de l'état de protection** répertorie les conditions définissant les états du poste client.

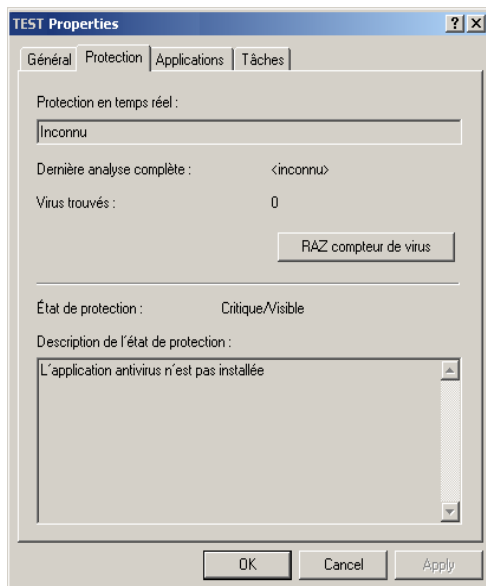


Figure 20. Affichage des caractéristiques système d'un client.
L'onglet **Protection**

L'onglet **Applications** (voir Figure 101) énumère toutes les applications Kaspersky Lab installées sur le poste client. Vous pouvez afficher des informations générales sur une application, contrôler son exécution, et configurer ses paramètres (pour des détails, voir section 7.9 à la page 138).

Sur l'onglet **Tâches** (voir Figure 21), vous pouvez contrôler des tâches pour des postes clients (afficher des tâches existantes, les supprimer et en créer de nouvelles, les lancer et les interrompre, modifier leurs paramètres, et afficher les comptes-rendus d'exploitation). Les informations sur les tâches reproduisent les données réceptionnées pendant la dernière session de synchronisation client-serveur. Le serveur d'administration questionne le client au sujet de l'état courant de tâche. Si la connexion échoue, l'état n'est pas affiché.

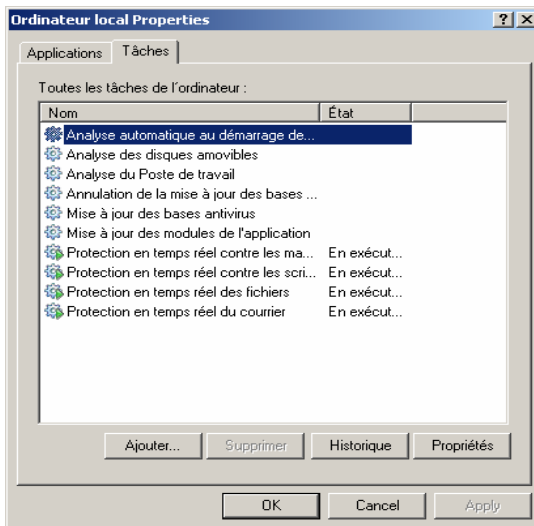


Figure 21. Affichage des caractéristiques système d'un client. L'onglet **Tâches**

3.2. Recherche d'un poste sur le réseau logique



Pour rechercher un ordinateur ou un groupe d'ordinateurs qui vérifient le critère spécifié,

sélectionnez l'entrée **<Nom du serveur d'administration>** du groupe administratif, ouvrez le menu contextuel puis sélectionnez **Rechercher un ordinateur**. Dans la boîte de dialogue, spécifiez les critères de recherche sous les onglets suivants : **Réseau**, **Application**, **État du poste**, **Protection Antivirus**.

Dans l'onglet **Réseau** (voir Figure 22), vous pouvez définir les critères de recherche suivants :

- **Nom de poste.**
- **Nom de l'ordinateur Windows.**
- **Domaine** auquel le poste appartient.
- **Intervalle d'adresses IP**

- **Intervalle après connexion précédente.** Spécifiez un intervalle de temps pendant lequel ce poste s'est connecté au serveur d'administration pour la dernière fois.

Trouver les ordinateurs

☒ Inclure des données avec les serveurs secondaires (jusqu'au niveau) : 2

Trouver maintenant

Réseau | Application | État du poste | Protection antivirus

Ignorer

Nom de poste :

Nom de l'ordinateur Windows :

Domaine :

☒ Intervalle d'adresses IP : à :

☒ Intervalle après connexion précédente : à :

Exporter dans fichier

Nom	Dom...	Derni...	Derni...	Etat	Derni...	Dom...	Nom ...
Test	Damain1			Ok	user		

Ordinateurs trouvés : 1

Figure 22. Recherche d'un ordinateur. L'onglet **Réseau**.

Sur l'onglet **Application** (voir Figure 23), spécifiez le critère suivant :

- **Nom de l'application.** Indiquez le nom de l'application installée sur le poste client.
- **Versión d'application.** Spécifiez la version de l'application installée sur le poste client.
- **Dernière mise à jour.** Spécifiez l'intervalle de temps pendant lequel la base antivirus et les composants d'application ont été mis à jour pour la dernière fois sur le poste client.

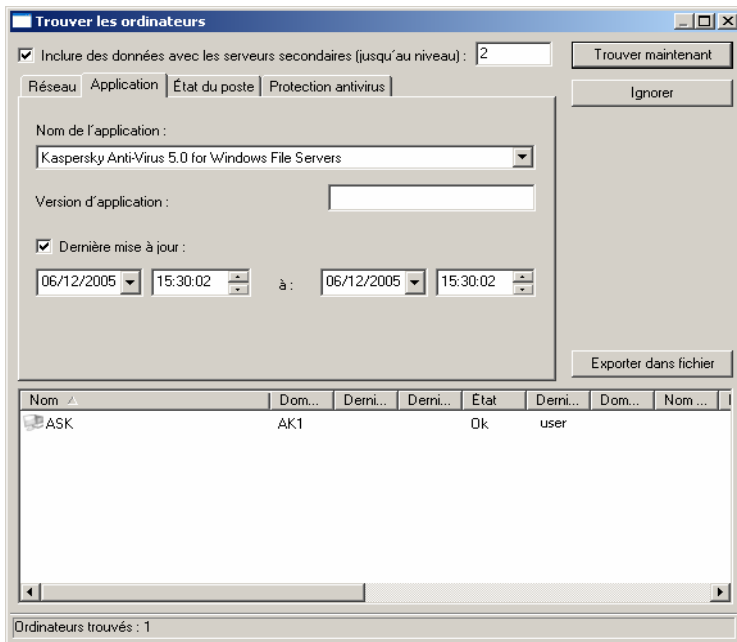
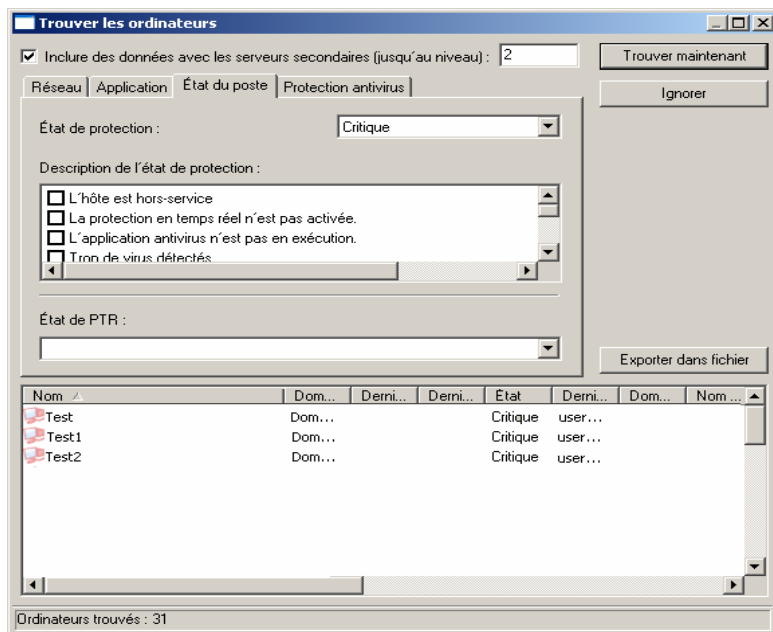


Figure 23. Recherche d'un ordinateur. L'onglet **Application**

Sur l'onglet **État du poste** (voir Figure 24), spécifiez le critère suivant :

- **État de protection.** Recherche d'ordinateurs avec les états suivants : **OK**, **Critique**, ou **Avertissement**.
- **Description de l'état de protection.** Cochez des conditions en fonction desquelles le poste client reçoit cet état
- **État de PTR.** Sélectionnez l'état actuel de protection en temps réel des ordinateur(s) que vous souhaitez trouver.

Figure 24. Recherche d'un ordinateur. L'onglet **État du poste**

Sur l'onglet **Protection** (voir Figure 25), indiquez le critère suivant :

- **Date des bases antivirus.**
- **Intervalle d'enreg. base antivirus.**
- **Dernière analyse complète.** Spécifiez l'intervalle de temps pendant lequel une analyse complète s'est déroulée pour la dernière fois.
- **Virus trouvés.**

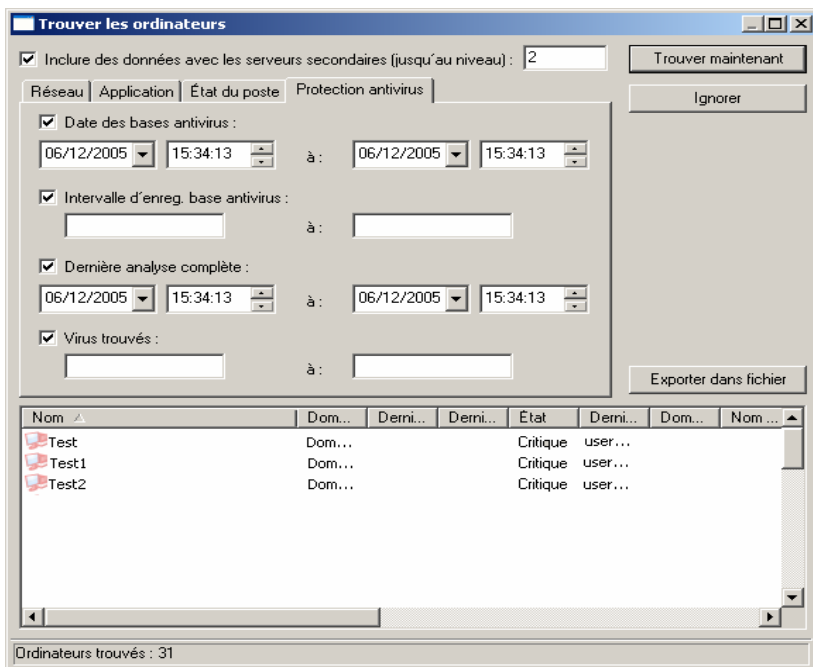


Figure 25. Recherche d'un ordinateur. L'onglet **Protection antivirus**.

Pour inclure dans la recherche tous les postes clients présents dans la structure des réseaux logiques des serveurs d'administration, cochez la case **Inclure des données avec les serveurs secondaires (jusqu'au niveau)**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

Une fois les critères définis, cliquez sur **Rechercher**. La liste des ordinateurs vérifiant les critères de recherche est affichée au bas de la boîte de dialogue. La liste contient des informations générales sur les ordinateurs détectés.



Pour enregistrer les résultats de la recherche dans un fichier de texte

cliquez sur **Exporter dans fichier** dans la boîte de dialogue Recherche d'ordinateurs (voir Figure 25) et spécifiez le fichier dans lequel vous souhaitez enregistrer les résultats.

3.3. Requêtes d'ordinateurs



Pour créer une requête d'ordinateurs:

1. Sélectionnez l'entrée Requêtes d'ordinateurs dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez la commande **Nouveau/Nouvelle requête**, ou utilisez son équivalent dans le menu **Action**.
2. Indiquez le nom de la requête dans la fenêtre ouverte (Fig. 27) et cliquez sur **Ok**.

Un nouveau dossier avec le nom spécifié pour la requête apparaîtra alors sous l'entrée **Requêtes d'ordinateurs** dans l'arborescence de console. Pour ajouter des ordinateurs à la requête, configurez les paramètres de la requête.

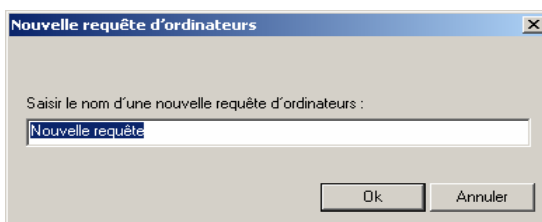


Figure 26. Création d'une requête d'ordinateurs



Pour configurer une requête d'ordinateurs:

1. Sélectionnez la requête que vous souhaitez configurer dans l'arborescence de console ou dans le panneau de résultats et utilisez la commande **Propriétés** dans le menu contextuel ou son équivalent dans le menu **Action**.
2. Ceci permet d'ouvrir la boîte de dialogue de configuration des requêtes (voir Figure 27) contenant les onglets suivants : **Général**, **Réseau**, **Application**, **État du poste** et **Protection antivirus**.

Dans l'onglet **Général** (voir Figure 28) vous pouvez modifier le nom de la requête et définir la zone de recherche des ordinateurs à l'aide de l'une des options suivantes:

- **Rechercher dans les groupes et le réseau** – La recherche s'effectue sur tous les ordinateurs présents dans le réseau,

qu'ils soient ou pas compris dans la structure du réseau logique.

- **Rechercher dans les groupes** – La recherche s'effectue uniquement sur les ordinateurs du réseau logique.
- **Rechercher dans le réseau** – La recherche s'effectue sur les ordinateurs non présents dans le réseau logique.

Pour inclure des données des serveurs d'administration secondaires dans la requête, cochez la case **Inclure des données avec les serveurs secondaires (jusqu'au niveau)**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

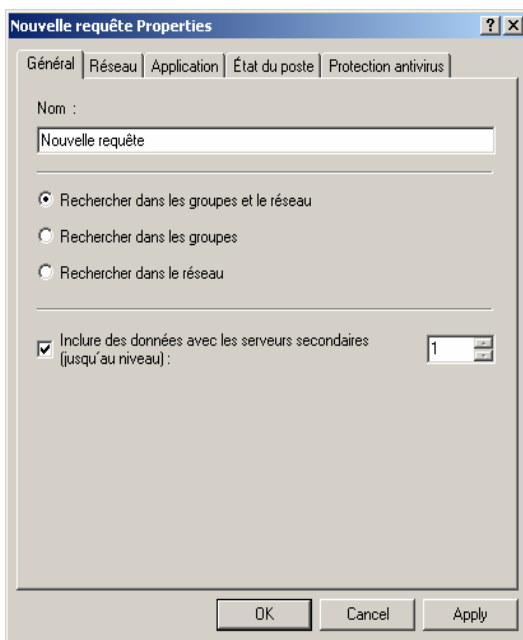


Figure 27. Configuration d'une requête d'ordinateurs
L'onglet **Réseau**

Spécifiez les attributs des ordinateurs à inclure dans la requête, depuis l'onglet Réseau (voir Figure 28). Vous pouvez utiliser les paramètres suivants :

- Nom de l'ordinateur dans le réseau logique ;
- Nom de l'ordinateur dans le réseau Windows;

- Domaine où sont inclus les ordinateurs ;
- L'intervalle des adresses IP des ordinateurs; pour cela, cochez la case **Intervalle d'adresses IP** et indiquez les adresses IP de début et de fin de l'intervalle ;
- L'heure de dernière connexion du poste client au serveur d'administration ; pour ce faire, cochez la case **Intervalle après connexion précédente** et spécifiez l'heure de début et de fin dans les zones **depuis** et **jusqu'à**.
- L'heure d'apparition des nouveaux ordinateurs dans le réseau; pour ce faire, cochez la case **Nouveaux ordinateurs trouvés pendant l'analyse du réseau** et spécifiez la période en jours dans la zone **Période de détection (jours)**.

Nouvelle requête Properties

Général Réseau Application État du poste Protection antivirus

Nom de poste :

Nom de l'ordinateur Windows :

Domaine :

☒ Intervalle d'adresses IP :

depuis : . . . à : . . .

☒ Intervalle après connexion précédente :

depuis :

à :

☒ Nouveaux ordinateurs trouvés pendant l'analyse du réseau

Période de détection (jours):

OK Cancel Apply

Figure 28. Configuration de la requête d'ordinateurs.
L'onglet **Réseau**

Pour spécifier l'application à installer sur les ordinateurs, utilisez l'onglet **Application** (voir Figure 29). Vous pouvez utiliser les paramètres suivants :

- Nom de l'application
- Version de l'application ;

- L'heure de dernière mise à jour de la version de l'application; pour ce faire, cochez la case **Dernière mise à jour** et spécifiez la date et l'heure de début et de fin de l'intervalle dans les zones **depuis** et **à**.

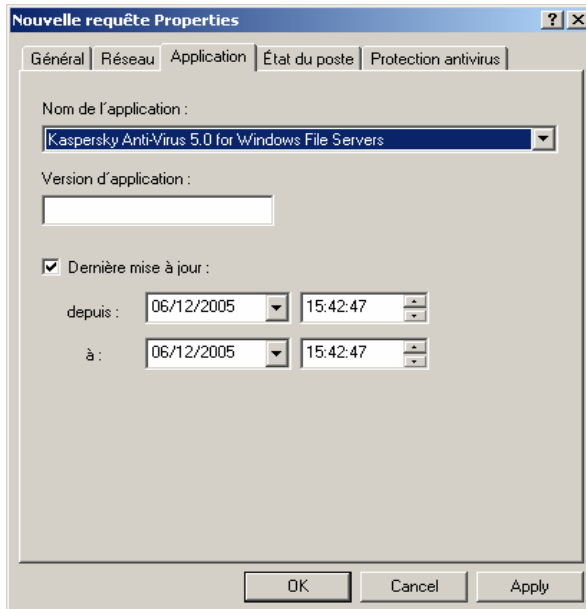


Figure 29. Configuration d'une requête d'ordinateurs
L'onglet **Applications**

Spécifiez les critères d'évaluation de la protection antivirus sur les ordinateurs qui vont être inclus dans la requête, depuis l'onglet **Protection antivirus** (voir Figure 30). Vous pouvez spécifier :

- la date de création de la base antivirus utilisée par l'application; pour ce faire, cochez la case **Date des bases antivirus** et spécifiez les heures de début et de fin de la plage horaire pendant laquelle la base sera créée ;
- Nombre d'enregistrements dans la base antivirus utilisée par les applications ; pour cela cochez la case **Intervalle d'enreg. base antivirus** et spécifiez les valeurs minima et maxima de ce paramètre.
- L'heure de dernière analyse complète de l'ordinateur par l'une des applications Kaspersky Lab ; pour ce faire, cochez la case **Dernière analyse complète** et spécifiez les dates et heures de

début et de fin de l'intervalle de temps pendant lequel l'analyse doit avoir été faite ;

- le nombre de virus détectés sur l'ordinateur ; pour ce faire, cochez la case **Virus trouvés** et spécifiez les valeurs minima et maxima de ce paramètre.

The screenshot shows a Windows-style dialog box titled "Nouvelle requête Properties". It has five tabs: "Général", "Réseau", "Application", "État du poste", and "Protection antivirus". The "Protection antivirus" tab is selected. Inside the dialog, there are several sections, each with a checked checkbox and associated input fields:

- Date des bases antivirus :** Includes "depuis :" and "à :" labels, each followed by a date/time picker showing "06/12/2005" and "15:43:24".
- Intervalle d'enreg. base antivirus :** Includes an "à :" label followed by an empty text input field.
- Dernière analyse complète :** Includes "depuis :" and "à :" labels, each followed by a date/time picker showing "06/12/2005" and "15:43:24".
- Virus trouvés :** Includes an "à :" label followed by an empty text input field.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Figure 30. Configuration d'une requête d'ordinateurs.
L'onglet **Protection antivirus**

Sur l'onglet **État du poste** (voir Figure 31), spécifiez les paramètres qui décrivent l'état des postes clients et celui de la tâche de protection en temps exécutée sur les ordinateurs. Pour ce faire :

- sélectionnez la valeur requise dans la liste déroulante **État du poste** : **Ok**, **Critique** ou **Avertissement**.
- sélectionnez les conditions en fonction desquelles le poste client reçoit l'état correspondant dans la liste **Description de l'état de protection**.
- sélectionnez l'état de la tâche de protection en temps réel exécutée sur les postes clients, inclus dans la requête à partir de la liste **État de PTR**.

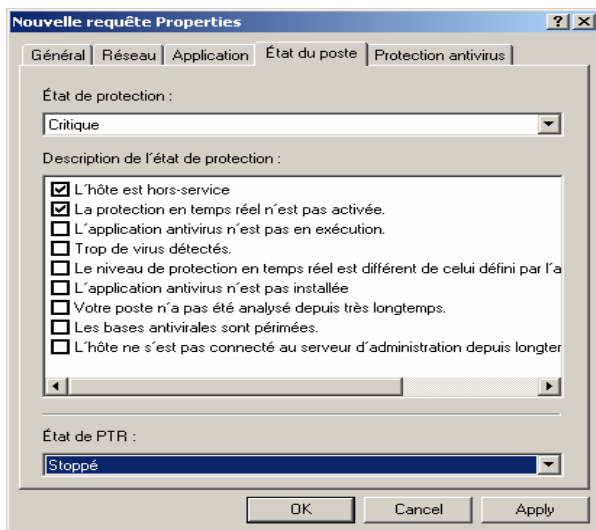


Figure 31. Configuration d'une requête d'ordinateurs
L'onglet **État du poste**

3. Quand vous aurez terminé la configuration, cliquez sur **Appliquer** ou sur **Ok**.

3.4. Création, modification et suppression des groupes du réseau logique



Pour ajouter un nouveau groupe à la structure du réseau logique

1. Pour créer un sous-groupe, sélectionnez un groupe parent dans l'arborescence de console ou dans le dossier **Groupes** du panneau de détails. Si vous voulez créer un groupe de niveau supérieur, sélectionnez le dossier **Groupes**.
2. Sélectionnez **Nouveau/Groupe...** dans le menu contextuel ou dans le menu **Action**. Un Assistant Nouveau groupe démarre. Suivez les instructions de l'Assistant.

3. Écrivez le nom du groupe afin de créer un dossier pour lui. Le nom du groupe doit être unique dans ce même niveau de hiérarchie (groupes).
4. Dans la boîte de dialogue suivante de l'Assistant, dans la section **Ordinateurs** définissez les actions à exécuter pour les postes clients du groupe qui sont restés inactifs pendant un certain intervalle de temps:
 - Si vous voulez que le serveur d'administration effectue une action quelconque, cochez la case **Informé l'administrateur après une période d'inactivité de** et indiquez le nombre de jours dans la zone **Jours** pour informer l'administrateur en cas d'inactivité de cet ordinateur. Après le temps indiqué, le serveur d'administration exécutera les actions sélectionnées.
 - Si vous voulez que des clients soient supprimés du groupe après quelques jours, cochez la case **Supprimer du groupe après une période d'inactivité de** puis indiquez le nombre de jours nécessaires dans la zone **Jours**. Après cette période, le serveur d'administration déplacera le client vers le groupe **Non attribué**.

Après la fin de l'Assistant, un nouveau dossier de groupe est affiché sous l'entrée **Groupes** de la console. Les sous-dossiers **Stratégies** et **Tâches** sont automatiquement créés dans le nouveau dossier du groupe. De nouveaux objets seront ajoutés à ces dossiers lors de la création des stratégies et des tâches du groupe.



Pour installer automatiquement les applications Kaspersky Lab sur tous les nouveaux ordinateurs du groupe :

1. Sélectionnez le groupe souhaité dans le dossier **Groupes** et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.
2. Dans la boîte de dialogue **Propriétés de <Nom de groupe>**, dans la section **Nouveau poste client dans le groupe** de l'onglet **Ordinateurs** (voir Figure 15), cochez ou annulez les cases correspondantes aux paquets d'installation (voir section 5.2 à la page 66) afin d'activer ou de désactiver l'installation non surveillée des applications Kaspersky Lab sur les clients. Par défaut, l'installation automatique des applications Kaspersky Lab est désactivée.



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

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



Pour déplacer un groupe :

sélectionnez le dossier correspondant dans l'arborescence de console ou dans le panneau de résultats puis utilisez les commandes **Couper / Coller** du menu contextuel ou du menu **Action**, ou effectuez la même opération à l'aide de la souris.



Pour renommer un groupe :

Sélectionnez un groupe dans l'arborescence de console ou dans le panneau de détails et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. Sur l'onglet **Général** de la boîte de dialogue **Propriétés de <Titre du groupe>**, modifiez le nom du groupe (voir Figure 14).



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



Pour supprimer un groupe de la structure du réseau logique,

sélectionnez le dossier correspondant dans l'arborescence de console ou dans le panneau de résultats puis utilisez la commande **Supprimer** du menu contextuel ou du menu **Action**.



Un groupe peut être supprimé du réseau logique s'il ne contient pas de serveurs secondaires, de groupes imbriqués ou de postes clients.

3.5. Ajout, déplacement et suppression d'un ordinateur d'un réseau logique



Pour ajouter un ou plusieurs ordinateurs au réseau logique :

1. Dans le dossier **Groupe**, choisissez le groupe auquel vous voulez ajouter un nouveau client. Pour ajouter un client au niveau supérieur de la hiérarchie, sélectionnez le dossier **Groupe**.
2. Ouvrez le menu contextuel et cliquez sur **Nouveau/Station de travail** (ou choisissez cette commande dans le menu **Action**) pour lancer un Assistant. Suivez les instructions de l'Assistant.
3. En premier lieu, spécifiez une méthode pour ajouter un ordinateur :
 - **Automatiquement** - L'ordinateur sera ajouté au groupe en fonction des réponses aux requêtes transmises sur le réseau Windows par le serveur d'administration. Cochez **Je veux les ajouter au groupe à partir du réseau de Windows** pour déplacer l'ordinateur du groupe **Non attribué** au groupe de destination.
 - **Manuellement** – L'ordinateur sera ajouté au groupe en fonction des données saisies directement par l'administrateur. Pour ajouter un ordinateur, cochez **Je veux définir les adresses IP des ordinateurs dans le groupe**. Dans ce cas, l'unicité des données est vérifiée pour éviter les conflits de noms. Si la base de données du serveur d'administration dispose sur cet ordinateur d'informations dans le réseau Windows, mais non dans le réseau logique, alors l'ordinateur sera intégré au groupe souhaité avec les propriétés de l'utilisateur.
4. Ensuite, vous aurez la possibilité de créer la liste des ordinateurs de ce groupe.

Si vous choisissez d'ajouter automatiquement des ordinateurs, l'Assistant présente le dossier **Non attribué**. Sélectionnez les ordinateurs à ajouter à

ce groupe. Vous pouvez sélectionner des ordinateurs de dossiers différents ou bien tous les ordinateurs du groupe.

Si vous choisissez d'ajouter manuellement des ordinateurs, vous devrez créer une liste d'ordinateurs dans ce groupe. Pour créer la liste, utilisez **Ajouter** et **Supprimer**, ou utilisez un fichier texte : pour ce faire, cliquez sur **Importer**. Pour les adresses du poste, utilisez des adresses IP (ou un plage d'adresses IP) ou des noms NetBIOS (noms des postes sur le réseau MS Windows). Pour importer la liste à partir d'un fichier, parcourez vos dossiers pour retrouver le fichier txt contenant les adresses d'ordinateur à ajouter. Chaque adresse doit figurer sur une ligne séparée.

Après la fin de l'Assistant, les ordinateurs, ajoutés au groupe souhaité, sont affichés dans le panneau de détails avec les noms attribués par le serveur d'administration.



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



Votre serveur d'administration peut être configuré pour que les nouveaux ordinateurs détectés sur le réseau Windows, soient ajoutés automatiquement à un certain groupe du réseau logique. Pour activer cette caractéristique :

ouvrez la boîte de dialogue des propriétés du **Réseau** et passez à l'onglet **Postes client** (voir Figure 32). Dans la section **Nouveaux ordinateurs dans le réseau** cochez la case **Inclure les ordinateurs dans la structure du groupe** et cliquez sur **Parcourir...** pour indiquer le groupe auquel vous voulez ajouter les nouveaux ordinateurs.

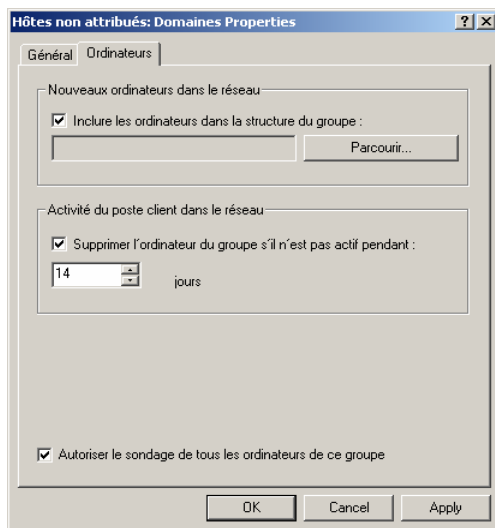


Figure 32. **Propriétés du groupe Non attribué.**
L'onglet **Ordinateurs**

Vous pouvez déplacer des clients d'un groupe à l'autre et les supprimer du réseau logique en utilisant les commandes standard **Couper/Coller** ou **Supprimer** du menu contextuel ou du menu **Action**. Les ordinateurs supprimés du réseau logique sont déplacés vers le groupe **Non attribué**.

Vous pouvez également faire glisser des ordinateurs vers leur emplacement cible, avec votre souris.

3.6. Déplacement d'un client vers un autre réseau logique



Pour créer une tâche de modification du serveur d'administration :

1. Connectez-vous au serveur d'administration auquel sont affectés les ordinateurs que vous voulez enlever (voir section 2.1 à la page 10).
2. Lancez l'Assistant de tâche de groupe ou de tâche globale (pour plus détails, voir Chapitre 7, page 109).

3. Au moment de sélectionner l'application et de définir le type de tâche (voir Figure 33), indiquez ce qui suit :
 - Dans la liste déroulante **Application– Kaspersky Lab Network Agent** ;
 - Dans la liste **Choisissez le type de tâche à exécuter – Tâche de modification de Kaspersky Administration Server**.

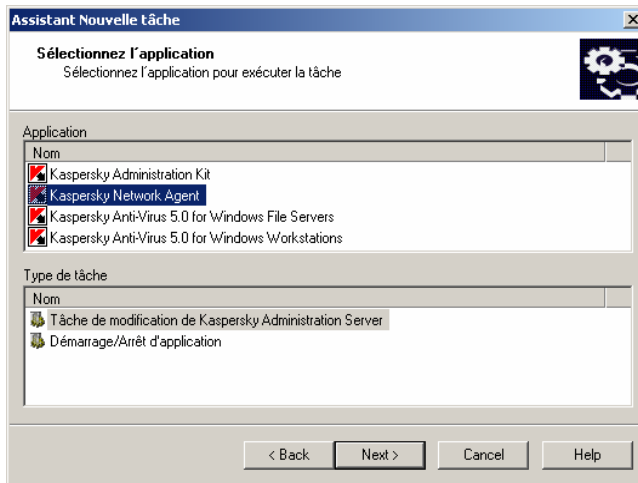


Figure 33. Création de la tâche de modification du serveur d'administration Kaspersky.
Choix de l'application à installer.

4. À l'étape suivante (voir Figure 34), définissez les paramètres employés par le composant Network Agent installé sur les clients, afin de se connecter au nouveau serveur.

Dans la section **Paramètres de connexion de Kaspersky Administration Server**, indiquez ce qui suit :

- Nouvelle adresse du serveur d'administration – dans la zone **Adresse**. Vous pouvez utiliser une adresse IP ou le nom de l'ordinateur sur le réseau (nom NetBIOS).
- Numéro de port utilisé pour se connecter au nouveau serveur d'administration – dans la zone **Port du serveur**.
- Numéro de port utilisé pour se connecter au nouveau serveur d'administration par protocole SSL – dans la zone **Port SSL du serveur**.

Dans la zone **Choisir le certificat...** spécifiez le fichier de certificat utilisé pour authentifier le nouveau serveur d'administration, dans la zone **Certificat de Serveur d'administration Kaspersky**.



Le fichier possède une extension **.cer** et se trouve placé dans le dossier **Cert** du répertoire de Kaspersky Administration Kit sur le serveur d'administration (vers lequel les ordinateurs sont déplacés). Vous pouvez copier le fichier de certification dans un dossier partagé ou une disquette. Cette copie peut être utilisée pour configurer des paramètres d'accès.

Figure 34. Création d'une tâche de modification du serveur d'administration.
Définition du serveur et sélection du certificat.

Par la suite, vous pouvez changer les paramètres de tâche dans l'onglet **Paramètres** (voir Figure 35) de la fenêtre de configuration des tâches (à propos des paramètres de tâches, voir section 7.4 à la page 120).

5. Si vous créez une tâche globale, vous devez constituer une liste de clients cible (voir section 7.2 à la page 118). Après la fin de la tâche, ces clients seront déplacés vers le groupe **Non attribué** de l'autre réseau logique, et affectés au serveur d'administration spécifié.



Si vous créez une tâche de groupe, tous les clients du groupe sélectionné seront affectés à un nouveau serveur d'administration.

6. Indiquez le compte utilisé au lancement par la tâche d'installation à distance (voir section 5.4 à la page 70).
7. Pour compléter la création de la tâche, programmez celle-ci pour la lancer à une certaine heure.

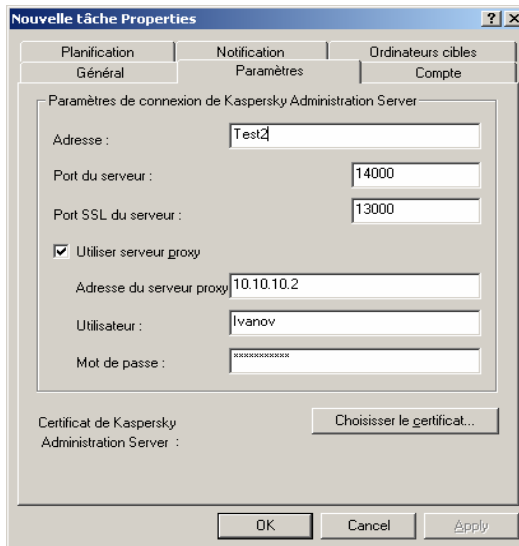


Figure 35. Affichage des propriétés de la tâche de modification du serveur d'administration.

3.7. Connexion locale du poste client au serveur d'administration



Pour connecter un poste client au Serveur d'administration :

depuis la ligne de commande du poste client, lancez l'outil **klmover.exe** compris dans le paquet d'installation de l'agent réseau.

Après l'installation de l'agent réseau, cet outil se trouve placé à la racine du dossier d'installation du composant et son exécution, en fonction des paramètres de ligne de commande, effectue les actions suivantes:

- connecter l'agent réseau au serveur d'administration, en utilisant les paramètres indiqués ;
- enregistrer les résultats de l'opération dans le fichier journal des événements, ou les afficher à l'écran.

Syntaxe de l'outil sur la ligne de commande :

- **klmover [-logfile <nomFichier>] ¹{ [-address <adresse serveur>] [-pn <numéro du port>] [-ps < numéro du port SSL>] [-noss1] [-cert <chemin du fichier certificat>] [-silent][<dupfix>]**

Description des paramètres :

- **-logfile <nomfichier>** – enregistre les résultats de l'exécution dans le fichier journal, par défaut les informations sont conservées dans le fichier stdout.tx ; si le paramètre n'est pas utilisé, les résultats et les messages d'erreur sont affichés à l'écran.
- **-address <adresse serveur>** – adresse du serveur d'administration de connexion, sous la forme d'une adresse IP, ou du nom NetBIOS ou DNS de l'ordinateur.
- **-pn <numéro du port>** – numéro de port à utiliser pour une connexion non sécurisée au serveur d'administration, par défaut le port 14000 est utilisé.
- **-ps <numéro du port SSL>** – numéro de port SSL à utiliser pour une connexion sécurisée au serveur d'administration sous protocole SSL. Par défaut le port **13000** est utilisé.
- **-noss1** – utilise une connexion non sécurisée au serveur d'administration ; si aucun modificateur n'est utilisé, la connexion à l'agent est établie à l'aide du protocole sécurisé SSL.
- **-cert <chemin complet du fichier certificat>** – utiliser le fichier de certificat spécifié pour l'authentification, afin d'accéder au nouveau serveur d'administration. Si aucun modificateur n'est utilisé, l'agent réseau recevra le certificat lors de la première connexion au serveur d'administration.
- **-silent** – exécute l'outil en mode silencieux; ce paramètre est utile, par exemple, pour exécuter l'outil à partir du scénario d'ouverture de session de l'utilisateur.

¹ В квадратных скобках приводятся необязательные ключи.

- **-dupfix** - Paramètre utilisé en cas d'installation de l'agent réseau par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

3.8. Vérification de la connexion du poste client au serveur d'administration



Pour vérifier la connexion du poste client au serveur d'administration :

depuis la ligne de commande du poste client, lancez l'outil **klnagchk.exe** compris dans le paquet d'installation de l'agent réseau.

Après l'installation de l'agent réseau, cet outil se trouve placé à la racine du dossier d'installation du composant et son exécution, en fonction des paramètres de ligne de commande, effectue les actions suivantes:

- il renvoie les valeurs des paramètres connexion de l'agent réseau installé sur le poste client, utilisés afin de se connecter au serveur d'administration, à l'écran ou dans un fichier journal ;
- il enregistre dans le fichier journal les statistiques de l'agent réseau (à partir du dernier démarrage du composant) et les résultats de son activité, ou les afficher à l'écran ;
- il tente de connecter l'agent réseau au serveur d'administration ;
- si la connexion n'a pas pu être établie, il envoie un paquet ICMP au poste sur lequel se trouve installé le serveur d'administration.

Syntaxe de l'outil sur la ligne de commande :

- **klnagchk [-logfile <nomFichier>] 2 [-sp] [-savecert <chemin du fichier certificat>] [-restart]**

Description des paramètres

- **-logfile <nomfichier>** – enregistre les valeurs des paramètres de connexion utilisées par l'agent réseau pour se connecter au serveur,

² Dans les crochets on amène les clés non obligatoires.

ainsi que les résultats de l'exécution ; par défaut les informations sont conservées dans le fichier **stdout.tx** ; si le paramètre n'est pas utilisé, les résultats et les messages d'erreur sont affichés à l'écran.

- **-sp** – affiche le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy; ce paramètre est utilisé si la connexion au serveur d'administration est effectuée via un serveur proxy.
- **-savecert <nomfichier>** – enregistre le certificat utilisé pour accéder au serveur d'administration dans le fichier spécifié.
- **-restart** – redémarre l'agent réseau après exécution de l'outil.

CHAPITRE 4. HIÉRARCHIE DES SERVEURS D'ADMINISTRATION

4.1. Connexion d'un serveur secondaire à un serveur primaire



Pour ajouter un serveur d'administration secondaire au réseau logique :

1. Sélectionnez le groupe administration souhaité, ouvrez le menu contextuel et cliquez sur **Nouveau / Serveur d'administration** item. La même option est disponible sous le menu **Action**. Un Assistant démarre. Suivez les instructions de l'Assistant.
2. Vous devez spécifier le nom du serveur secondaire. Saisissez-le manuellement. Le nouveau serveur d'administration sera affiché sous ce nom dans le groupe d'administration. Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie.
3. Dans la fenêtre suivante de l'Assistant, vous pouvez spécifier l'adresse réseau du serveur d'administration secondaire. Ensuite, le serveur d'administration primaire enverra une commande de connexion au serveur secondaire et transmettra toutes les propriétés (adresse réseau du serveur primaire, nom du serveur secondaire, certificat du serveur primaire).






Si vous ne souhaitez pas spécifier l'adresse réseau du serveur secondaire, cliquez simplement sur **Suivant**.

4. Spécifiez le certificat du serveur d'administration secondaire. Cliquez sur **Parcourir** pour retrouver le fichier de certification.

Après la fin des assistants, le serveur d'administration primaire ajoutera les données du serveur secondaire à la base. L'icône et le nom du nouveau serveur seront affichés dans le dossier Serveurs du groupe d'administration correspondant.



Pour configurer la connexion d'un serveur secondaire au serveur d'administration primaire,

1. Dans la console d'administration, sélectionnez le serveur d'administration nécessaire, ouvrez le menu contextuel et cliquez sur **Propriétés**. La même commande est disponible sous le menu **Action**. Dans la boîte de dialogue suivante, sélectionnez l'onglet **Paramètres**, où vous devez spécifier :
 - Adresse réseau du serveur d'administration secondaire
 - Nom de serveur d'administration secondaire, qui affichera sur le serveur primaire
 - Certificat du serveur primaire
2. Cliquez sur **Appliquer** ou sur **Ok**. Suite à cela, le serveur secondaire se connecte au serveur primaire et récupère toutes les stratégies et les tâches du groupe dans lequel il a été inclus.
3. Les stratégies et les tâches récupérées du serveur primaire sont affichées sur la serveur secondaire de la manière suivante :
 - L'icône suivante sera associée au nom d'une stratégie récupérée du serveur primaire –  (icône normale des stratégies – ).
 - L'icône  indiquera que la configuration de stratégie est verrouillée sur le serveur primaire (autrement dit, la configuration ne peut pas être modifiée sur le serveur secondaire).
 - L'icône suivante sera associée au nom d'une tâche de groupe récupérée du serveur primaire –  (icône normale des tâches – ).



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



Les tâches récupérées sur un serveur d'administration primaire ne peuvent pas être exécutées ou planifiées sur un serveur secondaire.

L'état du serveur d'administration secondaire, affiché dans le volet de résultats de la console d'administration sur le serveur primaire, devient Connecté.

4.2. Examen du réseau logique d'un serveur d'administration secondaire



Pour afficher la structure du réseau logique :

Sélectionnez le serveur d'administration secondaire requis. Dans le menu contextuel, cliquez sur **Connexion au serveur d'administration**. La même commande est disponible sous le menu **Action**.

La structure du réseau logique du serveur secondaire sélectionné apparaîtra dans la console d'administration. Ensuite, vous pouvez examiner la structure, comme décrite dans la section 3.1 à la page 28.

CHAPITRE 5. INSTALLATION ET DESINSTALLATION D'APPLICATIONS SUR DES CLIENTS

5.1. Affichage des paramètres du paquet d'installation



Pour examiner les propriétés et changer le nom du paquet d'installation dans la boîte de dialogue :

déployez l'entrée **Installation distante** dans l'arborescence de console, sélectionnez le paquet d'installation requis dans le panneau de résultats et utilisez la commande **Propriétés** dans le menu contextuel ou dans le menu **Actions**.

Ceci permet d'ouvrir la boîte de dialogue **Propriétés de <Nom du paquet d'installation>** (voir Figure 36) composée des onglets suivants : **Général**, **Paramètres**, **Licences** et **Redémarrage du S.E.**.

L'onglet **Général** (voir Figure 36) affiche des informations générales sur le paquet :

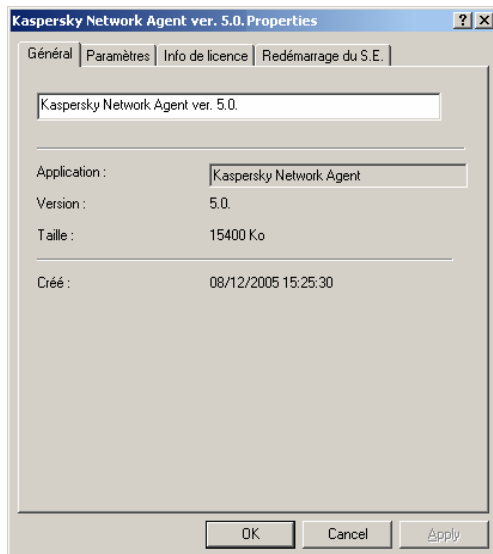


Figure 36. Boîte de dialogue Propriétés du paquet d'installation.
L'onglet **Général**

- Application
- Version
- Taille
- Créé(e)

L'onglet **Paramètres** (voir Figure 37) affiche les paramètres du paquet d'installation, qui correspondent à ceux de l'application pour laquelle le paquet a été créé. Ce sont des paramètres par défaut, qui peuvent être modifiés si nécessaire.

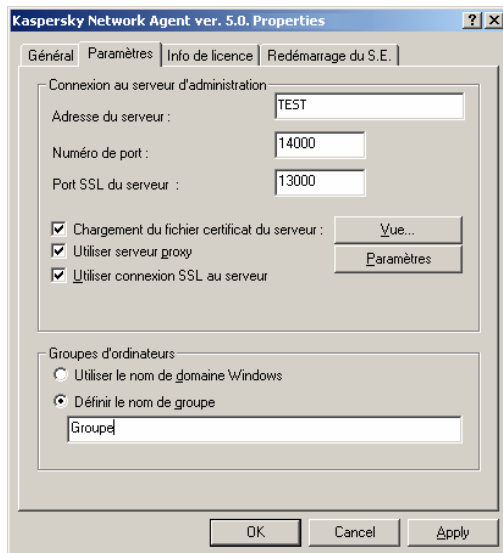


Figure 37. Boîte de dialogue Propriétés du paquet d'installation.
L'onglet **Paramètres d'installation**

L'onglet **Infos de licence** (voir Figure 38) présente des informations générales sur la licence de l'application contenue par le paquet.

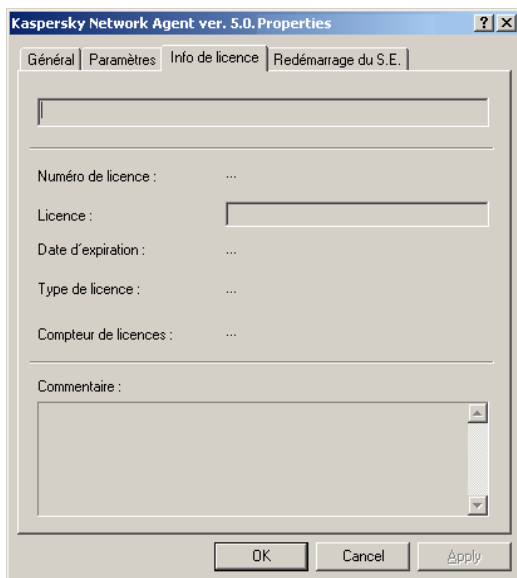


Figure 38. Fenêtre de propriétés du paquet d'installation
Onglet **Licence**

Dans la page **Redémarrage du S.E.** (voir Figure 39) vous pouvez définir les actions à réaliser lorsqu'il faut redémarrer l'ordinateur après l'installation de l'application.

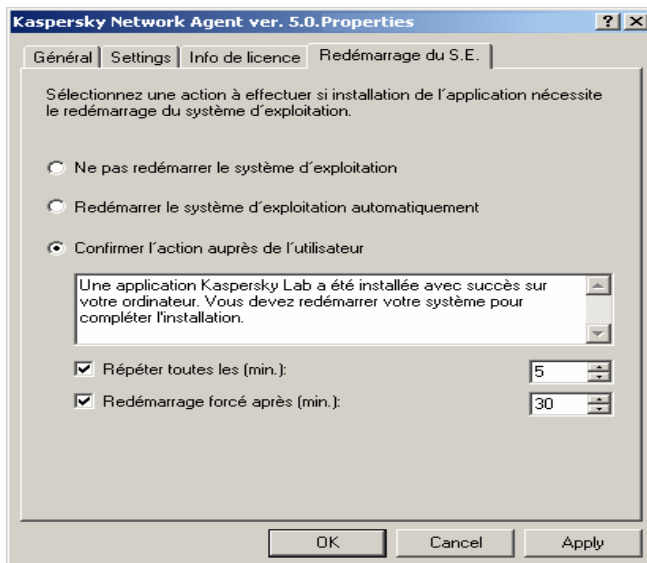


Figure 39. Fenêtre de propriétés du paquet d'installation
Onglet **Redémarrage du S.E.**

- **Ne pas redémarrer le système d'exploitation.**
- **Redémarrer le système d'exploitation automatiquement.**
- **Confirmer l'action auprès de l'utilisateur** – le choix de cette option permet de :
 - créer un message destiné à l'utilisateur qui sera affiché pour l'informer qu'il faut redémarrer le système d'exploitation, dans le champ associé;
 - spécifier la fréquence de la notification de redémarrage du système d'exploitation, en cochant la case **Répéter toutes les (min.)** et en spécifiant l'intervalle à utiliser pour afficher les notifications.
 - configurer le redémarrage automatique du système d'exploitation si l'ordinateur ne l'a pas été manuellement dans l'intervalle de temps spécifié, à compter de l'installation de l'application. Pour ce faire, cochez la case **Redémarrage forcé après (min.)** et spécifiez l'intervalle de temps souhaité.

5.2. Création de paquets d'installation



Pour créer un paquet d'installation :

1. Connectez-vous au serveur d'administration (voir section 2.1 à la page 10).
2. Dans l'arborescence de console, sélectionnez l'entrée **Installation distante**, ouvrez le menu contextuel et cliquez sur **Nouveau / Paquet** (cette commande se trouve également sous le menu **Action**) pour lancer un Assistant. Suivez les instructions de l'Assistant.
3. Vous pourrez spécifier le nom du paquet d'installation et l'application à installer à l'étape suivante (voir Figure 42) :

Lorsque vous créez un paquet pour l'installation d'une Application Kaspersky Lab, choisissez l'option **Générer un paquet d'application Kaspersky Lab.**, cliquez sur **Parcourir...** et sélectionnez le fichier contenant la description de l'application (le fichier possède une extension .kpd et accompagne le paquet d'installation de toutes les applications Kaspersky Lab compatibles avec l'installation à distance). Le nom de l'application apparaît dans la zone **Nom de l'application**, et le numéro de version, dans la zone **Version de l'application**.

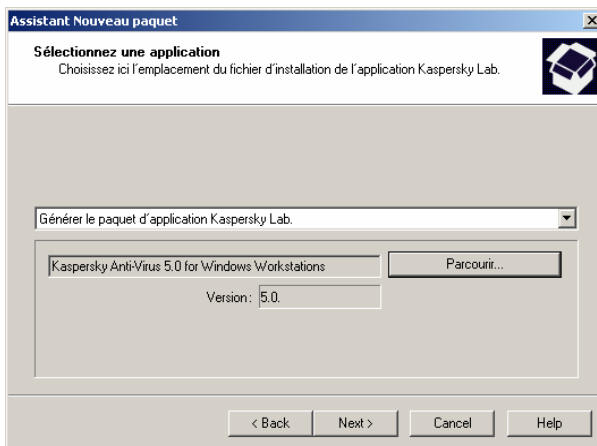


Figure 40. Création d'un paquet d'installation d'une application Kaspersky Lab.

Les paramètres du paquet d'installation sont définis par défaut, en fonction de l'application à installer. Vous pouvez changer les paramètres du paquet d'installation dans la boîte de dialogue Propriétés après la création du paquet (voir ci-dessus).

Lors de la création d'un paquet pour l'installation des autres applications :

- Sélectionnez Générer le paquet d'installation du fichier exécutable spécifié dans la liste déroulante ;
- Spécifiez le chemin du kit de distribution de l'application avec le bouton **Parcourir...**
- Cochez la case **Copier tout le dossier dans le paquet** si vous souhaitez inclure l'intégralité du dossier contenant le fichier de distribution dans le paquet d'installation.
- Spécifiez les paramètres de lancement de l'exécutable sur le champ de la ligne de commande, s'ils sont nécessaires pour installer l'application.

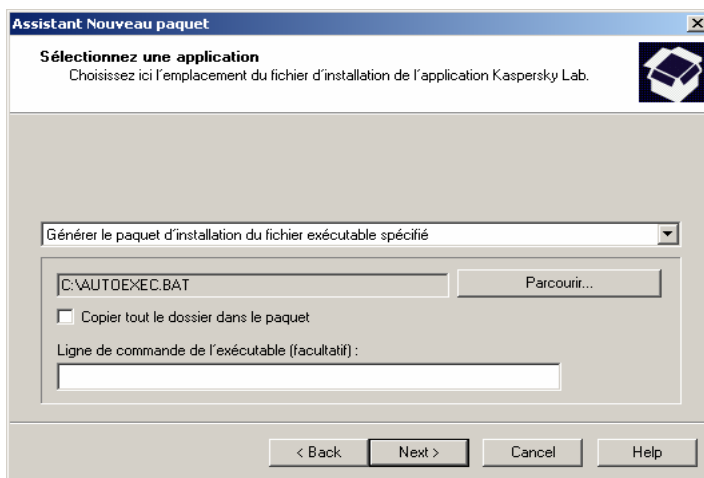


Figure 41. Création du paquet d'installation d'une installation spécifiée par l'utilisateur.

4. Dans la fenêtre suivante de l'Assistant (voir Figure 42), vous pouvez inclure une clé de licence dans le paquet d'installation en cliquant sur **Parcourir** puis en sélectionnant le fichier de licence (avec extension **.key**).

Si vous ne souhaitez pas ajouter une clé de licence au paquet d'installation, cliquez sur **Suivant**.

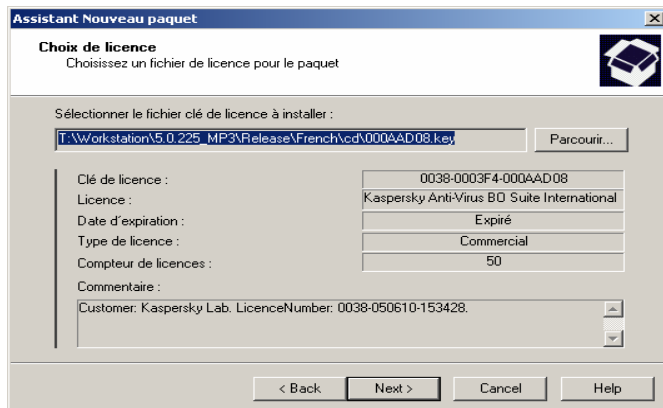


Figure 42. Création d'un paquet d'installation. Sélection d'une clé de licence.

5. Un ensemble de fichiers nécessaires pour installer l'application sur les clients est alors chargé dans le dossier partagé du serveur d'administration. Le serveur vérifie, dans le poste administrateur, la disponibilité du plug-in de console pour cette application. Si le plug-in n'a pas été installée ou si sa version est plus récente que celle de l'application, il sera respectivement installé, ou remplacé.



Le paquet d'installation de Network Agent est créé automatiquement pendant l'installation de Kaspersky Administration Kit. Le paquet peut être retrouvé sous l'entrée **Installation distante**.



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

Après la fin de l'Assistant, un nouveau paquet d'installation sera ajouté sous l'entrée **Installation distante** et présenté dans le panneau de détails.

5.3. Configuration des paramètres du paquet d'installation de Network Agent



Pour configurer le paquet d'installation de Network Agent :

sélectionnez l'onglet **Paramètres** (voir Figure 37) dans la fenêtre de configuration du paquet d'installation.

Cet onglet affiche les paramètres de fonctionnement suivants de l'agent réseau :

- Paramètres de connexion utilisés pour se connecter au serveur d'administration correspondant - dans le groupe de champs **Connexion au serveur** (pour plus de détails, voir section 6.3 à la page 104).
 - Adresse de l'ordinateur sur lequel est exploité le serveur d'administration.
 - Numéro de port utilisé pour se connecter au serveur.
 - Numéro de port utilisé pour se connecter au nouveau serveur d'administration par protocole SSL. Pour activer la connexion de SSL, cochez la case **Utiliser SSL pour se connecter au serveur**.
 - Fichier de certificat du serveur d'administration pour authentifier l'accès au nouveau serveur d'administration.
 - Configuration du serveur proxy – Pour spécifier la configuration, cliquez sur **Paramètres** puis saisissez l'adresse du serveur proxy, l'utilisateur et le mot de passe de connexion. Pour permettre la connexion via le serveur proxy, cochez la case **Utiliser serveur proxy**.

Après l'installation de Network Agent, vous pouvez changer les paramètres de connexion à l'aide des stratégies et des paramètres d'application.



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

- Un dossier du groupe **Non attribué** auquel de nouveaux ordinateurs seront ajoutés après l'installation de Network Agent – dans les zones **Nom de groupe par défaut** : Vous avez le choix parmi l'une des options suivantes :
 - **Utiliser le nom de domaine Windows** – Le client sera ajouté à un dossier qui correspond à son emplacement courant dans le réseau Windows : domaine ou groupe d'utilisateur (c'est l'option par défaut).
 - **Définir le nom de groupe** – Le client sera ajouté au dossier indiqué. Écrivez le nom du dossier dans la zone inférieure. Si le groupe **Non attribué** ne possède aucun dossier avec ce nom, il sera créé (vous pouvez également indiquer le nom du dossier existant dans le groupe **Non attribué**).

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

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



Pour créer une tâche globale de déploiement d'application :

1. Connectez-vous au serveur d'administration (voir section 2.1 à la page 10).
2. Sélectionnez l'entrée **Tâches** dans l'arborescence de console puis **Nouveau / Tâche** dans le menu contextuel ou dans le menu **Action** pour démarrer l'Assistant de création de tâche. Suivez les instructions de l'Assistant.
3. Indiquez le nom de tâche. Si le nom choisi existe déjà, **_1** sera automatiquement ajouté à la suite du nom.
4. Pour définir l'application et le type de tâche (voir Figure 43) sélectionnez l'application **Kaspersky Administration Kit** puis **Tâche de déploiement d'application** respectivement.

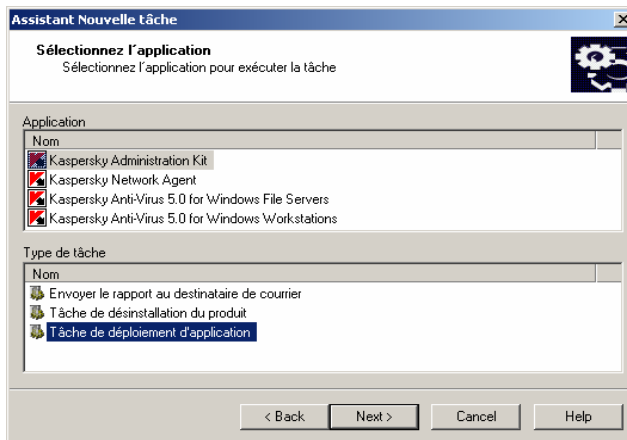


Figure 43. Configuration d'une tâche d'installation à distance. Définition du type de tâche

5. Définissez ensuite le paquet d'installation pour cette tâche (Figure 44). Sélectionnez le paquet souhaité parmi les autres paquets d'installation créés pour ce serveur d'administration, ou créez en un nouveau à l'aide du bouton **Créer...**

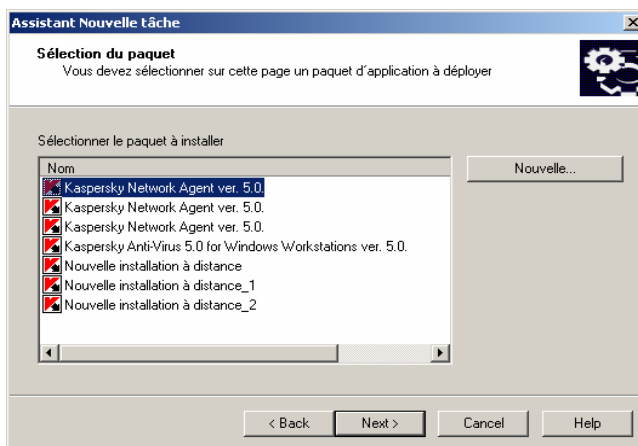


Figure 44. Création d'une tâche de déploiement d'application. Choix d'un paquet d'installation

6. Dans la fenêtre suivante de l'Assistant, indiquez l'une des méthodes d'installation (voir Figure 45):
 - **Utiliser l'installation par envoi** – Installation directe et forcée

- **Utiliser un script de connexion pour l'installation** – Installation en utilisant un script de connexion.

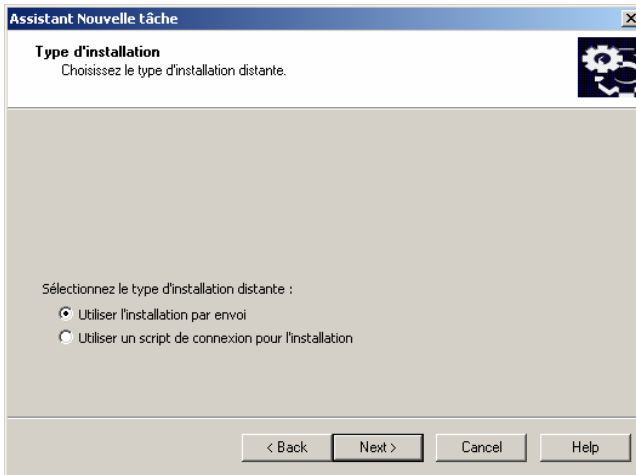


Figure 45. Création d'une tâche de déploiement d'application. Indication de la méthode d'installation

7. Si, au cours des étapes précédentes, vous avez sélectionné une méthode d'installation utilisant un scénario de démarrage, vous devrez sélectionner dans l'Assistant (voir Figure 46) les comptes des utilisateurs dont vous devez modifier le scénario de démarrage

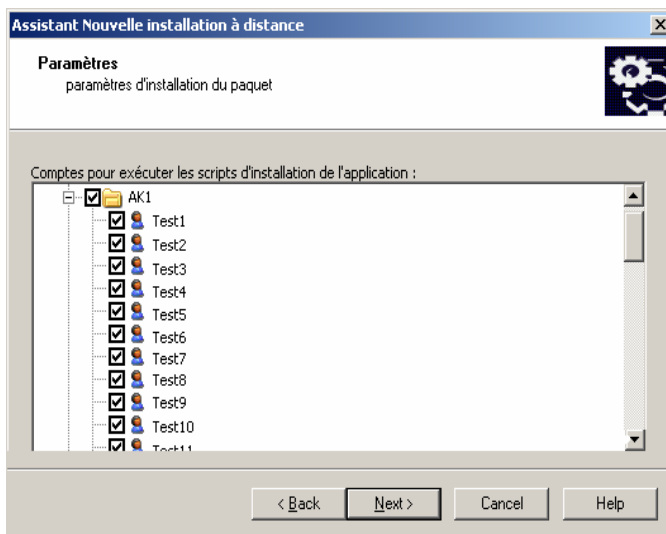


Figure 46. Sélection des comptes

Si vous choisissez la méthode d'installation par envoi ('push'), définissez une méthode de sélection des postes clients sur lesquels la tâche va être créée (voir. Figure 47)

- **Je veux sélectionner des ordinateurs à partir du réseau de Windows.** Dans ce cas, les postes clients seront sélectionnés automatiquement en fonction des données recueillies par le serveur d'administration pendant son exploration du réseau Windows.
- **Je veux définir des adresses IP pour les ordinateurs.** Les postes clients seront sélectionnés à la main.

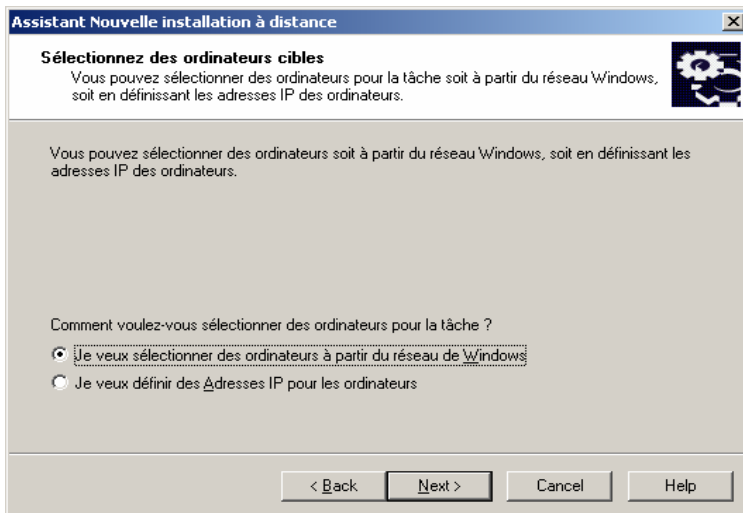


Figure 47. Choix d'une méthode de sélection de postes clients

Si les postes clients sont choisis d'après la structure de réseau Windows, la liste sera créée dans la boîte de dialogue de l'assistant (voir Figure 48) de manière semblable à l'ajout de postes sur le réseau logique (voir section 3.5 à la page 49).

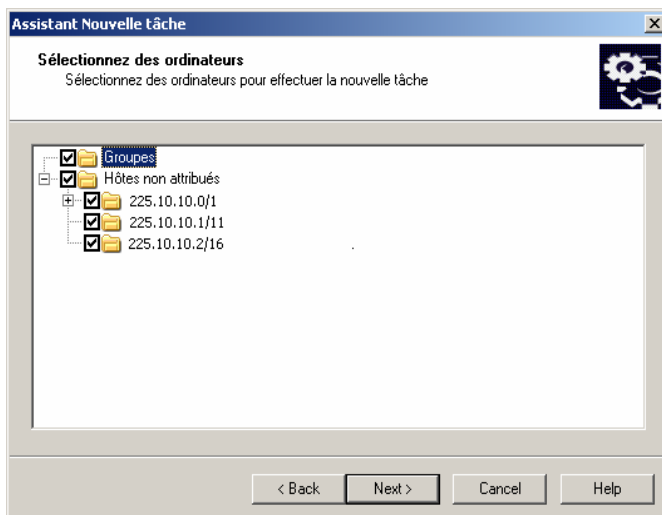


Figure 48. Création d'une liste d'ordinateurs sur lesquels installer des applications construites sur la structure de réseau Windows.

Si les postes clients vont être ajoutés manuellement, la liste sera complétée par ajout d'adresses IP (ou d'une plage d'adresses IP) de postes clients (voir Figure 49).

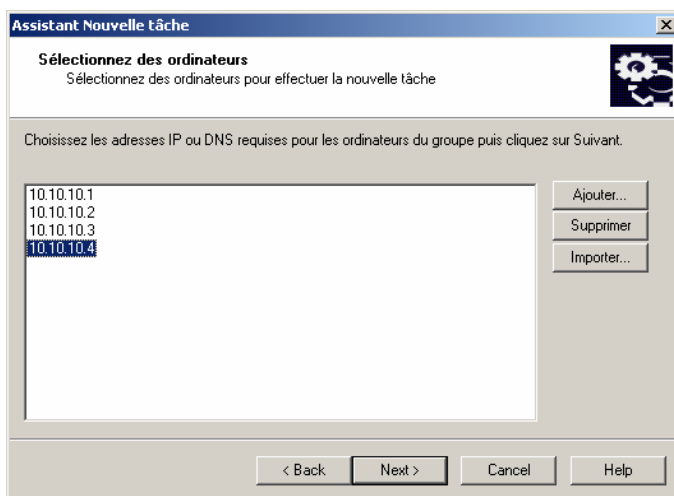


Figure 49. Création d'une liste d'ordinateurs à l'aide d'adresses IP.

8. Dans la fenêtre suivante de l'Assistant, définissez le compte utilisé pour démarrer la tâche d'installation à distance sur des clients (voir Figure 50).



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

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

Sélectionnez l'une des options suivantes :

- **Compte par défaut** – Exécute la tâche sous le compte par défaut si le serveur d'administration est lancé sous un compte d'utilisateur de domaine.
- **Compte spécifié** – Exécute la tâche sous le compte utilisateur spécifié, si le serveur d'administration est lancé sous le compte **Système local**, ou si le compte de service du serveur d'administration n'a pas de privilèges pour exécuter des tâches d'installation à distance.



Pour installer des applications Kaspersky sur les clients qui n'appartiennent pas à ce domaine, ouvrez une session en tant qu'utilisateur avec des privilèges d'administrateur, pour que ces clients puissent démarrer la tâche d'installation à distance.

Dans les zones ci-dessous, indiquez les informations sur l'utilisateur dont le compte satisfait les conditions requises

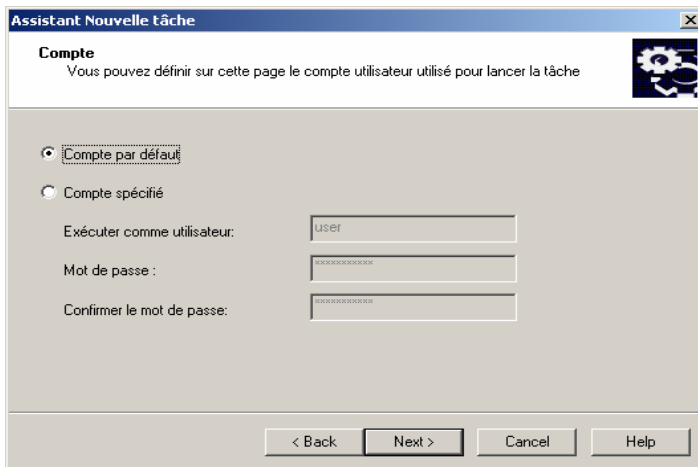


Figure 50. Sélection d'un compte.

9. Définition de la planification de la tâche (voir Figure 51).

- Dans la liste **Planification à exécuter**, choisissez l'une des options suivantes :
 - **Toutes les N heures**
 - **Chaque jour**
 - **Chaque semaine**
 - **Chaque mois**
 - **Une fois** – Lance la tâche de déploiement d'application une fois seulement, indépendamment des résultats de la tâche.
 - **Immédiatement** – Démarre la tâche immédiatement après avoir terminé l'Assistant.
- Configurez les paramètres de programme dans les zones correspondant au mode de démarrage choisi (pour des détails, voir section 7.1 à la page 109).

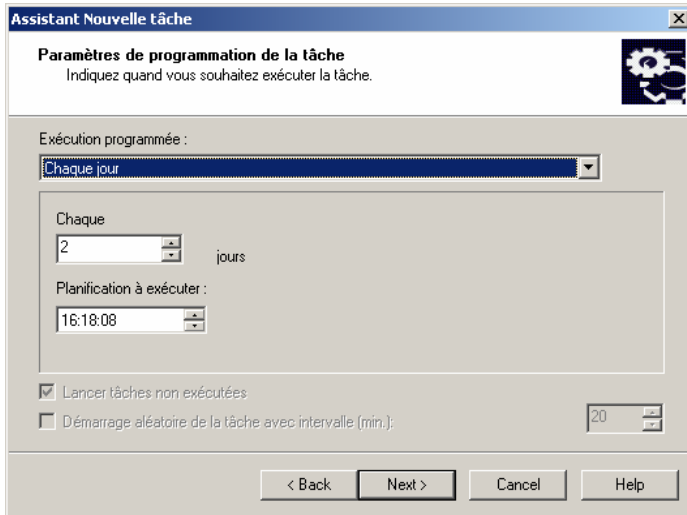


Figure 51. Planification de la tâche de déploiement d'applications.
La tâche est programmée pour commencer **Chaque jour**



Pour démarrer l'Assistant de création d'une tâche de déploiement d'application correspondant à un paquet d'installation spécifique,

déployez l'entrée **Installation distante** dans l'arborescence de console, sélectionnez le paquet d'installation requis dans le panneau de résultats et utilisez la commande **Installer** dans le menu contextuel ou dans le menu **Actions**. Ceci lance le nouvel Assistant de tâche décrit ci-dessus. Cet Assistant omet la sélection de l'application et du paquet d'installation. Suivez les instructions de l'Assistant.



Pour démarrer l'Assistant de création d'une tâche de groupe de déploiement,

sélectionnez l'entrée correspondant au groupe souhaité dans l'arborescence de console, et cliquez sur **Installer** dans le menu contextuel ou dans le menu **Action**. L'assistant de tâche de déploiement d'applications démarre. Cet Assistant omet la sélection du produit et du groupe d'ordinateurs. Suivez les instructions de l'Assistant.

5.5. Configuration de la tâche d'installation à distance

La tâche d'installation à distance est configurée de la même manière que les autres tâches (voir section 7.4 à la page 120). Par conséquent, nous ne décrirons parmi les paramètres présentés dans l'onglet **Paramètres**, que ceux qui sont spécifiques à chaque type de tâche.

Vous trouverez à la suite une description détaillée des paramètres spécifiques à un type de tâche en particulier, qui sont présentés sur l'onglet **Paramètres**.

Vous pouvez modifier les paramètres suivants dans le cas d'une tâche d'installation forcée (voir Figure 52):

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

Pour configurer d'autres paramètres, cliquez sur **Avancé** pour ouvrir la boîte de dialogue **Avancé** (voir Figure 53). Dans cette boîte de dialogue, procédez comme suit :

- Cochez la case **Ne pas installer sur des hôtes où ce produit est déjà installé** pour éviter d'installer l'application sur les ordinateurs qui l'ont déjà (cette case est cochée par défaut).
- Dans le groupe de zones **Télécharger le paquet d'installation**, cochez les cases :
 - **Télécharger le paquet à l'aide de dossiers partagés** pour transférer les fichiers d'installation de l'application, en utilisant les dossiers partagés du réseau Windows (par défaut).
 - **Télécharger le paquet avec Kaspersky Network Agent** pour transférer les fichiers d'installation de l'application en utilisant le composant Network Agent installé sur les clients (par défaut). Si cette case est cochée, spécifiez le nombre maximum d'ordinateurs pouvant télécharger simultanément de fichiers du serveur d'administration dans la zone **Nombre max. de téléchargements**.
- Dans la zone **Nombre de tentatives**, déterminez le nombre de tentatives d'installation de l'application, dans le cas d'une tâche d'installation à

distance planifiée. De nouvelles tentatives seront réalisées si des erreurs sont apparues au cours des installations précédentes.

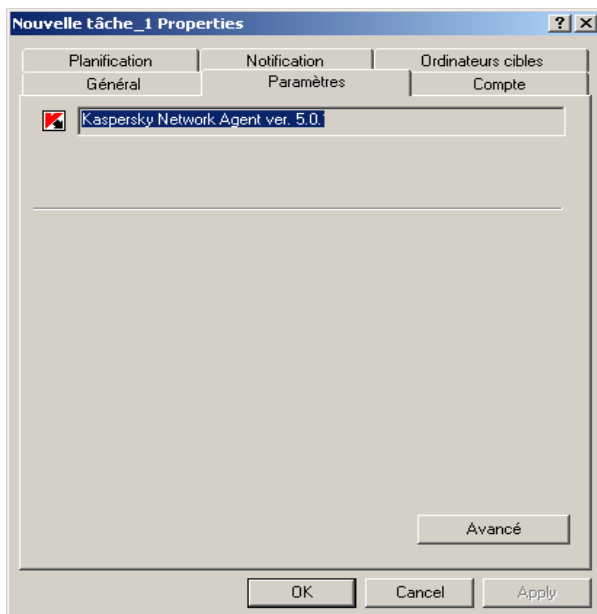


Figure 52. Paramètres de tâche d'installation à distance.

Méthode d'installation par envoi

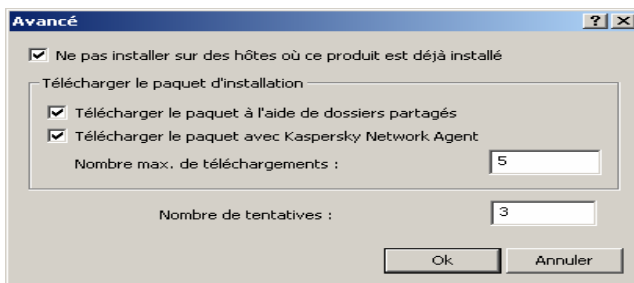


Figure 53. Tâche d'installation à distance.

La boîte de dialogue **Options avancées**.

Si vous configurez une tâche d'installation par script de connexion, vous pouvez modifier dans l'onglet **Paramètres** la liste de comptes d'utilisateur auxquels les modifications seront applicables (voir Figure 54). Utilisez les boutons **Ajouter** et **Supprimer** pour modifier la liste.

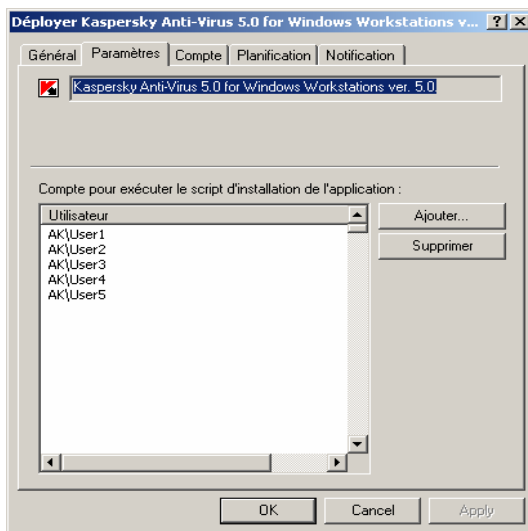


Figure 54. Configuration de la tâche d'installation à distance à l'aide de scripts.

5.6. Désinstallation à distance du logiciel



Pour désinstaller à distance des logiciels Kaspersky Lab :

1. Créez une tâche similaire à celle utilisée pour l'installation (le déploiement) à distance (section 5.4 à la page 70), sélectionnez **Désinstallation d'application à distance** dans le type de tâche.



Afin de s'assurer du bon fonctionnement de la tâche, décochez la case **Ne pas installer sur des hôtes où ce produit est déjà installé** dans l'onglet **Avancé** (voir Figure 53).

La tâche que vous aurez créée sera exécutée conformément à sa planification.

5.7. Assistant de déploiement d'application



Pour installer l'application avec l'Assistant de déploiement d'application :

1. Connectez-vous au serveur d'administration (voir section 2.1 à la page 10).
2. Dans l'arborescence de console de la fenêtre principale de Kaspersky Administration Kit, sélectionnez **Kaspersky Lab Administration Server (<Nom de serveur>)** et ouvrez le menu contextuel. Cliquez sur **Assistant de déploiement d'application** dans le menu contextuel ou dans le menu **Action** pour lancer l'Assistant. Suivez les instructions de l'Assistant.
3. Dans la boîte de dialogue qui s'affiche (voir Figure 55), indiquez le paquet d'installation que vous allez utiliser. Si vous voulez installer une application à partir du fichier d'installation, ou si le paquet d'installation n'a pas encore été créé, créez un nouveau paquet d'installation. Pour ce faire, cliquez sur **Nouveau...** pour lancer l'Assistant de création d'un paquet d'installation (voir section 5.2 à la page 66).

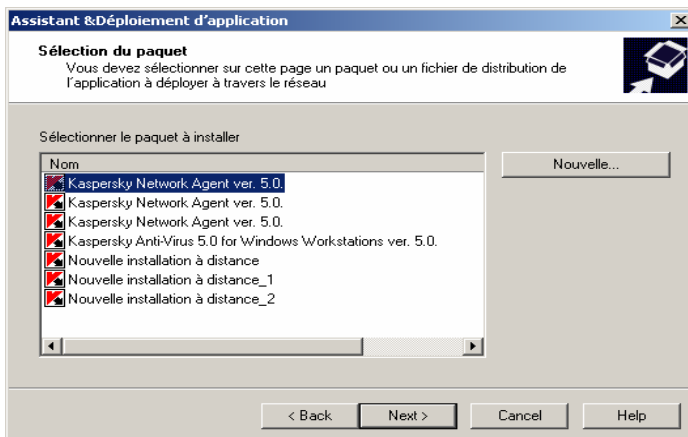


Figure 55. Assistant de déploiement d'application.
Choix d'un paquet d'installation

4. Spécifiez des ordinateurs sur lesquels vous souhaitez installer des applications Kaspersky Lab (voir Figure Figure 56) dans la fenêtre de l'Assistant. Sélectionnez l'une des options suivantes :

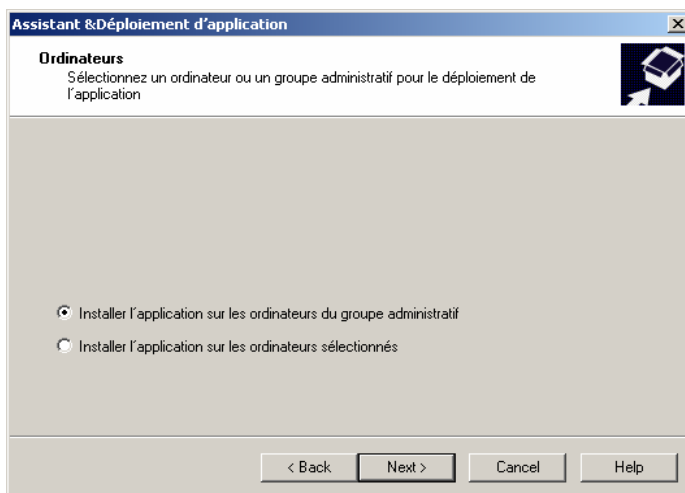
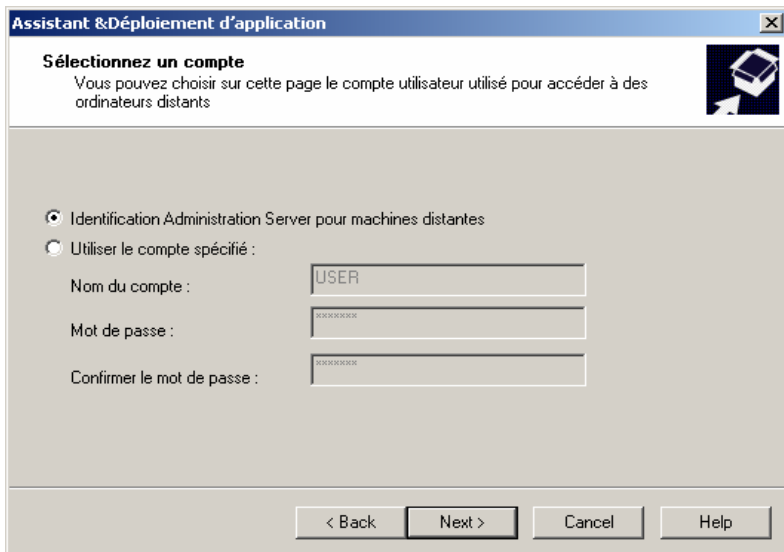


Figure 56. Sélection du type de tâche

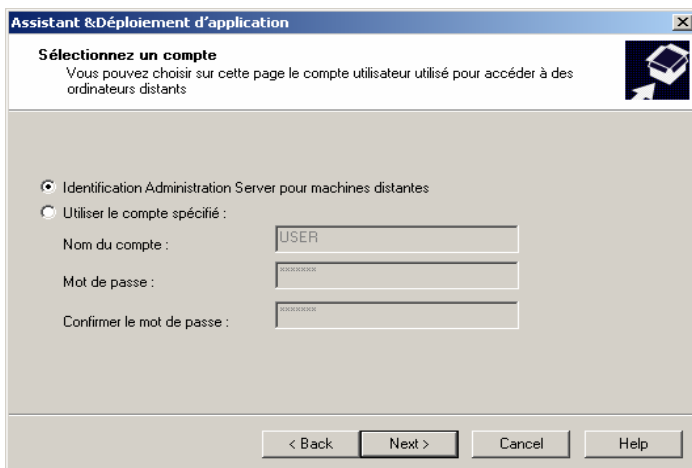
- **Installer l'application sur les ordinateurs sélectionnés**, cette option permet de créer une tâche de groupe de déploiement d'application à la fin de l'Assistant.
 - **Installer l'application sur les ordinateurs du groupe administratif** – le résultat de l'Assistant est la création d'une tâche globale.
5. Ensuite, après la création d'une tâche de groupe, spécifiez le groupe dans lequel les applications des postes clients vont être déployées (voir Figure 57) ou sélectionnez des ordinateurs pour leur installation. Si l'application doit être installée sur les postes clients du réseau logique, sélectionnez le groupe **Groupes**.



The screenshot shows a Windows-style dialog box titled "Assistant & Déploiement d'application". The main heading is "Sélectionnez un compte". Below it, a subtitle reads: "Vous pouvez choisir sur cette page le compte utilisateur utilisé pour accéder à des ordinateurs distants". There are two radio buttons: the first is selected and labeled "Identification Administration Server pour machines distantes"; the second is labeled "Utiliser le compte spécifié :". Below the second option are three text input fields: "Nom du compte :" (containing "USER"), "Mot de passe :", and "Confirmer le mot de passe :". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 57. Assistant de déploiement d'application.
Choix d'un groupe

6. Vous devez ensuite spécifier le compte utilisé pour l'exécution de la tâche de déploiement des ordinateurs clients (pour plus de détails, voir section 5.4 à la page 70).



This screenshot is identical to the previous one, but the second radio button, "Utiliser le compte spécifié :", is now selected. The text input fields for "Nom du compte :", "Mot de passe :", and "Confirmer le mot de passe :" remain the same.

Figure 58. Sélection du compte utilisateur

7. Ensuite, une boîte de dialogue affiche ensuite la progression de la tâche de déploiement sur les postes clients du groupe sélectionné (voir Figure 59). Pour afficher les détails d'exécution de la tâche sur des clients séparés, cliquez sur **Résultats**.

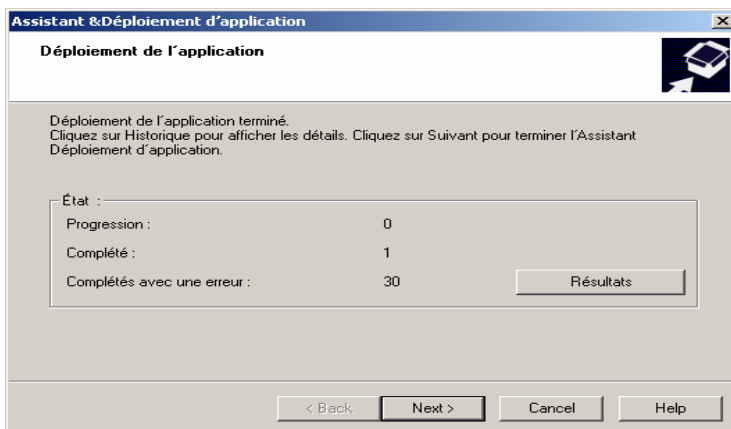


Figure 59. Exécution d'une tâche de déploiement

5.8. Installation locale de l'agent réseau



Pour installer Network Agent en local :

1. Exécutez le fichier **setup.exe** dans le dossier **NetAgent** du CD d'installation de Kaspersky Administration Kit. L'Assistant d'installation vous invite à configurer les paramètres d'installation. Suivez les instructions de l'Assistant.
2. Les premières étapes de l'installation couvrent la récupération et la copie de fichiers sur votre disque dur, l'acceptation du contrat de licence, et la saisie des informations utilisateur.
3. Dans la boîte de dialogue **Choisissez un répertoire de destination** indiquez le dossier de destination de Network Agent. L'emplacement par défaut est **Program Files\Kaspersky Lab\NetworkAgent**. Si ce dossier n'existe pas, il sera créé automatiquement. Cliquez sur **Parcourir** pour sélectionner un autre emplacement.

4. Dans la fenêtre de l'Assistant du **Serveur d'administration** (voir Figure 60), indiquez les paramètres suivants, afin que Network Agent puisse se connecter au serveur d'administration :
- Le champ **Adresse du serveur** contient l'adresse de l'ordinateur sur lequel est ou va être exploité le serveur d'administration. Vous pouvez utiliser une adresse IP ou le nom de l'ordinateur sur le réseau (nom NetBIOS).
 - Le champ **Port du serveur** donne le numéro de port utilisé par Network Agent pour se connecter au serveur d'administration. Le port par défaut est **14000**. Si ce port est déjà en service, vous pouvez en changer. N'utilisez que des multiples de dix.
 - Le champ **Port SSL du serveur** donne le numéro de port utilisé pour une connexion SSL au serveur d'administration. Le port par défaut est **13000**. Si ce port est déjà en service, vous pouvez en changer. N'utilisez que des multiples de dix dans ce champ. Pour activer la connexion SSL, cochez la case **Utiliser SSL pour se connecter au serveur**.

Assistant d'installation - Kaspersky Network Agent

Administration Server

Selectionnez un Administration Server

Selection de l'ordinateur d'installation de Kaspersky Administration Server.

Nom du serveur :

Definir le port de Administration Server dans l'intervalle 1 a 65 535.

Port du serveur :

Definir le port SSL de Administration Server. La valeur doit se trouver dans l'intervalle 1-65535.

Port SSL du serveur :

☒ Utiliser SSL pour se connecter au serveur

< Precedent Suivant > Annuler

Figure 60. Installation de Network Agent.
Configuration de la connexion

5. Spécifiez le dossier du groupe **Non attribué** où ce client sera ajouté par le serveur d'administration. Indiquez les options suivantes (voir Figure 61):
- **Nom de groupe par défaut** – Le client sera ajouté à un dossier qui correspond à son emplacement courant dans le réseau

Windows – domaine ou groupe d'utilisateur (option active par défaut).

- **Définir le nom de groupe** – Le client sera ajouté au dossier indiqué. Écrivez le nom du dossier dans la zone inférieure. Si le groupe **Non attribué** ne possède aucun dossier avec ce nom, il sera créé (vous pouvez également indiquer le nom du dossier existant dans le groupe **Non attribué**).

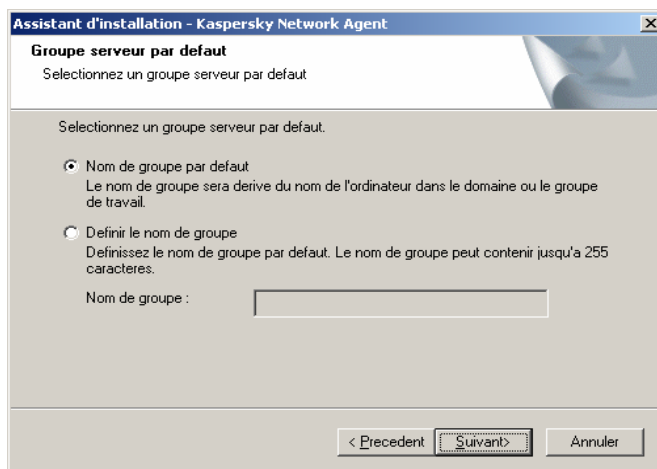


Figure 61. Installation de Network Agent.

Définition d'un dossier dans le groupe **Non attribué** pour y placer de nouveaux ordinateurs

6. À l'étape suivante (voir Figure 62), indiquez comment le certificat du serveur d'administration sera récupéré. Sélectionnez l'une des options suivantes :
 - **Fichier de certification par défaut** – le certificat du serveur d'administration sera envoyé lors de la première connexion de Network Agent au serveur d'administration (valeur par défaut).
 - **Sélectionnez un fichier de certification** – Le serveur d'administration sera authentifié en utilisant un certificat choisi par l'administrateur. Cliquez sur Parcourir pour retrouver le fichier nécessaire.



Le fichier possède une extension **.cer** et se trouve placé dans le dossier **Cert** du répertoire de Kaspersky Administration Kit sur le serveur d'administration. Vous pouvez copier le fichier de certification dans un dossier partagé ou une disquette. Cette copie peut être utilisée pendant l'installation de Network Agent.

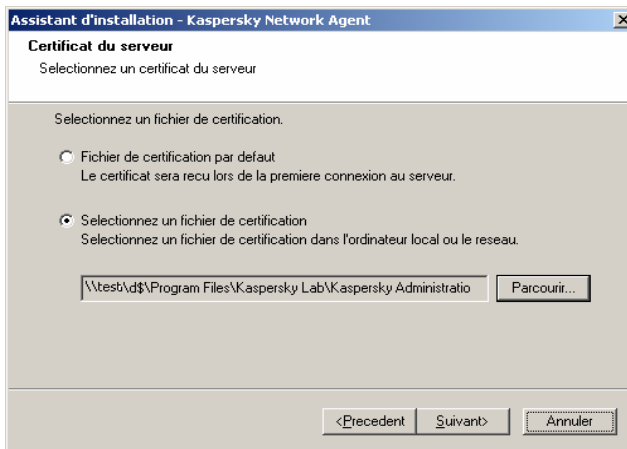


Figure 62. Installation de Network Agent.

Choix d'une méthode de réception du certificat du serveur d'administration.

7. Dans la dernière boîte de dialogue de l'Assistant (Figure 63), cochez la case **Exécuter Kaspersky Network Agent** pour lancer Network Agent juste après la fin de l'installation. Si vous voulez lancer Network Agent plus tard, annulez la sélection de cette case.



Si vous prévoyez d'utiliser le même disque dur de l'ordinateur sur lequel vous prévoyez d'installer l'agent réseau, il faut décocher la case **Exécuter Kaspersky Network Agent** pour créer l'image disque de déploiement sur les autres ordinateurs.

Si vous lancez l'agent réseau avant de créer l'image disque, ce composant ne peut pas être restauré correctement. Le serveur d'administration considèrera tous les ordinateurs comme un même ordinateur.

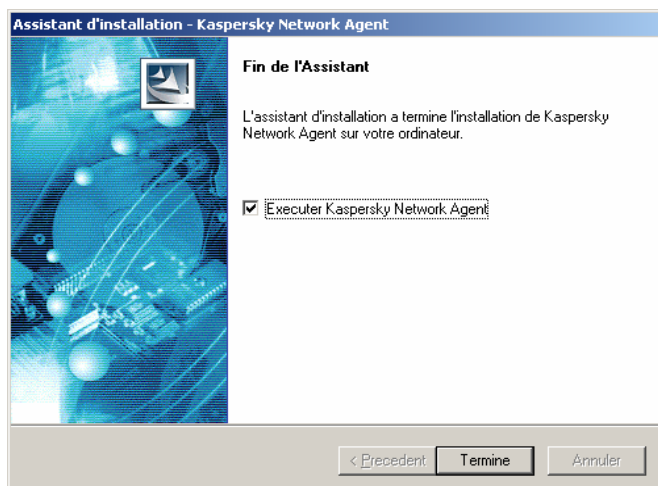


Figure 63 Installation de Network Agent. Configuration du lancement de Network Agent

À la fin de l'installation, Network Agent sera installé sur votre ordinateur avec les paramètres suivants :

- Nom – **Kaspersky Network Agent**
- **Automatique** lancement au démarrage du système d'exploitation
- Le compte **Système local**.

Vous pouvez afficher les propriétés du service **Kaspersky Network Agent**, le lancer et l'arrêter, et surveiller son exécution à partir de l'outil **Services**, qui est l'outil standard d'administration de Windows.

5.9. Installation locale du plug-in de console de Network Agent



Pour installer le plug-in de console de Network Agent :

Exécutez le fichier **klcfginst.msi** dans le CD d'installation de l'ordinateur disposant de la console d'administration. Ce fichier est inclus avec toutes les applications pouvant être contrôlées par Kaspersky Administration Kit. L'Assistant vous guidera à travers l'installation. Suivez les instructions de l'Assistant.



Le fichier d'installation **klcfginst.msi** du plug-in de console de Network Agent se trouve dans le dossier **NetAgent** du paquet d'installation de Kaspersky Administration Kit.

5.10. Installation d'applications en mode silencieux



Pour installer une application en mode silencieux :

1. Créez le paquet d'installation nécessaire (voir section 5.2 à la page 66) si vous ne l'avez pas fait pour cette application.
2. Sur l'ordinateur où vous voulez installer l'application en mode silencieux, dans le paquet d'installation, exécutez **setup.exe** avec la bascule **/s**.



Des paquets d'installation sont entreposés sur le serveur d'administration dans le dossier **Packages**, dans un dossier partagé spécifié pendant l'installation du serveur d'administration.

CHAPITRE 6. GESTION DE STRATEGIES

6.1. Création d'une stratégie pour une application



Pour créer une nouvelle stratégie de groupe :

1. Dans l'arborescence de console, choisissez le groupe dans lequel vous allez créer une stratégie. Dans le dossier du groupe, sélectionnez le dossier **Stratégies** et cliquez sur **Nouveau/Stratégie** dans le menu contextuel ou dans le menu **Action** afin de lancer un Assistant de nouvelle stratégie. Suivez les instructions de l'Assistant.
2. Vous devez maintenant indiquer le nom et l'application cible de la stratégie.

Écrivez le nom de la stratégie. Si une stratégie de ce nom existe déjà, un **_1** sera automatiquement ajouté à la fin du nouveau nom.

Sélectionnez une application dans la liste **Nom de l'application** (Figure 64). La liste déroulante inclut toutes les applications qui possèdent un plug-in de console installé sur le poste administrateur.



Pour une application donnée, une seule stratégie de groupe peut être affectée à un groupe. Il n'est pas possible de créer des stratégies pour les applications elles-mêmes.

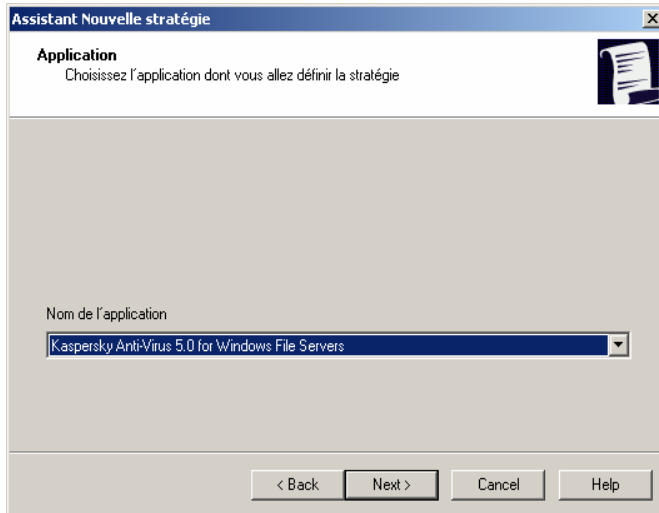


Figure 64. Création d'une stratégie. Choix d'une application

3. Pour mettre en œuvre la stratégie créée en tant que stratégie active de l'application, activez-la en cochant la case **Activer la stratégie** (voir Figure 65).



Il est possible de créer de nombreuses stratégies de groupe pour une application, mais une seule d'entre elles peut être celle active.

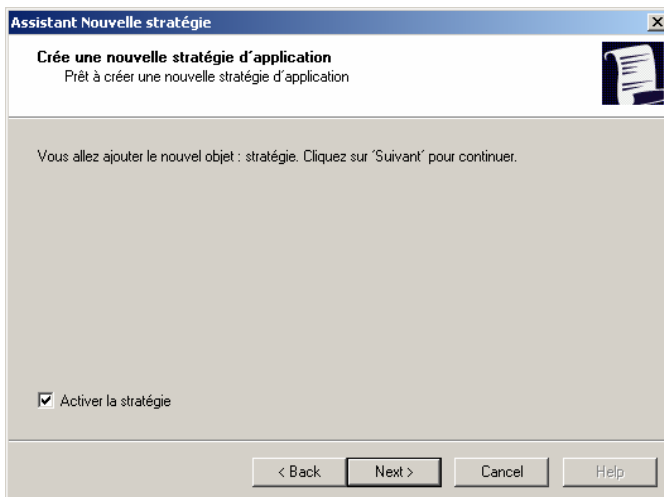




Figure 65. Création d'une stratégie. Activation de la stratégie

4. Vous devez ensuite considérer les paramètres généraux de la stratégie et configurer ceux de l'application sélectionnée (Figure 66). Vous pouvez verrouiller les paramètres de stratégie des sous-groupes, des paramètres d'application, ou des paramètres de tâche. Les paramètres de stratégie qui peuvent être verrouillés sont identifiés par l'icône . Cliquez sur cette icône pour verrouiller un paramètre. L'icône changera en .



Les paramètres de l'application locale sont prioritaires sur les paramètres de stratégie. Pour qu'une stratégie puisse avoir un effet sur des postes clients, vous devez verrouiller certains paramètres.

Lors de la création d'une stratégie, vous ne pouvez configurer qu'un ensemble minimum de paramètres, ceux nécessaires au bon fonctionnement de l'application. Tous autres paramètres prendront des valeurs par défaut, correspondant à celles définies lors de l'installation locale de l'application. La stratégie ainsi configurée peut être modifiée plus tard (voir section 6.2 à la page 94).

Pour plus d'informations sur la configuration de la stratégie pour chaque application, reportez-vous à la documentation correspondante.

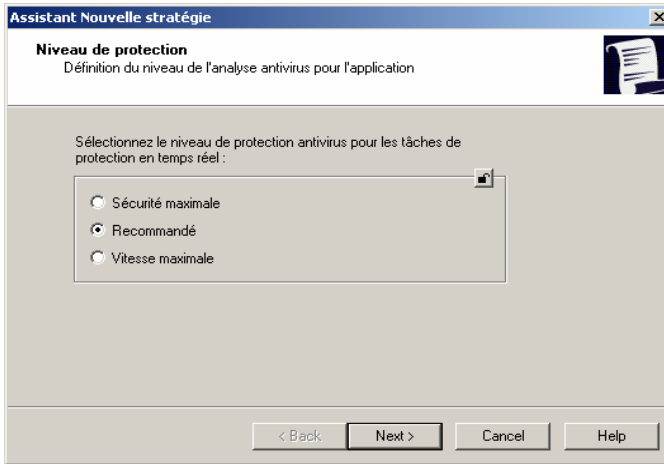


Figure 66. Création d'une stratégie pour Kaspersky Antivirus 5.0 pour Windows Workstations

6.2. Affichage et modification d'une stratégie



Pour afficher ou modifier des paramètres de stratégie de groupe :

Dans l'arborescence de console, choisissez le groupe requis et cliquez sur le dossier **Stratégies** dans ce groupe. Dans le panneau de détails, vous verrez la liste de toutes les stratégies créées pour ce groupe. Sélectionnez une stratégie et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.

La boîte de dialogue **Propriétés de <Nom de stratégie>** s'affiche avec plusieurs onglets permettant de configurer la stratégie de groupe d'une application : Les onglets sont spécifiques à chaque application et leur description figure dans la documentation correspondante. Remarquez que les onglets **Général**, **Contrôle** et **Traitement des événements** sont communs à toutes les applications.

L'onglet **Général** (voir Figure 67) affiche des informations générales sur la stratégie :

- Nom de stratégie
- Nom de l'application pour laquelle la stratégie est créée (par exemple, Kaspersky Antivirus 5.0 pour Windows Workstations)
- Version de l'application
- Date et heure de création
- Date et heure de la dernière modification
- Case **Activer la stratégie en fonction de l'événement** et la liste utilisée pour sélectionner un événement qui déclenche l'activation de la stratégie
- Case **Activer la stratégie** qui détermine si la stratégie est celle active pour l'application.

Sur cet onglet, vous pouvez :

- renommer la stratégie ;
- définir l'activation automatique de la stratégie au déclenchement d'un certain événement, et sélectionner cet événement ;
- activer ou désactiver une stratégie.

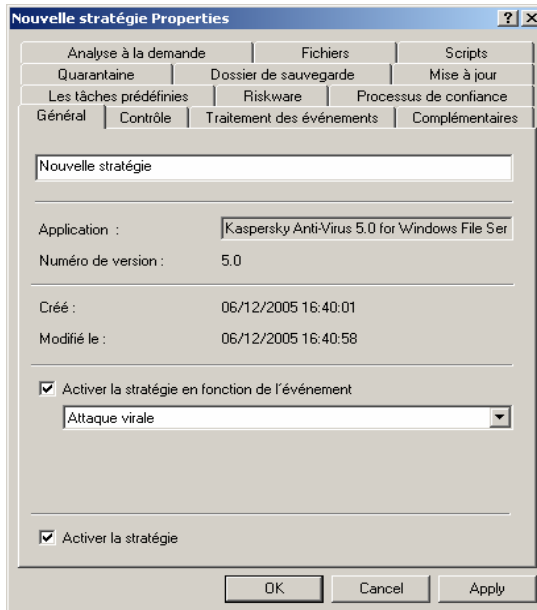


Figure 67. Modification d'une stratégie. L'onglet **Général**

L'onglet **Contrôle** (voir Figure 68) affiche les résultats de l'application de la stratégie sur les postes clients présents dans le groupe. L'onglet présente les numéros des ordinateurs pour lesquels la stratégie était :

- Définie
- Appliquée
- En attente
- Échec

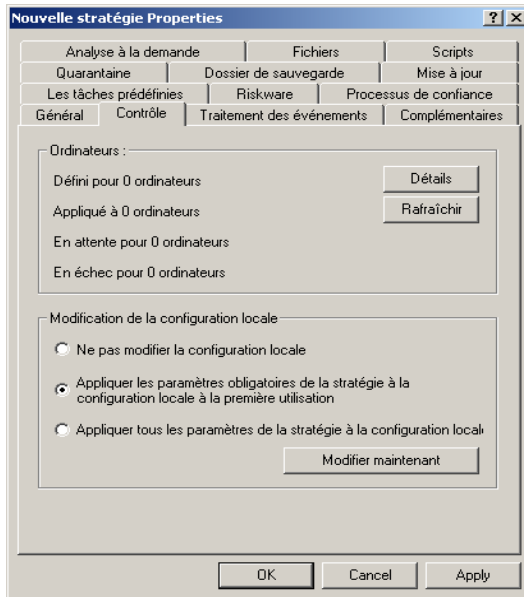
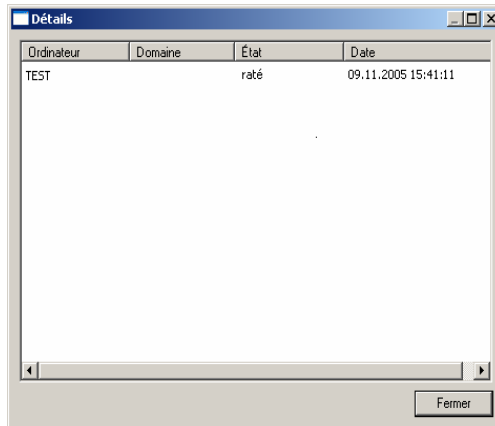


Figure 68. Modification d'une stratégie. L'onglet **Contrôle**

Des comptes-rendus détaillés de la mise en place de la stratégie sur chaque client sont disponibles dans la boîte de dialogue (voir Figure 69) que vous pouvez ouvrir avec le bouton **Détails**. La boîte de dialogue **Détails** présente un tableau avec les colonnes suivantes :

- **Ordinateur** – Nom du client
- **Domaine** – Nom du domaine auquel le client appartient
- **État**– L'une des valeurs suivantes :
 - **En attente** – les paramètres de cette stratégie ont été modifiés sur le serveur Administration Kit, mais n'ont pas encore été synchronisés avec les postes de travail ;
 - **Terminée** – la stratégie pour une application sur cet ordinateur a été appliquée avec succès ;
 - **Planification** – La stratégie d'une application n'est pas encore appliquée sur cet ordinateur ;

- **Échec** – L'application de la stratégie a échoué sur cet ordinateur (l'ordinateur a été arrêté, déconnecté, l'application ne s'exécute pas, ou n'a pas été installée).
- **Date** : la date et l'heure de l'événement ;



Ordinateur	Domaine	État	Date
TEST		raté	09.11.2005 15:41:11

Figure 69. Résultats de l'application de la stratégie sur les clients d'un groupe

L'onglet **Traitement des événements** (voir Figure 70) affiche les paramètres de traitement des événements associés aux applications : quel type d'événements enregistrer, comment informer l'administrateur ou d'autres utilisateurs sur des événements concernant la protection antivirus, et où stocker les journaux des événements.

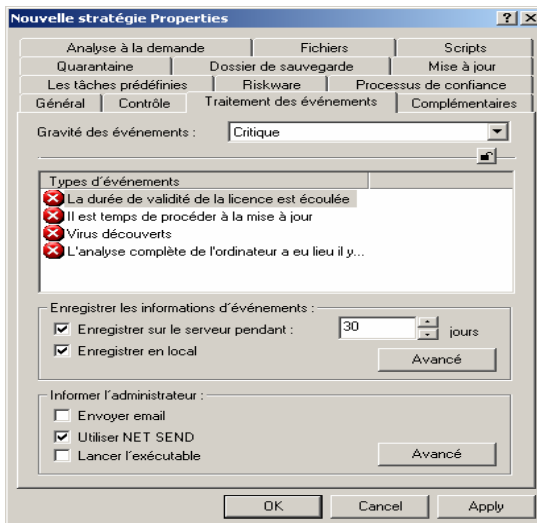


Figure 70. Modification d'une stratégie. L'onglet **Traitement des événements** (onglet)

Après la création de la stratégie, les valeurs de l'onglet **Traitement des événements** correspondent aux paramètres par défaut de l'application. Ces paramètres sont spécifiques à chaque application de Kaspersky Lab et vous trouverez des informations supplémentaires dans la documentation de chaque application. Au besoin, vous pouvez modifier les paramètres de stratégie selon vos nécessités.

Les événements liés à la protection antivirus de toutes les applications Kaspersky Lab peuvent avoir les degrés de gravité suivants :

- **Critique** – Un événement critique (par exemple, la détection d'un virus)
- **Erreur** – Défaillance de l'application (par exemple, la licence a expiré)
- **Avertissement** – Un message d'avertissement (par exemple, la détection d'un objet suspect ou des archives protégées par mot de passe)
- **Info** – Message d'information (par exemple, un objet a été désinfecté ou supprimé).

Il est possible de définir des règles de manipulation d'événements pour chaque niveau de gravité.

1. Dans la liste déroulante, sélectionnez le niveau de gravité : **Critique, Erreur, Avertissement** ou **Info**.
2. Les événements correspondant au niveau de gravité choisi seront affichés dans la zone **Types d'événements** inférieure. La liste d'événements est propre à chaque application. Pour plus d'informations sur les événements, reportez-vous à la documentation de l'application. Pour choisir les types d'événements à enregistrer, appuyez sur les touches **Majus** et **Ctrl** de votre clavier.
3. Dans la section **Enregistrer les informations d'événements**, cochez :
 - La case **Enregistrer sur le serveur pendant** pour que le serveur d'administration enregistre les événements qui se produisent pour tous les clients du groupe. Dans la zone **Jours**, indiquez le nombre de jours d'enregistrement par le serveur. Après la fin de la période d'enregistrement indiquée, l'entrée correspondante à cet événement sera supprimée. Vous pouvez examiner les comptes-rendus d'événement entreposés sur le serveur d'administration à partir de la console du poste administrateur. Les événements sont enregistrés dans l'entrée Événements de l'arborescence de console.
 - La case **Enregistrer en local** pour enregistrer des événements en local sur chaque client. Dans ce cas, vous ne pouvez examiner les journaux d'événement qu'à partir de la console d'administration installée en local (poste Ordinateur local).

Pour configurer le journal des événements de Windows afin qu'il enregistre les événements concernant la protection antivirus, cliquez sur **Options avancées** pour ouvrir la boîte de dialogue **Enregistrement d'événements** (voir Figure 71) et cochez les options suivantes :

- La case **Journal d'événements de Windows du serveur** pour activer l'enregistrement de tous les événements associés à tous les clients du groupe dans le journal d'événement de Windows, sur un ordinateur équipé du serveur d'administration.
- La case **Journal d'événements de Windows de l'hôte** pour que chaque client enregistre les événements en local, dans leur propre journal d'événement de Windows.

L'information peut être affichée dans l'**Observateur d'événements**, l'outil de gestion d'événement standard de Windows.

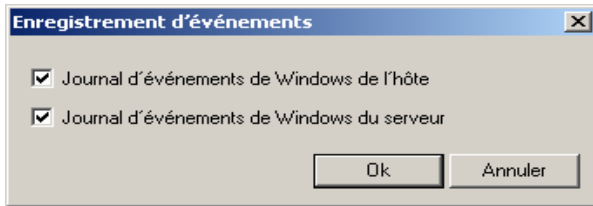


Figure 71. Boîte de dialogue **Enregistrement d'événements**

4. Dans le groupe **Informier l'administrateur**, indiquez comment les notifications seront envoyées à l'aide des options suivantes :
 - **Envoyer e-mail** – Envoi de notifications par l'intermédiaire d'un serveur de messagerie
 - **Utiliser NET SEND** – Envoi de notifications par l'intermédiaire du service NET SEND
 - **Lancer l'exécutable** – Exécuter un programme ou un script dans le cas d'un certain événement.

Vous pouvez cocher plusieurs cases à la fois.

5. Configurez les paramètres du mode de notification choisi. Cliquez sur **Avancé** pour ouvrir la boîte de dialogue **Options avancées**, et spécifier ce qui suit (voir Figure 72):

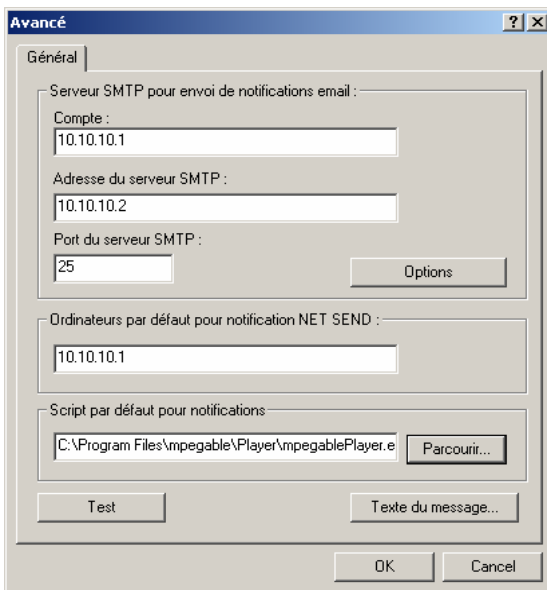


Figure 72. Sélection du mode de notification. Indication des paramètres de notification

- Dans le groupe de zones **Serveur SMTP pour envoi de notification email**, configurez les paramètres de messagerie suivants :
 - Indiquez l'adresse de messagerie du destinataire dans la zone **Compte**. Vous pouvez indiquer plusieurs adresses séparées par une virgule ou un point-virgule.
 - Saisissez l'adresse du serveur de messagerie dans la zone **Adresse du serveur SMTP**. Vous pouvez utiliser une adresse IP ou un nom NetBIOS.
 - Spécifier le numéro de port du serveur SMTP dans la zone **Port du serveur SMTP**. Le numéro de port par défaut est 25.
- Indiquez les adresses, sur le réseau local, des ordinateurs destinataires des notifications, dans le groupe de champs **Ordinateurs par défaut pour notification NET SEND**. Vous pouvez également utiliser une adresse IP ou un nom NetBIOS. Vous pouvez écrire plus d'une adresse séparée par une virgule ou un point-virgule.

- Indiquez le chemin d'accès au script à exécuter en cas d'événement dans la zone **Script par défaut pour notifications**.



Les noms des variables d'environnement du module exécutable coïncident avec les noms des paramètres de remplacement employés pour composer le message de notification (voir ci-dessous).

- Écrivez le texte de la notification à envoyer aux destinataires définis. Cliquez sur **Texte du message** et rédigez le modèle dans la boîte de dialogue affichée (voir Figure 73).

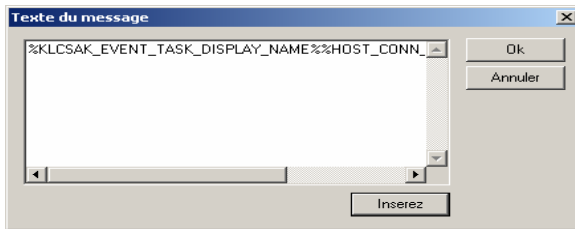


Figure 73. Indication des paramètres de notification. Rédaction d'un message de notification

Le texte de la notification peut donner des informations sur l'événement enregistré. Pour apporter ces explications, sélectionnez les paramètres suivants dans les listes déroulantes disponibles à travers le bouton **Insérer** :

- **Gravité événement** – Gravité de cet événement.
- **À partir de l'ordinateur** – Nom du client sur lequel cet événement s'est produit.
- **À partir du domaine** – Nom du domaine contenant l'ordinateur.
- **Événement** – Type d'événement.
- **Description d'événement** – Description d'événement.
- **Heure d'enregistrement** – Moment où cet événement a été enregistré.
- **Nom de tâche.**
- **Application.**

- o **Version.**
- o **Adresse IP**
- o **Adresse IP de la connexion.**
- Expéditeur et sujet du message de notification. Pour ce faire, cliquez sur **Paramètres** puis, dans la nouvelle fenêtre (voir Figure 74), complétez les champs **De :** et **Sujet :**.

L'activation des zones dépend du mode de notification sélectionné dans le groupe Notification.

Les paramètres par défaut sont ceux définis dans l'onglet **Notification** des propriétés du serveur d'administration (voir section 8.2 à la page 143).

Pour vérifier que les paramètres spécifiés sur cet onglet sont corrects, essayez d'envoyer un message de test. Pour ce faire, cliquez sur **Test**. Les messages créés d'après le modèle spécifié seront envoyés à l'adresse indiquée dans les paramètres.

6. Après avoir configuré tous les paramètres nécessaires, cliquez sur **Appliquer** et continuez avec le niveau de gravité suivant.

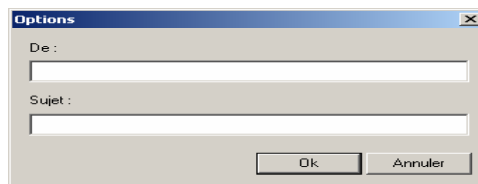


Figure 74. Indication des paramètres de notification. Spécification de l'expéditeur et du sujet du message

6.3. Activation d'une stratégie



Pour définir une stratégie de groupe active l'application,

1. Sélectionnez la stratégie de groupe souhaitée dans le panneau de résultats, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**, ou utilisez son équivalent du menu **Action**.
2. Dans la fenêtre de configuration de la stratégie de groupe **Propriétés: <Nom de stratégie>**, sélectionnez l'onglet Général (voir Figure 67).

3. Cochez la case **Activer la stratégie**.



Pour désactiver la stratégie, décochez cette case.

4. Cliquez sur **Appliquer** ou sur **Ok**.



Pour activer une stratégie de groupe automatiquement lors d'un certain événement,

1. Sélectionnez le groupe souhaité dans le panneau de résultats, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**, ou utilisez son équivalent du menu **Action**.
2. Sélectionnez **Général** (voir Figure 67) dans la fenêtre de configuration de la stratégie de groupe de l'application **Propriétés: <Nom de stratégie>**.
3. Cochez la case **Activer la stratégie en fonction de l'événement** et sélectionnez l'événement souhaité dans la liste déroulante.



Pour annuler l'activation automatique de la stratégie en fonction d'un événement, il faut désactiver la case.

4. Cliquez sur **Appliquer** ou sur **Ok**.



Si vous désactivez la stratégie en fonction de l'événement, vous ne pouvez rétablir la stratégie précédente que manuellement.

6.4. Création d'une stratégie pour Network Agent

Pour créer une stratégie pour Network Agent (voir Figure 75), configurez les paramètres suivants :

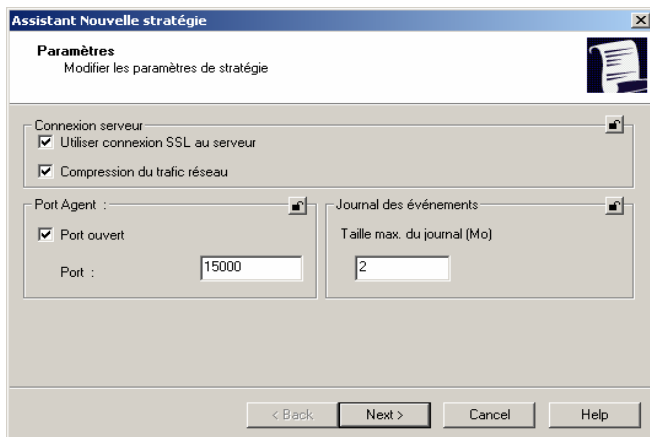


Figure 75. Configuration d'une stratégie pour l'agent réseau

- Dans le groupe **Connexion serveur**, cochez la case **Utiliser connexion SSL** pour activer la connexion par un port sécurisé SSL (en utilisant le protocole SSL).
- La section **Port Agent** permet de d'activer une connexion client/serveur par l'intermédiaire d'un port UDP et de définir le numéro du port. Pour activer la connexion d'un port UDP, cochez la case **Port ouvert** et écrivez le numéro de port dans la zone **Port**. La valeur par défaut est 15000. Si ce port est déjà en service, vous pouvez changer son numéro. Le port doit être un multiple de dix.



Si un poste client fonctionne sous Windows XP SP2, le pare-feu incorporé verrouillera le port UDP 15000. Vous devez donc ouvrir manuellement ce port pour faciliter l'accès au serveur d'administration.

- Dans le groupe **Journal des événements**, indiquez la taille du journal. Saisissez la taille maximum du fichier journal dans la zone **Taille max. du journal (Mo)**.

Pour modifier la stratégie de Network Agent (Figure 76), vous pouvez ajuster les paramètres précédents et définir la période de synchronisation en minutes. Les données du poste client et du serveur d'administration seront synchronisées une fois pendant la période de temps indiquée dans la zone **Période de connexion, min.**

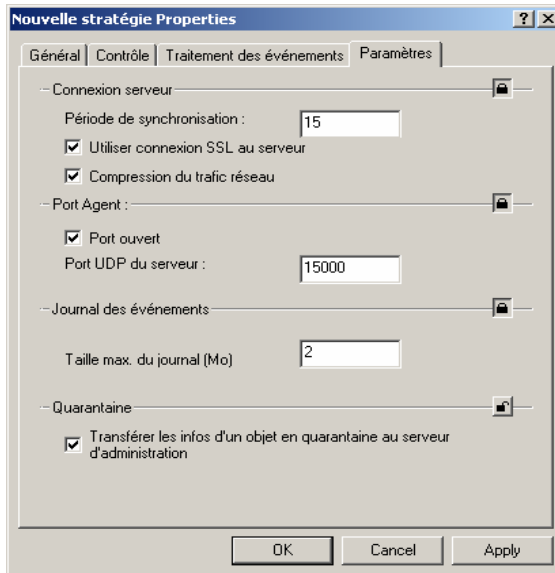


Figure 76. Modification d'une stratégie pour Network Agent

6.5. Exportation et importation de stratégies



Pour exporter une stratégie :

Dans l'arborescence de console, choisissez le groupe requis et cliquez sur l'entrée **Stratégies**. Dans le panneau de résultats, vous verrez la liste de toutes les stratégies existantes pour ce groupe. Sélectionnez une stratégie, ouvrez le menu contextuel et cliquez sur **Exporter**. La même commande est disponible sous le menu **Action**.

Dans la fenêtre ouverte, spécifiez le nom de fichier et l'emplacement sous lequel vous allez enregistrer la stratégie. Cliquez sur **Enregistrer**.



Pour importer une stratégie :

Dans l'arborescence de console, choisissez le groupe requis. Ouvrez le menu contextuel du dossier **Stratégies** puis cliquez sur **Toutes les tâches/Import**. La même commande est disponible sous le menu **Action**

Dans la fenêtre ouverte, spécifiez le nom de fichier d'importation de la stratégie puis cliquez sur **Ouvrir**.



Si le groupe contient déjà une stratégie pour cette application, l'importation de la nouvelle stratégie ne se fera pas.

CHAPITRE 7. ADMINISTRATION DE TACHES

7.1. Création d'une tâche de groupe



Pour indiquer une nouvelle tâche de groupe :

1. Dans l'arborescence de console, choisissez le groupe dans lequel vous allez créer la tâche et sélectionnez le dossier **Tâches** pour ce groupe. Dans le menu contextuel ou dans le menu **Action**, cliquez sur **Nouveau/Tâche** pour lancer un nouvel Assistant de tâche. Suivez ses instructions.
2. Indiquez le nom de tâche. Si une tâche de ce nom existe déjà dans le groupe, un **_1** sera automatiquement ajouté au nouveau nom.
3. Sélectionnez ensuite l'application pour laquelle vous voulez créer une tâche et définissez le type de tâche (voir Figure 77).

Sélectionnez une application dans la liste déroulante. La liste affiche toutes les applications Kaspersky Lab qui possèdent un plug-in de console installé sur le poste administrateur.

Sélectionnez le type de tâche dans la liste **Choisissez le type de tâche à exécuter**. Les tâches énumérées sont celles disponibles pour l'application choisie.

Si vous créez une tâche de déploiement d'application, choisissez l'application **Kaspersky Administration Kit**, et le type de tâche **Tâche de déploiement de l'application** (voir section 5.4 à la page 70).

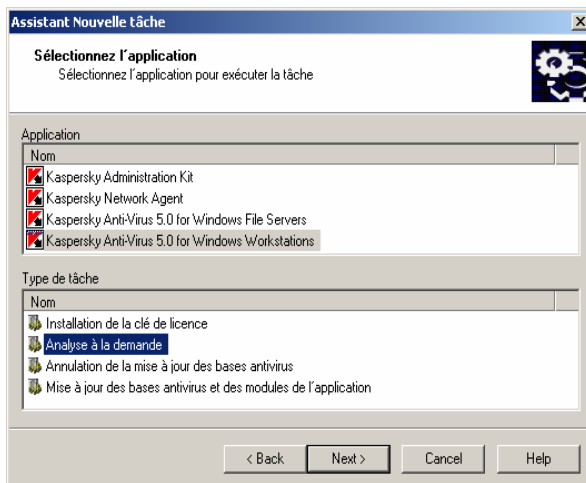


Figure 77. Création d'une tâche. Sélection d'une application et du type de tâche

4. Configurez ensuite les paramètres de tâche selon l'application choisie (voir Figure 78). Quelques paramètres sont définis par défaut. Pour plus de détails au sujet de la configuration de tâche, reportez-vous à la documentation de l'application en particulier.

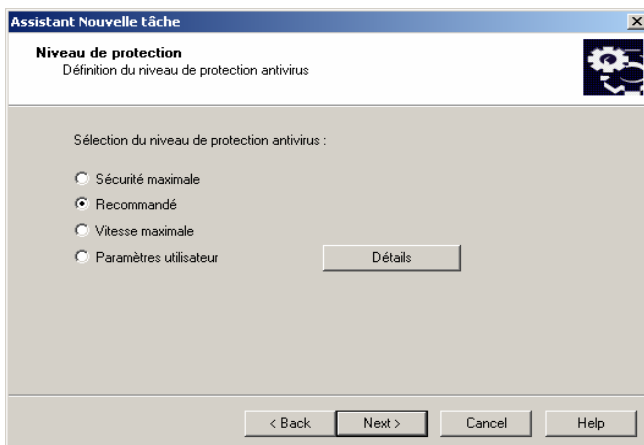


Figure 78. Configuration d'une tâche pour Kaspersky Antivirus 5.0 pour Windows Workstations

5. Dans la fenêtre suivante de l'Assistant, spécifiez le compte utilisé sur les postes clients pour démarrer la tâche (voir Figure 79).

Sélectionnez l'une des options ci-dessous :

- **Compte par défaut** – La tâche utilise le compte de l'application qui exécute cette tâche.
- **Compte spécifié** – Vous devrez renseigner les détails d'un compte (utilisateur et mot de passe) possédant des droits suffisants pour accéder à cet objet. Par exemple, pour tâche d'analyse à la demande, des permissions d'accès à l'objet analysé sont nécessaires, tandis que pour une tâche de mise à jour, il faut des droits d'accès au dossier public sur le serveur d'administration ou des droits d'utilisateur autorisé du serveur proxy.

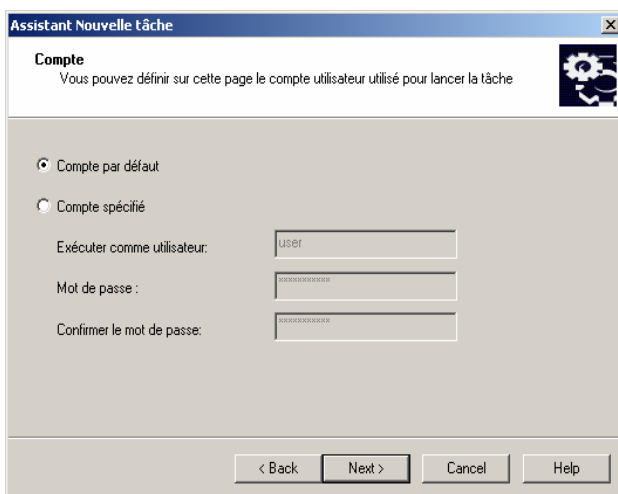


Figure 79. Création d'une tâche. Sélection d'un compte

6. Définissez la fréquence et l'heure de démarrage de la tâche.
- Dans la liste **Planification à exécuter**, définissez le démarrage de la tâche :
 - **Toutes les N heures;**
 - **Chaque jour;**
 - **Chaque semaine;**

- o **Chaque mois;**
 - o **Une fois;**
 - o **Au lancement de l'application** – Lance la tâche au démarrage de l'application.
 - o **Manuellement** – Démarre la tâche manuellement à partir de la fenêtre principale de Kaspersky Administration Kit, en cliquant sur **Démarrer** dans le menu contextuel ou dans le menu **Action**.
 - o **Immédiatement** – Démarre la tâche immédiatement après avoir terminé l'Assistant.
- Spécifiez les options de planification dans les zones appropriées du programme sélectionné.

Si vous avez programmé la tâche **Toutes les N heures** (voir Figure 80), indiquez ce qui suit :

Assistant Nouvelle tâche

Paramètres de programmation de la tâche
Indiquez quand vous souhaitez exécuter la tâche.

Exécution programmée :
Tous les N jours

Chaque
1 jour

Démarrer à :
17:51:28

☒ Lancer tâches non exécutées

☒ Démarrage aléatoire de la tâche avec intervalle (min.): 20

< Back Next > Cancel Help

Figure 80. Programmation d'une tâche exécutée **Toutes les N heures**

- o La fréquence des démarrages de tâche dans la zone **Chaque heure** et la date et heure de départ dans la zone **Planification à exécuter**.

Par exemple, si la valeur 2 est affectée à la zone **Chaque heure** et la valeur du 3 août 2004 à 15:00:00 se trouve dans la zone **Planification à exécuter**, la tâche démarrera

toutes les deux heures à partir de 15 heures, le 3 août 2004.

La fréquence est définie par défaut à 6 et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- o La procédure que la tâche doit démarrer si le poste client n'est pas disponible (éteint, déconnecté du réseau, etc.) ou si l'application n'est pas lancée à l'heure programmée.

Cochez la case **Lancer tâches non exécutées** pour que le système essaie d'exécuter un tâche lors de la prochaine ouverture de l'application sur ce poste client.

Si la case n'est pas cochée (son état par défaut), l'exécution des tâches sur les postes clients se fera uniquement comme programmé.

- o Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients. Cette possibilité est offerte pour résoudre le problème des appels au serveur d'administration simultanément par de nombreux postes clients lors du lancement de la tâche.

Cochez la case **Démarrage aléatoire de la tâche** et indiquez l'intervalle de temps (en minutes) pendant lequel les postes clients appelleront le serveur d'administration après le démarrage de la tâche, au lieu de le faire simultanément.

Par défaut, cette case n'est pas cochée.

Si vous avez programmé la tâche **Chaque jour** (voir Figure 81), indiquez ce qui suit :

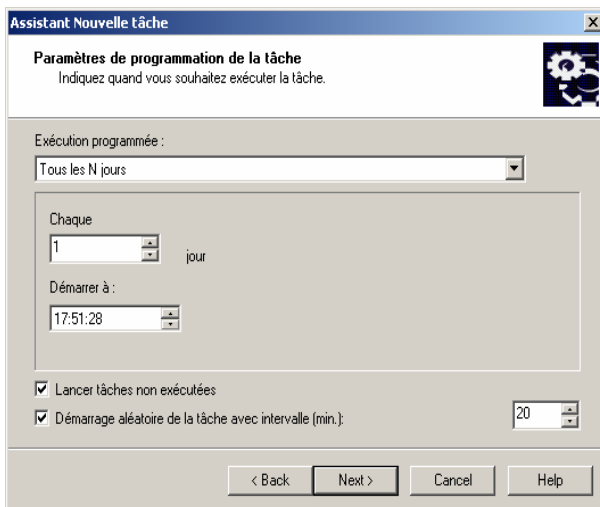


Figure 81. Programmation d'une tâche exécutée **chaque jour**

- o La fréquence des démarrages de tâche dans la zone **Tous les N jours** et l'heure de départ dans la zone **Planification à exécuter**.

Par exemple, si le champ **Tous les N jours** affiche la valeur 2 et le champ **Planification à exécuter** indique 15:00:00, la tâche commencera une fois tous les deux jours à 3 heures de l'après midi.

La valeur par défaut du champ **Tous les N jours** est 2 et l'heure système est utilisée par défaut comme heure de départ.

- o Pour des instructions sur la marche à suivre lorsqu'un client est temporairement indisponible, voir ci-dessus.
- o Pour l'option de planification aléatoire, voir ci-dessus

Si vous avez programmé la tâche **Toutes les N semaines** (Figure 82) indiquez ce qui suit :

Assistant Nouvelle tâche

Paramètres de programmation de la tâche
Indiquez quand vous souhaitez exécuter la tâche.

Exécution programmée :
Toutes les N semaines

Chaque
1 semaine

Démarrer à :
18:36:34

Jour de la semaine :
lundi

☒ Lancer tâches non exécutées

☒ Démarrage aléatoire de la tâche avec intervalle (min.): 20

< Back Next > Cancel Help

Figure 82. Programmation d'une tâche hebdomadaire

- o La fréquence des démarrages de tâche dans la zone **Chaque** et l'heure de départ dans la zone **Planification à exécuter**. Par défaut, la tâche démarrera le dimanche à 18:00:00. Vous pouvez modifier l'heure de départ, si nécessaire.

Par exemple, si la valeur de la zone **Chaque** est **Dimanche** et la valeur du champ **Planification à exécuter** est 3:00:00 AM, la tâche commencera chaque **Dimanche** à 3 heures du matin.

- o Pour des instructions sur la marche à suivre lorsqu'un client est temporairement indisponible, voir ci-dessus.
- o Pour l'option de planification aléatoire, voir ci-dessus.

Si vous avez programmé la tâche **Chaque mois** (Figure 83), indiquez ce qui suit :

- o La fréquence des démarrages de tâche dans la zone **Chaque jour dans le mois** et l'heure de départ dans la zone **Planification à exécuter**.

Par exemple, si la valeur de la zone **Chaque jour dans le mois** contient **20** et la valeur du champ **Planification à**

exécuter est 3:00:00 AM, la tâche commencera le 20 de chaque mois à 3 heures du matin.

La valeur par défaut du champ **Chaque jour dans le mois** contient **1** et l'heure système est utilisée dans le champ **Planification à exécuter**.

- Pour des instructions sur la marche à suivre lorsqu'un client est temporairement indisponible, voir ci-dessus.
- Pour l'option de planification aléatoire, voir ci-dessus.

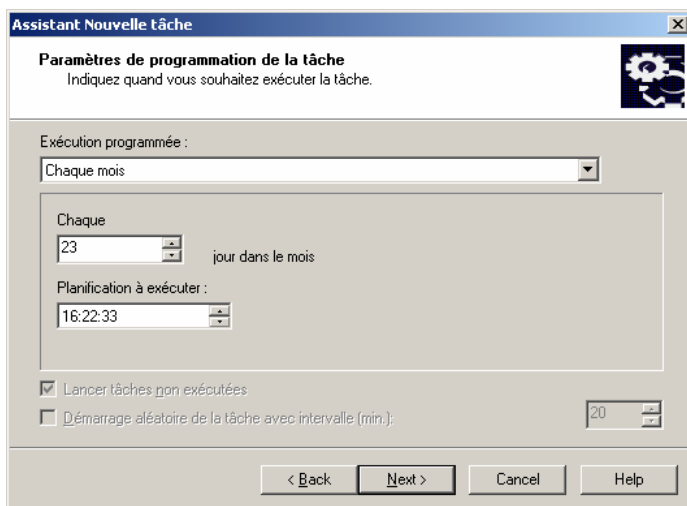


Figure 83. Programmation d'une tâche mensuelle

Si vous définissez le démarrage de la tâche **Une fois** (Figure 84), indiquez ce qui suit :

- La date de démarrage de la tâche dans la zone **Exécuter pendant**, et l'heure de démarrage dans la zone **Planification à exécuter**. Les valeurs de ces champs sont définies automatiquement et correspondent à la date et à l'heure courantes du système. Vous pouvez les modifier si nécessaire.
- Pour des instructions sur la marche à suivre lorsqu'un client est temporairement indisponible, voir ci-dessus.
- Pour plus d'informations sur l'option de planification aléatoire, voir ci-dessus.

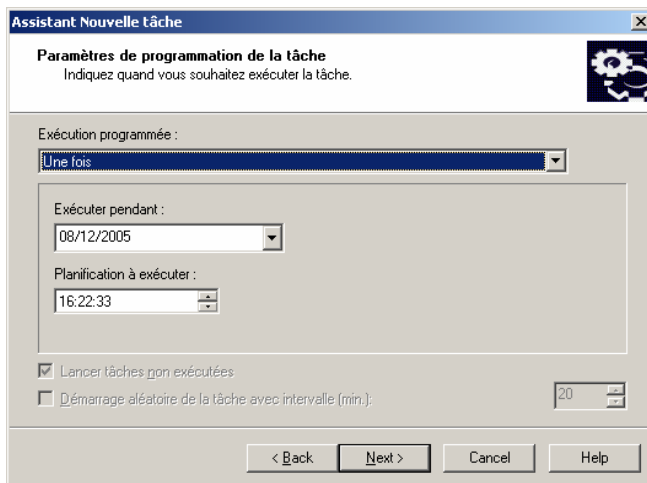


Figure 84. Programmation d'une tâche exécutée une seule fois

Si vous définissez le démarrage de la tâche **Manuellement** (Figure 85), **Au lancement de l'application** ou immédiatement après la création de la tâche, définissez l'intervalle de lancement aléatoire de la tâche sur les postes clients (voir ci-dessus).

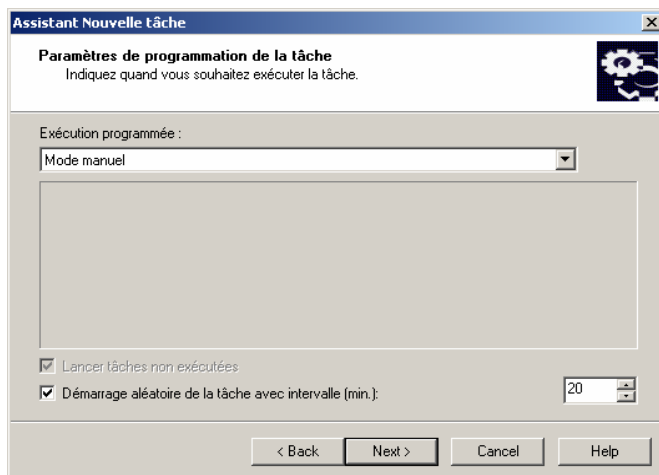


Figure 85. Configuration du démarrage manuel d'une tâche

Après la fin de l'Assistant, la tâche que vous venez de créer sera ajoutée aux dossiers **Tâches** des groupes et sous-groupes correspondants, et affichée dans le panneau de détails. Au besoin, vous pouvez configurer des paramètres de tâche (voir section 7.4 à la page 120).

7.2. Création d'une tâche globale



Pour créer une tâche globale :

Dans l'arborescence de console, sélectionnez l'entrée **Tâches** et cliquez sur **Nouveau/Tâche** dans le menu contextuel ou dans le menu **Action** afin de démarrer un nouvel Assistant de tâche.

Cet Assistant est semblable à celui utilisé pour la création de tâches de groupe. Une étape supplémentaire intervient si, pour créer une tâche, vous devez sélectionner des clients à partir du réseau logique (Figure 86).

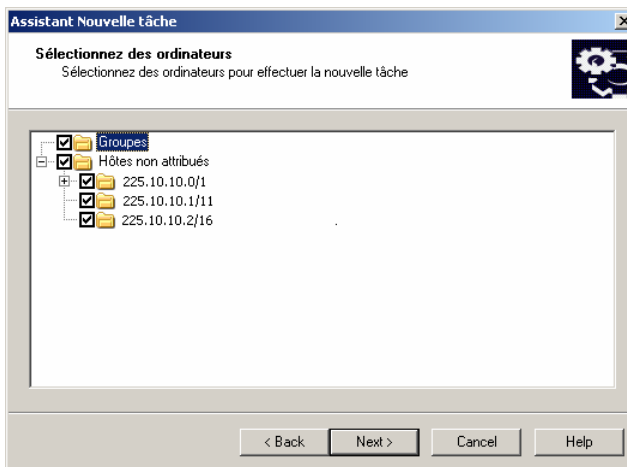


Figure 86. Création d'une tâche globale.
Sélection des clients sur lesquels cette tâche va être exécutée

Sélectionnez les clients du réseau logique pour lesquels vous voulez créer la tâche. Vous pouvez choisir les ordinateurs de différents dossiers,

ou tous les ordinateurs du dossier courant (voir section 5.3 à la page 69).



Les tâches globales ne seront exécutées que sur les clients indiqués. Si de nouveaux postes clients sont ajoutés au groupe sélectionné, la tâche ne sera pas exécutée sur ceux-ci. Vous devez créer une nouvelle tâche ou modifier de manière appropriée les paramètres courants de tâche.

Après la fin de l'Assistant, la tâche globale sera ajoutée à l'entrée **Tâches** dans l'arborescence de console et affichée dans le panneau de détails. Les tâches globales permettent d'effectuer toutes les opérations disponibles pour des tâches de groupe.

7.3. Création d'une tâche locale



Pour créer une tâche locale pour un poste client :

1. Dans le dossier **Groupes**, sélectionnez un groupe contenant le poste client cibles. Dans le panneau de détails, sélectionnez le client dont vous souhaitez modifier les paramètres d'application et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. La boîte de dialogue **Propriétés de <Nom de poste>** s'affiche ensuite dans la fenêtre principale de l'application (Figure 18).
2. Reportez-vous à l'onglet **Tâches** (voir Figure 87). L'onglet affiche toutes les tâches créées pour ce client. Pour créer une nouvelle tâche locale, cliquez sur **Ajouter**. Pour configurer des paramètres de tâche, cliquez sur **Propriétés**.

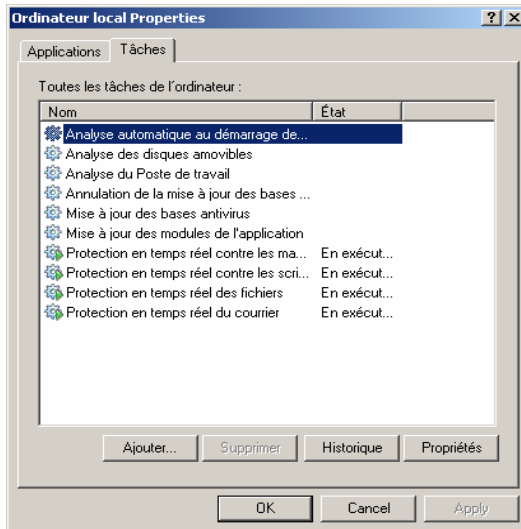


Figure 87. Création d'une tâche locale. L'onglet **Tâches**

Pour plus d'informations sur la création et la configuration d'une tâche locale, reportez-vous à la documentation des applications correspondantes.

7.4. Affichage et modification des paramètres de tâche



Pour afficher et/ou modifier les paramètres de tâche :

- Si vous souhaitez créer ou modifier une tâche de groupe, sélectionnez un groupe cible dans l'arborescence de console puis le dossier **Tâches de groupe** dans ce groupe. Le panneau de détails affiche toutes les tâches attribuées à ce groupe. Sélectionnez la tâche souhaitée et choisissez **Propriétés** dans le menu contextuel (ou dans le menu **Action**).
- Pour modifier les propriétés globales de tâche, sélectionnez l'entrée **Tâches globales** dans l'arborescence de console puis sélectionnez une tâche cible dans le panneau de détails. Cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.

Cela entraînera l'ouverture de la fenêtre **Propriétés de <Nom de la tâche>** avec les onglets suivants : **Général**, **Paramètres**, **Compte**, **Planification**, et **Notification**. La boîte de dialogue des propriétés de tâche globale possède également un onglet **Ordinateurs cibles**.



La boîte de dialogue **Propriétés de <Nom de tâche>** affiche les paramètres par défaut pour ce type, ou la dernière modification des paramètres. Les paramètres de stratégie de groupe des tâches globales ne sont pas affichés.

Vous pouvez afficher les paramètres réels de cette tâche dans la boîte de dialogue **Propriétés de <Nom de poste>** de l'onglet **Tâches** (Figure 87).

L'onglet **Général** (voir Figure 88) affiche des informations générales à propos de la tâche :

- Nom de tâche (vous pouvez le modifier si nécessaire)
- Nom de l'application (par exemple, la tâche a été créée pour Kaspersky Antivirus 5.0 pour Windows Workstations)
- Version de l'application
- Type de tâche
- Le nom du groupe utilisé pour la création de la tâche (le champ est vide dans le cas de tâches globales)
- Date et heure de création
- Dernière commande utilisée manuellement (**Démarrer**, **Stopper**, **Pause**, **Continuer**).

Dans la partie inférieure de l'onglet figurent des informations sur la progression de la tâche sur les postes clients du groupe (si une tâche globale a été définie pour ces ordinateurs). Pour afficher les détails d'exécution de la tâche, cliquez sur **Historique** (voir section 7.8 à la page 131).

Sur cet onglet, les boutons suivants vous permettent de contrôler la tâche manuellement : **Démarrer**, **Stopper**, **Pause** et **Continuer**.

Vous pouvez retirer temporairement la tâche de la liste de tâches programmées. Pour cela, annulez la case **Activé (la tâche est lancée aux heures planifiées)**. Bien que la tâche ne soit pas supprimée, elle ne sera pas non plus lancée à moins de cocher la case **Activé (la tâche est lancée aux heures planifiées)**.

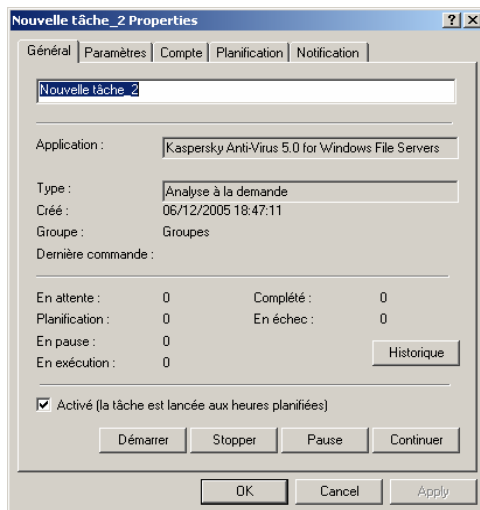


Figure 88. Modification des paramètres de tâche. L'onglet **Général**

L'onglet **Paramètres** (voir Figure 89) affiche les paramètres de tâche spécifiques de chaque application. Pour plus d'informations sur cet onglet, reportez-vous à la documentation correspondante.

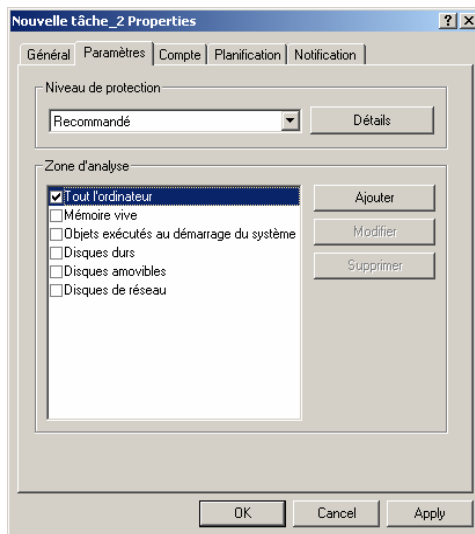


Figure 89. Modification des paramètres de tâche. Onglet **Paramètres**

Dans l'onglet **Compte** (voir Figure 90), vous pouvez spécifier un compte sous lequel la tâche sera exécutée :

- **Compte par défaut.** La tâche s'exécutera sous le compte de l'application qui l'aura prise en charge.
- **Compte spécifié.** Si vous sélectionnez cette option, spécifiez le compte (utilisateur et mot de passe) avec des privilèges appropriés. Par exemple, dans le cas d'une analyse à la demande, le compte doit avoir des privilèges d'accès sur l'objet analysé ; dans le cas des tâches de mise à jour, le compte doit avoir accès au dossier partagé sur le serveur d'administration, ou être autorisé sur le serveur proxy.

Ceci permet d'éviter des problèmes pendant l'analyse à la demande et pendant les tâches de mise à jour, lorsque l'utilisateur ne possède pas les privilèges requis pour effectuer cette tâche.

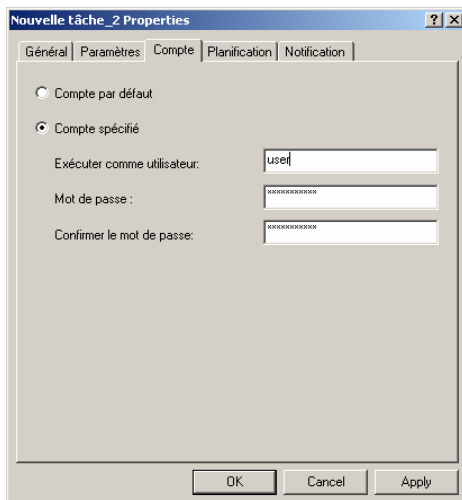


Figure 90. Modification des paramètres de tâche. L'onglet **Compte**

Sur l'onglet **Planification** (voir Figure 91) vous pouvez modifier les options de planification de la tâche, configurer le démarrage automatique du système d'exploitation sur les postes désactivés lors du démarrage de la tâche, ou limiter la durée d'exécution de la tâche.

Le contenu et la logique de l'onglet Planification sont analogues à ceux utilisés pour la configuration des paramètres lors de la création de la tâche.

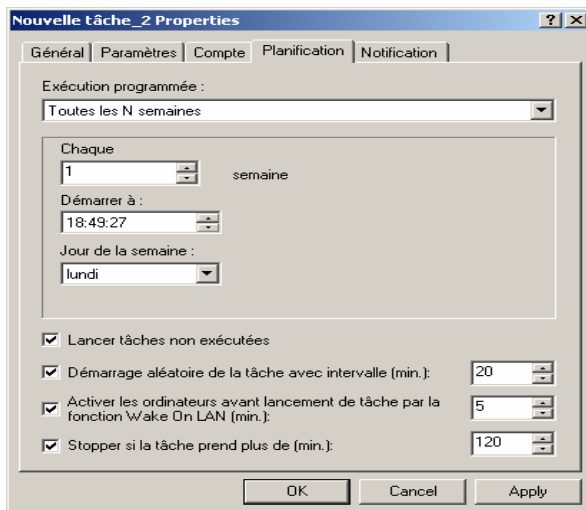


Figure 91. Modification des paramètres de tâche. L'onglet **Planification**

Sur l'onglet **Notification** (voir Figure 92), vous pouvez configurer l'envoi des notifications, avec les comptes-rendus d'activité des tâches.

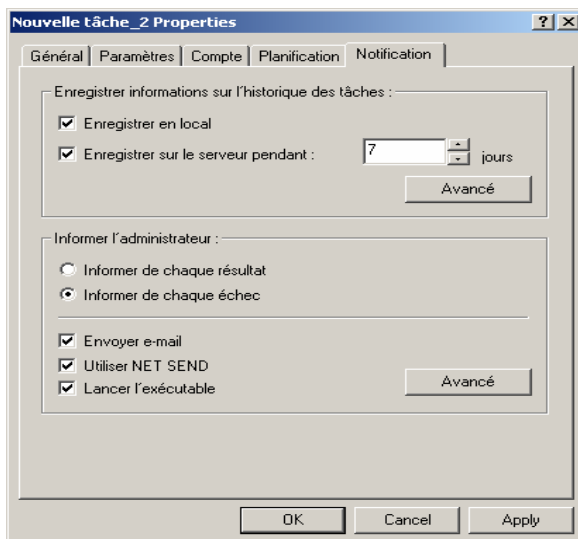


Figure 92. Modification des paramètres de tâche. L'onglet **Notification**

- Dans les zones **Enregistrer informations sur l'historique des tâches**, définissez les options d'enregistrement utilisées par l'historique des tâches :
 - Cochez la case **Enregistrer en local** pour stocker en local les informations sur chaque client.
 - Cochez l'option **Enregistrer sur le serveur pendant** pour stocker de manière centraliser l'historique des tâches envoyé par les clients au serveur d'administration. Dans la zone **jours**, indiquez la durée de stockage de l'historique des tâches sur le serveur. Après la fin de la période indiquée, l'information sera supprimée du serveur.

Pour enregistrer les événements associés aux tâches dans le journal des événements de **Windows**, cliquez sur **Avancé** pour ouvrir la boîte de dialogue **Enregistrement d'événements** (voir Figure 71), et procédez comme pour la définition des paramètres de notification sur l'onglet **Traitement des événements** (voir section 6.2 à la page 94):

- Dans le groupe **Informier l'administrateur**, indiquez le type de comptes-rendus de tâche que vous-même (ainsi que d'autres utilisateurs) voulez recevoir, et configurez en conséquence les paramètres de notification.
 - Cochez **Informier de chaque résultat** pour être informé de tous les événements d'exécution des tâches.
 - Vérifiez **Informier de chaque échec** pour être informé uniquement des erreurs.

Sélectionnez et configurez les paramètres de notification comme pour les notifications d'une stratégie sur l'onglet **Traitement des événements** (voir section 6.2 à la page 94). Les paramètres par défaut utilisés par le programme sont ceux du serveur d'administration (voir section 8.2 à la page 143).

La boîte de dialogue des propriétés de tâche globale possède l'onglet **Ordinateurs cibles** (voir Figure 93). Il contient la liste des clients du réseau logique sur lesquels la tâche sélectionnée est exploitée. Vous pouvez ajouter et enlever des clients de la liste.

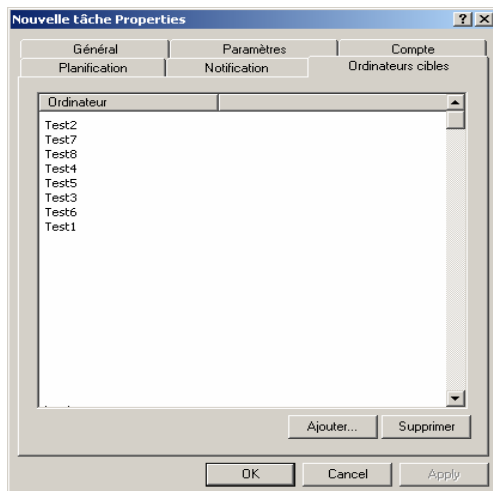


Figure 93. Modification des paramètres de tâche globale. L'onglet **Ordinateurs cibles**



Pour être sûr que la tâche est bien exécutée sur les postes qui se trouvaient éteints à l'heure d'exécution programmée,

dans l'onglet **Planification** de la boîte de dialogue de configuration de la tâche (voir Figure 91), cochez la case **Activer les ordinateurs avant lancement de tâche par la fonction Wake On LAN (min.)**. Ensuite, spécifiez l'heure souhaitée. Ceci a pour effet de démarrer le système d'exploitation sur ces postes, avant de lancer la tâche.



Pour limiter la durée d'exécution de la tâche,

dans l'onglet **Planification** de la boîte de dialogue de configuration de la tâche (voir Figure 91), cochez la case **Arrêter si la tâche dure plus de (min.)** et spécifiez une temporisation avant arrêt de la tâche.

7.5. Tâche de démarrage / d'arrêt de l'application



Pour démarrer ou arrêter l'application sur les postes clients,

créez une tâche de groupe, globale ou locale. Dans les paramètres de tâche, indiquez également ce qui suit :

- sélectionnez l'application **Agent réseau (Network Agent)** et le type de tâche **Démarrage /Arrêt d'application**.
- Dans la boîte de dialogue **Paramètres de tâche** (voir Figure 94), sélectionnez une ou plusieurs applications en cochant les cases correspondantes dans la liste. Sélectionnez l'une des options suivantes dans la liste déroulante de la partie inférieure de la fenêtre :
 - **Stopper l'application**
 - **Démarrer l'application**

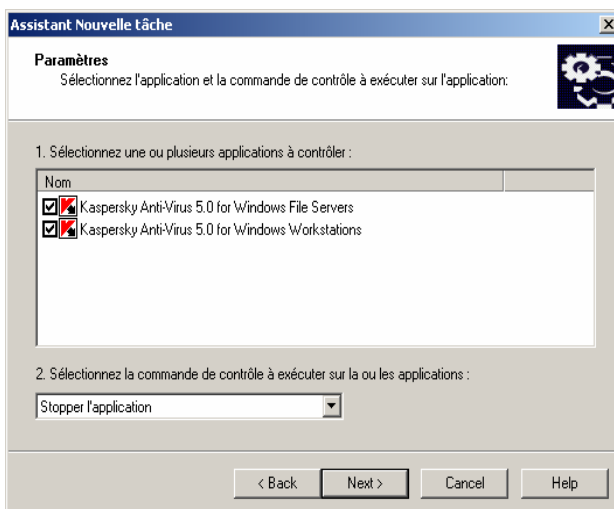


Figure 94. Tâche de démarrage / d'arrêt de l'application.
Paramètres de tâche

Pendant la modification des paramètres de la tâche de démarrage / arrêt de l'application, (voir Figure 95), vous pouvez modifier les paramètres précédents.

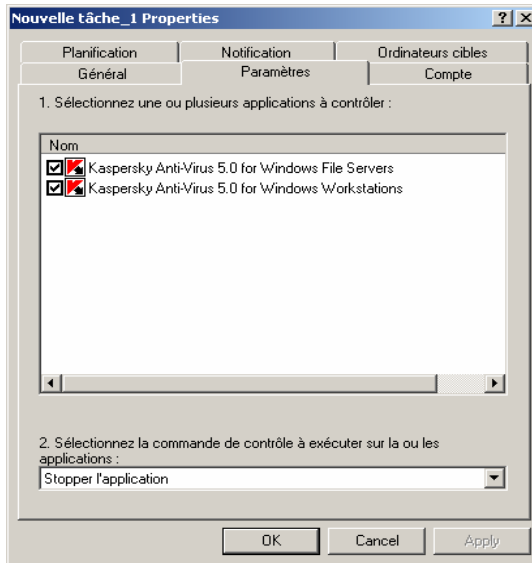


Figure 95. Modification de la tâche de démarrage / arrêt de l'application

7.6. Exportation et importation de tâches



Pour exporter une tâche du groupe d'administration dans un fichier :

Dans l'arborescence de console, choisissez la tâche requise et cliquez sur l'entrée **Tâches**. Le panneau de résultats affichera la liste de toutes les tâches créées pour ce groupe. Sélectionnez une tâche, ouvrez le menu contextuel et cliquez sur **Exporter**. La même commande est disponible sous le menu **Action**.

Dans la fenêtre ouverte, spécifiez le nom de fichier et l'emplacement sous lequel vous allez enregistrer la tâche. Cliquez sur **Enregistrer**.



Pour importer une tâche depuis un fichier :

Dans l'arborescence de console, choisissez le groupe requis. Ouvrez le menu contextuel du dossier **Tâches** puis cliquez sur **Importer**. La même commande est disponible sous le menu **Action**

Dans la fenêtre ouverte, spécifiez le nom de fichier d'importation de la tâche puis cliquez sur **Open**.

7.7. Démarrage et arrêt des tâches



Pour démarrer/stopper manuellement une tâche :

Dans le panneau de détails, sélectionnez la tâche cible (globale ou de groupe) et ouvrez le menu contextuel. Cliquez sur **Démarrer / Stopper** dans le menu contextuel ou dans le menu **Action**.



Pour suspendre / continuer une tâche en cours :

Dans le panneau de détails, sélectionnez la tâche cible (globale ou de groupe) et ouvrez le menu contextuel. Cliquez sur **Suspendre / Continuer** dans le menu contextuel ou dans le menu **Action**.

Pour effectuer ces opérations, cliquez sur **Démarrer**, **Stopper**, **Pause** ou **Continuer** (voir section 7.4 à la page 120) dans l'onglet **Général** de la boîte de dialogue de propriétés de la tâche.



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

7.8. Suivi et affichage des comptes-rendus d'activité des tâches



Pour lancer la surveillance des performances de tâche :

ouvrez la fenêtre de configuration de la tâche souhaitée (voir 7.4 à la page 120) et basculez sur l'onglet **Général** (voir Figure 88). Les informations suivantes seront affichées dans la partie inférieure de l'onglet :

- **En attente**- Nombre d'ordinateurs pour lesquels les paramètres de tâche ont été modifiés sur le serveur, sans que les modifications ne soient encore synchronisées avec le client.
- **Planification** – Nombre d'ordinateurs pour lesquels cette tâche est planifiée et synchronisée avec le serveur d'administration.
- **En pause** – Nombre d'ordinateurs sur lesquels cette tâche est suspendue.
- **En exécution** – Nombre d'ordinateurs sur lesquels cette tâche fonctionne.
- **Complétés** – Nombre d'ordinateurs sur lesquels cette tâche s'est terminée avec succès.
- **En échec** – Nombre d'ordinateurs sur lesquels la tâche a échoué.

Des informations similaires sur des tâches en particulier sont affichées dans la fenêtre principale du programme, quand vous affichez les propriétés des tâches de groupe ou des tâches globales.



Pour afficher les résultats d'activité des tâches entreposés sur le serveur d'administration :

Ouvrez la boîte de dialogue **Propriétés de <Nom de tâche>** pour la tâche souhaitée (voir section 7.4 à la page 120), sélectionnez l'onglet **Général** (voir Figure 88), et cliquez sur **Résultats**.

Ceci ouvrira la boîte de dialogue des résultats d'activité de la tâche (voir Figure 96). La partie gauche de la boîte de dialogue contient la liste de tous les postes clients pour lesquels la tâche est définie. La partie droite présente les résultats de l'exécution des tâches sur le poste client sélectionné.

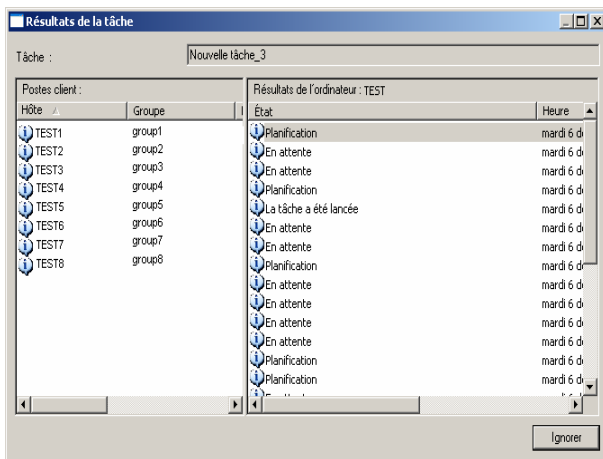


Figure 96. Affichage de l'historique des tâches entreposé sur le serveur d'administration

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

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



Pour afficher l'historique des tâches entreposé sur l'ordinateur local :

1. Exécutez la console d'administration sur le poste client.
2. Sélectionnez l'entrée **Ordinateur local** dans l'arborescence de console et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.
3. Dans la boîte de dialogue **Propriétés de Ordinateur local** reportez-vous à l'onglet **Tâches** (voir Figure 97). Sélectionnez la tâche dont vous souhaitez afficher les détails et cliquez sur **Résultats**.

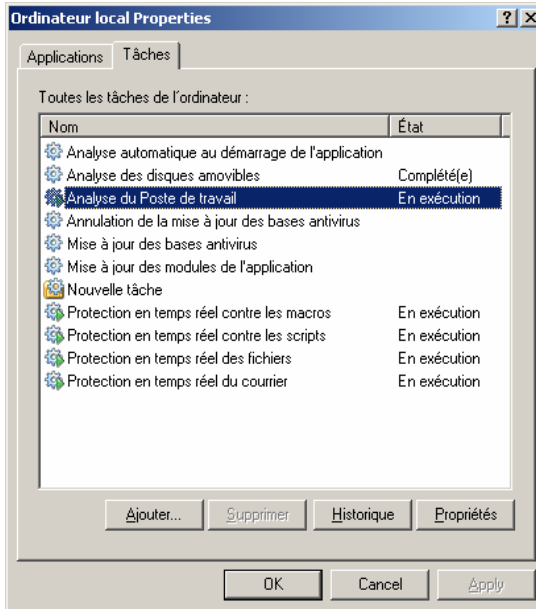


Figure 97. La boîte de dialogue **Propriétés de Ordinateur local**. L'onglet **Tâches**

La boîte de dialogue **Résultats de la tâche** (voir Figure 98) affiche les résultats d'exécution de la tâche sélectionnée, enregistrés pour ce poste, avec des indication sur l'heure exacte et des descriptions complémentaires.



La progression de la tâche (sauf pour les tâches de protection en temps réel) est affichée sous forme de pourcentage dans la colonne **État** de l'onglet **Tâches** (voir Figure 97).

Pour simplifier l'affichage et la recherche des informations nécessaires, la solution offerte est de configurer des filtres personnalisés. L'utilisation de filtres permet d'effectuer des recherches et de filtrer les informations non nécessaires et qui, sans l'application de filtres, gêneraient la consultation ; seules les informations qui satisfont les critères du filtre deviennent ainsi disponibles. Ceci devient vite indispensable quand les informations conservées dans le serveur d'administration atteignent un grand volume.

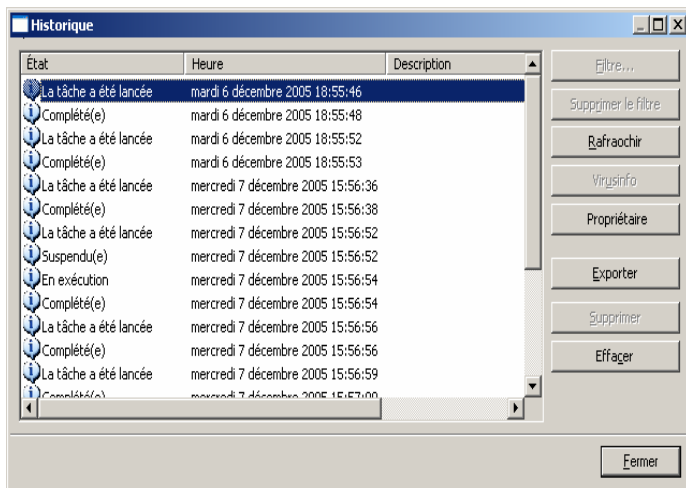


Figure 98. Affichage des résultats d'exécution de la tâche pour un ordinateur spécifique



Pour configurer le filtre d'affichage des informations dans la fenêtre Résultats de la tâche

1. Cliquez sur **Filtre** ou sur son équivalent dans le menu contextuel. Ceci permet d'ouvrir la boîte de dialogue de configuration des filtres (voir Figure 99). Configurez les paramètres du filtre.
2. Dans l'onglet **Événements** (voir figure 102) sélectionnez les types d'événements et de résultats d'exécution de la tâche qui seront affichés après application du filtre.
 - Spécifiez le type d'événements dans le groupe de champs **Types d'événements** :
 - Sélectionnez le niveau de gravité de la tâche dans la liste déroulante :



Certains types d'événements définis pour chaque application peuvent se produire pendant le fonctionnement de cette application. Chaque événement peut avoir une caractéristique qui reflète son niveau d'importance. Des événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

- Pour s'assurer que le filtre contient des événements d'un certain type seulement, cochez la case **Événements** et sélectionnez le type requis dans la liste déroulante. Si le type d'événement n'est pas spécifié, tous les types seront reproduits.
- Si vous souhaitez afficher les résultats d'exécution de la tâche, cochez la case **Résultats de la tâche** et sélectionnez l'état de la tâche que vous souhaitez examiner.
- Cochez la case **Afficher uniquement les derniers résultats de la tâche** si vous souhaitez afficher uniquement des informations sur les résultats de la dernière exécution de la tâche.
- Si vous souhaitez limiter la quantité d'informations affichées après application du filtre, cochez la case **Réduire le nombre d'événements affichés** et spécifiez le nombre de lignes maximum du tableau.

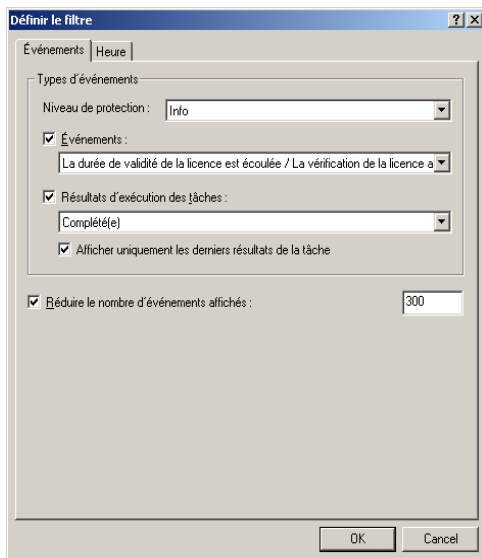


Figure 99.. Configuration du filtre d'événements
L'onglet **Événements**

3. Spécifiez l'heure d'enregistrement des événements et des résultats d'exécution de la tâche dans l'onglet **Heure** (voir Figure 100).

Vous pouvez sélectionner les options suivantes :

- **Pendant une période de** et spécifiez le début et la fin de la période couverte. Pour ce faire, sélectionnez les zones **Événements de la date** dans les zones **Depuis** et **Jusqu'à** et indiquez la date et l'heure exactes. Si toutes les informations enregistrées sont nécessaires, sélectionnez **Premier événement** et **Dernier événement**.
- **Pendant les derniers jours** et précisez le nombre de jours.

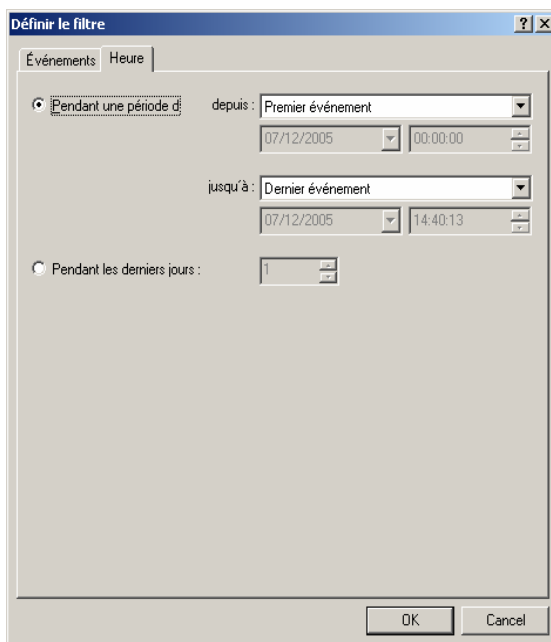


Figure 100. Configuration du filtre d'événements.
L'onglet **Heure**

3. Quand vous aurez terminé la configuration du filtre, cliquez sur **Ok**. Après cela, seules les informations qui vérifient les paramètres indiqués seront affichées dans la fenêtre **Résultats de la tâche**.



Pour supprimer le filtre,

cliquez sur **Supprimer le filtre** ou sur son équivalent dans le menu contextuel.

7.9. Déploiement de tâches de groupe sur des serveurs d'administration secondaires

Les résultats du déploiement de tâches sur les serveurs d'administration secondaires sont affichés sur la fenêtre **Historique** (voir Figure 96) dans la fenêtre de propriétés de la tâche de groupe du serveur d'administration secondaire.

CHAPITRE 8. CONTROLE DES PARAMETRES D'APPLICATION

8.1. Affichage des paramètres d'application



Pour afficher et configurer les paramètres d'application :

1. Sélectionnez dans le dossier **Groupes** un groupe contenant le poste client souhaité. Dans le panneau de détails, choisissez l'ordinateur sur lequel l'application cible est installée. Cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.
2. La boîte de dialogue **Propriétés de <Nom de poste>** contenant plusieurs onglets est affichée dans le programme principal. Reportez-vous à l'onglet **Applications** (voir Figure 101). Cet onglet énumère toutes les applications Kaspersky Lab installées sur le poste client et affiche des informations d'ordre général à leur sujet. Si le poste client est un poste administrateur et/ou un serveur d'administration, la liste inclut les composants de Kaspersky Administration Kit (Network Agent et/ou Administration Server).

Sélectionnez l'application cible. Vous pouvez :

- Afficher la liste des événements d'application qui se sont produits sur le client et qui ont été enregistrés par le serveur d'administration : cliquez sur **Événements** (voir section 11.1 à la page 164).
- Afficher les statistiques courantes sur l'exécution de l'application : cliquez sur **Statistiques**. Le serveur d'administration effectue une requête au client pour obtenir cette information. En cas d'échec de connexion, un message d'erreur approprié est affiché.
- Afficher des informations générales sur une application et configurer les paramètres d'application : cliquez sur **Propriétés**

dans la boîte de dialogue **Propriétés de l'application** "<Application>" (voir Figure 102).

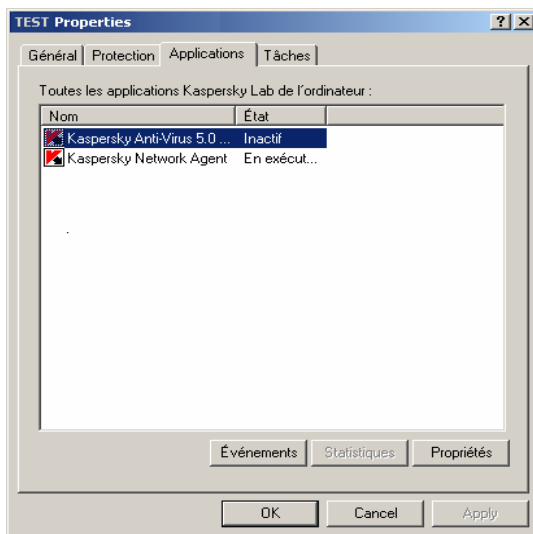


Figure 101. Boîte de dialogue de propriétés du client.
L'onglet **Applications**

La boîte de dialogue contient plusieurs onglets. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation client/serveur. Les onglets sont spécifiques à chaque application. Pour plus d'informations sur les onglets, reportez-vous à la documentation correspondante de l'application. Les onglets **Général**, **Licences** et **Traitement des événements** sont communs à toutes les applications.

Sur l'onglet **Général** (voir Figure 102), vous pouvez afficher des informations générales sur l'application, la démarrer ou la stopper, afficher les paramètres du plug-in correspondant dans le poste administrateur en cliquant sur **Infos Plug-in...**(voir Figure 106).

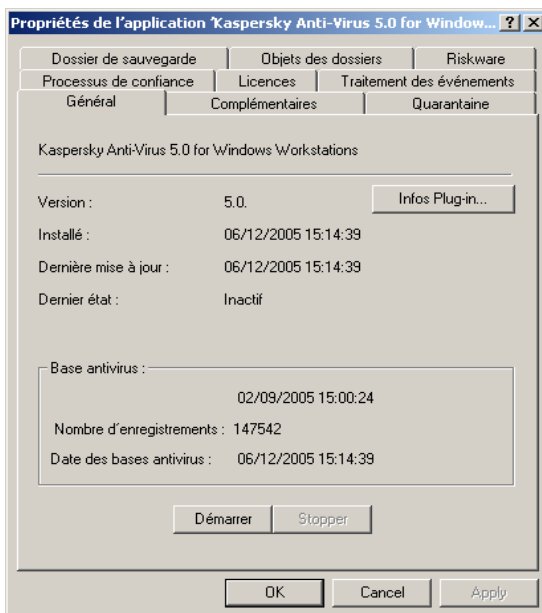


Figure 102. Boîte de dialogue Propriétés d'application.
L'onglet **Général**

L'onglet **Licences** permet d'afficher des détails sur les clefs de licence actuelle et de réserve installée sur un poste client.

Dans la zone **Clé de licence courante**, vous pouvez afficher les données de la clé de licence courante :

- **Numéro de série**
- **Type** – Type de la clé installée (par exemple, commerciale ou d'essai)
- **Date d'activation** – Date d'activation de la clé
- **Date d'expiration** – Date d'expiration de la licence
- **Période de licence** – Période de validité de la licence
- **Limite compteur d'ordinateurs** – Nombre maximum d'ordinateurs sur lesquels il est possible d'installer cette clé de licence.

La zone **Clé de licence de réserve** affiche les données de la clé de licence de réserve :

- **Numéro de série** – Numéro de série
- **Type** – Type de la clef installée (par exemple, commerciale ou d'essai)
- **Durée de validité** – Période de validité de la licence
- **Limite compteur d'ordinateurs** – Nombre maximum d'ordinateurs sur lesquels il est possible d'installer cette clef de licence.

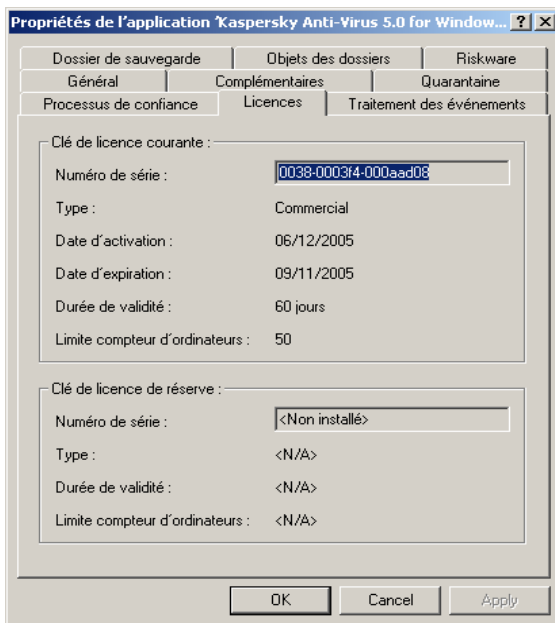


Figure 103. Boîte de dialogue Propriétés d'application.
L'onglet **Licences**

L'onglet **Traitement des événements** (voir Figure 104) affiche des règles de manipulation des événements qui se sont produits sur un poste client. Vous pouvez les afficher et faire les changements nécessaires. Cet onglet est identique à l'onglet **Traitement des événements** de la boîte de dialogue **Propriétés de <Stratégie>** (voir section 6.2 à la page 94).

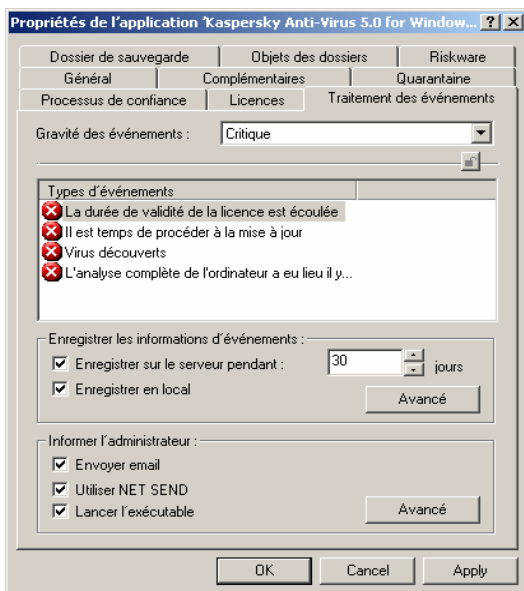


Figure 104. Boîte de dialogue Propriétés d'application.
L'onglet **Traitement des événements**

8.2. Paramètres du serveur d'administration



Pour afficher les paramètres du serveur d'administration :

Sélectionnez l'entrée **Kaspersky Administration Server (<Nom du serveur>)** dans l'arborescence de console, qui correspond au serveur d'administration requis, et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. Ceci ouvrira la boîte de dialogue **Propriétés de Kaspersky Administration Server (<Nom du serveur>)** contenant les onglets **Général**, **Paramètres**, **Traitement des événements**, **Notification**, **Attaques de virus** et **Sécurité**.

L'onglet **Général** (voir Figure 106) affiche le nom et le numéro de version du composant serveur d'administration, ainsi que le nom de l'ordinateur dans le réseau Windows sur lequel ce composant est installé.

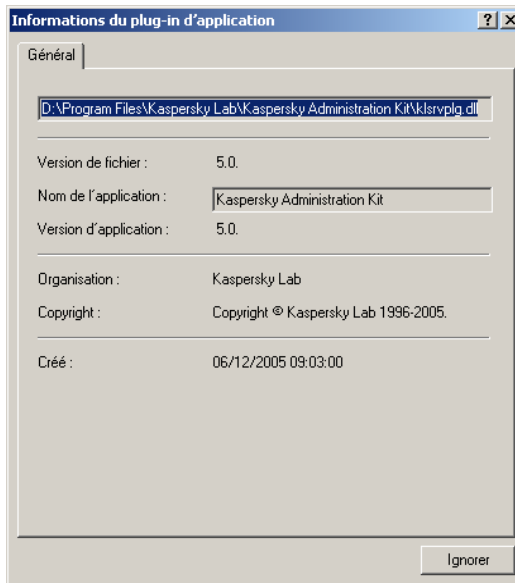


Figure 105. Affichage des propriétés du plug-in d'application.
Informations du plug-in d'application du serveur d'administration

Cet onglet possède également un onglet **Statistiques** pour examiner des statistiques générales sur le serveur d'administration sélectionné, et un bouton **Infos Plug-in...** qui ouvre la boîte de dialogue **Informations du plug-in** du serveur d'administration (voir Figure 105). L'information suivante est affichée sur le plug-in :

- Chemin d'accès complet au plug-in
- Version de fichier
- Nom de l'application qui inclut ce plug-in (**Kaspersky Administration Kit**)
- Version de l'application
- Informations sur le fabricant (**Kaspersky Lab**) et sur le copyright
- Date et heure de création du plug-in.

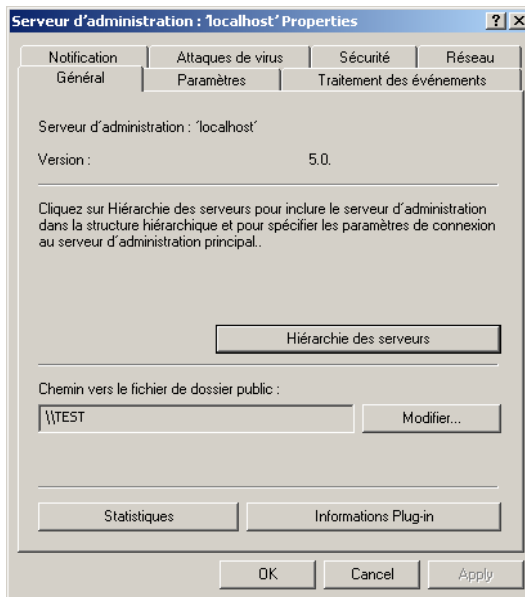


Figure 106. Affichage des propriétés du serveur d'administration.
L'onglet **Général**

L'onglet inclut également un bouton **Hiérarchie du serveur...** qui ouvre la boîte de dialogue de modification des propriétés du serveur secondaire sélectionné (voir Figure 107). Dans cette boîte de dialogue, vous pouvez :

- Spécifier si ce serveur d'administration est un serveur secondaire
- Spécifier l'adresse et le port du serveur d'administration primaire
- Spécifier ou modifier le chemin d'accès au certificat du serveur d'administration primaire
- Définir les paramètres du serveur proxy pour se connecter au serveur d'administration primaire (si nécessaires)

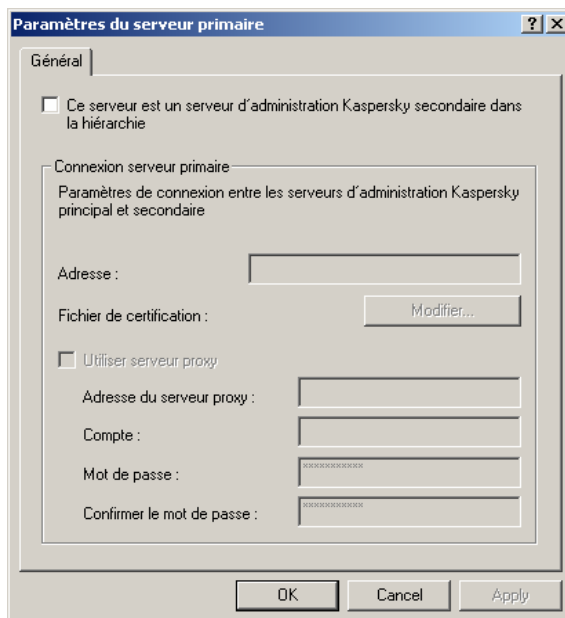


Figure 107. Propriétés d'un serveur d'administration secondaire

L'onglet **Paramètres** (voir Figure 108) affiche les propriétés du serveur d'administration. Le groupe **Emplacement du serveur** possède les zones suivantes :

- **Port du serveur** – Numéro de port utilisé pour se connecter au serveur d'administration. Le numéro de port par défaut est 14000. Si ce port est déjà en service, vous pouvez en changer.
- **Port SSL du serveur** – Affiche le numéro de port SSL utilisé pour établir une connexion sécurisée avec le serveur d'administration. Le port par défaut est **13000**.

La notation décimale doit être utilisée.

La section **Actualisation des informations réseau** inclut les paramètres suivants, destinés au rafraîchissement des informations sur la structure de réseau Windows par le serveur d'administration :

- **Intervalle d'exploration du réseau (min)** – Intervalle utilisé dans le réseau Windows pour identifier les nouveaux ordinateurs qui se connectent ou les ordinateurs qui se déconnectent (en minutes).

- **Intervalle d'interrogation du domaine (min)** – Intervalle de sondage du domaine réseau Windows, sur les ordinateurs existants (en minutes).

Dans le champ **Nombre maximum d'événements stockés dans la base**, indiquez le nombre maximum d'événements stockés dans la base du serveur d'administration.

Vous pouvez modifier si nécessaire ces paramètres.

The image shows a Windows-style dialog box titled "Serveur d'administration : 'localhost' Properties". It has four tabs: "Notification", "Attaques de virus", "Sécurité", and "Réseau". The "Paramètres" tab is selected. Inside, there are three main sections. The first, "Emplacement du serveur", contains two text boxes: "Port du serveur :" with the value "14000" and "Port SSL du serveur :" with the value "13000". The second section, "Actualisation des informations réseau", contains two text boxes: "Intervalle d'exploration du réseau (min)" with the value "5" and "Intervalle d'interrogation du domaine (min)" with the value "30". The third section, "Nombre maximum d'événements stockés dans la base", has a text box with the value "400000". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".


Figure 108. Affichage des propriétés du serveur d'administration.
L'onglet **Paramètres**

L'onglet **Traitement des événements** (voir Figure 109) affiche des règles pour manipuler des événements par le serveur d'administration. Cet onglet est identique à l'onglet **Traitement des événements** de la boîte de dialogue de propriétés de la stratégie du groupe (voir section 6.2 à la page 94).

Les événements serveur sont décrits plus en détail à la suite. Les événements du serveur d'administration, comme pour d'autres applications Kaspersky Lab contrôlées par Kaspersky Administration Kit, peuvent être rangés dans l'un des quatre degrés de gravité : **Critique**, **Erreur**, **Avertissement** et **Info**.

La liste suivante affiche des événements inclus dans chaque niveau de gravité :

- **Événements critiques :**
 - **Le nombre d'ordinateurs autorisés pour la clé a été dépassé** – Nombre excessif de licences pour la clé.
 - **Attaque virale !** – L'activité virale dépasse la limite prédéfinie.



La réponse du serveur d'administration à l'événement **Attaque virale !** est extrêmement importante, plus spécialement en cas d'inflation du nombre virus et d'augmentation des risques d'attaque.
 - **L'hôte est hors-service** – Impossible d'établir une connexion avec l'agent réseau installé sur le poste client.
 - **L'hôte est en état critique** - Un poste avec une configuration en état « Critique » a été détecté sur le réseau.
- **Erreur :**
 - **Espace insuffisant sur l'unité de disque** – Il ne reste plus d'espace libre sur le disque utilisé par le serveur d'administration pour enregistrer ses données d'exploitation.
 - **Le dossier partagé n'est pas disponible** – Le dossier partagé de mise à jour des bases antivirus et des modules n'est pas disponible.
 - **La base de données du serveur d'administration est indisponible** – La base du serveur n'est pas accessible.
 - **La base de données du serveur d'administration est saturée** – Il n'y a plus d'espace disponible dans la base de données du serveur.
- **Avertissement :**
 - **Plus de 100%% du nombre autorisé d'ordinateurs pour la clé sont actifs** – Le nombre de licences pour cette clé est supérieur à 100%.
 - **La période d'inActivité du poste client dans le réseau a été trop longue** – Un ordinateur est resté longtemps invisible sur le réseau Windows.

- **Conflit de noms d'hôtes** – L'exclusivité des noms de clients à l'intérieur d'un niveau de hiérarchie a été violée.
- **Volumes presque saturés** – Trop peu d'espace libre est resté sur les disques durs.
- **La base de données de Administration Server est presque saturée** – Trop peu d'espace reste libre dans la base de données du serveur d'administration.
- **L'hôte est peut-être hors-service** - La connexion avec l'agent réseau installé sur le poste client est peut-être perdue.
- **L'hôte est en état d'avertissement** - Un poste avec une configuration en état « Avertissement » a été détecté sur le réseau.
- **Information :**
 - **Plus de 90%% du nombre autorisé d'ordinateurs pour la clé sont actifs** – Le nombre de licences pour cette clef est supérieur à 90%.
 - **Trouvé nouvel hôte** – Un nouveau client a été trouvé pendant l'exploration du réseau.
 - **L'hôte a été automatiquement ajouté au groupe** – Un nouveau client a été automatiquement inclus dans un groupe, conformément à la configuration sous l'entrée **Non attribué**.
 - **Cet ordinateur est resté inactif trop longtemps et a été retiré du groupe** – Un poste client n'a pas répondu pendant longtemps et a été enlevé du réseau logique.
 - La connexion avec un serveur secondaire est établie.
 - La connexion avec un serveur principal est établie.
 - Audit : Connexion au serveur d'administration.
 - Audit : Modification d'un objet.
 - Audit : Modification d'état d'un objet.
 - Audit : Modification des paramètres de groupe.

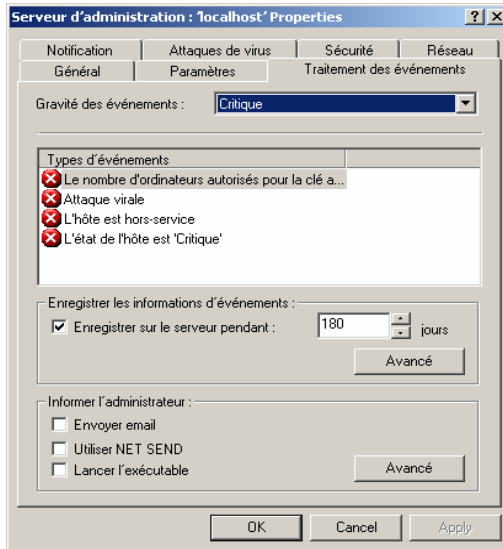


Figure 109. Affichage des propriétés du serveur d'administration.
L'onglet **Traitement des événements**

Sur l'onglet **Notification** (Figure 110), vous pouvez définir des paramètres pour informer l'administrateur, ainsi que d'autres utilisateurs, sur les événements envoyés au serveur d'administration par les applications antivirus. Ces paramètres sont employés par les stratégies d'application en tant que paramètres par défaut.

Pour minimiser l'impact sur l'exécution du serveur, limitez le nombre de notifications envoyées par le serveur d'administration. Pour fixer cette limite, cliquez sur **Limiter notifications...** et spécifiez ce qui suit (voir Figure 111):

- Nombre maximum des notifications envoyées par le serveur d'administration.
- Période de temps pendant lequel le serveur d'administration peut générer des notifications.

Ce sont les paramètres par défaut utilisés pour les applications de Kaspersky Lab.

Pour vérifier que les paramètres spécifiés sur cet onglet sont corrects, essayez d'envoyer un message de texte. Pour ce faire, cliquez sur **Test**.

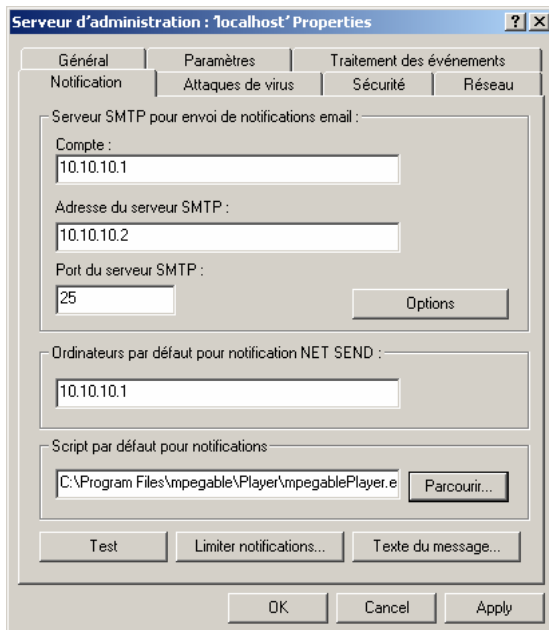


Figure 110. Affichage des propriétés du serveur d'administration.
L'onglet **Notification**

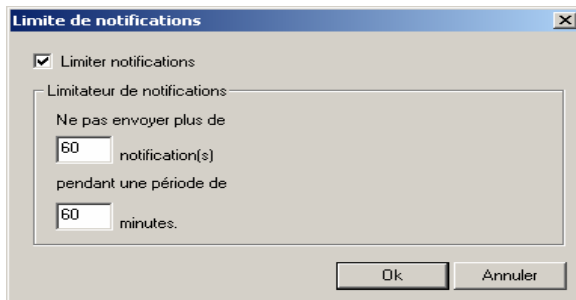


Figure 111. Limite au nombre de notifications

Sur l'onglet **Attaques de virus** (voir Figure 112), vous pouvez définir comme **Critères d'envoi d'événements en cas d'attaque virale**, le nombre maximum des virus détectés pendant un intervalle de temps spécifié. Si le nombre de virus détectés pendant une courte période dépasse cette limite, l'événement est identifié comme une **Attaque de**

virus. Ce paramètre permet à l'administrateur de préparer et de répondre à une attaque.

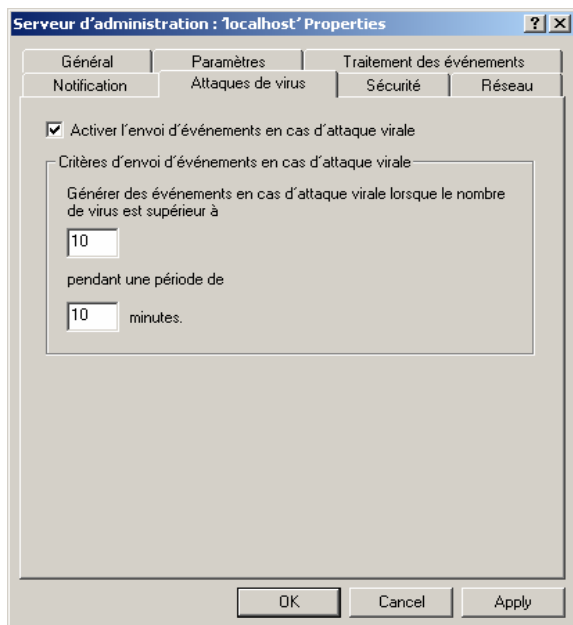


Figure 112. Affichage des propriétés du serveur d'administration.
L'onglet **Attaques de virus**

Cochez la case **Activer l'envoi d'événements en cas d'attaque virale** pour détecter l'activité des virus dans votre réseau logique. Dans le groupe **Critères d'envoi d'événements en cas d'attaque virale**, placez les paramètres suivants qui définissent le seuil d'activité de virus :

- Dans la zone supérieure, écrivez le nombre total de virus qu'il faut détecter sur tous les clients du réseau logique
- Dans la zone inférieure, indiquez la durée (en minutes) pendant laquelle ce nombre de virus doit être détecté.

L'onglet **Sécurité** (voir Figure 4) permet de configurer les droits d'accès au réseau logique du serveur d'administration logique.

8.3. Configuration de Network Agent

Lorsque vous configurez Network Agent, en plus des onglets **Général**, **Licences** et **Traitement des événements**, la boîte de dialogue **Propriétés de l'application "Kaspersky Lab Network Agent"** (voir Figure 113) possède un onglet **Paramètres**. Les options affichées sur cet onglet sont identiques à celles de l'onglet **Paramètres** de la boîte de dialogue paramètres de stratégie de Network Agent (voir section 6.3 à la page 104).

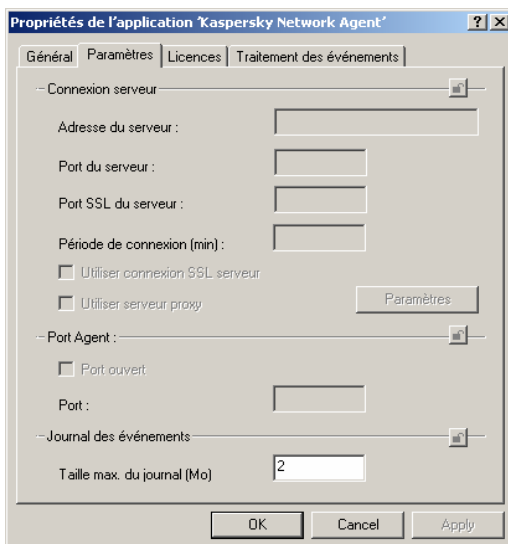


Figure 113. Boîte de dialogue de propriétés de l'agent réseau

CHAPITRE 9. MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES DE PROGRAMME

9.1. Création de la tâche de mise à jour

Le téléchargement des mises à jour à partir d'une seule source est une tâche globale (voir section 7.2 à la page 118). Pour créer la tâche de téléchargement des mises à jour, sélectionnez **Kaspersky Administration Kit** en tant qu'application cible de la tâche, et **Tâche de téléchargement des mises à jour** en tant que type de tâche (voir Figure 114).

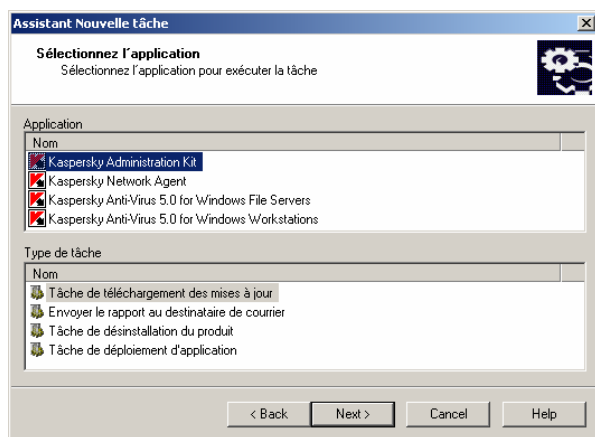


Figure 114. Création d'une tâche de mise à jour.
Choix de l'application et du type de tâche

C'est lors de l'étape de configuration des paramètres de tâche (voir Figure 115) que se crée la liste des sources de mise à jour. Vous pouvez configurer les paramètres de connexion avec les serveurs de mise à jour et déterminer si les tâches de réception des mises à jour par les serveurs d'administration

secondaires peuvent être démarrées automatiquement immédiatement, une fois reçues les mises à jour sur le serveur principal.

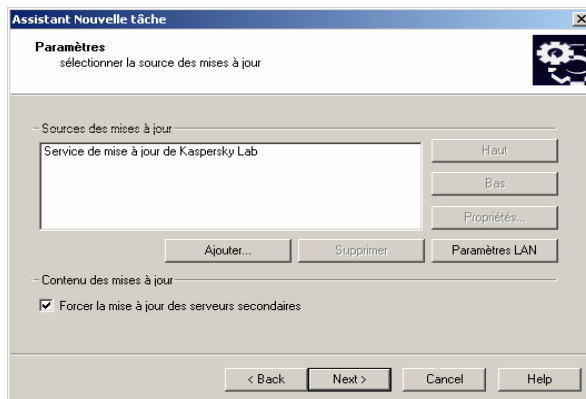


Figure 115. Création d'une tâche de mise à jour.
Configuration de la réception des mises à jour

Vous pouvez créer la liste des sources de mises à jour à l'aide des boutons **Ajouter** et **Supprimer**.

Pour ajouter une source de mises à jour à la liste, cliquez sur **Ajouter** et sélectionnez l'une des options suivantes dans la fenêtre **Propriétés de la source des mises à jour** ouverte (voir Figure 116):

- **Service de mise à jour de Kaspersky Lab** – pour la réception des mises à jour par Internet, en utilisant les serveurs FTP et HTTP Kaspersky. Vous pouvez modifier les paramètres du serveur proxy dans la boîte de dialogue de configuration de la tâche (voir Figure 118).

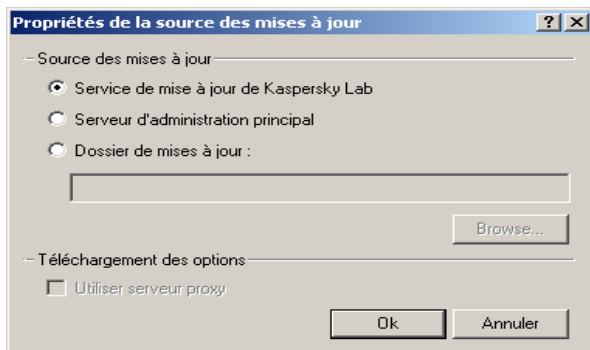


Figure 116. Configuration de la source des mises à jour

- **Serveur d'administration principal** – pour recevoir les mises à jour à partir du dossier public du serveur d'administration.
- **Dossier de mises à jour** – pour recevoir les mises à jour à partir d'un dossier réseau. Si vous choisissez cette option, spécifiez l'adresse du dossier contenant les mises à jour.

Pour configurer la connexion au serveur de mises à jour, cliquez sur **Paramètres LAN** et spécifiez les paramètres requis dans la fenêtre ouverte (voir Figure 117).

- Si la connexion au serveur de mises à jour se fait par un serveur proxy, cochez la case **Avec proxy** et indiquez l'adresse et le numéro de port utilisés pour la connexion. Seules les notations décimales sont permises (par exemple, **Adresse** 125.2.19.1, **Port**: 3128).
- Si l'accès au serveur proxy est protégé par mot de passe, spécifiez les paramètres d'authentification utilisateur du proxy. Pour ce faire, sélectionnez le type d'autorisation utilisé : NTLM ou Basic. Si vous choisissez le mode Basic, complétez les champs **Utilisateur** et **Mot de passe**.
- Cochez la case **Utiliser le mode FTP passif** pour forcer le mode passif lors des mises à jour en utilisant le protocole FTP., décochez-la pour utiliser le mode actif. Il est conseillé d'utiliser le mode passif.
- Dans la zone **Temporisation de connexion**, **sec** spécifiez le délai maximum de connexion au serveur de mises à jour. Si la connexion échoue, après un certain délai une nouvelle tentative est faite pour connecter au serveur de mises à jour suivant.

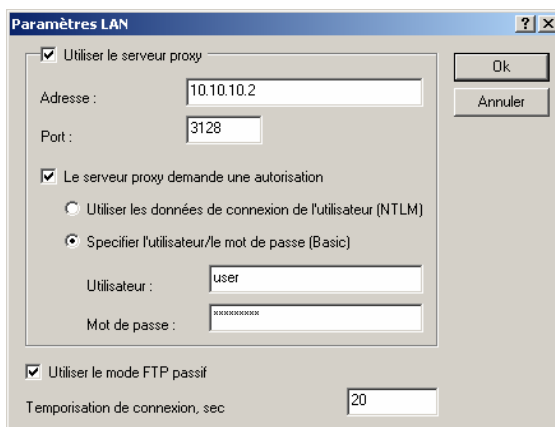


Figure 117. Configuration des paramètres utilisés pour se connecter au serveur de mises à jour

Pour vous assurer que les tâches de récupération des mises à jour par les serveurs d'administration sont lancées automatiquement après leur réception par le serveur d'administration principal, et sans tenir compte de la programmation prévue dans la configuration de ces tâches, cochez la case **Forcer la mise à jour des serveurs secondaires**.

9.2. Configuration de la tâche de mise à jour

L'onglet **Paramètres** permet de modifier la configuration de la tâche de mise à jour, en procédant comme ceci (voir Figure 118):

- Définissez le contenu des mises à jour à télécharger à partir d'une source de mise à jour dans le groupe de champs **Contenu des mises à jour**. Pour ce faire, sélectionnez l'une des options suivantes:
 - **Télécharger toutes les mises à jour disponibles**
 - **Télécharger uniquement les mises à jour sélectionnées**, pour recopier uniquement les mises à jour de bases antivirus et de modules d'applications sélectionnées. Dans ce cas, cochez les cases associées aux noms des application dont vous souhaitez télécharger les mises à jour.



Les mises à jour de la base antivirus et des modules de programme sont enregistrées dans le dossier partagé spécifié sur le Serveur d'administration.

- Gérez le démarrage automatique des tâches de récupération des mises à jour par les serveurs secondaires d'administration en cochant la case **Forcer la mise à jour des serveurs secondaires**;
- Affichez l'emplacement du dossier contenant les mises à jour récupérées depuis la source, dans la zone **Répertoire pour la source locale des mises à jour**.

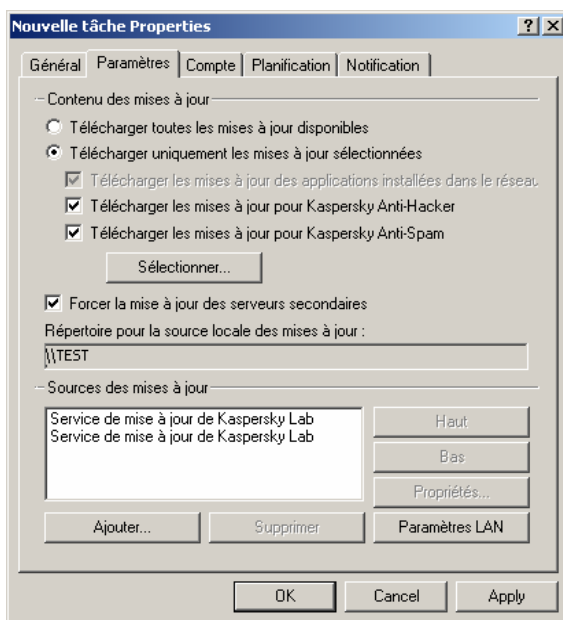


Figure 118. Configuration de la tâche de mise à jour.
L'onglet **Paramètres**

- Redéfinissez la méthode de récupération des mises à jour et les paramètres de connexion aux serveurs de mise à jour dans le groupe de champs **Source de mises à jour** (voir section 9.1 à la page 154).

9.3. Affichage de la liste de mise à jour

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



Pour afficher les propriétés de mise à jour :

Sélectionnez la mise à jour requise dans le panneau de détails et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. La boîte de dialogue **Propriétés de <Nom de mise à jour>** s'affiche (voir Figure 119).

L'onglet **Général** affiche les informations suivantes :

- Nom de l'application mise à jour ; dans le cas de la mise à jour d'une base antivirus, la valeur de cette zone est **Base antivirus**.
- Date de création de la base antivirus
- Taille de la mise à jour enregistrée sur le serveur d'administration
- Date où la mise à jour a été copiée vers le serveur d'administration

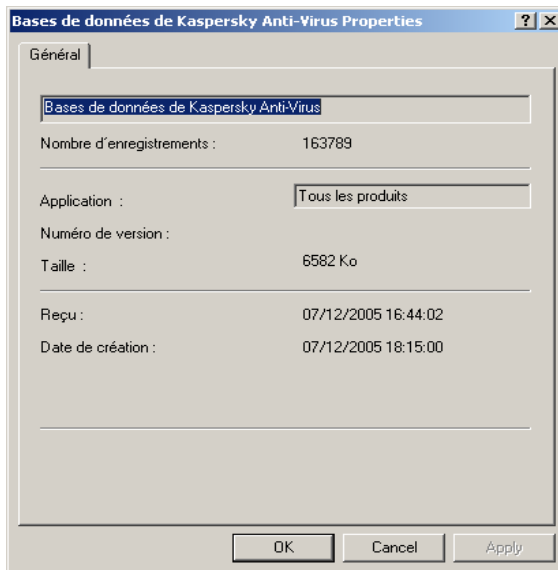


Figure 119. Affichage des propriétés des mises à jour téléchargées

9.4. Déploiement de mises à jour automatiques



Pour que le serveur puisse transférer les mises à jour vers les clients immédiatement après le téléchargement :

Sélectionnez l'entrée **Mises à jour** dans l'arborescence de console et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**. Dans la boîte de dialogue **Propriétés de Mises à jour** qui s'affiche à l'écran (voir Figure 120), cochez la case **Déploiement automatique de la base antivirus sur tous les clients**.

En fonction des paramètres courants de l'entrée **Mises à jour**, le serveur d'administration créera automatiquement des tâches de groupe pour le niveau hiérarchique supérieur (le groupe **Groupe**) applicables à toutes les applications KL installées sur les clients du réseau logique. Ces tâches sont affichées dans le dossier **Tâches** du groupe **Groupe**. Vous pouvez supprimer ces tâches uniquement si vous annulez la coche **Déploiement automatique de la base antivirus sur tous les clients**. Après avoir téléchargé les mises à jour depuis

Internet, le serveur d'administration exécutera les tâches correspondantes sur tous les clients. Vous pouvez modifier la configuration de la tâche de mise à jour automatique comme pour celle de toutes les autres tâches de mise à jour (voir section 9.2 à la page 157).

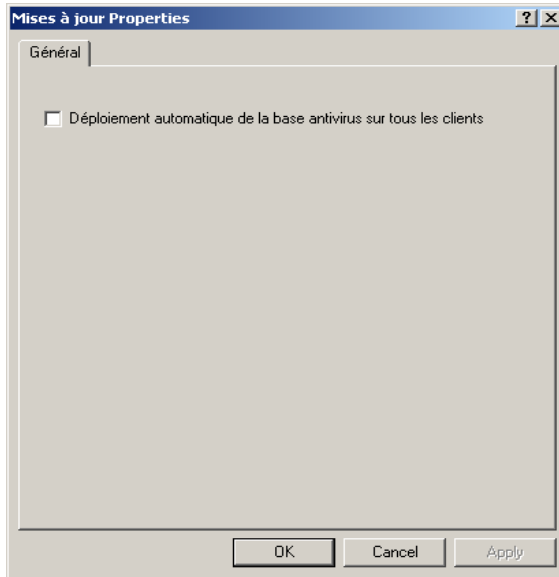


Figure 120. La boîte de dialogue **Propriétés de Mises à jour**



Pour vous assurer que les tâches de récupération des mises à jour par le serveur d'administration principal sont redistribuées automatiquement sur les serveurs secondaires immédiatement après leur réception,

dans les paramètres de la tâche de récupération des mises à jour par le serveur d'administration (voir Figure 115 et Figure 118) cochez la case **Forcer la mise à jour des serveurs secondaires**.

Immédiatement après la réception des mises à jour par le serveur d'administration principal, des tâches de récupération des mises à jours par les serveurs d'administration secondaires seront automatiquement lancées, indépendamment de la planification prévue dans la configuration de ces tâches.

CHAPITRE 10. OPERATIONS SUR LA QUARANTAINE



Pour afficher les propriétés d'un objet en quarantaine :

sélectionnez l'entrée **Quarantaine** dans l'arborescence de console, sélectionnez l'objet souhaité dans le panneau de résultats et utilisez la commande **Propriétés** dans le menu contextuel ou son équivalent dans le menu **Action**.

La fenêtre ouverte contiendra les informations suivantes sur l'objet :

- nom sous lequel l'objet avait été délivré pour son traitement par l'application antivirus ;
- description de l'objet,
- action réalisée sur l'objet par l'application antivirus ;
- nom du poste où l'objet est conservé ;
- état attribué à l'objet par l'application antivirus ;
- nom du virus présent ou soupçonné dans l'objet ;
- date de mise en quarantaine ;
- chemin d'accès au dossier de quarantaine où l'objet se trouve placé ;
- nom de l'utilisateur qui a mis l'objet en quarantaine ;

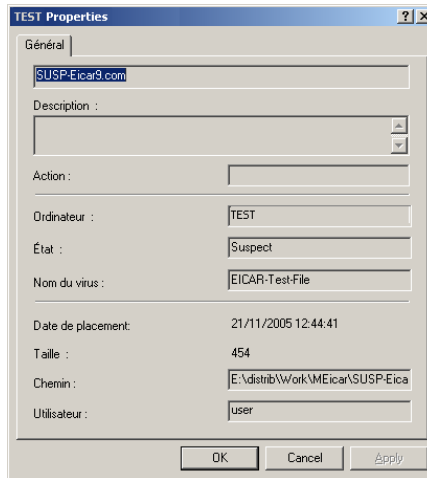


Figure 121. Affichage des propriétés d'un objet en quarantaine



Pour supprimer un objet de la quarantaine:

sélectionnez l'entrée **Quarantaine** dans l'arborescence de console, sélectionnez l'objet souhaité dans le panneau de résultats et utilisez la commande **Supprimer** dans le menu contextuel ou son équivalent dans le menu **Action**.

L'application antivirus qui avait mis cet objet en quarantaine sur le poste client supprimera l'objet de la quarantaine.



Pour analyser le dossier de quarantaine sur le poste client :

sélectionnez le poste **Quarantaine** dans l'arborescence de console, sélectionnez l'objet que vos souhaitez analyser dans le panneau de résultats et utilisez la commande **Analyse des objets placés en quarantaine** dans le menu contextuel ou son équivalent dans le menu **Action**.

Une tâche d'analyse à la demande du dossier de quarantaine sera lancée sur le poste client de l'application qui aura mis l'objet sélectionné en quarantaine.

CHAPITRE 11. ÉVÉNEMENTS, RAPPORTS ET NOTIFICATIONS

11.1. Enregistrement et affichage des événements et réception des notifications



Pour afficher le journal d'événements de Kaspersky Administration Kit entreposé sur le serveur d'administration :

Connectez-vous au serveur d'administration (voir section 2.1 à la page 10), ouvrez l'entrée **Événements** dans l'arborescence de console et sélectionnez le dossier correspondant au niveau de gravité que vous souhaitez examiner : **Messages d'information, graves, de défaillance ou d'avertissement**. Pour afficher tous les événements et les résultats, choisissez le dossier **Tous les événements**.

Le panneau de détails présente alors un tableau (voir Figure 122) énumérant tous les événements entreposés sur ce serveur d'administration (pour tous les groupes et applications installées) avec le niveau d'importance demandé. Le tableau possède les colonnes suivantes :

- **Gravité** – Degré d'importance de l'événement
- **Hôte** – Nom du client sur lequel l'événement s'est produit
- **Groupe** – Nom du groupe auquel appartient ce client
- **Application** – Application qui a produit cet événement
- **Version** – Version de l'application
- **Événement** – Nom de l'événement
- **Heure** – Moment où cet événement a été enregistré
- **Description** – Description d'événement.

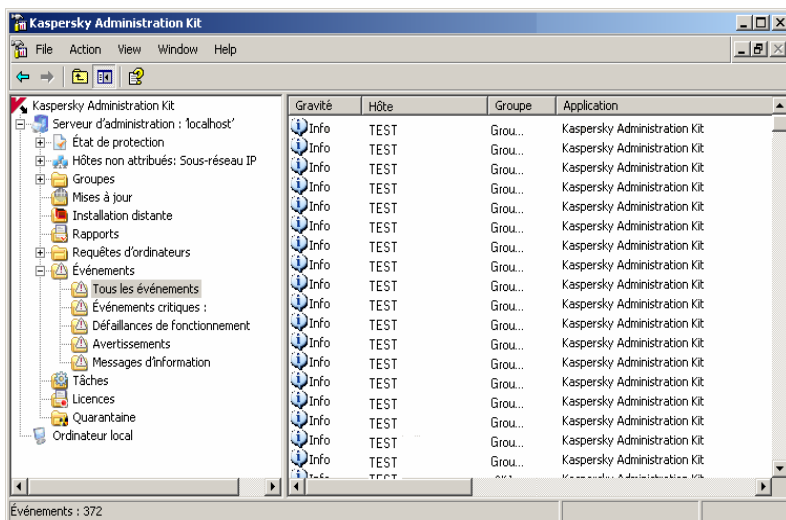


Figure 122. Affichage des événements entreposés sur le serveur d'administration

Vous pouvez trier les données dans n'importe quelle colonne, en ordre croissant ou décroissant, modifier l'ordre des colonnes, en ajouter ou en supprimer.

Pour simplifier l'affichage et la recherche des informations nécessaires, il est prévu de pouvoir créer et configurer des requêtes définies par l'utilisateur. L'utilisation de filtres permet d'effectuer des recherches et de filtrer les informations non nécessaires et qui, sans l'application de filtres, gêneraient la consultation ; seules les informations qui satisfont les critères de la requête. Ceci devient vite indispensable dès que les informations conservées dans le serveur sont volumineuses.



Pour créer une requête:

1. Sélectionnez l'entrée Événements dans l'arborescence de console, ouvrez le menu contextuel et utilisez la commande **Nouveau/Nouvelle requête** ou son équivalent dans le menu **Action**.
2. Dans la fenêtre ouverte, indiquez le nom de la requête (voir Figure 123) puis cliquez sur **Ok**.

Un nouveau dossier avec le nom spécifié pour la requête sera créé dans l'arborescence de console ; la structure de ce dossier contient tous les événements et les résultats de l'exécution de la tâche tels que

conservés sur le serveur d'administration. Pour rechercher des événements, vous devez configurer les paramètres de la requête.

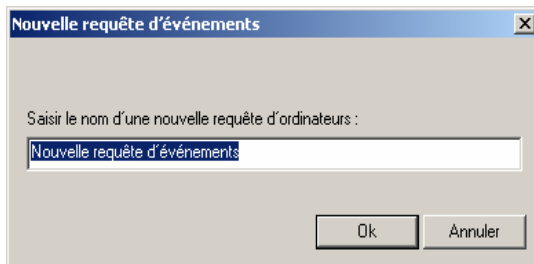


Figure 123. Création d'une requête d'événements



Pour personnaliser une requête:

1. Sélectionnez la requête souhaitée dans l'arborescence de console ou dans la panneau de résultats et choisissez **Propriétés** dans le menu contextuel ou son équivalent dans le menu **Action**.
2. Ceci permet d'ouvrir la boîte de dialogue de configuration des requêtes (voir Figure 124), qui contient les onglets suivants : **Général**, **Événements**, **Ordinateurs** et **Heure**.

L'onglet **Général** vous permet de changer le nom de la requête.

L'onglet **Événements** (voir Figure 124) permet de définir quels types d'événements et de résultats de tâche devront être compris dans la requête :

- Spécifiez dans le groupe de champs **Application** :
 - Nom de l'application dont vous souhaitez examiner l'activité ;
 - Numéro de version de l'application ;
 - nom de la tâche dont vous souhaitez examiner les résultats.
- Définissez les caractéristiques des événements dans le groupe de champs **Types d'événements**:
 - Sélectionnez le niveau d'importance de l'événement dans la liste déroulante.

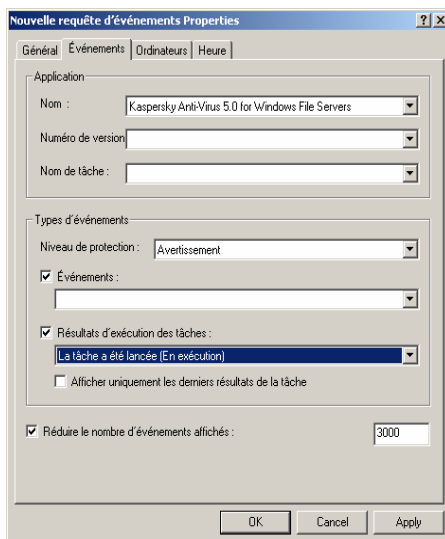


Figure 124. Configuration d'une requête d'événements.
L'onglet **Événements**



Certains types d'événements définis pour chaque application peuvent se produire pendant le fonctionnement de cette application. Chaque événement possède une caractéristique qui reflète son niveau d'importance. Les événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

- Pour s'assurer que le filtre contient des événements d'un certain type seulement, cochez la case **Événements** et sélectionnez le type requis dans la liste déroulante. Si le type d'événement n'est pas spécifié, tous les types seront affichés.
- Pour vous assurer que la requête contient les résultats de l'exécution des tâches, cochez la case **Résultats d'exécution de la tâche** et sélectionnez l'état de la tâche que vous souhaitez examiner.
- Cochez la case **Afficher uniquement les derniers résultats de la tâche** pour afficher uniquement les résultats de la dernière exécution de la tâche.

- Si vous souhaitez limiter la quantité d'informations affichées après application du filtre, cochez la case **Réduire le nombre d'événements affichés** et spécifiez le nombre de lignes maximum du tableau.

L'onglet **Ordinateurs** (voir Figure 125) permet de définir quels types d'événements et de résultats de tâche devront être compris dans la requête. Vous pouvez utiliser les paramètres suivants :

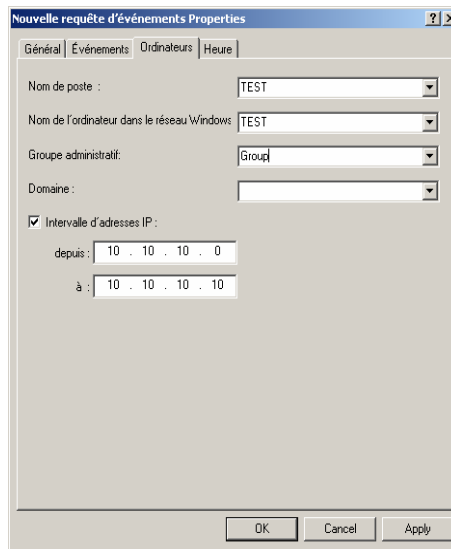
The image shows a Windows-style dialog box titled "Nouvelle requête d'événements Properties". It has four tabs: "Général", "Événements", "Ordinateurs", and "Heure". The "Ordinateurs" tab is selected. Inside the dialog, there are several fields: "Nom de poste :" with a dropdown menu showing "TEST"; "Nom de l'ordinateur dans le réseau Windows" with a dropdown menu showing "TEST"; "Groupe administratif:" with a dropdown menu showing "Group"; and "Domaine :" with an empty dropdown menu. Below these is a checked checkbox labeled "Intervalle d'adresses IP :". Under the checkbox, there are two IP address input fields. The first is labeled "depuis :" and contains the value "10 . 10 . 10 . 0". The second is labeled "à :" and contains the value "10 . 10 . 10 . 10". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Figure 125. Configuration d'une requête d'événements.
L'onglet **Ordinateurs**

- Nom de l'ordinateur dans le réseau logique ;
- Nom de l'ordinateur dans le réseau Windows ;
- Groupe administratif ;
- Domaine ;
- Pour spécifier l'intervalle des adresses IP des ordinateurs, cochez la case **Intervalle d'adresses IP** et renseignez les adresses de début et de fin.

Spécifiez l'heure d'enregistrement des événements et des résultats d'exécution de la tâche dans l'onglet **Heure** (voir Figure 126).

The screenshot shows a Windows-style dialog box titled "Nouvelle requête d'événements Properties". It has four tabs: "Général", "Événements", "Ordinateurs", and "Heure". The "Heure" tab is selected. Inside the dialog, there are two radio button options. The first option, "Pendant une période de", is selected. It has two sub-sections: "depuis :" and "jusqu'à :". Each sub-section has a dropdown menu (both set to "Déclenchement"), a date field (both set to "07/12/2005"), and a time field (the first is "00:00:00" and the second is "17:00:24"). The second radio button option is "Pendant les derniers jours :", followed by a small numeric input field containing the number "7". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Figure 126. Configuration de la requête d'événements.
L'onglet **Heure**

Vous pouvez sélectionner les options suivantes :

- **Pendant une période de** et spécifiez le début et la fin de la période couverte. Pour ce faire, sélectionnez les zones **Événements de la date** dans les zones **Depuis** et **Jusqu'à** et indiquez la date et l'heure exactes. Si toutes les informations enregistrées sont nécessaires, sélectionnez **Premier événement** et **Dernier événement**.
 - **Pendant les derniers jours** et précisez le nombre de jours.
3. Quand vous aurez terminé de configurer la requête, cliquez sur Appliquer ou sur Ok. Le tableau d'événements n'affichera que les informations qui vérifient les paramètres requis.



Pour enregistrer les informations sur les événements d'un fichier :

1. Sélectionnez dans l'arborescence de console la requête contenant les événements recherchés et utilisez la commande Toutes les tâches/Exporter du menu contextuel ou son équivalent dans le menu Action. Ceci permet de lancer l'assistant.
2. Au cours de cette première étape de l'assistant, spécifiez le chemin et le nom du fichier dans lequel les informations sont enregistrées. Si vous souhaitez n'enregistrer que les événements sélectionnés dans le panneau de résultats, cochez la case **Exporter uniquement les événements sélectionnés**.
3. Au cours de la seconde étape, choisissez le format d'exportation des événements:
 - **Exporter au format de texte séparé par des tabulations** - fichier texte
 - **Exporter au format de texte UNICODE séparé par des tabulations** – fichier au format UNICODE.
4. Pour compléter l'assistant, cliquez sur **Terminer**.



Pour supprimer des événements satisfaisant certains critères :

Créez et appliquez une requête avec les critères souhaités. Supprimez ensuite les événements du panneau de résultats avec l'option **Effacer** du menu contextuel.

Le programme ne supprimera que les événements qui satisfont les paramètres de la requête sous l'entrée **Événements**.



Pour afficher le contenu du journal d'événements de Kaspersky Administration Kit entreposé sur le poste client :

1. Exécutez la console d'administration sur le poste client.
2. Sélectionnez l'entrée **Ordinateur local** dans l'arborescence de console, et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.
3. La boîte de dialogue **Propriétés de Ordinateur local** apparaît. Dans cette boîte de dialogue, ouvrez l'onglet **Applications** (voir Figure 127), choisissez une application dont vous voulez afficher l'historique des événements, puis cliquez sur **Événements**.

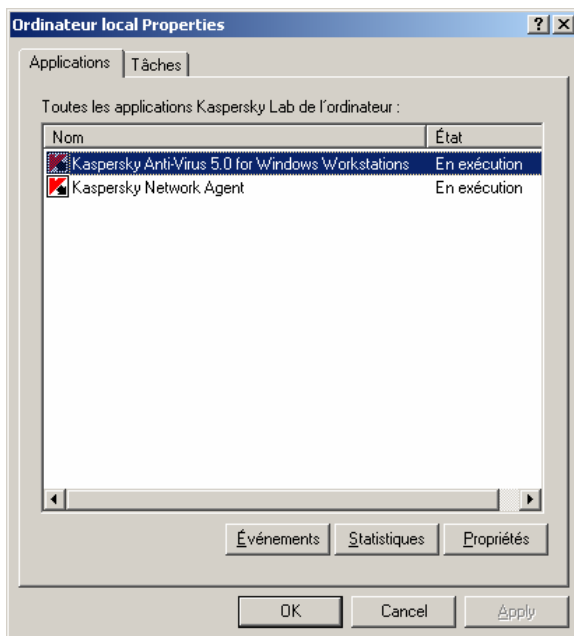


Figure 127. La boîte de dialogue **Propriétés de Ordinateur local**. L'onglet **Applications**

Ceci permet d'ouvrir une boîte de dialogue (voir figure 133) avec un tableau d'événements générés par cette application sur le poste client choisi. Le tableau possède les colonnes suivantes :

- **Gravité** – Degré d'importance de l'événement
- **Tâches** - Nom de tâche
- **Événement** – Type d'événement
- **Heure** – Heure d'enregistrement de l'événement
- **Description d'événement** – Description d'événement.

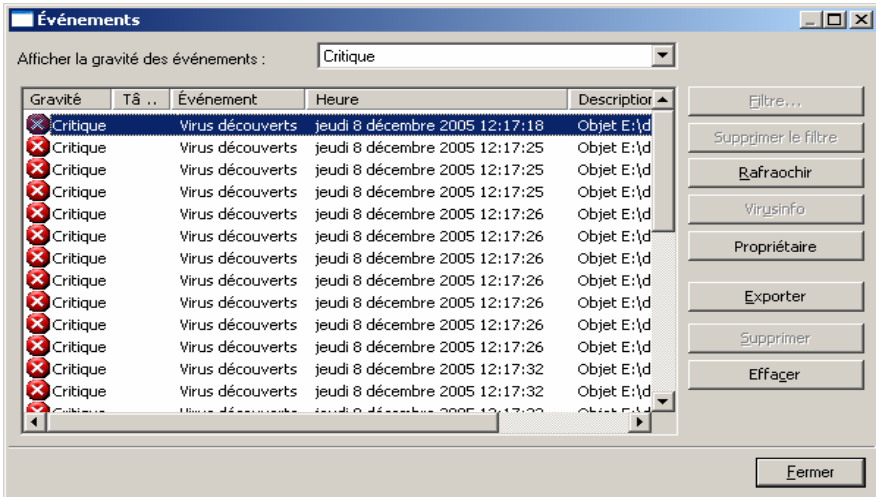


Figure 128. Affichage des événements entreposés sur le serveur d'administration

11.2. Affichage et modification des modèles de rapport



Pour afficher et/ou modifier un modèle de rapport :

Connectez-vous au serveur d'administration cible (voir section 2.1 à la page 10) et sélectionnez l'entrée **Rapports** dans l'arborescence de console. Une liste de modèles de rapport existants sera affichée dans le panneau de détails. Sélectionnez le modèle et cliquez sur **Propriétés** dans le menu contextuel ou dans le menu **Action**.

La boîte de dialogue **Propriétés de <Nom de modèle de rapport>** s'affiche (voir Figure 129). Les onglets de cette boîte de dialogue sont propres à chaque type de rapport et contiennent les options suivantes :

- **Général** – Affiche des informations générales sur un modèle ; permet d'inclure des données provenant de serveurs secondaires ; contient un bouton permettant de créer un rapport.
- **Intervalle de temps** – Pour définir la période couverte par le rapport.

- **Champs détails** – Définit les champs à inclure dans le rapport et l'ordre de tri des entrées.
- **Champs récapitulatifs** – Permet de spécifier les champs récapitulatifs à inclure dans les rapports, et de définir l'ordre de tri des entrées dans ces rapports.
- **Totaux** – Permet de définir une liste de champs récapitulatifs (totalisés) présents dans le rapport.
- **Groupe cible** – Spécification de groupes ou d'ordinateurs de différents groupes couverts par le rapport.

The screenshot shows a Windows-style dialog box titled "Rapport d'activité antivirus Properties". It has three tabs: "Champs récapitulatifs", "Totaux", and "Groupe cible". The "Général" sub-tab is selected under "Champs récapitulatifs". The dialog contains the following elements:

- A text field with the value "Rapport d'activité antivirus".
- A checked checkbox labeled "Imprimer la version".
- A "Modèle :" label followed by a text field containing "Rapport d'activité antivirus".
- A "Description :" label followed by a text area containing "Ce rapport contient des informations concernant l'activité antivirus".
- Fields for "Créé :" and "Modifié le :", both showing the date and time "07/12/2005 16:29:39".
- A checked checkbox labeled "Inclure les données à partir des serveurs d'administration Kaspersky secondaires".
- A "Jusqu'au niveau d'imbrication :" label followed by a spinner box set to "1".
- A "Générer..." button.
- Standard "OK", "Cancel", and "Apply" buttons at the bottom.

Figure 129. La boîte de dialogue Propriétés du Rapport d'activité antivirus.
L'onglet **Général**

Pour personnaliser les paramètres des modèles, suivez les mêmes étapes que pour la création de modèles (voir section 11.3 à la page 173). Cliquez sur le bouton **Appliquer** ou **Ok** pour appliquer les paramètres.

11.3. Création d'un modèle de rapport



Pour créer un modèle de rapport :

1. Sélectionnez l'entrée **Rapports** dans l'arborescence de console et cliquez sur **Nouveau** dans le menu contextuel ou dans le menu **Action** pour lancer un Assistant. Suivez les instructions de l'Assistant.
2. Indiquez le nom de modèle. Si un modèle de ce nom existe déjà, un **_1** sera automatiquement ajouté au nouveau nom.
3. Sélectionnez le type de rapport. Les étapes suivantes dépendent de votre choix.
4. Indiquez la période couverte par le rapport (voir Figure 130). Vous pouvez choisir des dates fixes de rapport ou laisser la date de fin sans définir. Dans ce second cas, le programme utilisera la date courante du système pour la date de fin du rapport. Vous pouvez également choisir l'option **Des derniers jours** et préciser le nombre de jours dans le champ associé.

Cette étape n'est pas requise pour des rapports sur l'état actuel, par exemple, pour des rapports sur la protection antivirus courante.

The screenshot shows a Windows-style dialog box titled "Assistant Nouveau rapport". Inside, the section "Choix de la période de rapport" is active, with the instruction "Vous pouvez choisir sur cette page l'intervalle de temps du nouveau rapport". There are three radio button options for selecting the time period:

- ☒ De : [07/12/2005] à : [07/12/2005]
- ☐ De : [07/12/2005] à la date courante
- ☐ Des derniers jours : [1]

At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 130. Création d'un modèle de rapport. Définir la période de rapport

5. Spécifiez les objets pour lesquels vous voulez créer le rapport (voir Figure 131).
 - **Je veux créer un rapport sur un groupe** – Crée un rapport sur les ordinateurs appartenant à un groupe.
 - **Je veux créer un rapport sur une liste d'ordinateurs** – Crée un rapport pour des ordinateurs de différents groupes.

Si un rapport peut être uniquement créé pour le réseau en entier, par exemple un **Rapport sur les licences**, alors cette étape et la prochaine seront omises.

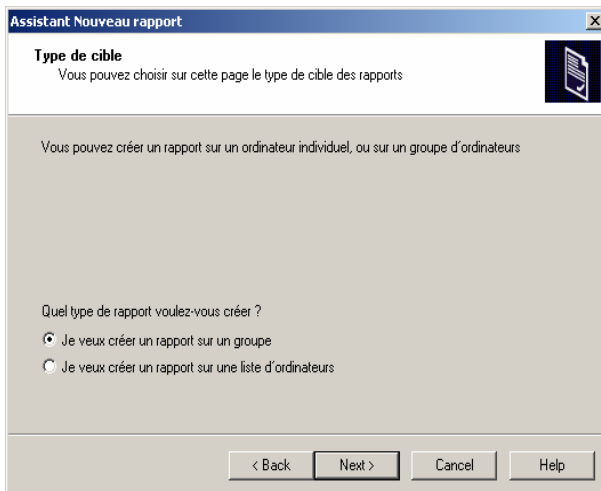


Figure 131. Création d'un modèle de rapport.
Sélection des objets du rapport

6. Choisissez le groupe ou des clients spécifiques dans différents groupes, sur lesquels vous allez créer un rapport (voir Figure 132) et terminez l'Assistant.

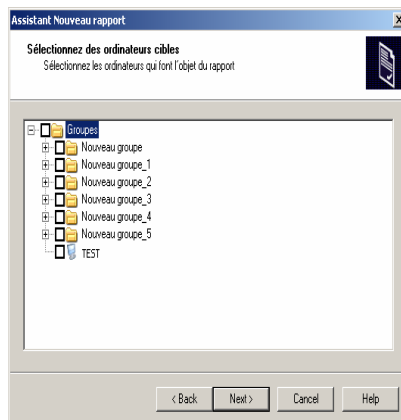


Figure 132. Création d'un modèle pour des rapports de protection. Choix des clients

Après la fin de l'Assistant, le nouveau modèle sera ajouté à l'entrée **Rapports** dans l'arborescence de console et affiché dans le panneau de détails. Le modèle peut être utilisé pour créer et afficher des rapports.

11.4. Génération et affichage de rapports



Pour générer un rapport en utilisant un modèle :

Connectez-vous au serveur d'administration cible et sélectionnez l'entrée **Rapports** dans l'arborescence de console. Le panneau de détails présente une liste de modèles de rapport disponibles. Sélectionnez le modèle requis et cliquez sur **Générer** dans le menu contextuel ou dans le menu **Action**, afin de générer un rapport. Si vous voulez afficher le rapport, le navigateur ouvrira une fenêtre avec le rapport généré. Le contenu du rapport correspond au modèle sélectionné, avec les éléments suivants (voir Figure 133):

- Le logo de la société, le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur les objets couverts par le rapport.
- Données récapitulatives (champs calculés et récapitulatifs du rapport) ;
- Diagramme illustrant les données générales du rapport ;
- Tableau avec les données accumulées
- Tableau avec les données détaillées.

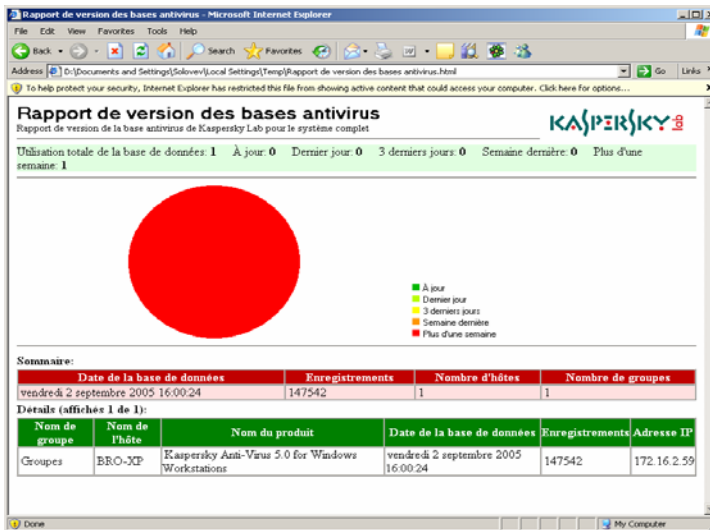


Figure 133. Création d'un modèle pour des rapports de protection. Choix des clients

11.5. Génération de rapports récapitulatifs sur des serveurs d'administration secondaires



Pour créer ce genre de rapports :

Sélectionnez le modèle de rapport souhaité sous l'entrée **Rapports** sur le serveur d'administration primaire. Dans le menu contextuel, cliquez sur **Propriétés** puis sur l'onglet **Général** (voir Figure 129), définissez les paramètres suivants :

- **Inclure les données à partir des serveurs d'administration secondaires** (case à cocher)
- Le degré d'imbrication des serveurs d'administration en fonction de leur hiérarchie (**Jusqu'au niveau d'imbrication**).

Cliquez sur **Générer**.

Ensuite, le rapport sera affiché dans la fenêtre de votre navigateur.



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

CHAPITRE 12. GESTION DES CLES DE LICENCE

12.1. Afficher des informations sur les clés de licence.



Pour afficher les informations relatives aux clés de licence installées :

Connectez-vous au serveur d'administration cible (voir 2.1, page 10) et sélectionnez l'entrée **Gestion des clés de licence** dans l'arborescence de console. Le panneau de résultats montrera la liste des clés de licence installées sur les postes clients.

Les informations suivantes sont proposées pour chacune des clés :

- **Numéro de série** – Numéro de série de la clé de licence.
- **Type** – Type de clef installée, par exemple, par exemple **commerciale**, **essai**, etc.
- **Nombre max. d'ordinateurs** – Nombre maximum d'ordinateurs sur lesquels il est possible d'installer la clef de licence.
- **Durée de validité** – Période de validité de la licence



Pour afficher les informations relatives à une clé de licence spécifique :

sélectionnez la clé de licence correspondante dans le panneau de résultats puis utilisez la commande Propriétés du menu contextuel ou du menu **Action**.

Ceci permet d'ouvrir la boîte de dialogue **Propriétés:<numéro de série de la clé>** contenant les onglets **Général** et **Objets** (voir figure 139).

L'onglet **Général** (voir Figure 134) contient les informations suivantes sur la clé :

- Numéro de série de la clé de licence ;

- Type de clé ;
- Durée de validité ;
- Nombre max. d'ordinateurs.

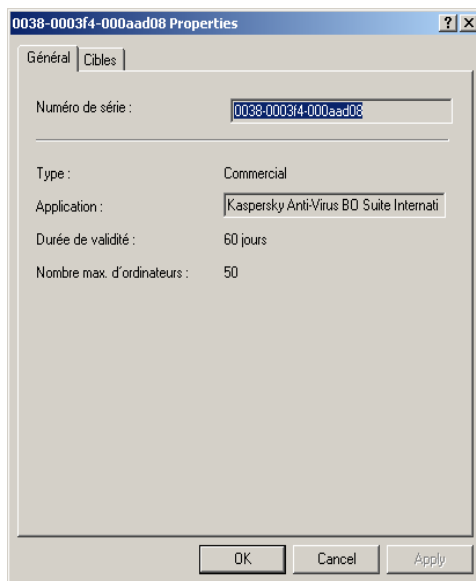


Figure 134. Clé de licence .
L'onglet **Général**

L'onglet **Objets** (voir Figure 135) contient la liste des postes clients sur lesquels cette clé est installée. La liste fournit les informations suivantes :

- Nom du poste client ;
- Groupe administratif ;
- Si la clé est utilisée (ou pas) en tant que clé active
- Date d'expiration de la clé ;
- Date d'activation de la clé sur les postes clients.

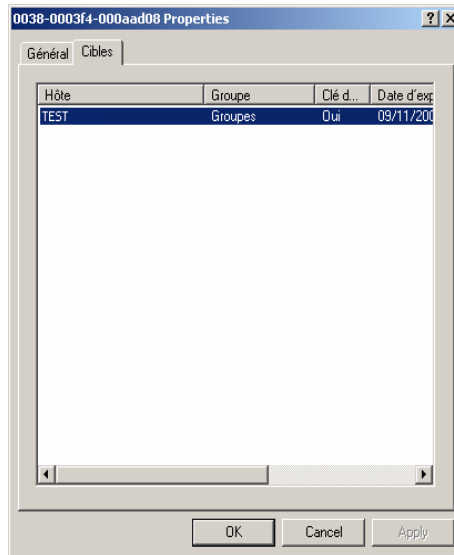


Figure 135. Propriétés de la clé de licence.
L'onglet **Objets**

Pour vérifier quelles clés de licence sont installées pour l'application sur un poste client spécifique, utilisez la fenêtre de configuration des propriétés de l'application.

12.2. Ajout d'une nouvelle clé de licence



Pour installer une nouvelle clé de licence,

créez et lancez une tâche d'installation de clé de licence.

Une tâche d'installation de la clé de licence peut agir comme tâche de groupe, tâche globale, ou tâche locale (voir Chapitre 7 à la page 109). Lors de la création de cette tâche :

- sélectionnez l'application à laquelle vous affectez la licence, pour créer la tâche ;

- sélectionnez **Paquet d'installation de la clé de licence** comme type de tâche.

Lors de la configuration de tâche (voir figure 141), spécifiez le fichier de clé de licence à installer (*.key). Si cette clé va être utilisée en tant que clé active, et qu'elle doit remplacer la clé actuelle immédiatement après l'installation, cochez la case **Utiliser en tant que clé de licence actuelle**. Si la clé va servir comme clé de réserve, ne cochez pas cette case. La clé de licence de réserve ne s'active qu'après expiration de la clé de licence courante. Des informations supplémentaires sur la clé de licence figure dans la zone **Renseignements relatifs à la clé de licence**.

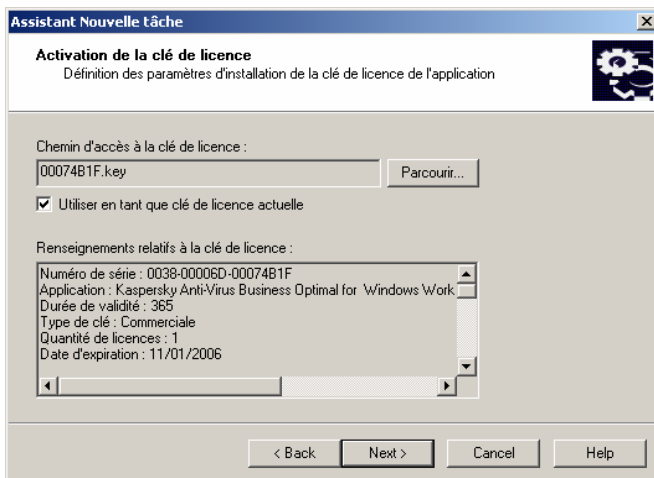


Figure 136. Création d'une tâche d'installation de clé de licence
Sélection d'une clé de licence



Pour démarrer l'Assistant d'installation de la clé de licence :

sélectionnez l'entrée **Gestion des clés de licence** dans l'arborescence de console et utilisez la commande **Ajouter clé de licence** dans le menu contextuel ou dans le menu **Action**. Ceci permet de démarrer un assistant de création de tâche globale qui saute l'étape de sélection du type de tâche, qui est spécifié par défaut.

Les tâches créées à l'aide de l'Assistant d'installation de clés sont des tâches globales situées dans l'entrée **Tâches** de l'arborescence de console.

Quand vous modifiez les paramètres de la tâche d'installation de la clé de licence sur l'onglet **Paramètres** (voir Figure 137), vous pouvez remplacer le fichier de licence à installer, et cocher la Utiliser en tant que clé de licence actuelle pour en faire la clé active de l'application. Si la case n'est pas cochée, la clé servira de clé de réserve. Des informations supplémentaires sur la clé de licence figurent dans la zone **Renseignements relatifs à la clé de licence**.

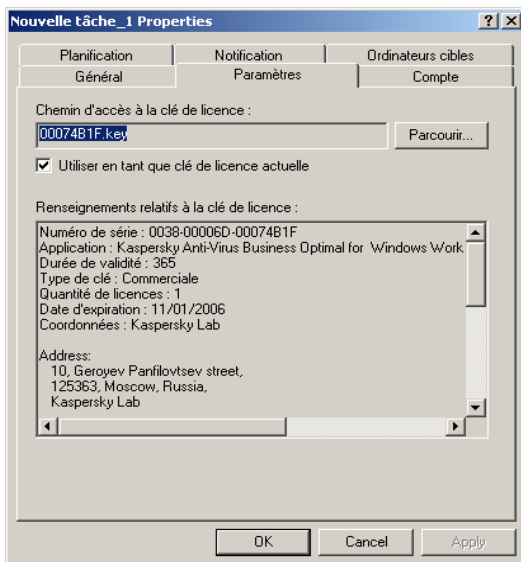


Figure 137. Modification d'une tâche d'installation de clé de licence

12.3. Création et affichage de rapports sur les clés de licence



Pour créer un rapport sur l'état des clés de licence installées sur les postes clients du réseau logique :

utilisez le modèle intégré de rapport, Rapport sur les licences, ou créez un nouveau modèle de même type (voir section 11.3 à la page 174).

Un rapport créé sur le modèle **Rapport sur les licences** contient des informations complètes sur toutes les clés installées sur les postes clients du

réseau logique, y compris les clés actives et de réserve, en indiquant les ordinateurs sur lesquels ces clés sont utilisées, avec les limitations de licence.

CHAPITRE 13. COPIE DE SAUVEGARDE ET RESTAURATION DES DONNEES DU SERVEUR D'ADMINISTRATION



Pour créer une copie de sauvegarde des données du serveur d'administration :

- créez et lancez une tâche globale pour la copie de sauvegarde (voir section 13.1 à la page 186) à l'aide de la **Console d'administration**
ou
- exécutez l'outil **klbackup** sur le poste où le serveur d'administration se trouve installé, avec les paramètres correspondants de la ligne de commande (voir section 13.2 à la page 189). Cet outil est fourni avec le paquet de distribution Kaspersky Administration Kit et se trouve à la racine du dossier d'installation du serveur d'administration.



Pour rétablir les données du serveur d'administration:

exécutez l'outil **klbackup** sur le poste où le serveur d'administration se trouve installé, avec les paramètres correspondants de la ligne de commande (voir section 13.2 à la page 189).

13.1. Tâche de copie de sauvegarde



Pour créer une tâche de copie de sauvegarde des données du serveur d'administration:

sélectionnez l'entrée **Tâche globale** dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez la commande **Nouveau/Tâche** ou utilisez son équivalent du menu **Action**. Ceci permet de lancer l'assistant de création de tâche (voir Chapitre 7 à la page 109).

Créer une tâche globale (voir Chapitre 7 à la page 109). Lors de la création d'une tâche, spécifiez les valeurs suivantes pour les paramètres :

Choisissez Kaspersky Administration en tant qu'application pour laquelle vous allez créer la tâche (voir Figure 138), et en tant que type de tâche, sélectionnez **Copie de sauvegarde**.

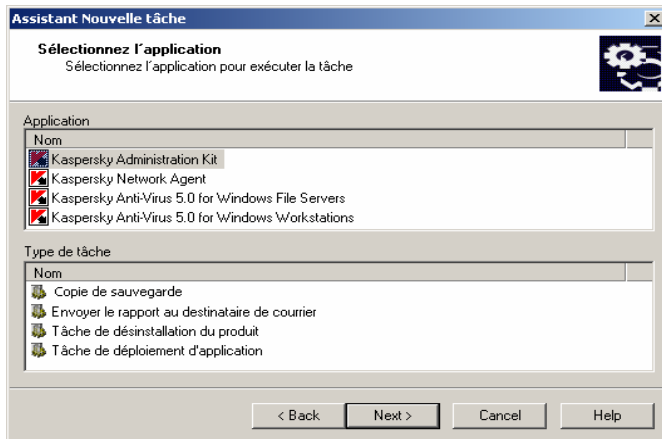


Figure 138. Création d'une tâche de copie de sauvegarde.
Choix de l'application et du type de tâche

Spécifiez à cette étape de la configuration (voir Figure 139):

- le dossier destination des données de sauvegarde ; ce dossier doit être disponible en écriture à la fois pour le serveur d'administration et pour le serveur SQL sur lequel se trouve installée la base de données du serveur d'administration ;
- le mot de passe à utiliser pour coder/décoder le certificat du serveur d'administration ;

La copie de sauvegarde est générée dans le dossier spécifié, en tant que sous-dossier portant un nom composé de la date et de l'heure de l'opération, dans un format de mise en forme de **klbackup**, comme ceci : **AAAA-MM-JJ # HH-MM-SS**. L'information suivante sera enregistrée dans ce dossier :

- la base de données du serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le serveur d'administration);
- données de configuration de la structure du réseau logique et des postes clients ;

- entrepôt des paquets de déploiement des applications (le contenu du dossier Packages);
- Certificat du serveur d'administration.

Vous pouvez réduire le nombre de copies de sauvegarde - c'est à dire, le nombre maximum de sous-dossiers pouvant figurer dans l'espace de sauvegarde. Pour ce faire cochez la case **Réduire le nombre de copies de sauvegarde conservées** et spécifiez le nombre de copies requis. Si la limite est atteinte, les copies précédentes plus anciennes, conservées dans l'espace de sauvegarde, seront supprimées.

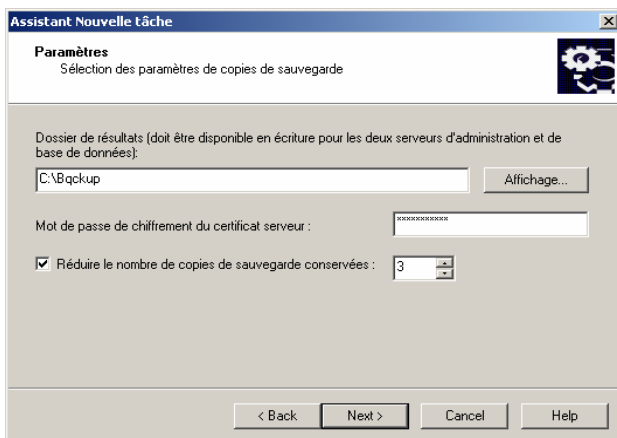


Figure 139. Création d'une tâche de copie de sauvegarde.
Configuration des paramètres



Pour configurer une tâche de copie de sauvegarde des données du serveur d'administration:

1. Sélectionnez les tâches correspondantes de l'entrée Tâches globales, dans le panneau de résultats, ouvrez le menu contextuel et sélectionnez la commande Propriétés, ou utilisez son équivalent du menu **Action**.
2. Dans la fenêtre ouverte, sélectionnez l'onglet **Paramètres** (voir Figure 140). Cet onglet affiche les mêmes paramètres définis lors de la création de la tâche :
 - Dossier destination des copies de sauvegarde ;
 - Mot de passe à utiliser pour code/décoder le certificat du serveur d'administration ;

- Limitations au nombre de copies de sauvegarde.

Spécifiez les valeurs requises des paramètres.

3. Quand vous aurez terminé la configuration, cliquez sur **Appliquer** ou sur **Ok**.

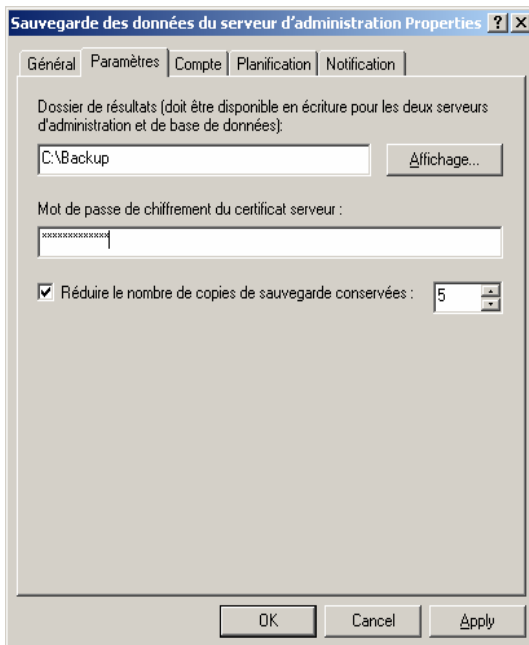


Figure 140. Configuration de la tâche de copie de sauvegarde

13.2. Utilitaire de copie de sauvegarde



Pour créer une copie de sauvegarde des données du serveur d'administration manuellement:

exécutez l'outil **klbackup** sur le poste où le serveur d'administration se trouve installé, en utilisant les paramètres requis sur la ligne de commande.

Syntaxe de l'outil sur la ligne de commande :

- **klbackup [-logfile LOGFILE]³ -path BACKUP_PATH [-use_ts][[-restore] -savecert PASSWORD**

Description des paramètres :

- **-logfile LOGFILE** – enregistre un rapport sur l'exécution de la tâche de copie/restauration des données du serveur d'administration.
- **-path BACKUP_PATH** – enregistre les données dans le dossier **BACKUP_PATH**/restaure à partir des données du dossier **BACKUP_PATH** (paramètre obligatoire).



Le compte du serveur de base de données et l'outil **klbackup** doivent posséder les droits nécessaires pour pouvoir écrire dans le dossier **BACKUP_PATH**.

- **-use_ts** – Lors de la sauvegarde, les données sont recopiées dans le dossier désigné d'après la date et l'heure de l'opération, au format **klbackup YYYY-MM-DD # HH-MM-SS**, **imbriqué dans le dossier BACKUP_PATH**. Si aucun paramètre de ligne de commande n'est spécifié, les données seront enregistrées à la racine du dossier **BACKUP_PATH**.



Si l'on essaie sauvegarder des données dans un dossier dans lequel il existe déjà une copie de sauvegarde, un message d'erreur apparaît et aucune mise à jour ne se produit.

L'utilisation du paramètre **-use_ts** permet de gérer les archives de données du serveur d'administration. Par exemple, si le dossier **C:\KLBackups** a été spécifié en utilisant le paramètre **-path**, alors les données sur l'état du serveur d'administration datant du 19 juin 2003, à 11 heures 30 et 18 secondes, seront enregistrées dans le dossier **klbackup 2003-06-19 # 11-30-18**.

- **-restore** – Restaurer les données du serveur d'administration. La restauration des données se fera en fonction des informations conservées dans le dossier **BACKUP_PATH**. Si le paramètre n'est pas utilisé, la copie de sauvegarde des données se fera dans le dossier **CHEMIN_SAUVEGARDE**.

³ В квадратных скобках приводятся необязательные ключи.

- **-savecert PASSWORD** – La fonction Enregistrer / Restaurer le Certificat du serveur d'administration utilise le mot de passe spécifié par le paramètre **PASSWORD** pour coder ou décoder le certificat



La restauration complète des données du système d'administration nécessite une sauvegarde impérative du certificat du serveur d'administration. Le paramètre **PASSWORD** doit être spécifié.



Lors de la restauration du certificat, il faut fournir le même mot de passe que celui utilisé pour la copie de sauvegarde. Si le mot de passe est incorrect, le certificat ne sera pas reconstitué.



Au cours de la restauration des données du serveur d'administration, si le chemin jusqu'au dossier public change, il faudra alors vérifier la bonne exécution des tâches dans ce dossier (tâches de mise à jour, de déploiement) et, si nécessaire, modifier la configuration.

ANNEXE A. QUESTIONS FREQUENTES

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



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

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



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

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

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

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

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

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

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



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

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

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



Question : Mon application antivirus ne fonctionne pas.

Que dois-je faire ?

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

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

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

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

3. Mentionnez au début de votre message la version exacte du système d'exploitation, la distribution de Kaspersky Anti-Virus et le numéro de votre licence.
4. Décrivez clairement et brièvement le problème. N'oubliez pas qu'au moment même où ils lisent vos explications, les membres du service technique ne savent encore rien de votre problème. Ils ne pourront vous aider qu'après l'avoir compris complètement et simulé.
5. Envoyez les données suivantes au service technique (créez un fichier compressé avant de les envoyer) :
 - Fichier journal antivirus ;
 - Clé de licence ;
6. Ne manquez pas d'indiquer également la présence de :
 - un contrôleur SCSI ;
 - un processeur très ancien ou récent, de plusieurs processeurs ;
 - une mémoire inférieure à 64 Mo ou supérieure à 2 Go.
7. Spécifiez le niveau de trafic journalier et les moments de pointe de surcharge.



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

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

- Mauvaise configuration du réseau :

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

- Internet n'est pas configuré sur l'ordinateur;
- Les paramètres de MS Internet Explorer ne sont pas accessibles ou n'ont pas été saisis;
- Le serveur proxy requiert une autorisation.

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

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

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

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

ANNEXE B. GLOSSAIRE

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

A

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

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

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

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

B

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

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

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

C

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

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

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

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

D

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

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

E

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

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

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

G

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

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

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

I

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

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

Installation par envoi – Méthode d'installation à distance (en anglais: Push) permettant d'installer le logiciel Kaspersky Lab sur des ordinateurs spécifiques de votre réseau logique. Dans le cas d'une installation par envoi, le serveur d'administration doit disposer des privilèges nécessaires pour exécuter les applications sur les clients distants. Cette méthode est recommandée pour des ordinateurs sous MS Windows NT/2000/2003/XP, qui prennent en charge cette caractéristique, ou sur des ordinateurs sous MS Windows 98/Me, sur lesquels Network Agent est installé.

Installation par script – Méthode d'installation qui fait dépendre la tâche d'installation distante d'un ou de plusieurs comptes utilisateur spécifiques. Quand l'utilisateur spécifique ouvre une session sur le domaine, l'installation de l'application s'effectue sur poste client utilisé. Cette méthode est recommandée pour des ordinateurs exploités sous MS Windows 95/98/Me

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

K

Kaspersky Administration Kit – Application spécialisée dans l'exécution centralisée des tâches administratives principales. Il offre un contrôle

complet sur la stratégie antivirus de l'entreprise utilisatrice d'applications Kaspersky Lab.

M

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

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

N

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

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

- Critique
- Erreur
- Avertissement
- Info

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

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

O

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

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

Objets de démarrage – Un ensemble de programmes nécessaires pour le lancement et le bon fonctionnement du système d'exploitation, et du reste des logiciels installés dans l'ordinateur. Votre système d'exploitation lance ces objets à chaque démarrage. Certains virus

tendent d'infecter ces objets et causent la défaillance du système au démarrage.

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

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

P

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

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

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

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

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

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

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

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

Q

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

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

R

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

- Base de données du serveur d'administration qui entrepose les stratégies, les tâches, les paramètres d'application, et les événements enregistrés sur le serveur d'administration;
- Informations sur les configurations des réseaux logiques et des clients ;
- Fichiers pour l'installation à distance des applications (contenu du dossier Packages);
- Certificat du serveur d'administration

S

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

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

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

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

Seuil d'activité virale – Nombre de virus détectés dans un intervalle de temps déterminé. Si ce nombre est dépassé, la situation est identifiée comme une **Attaque virale**. Ce paramètre est important dans l'identification des épidémies, car il détermine le temps de réaction administrative face à de nouvelles menaces, et l'application des mesures préventives destinées à protéger le réseau.

Stratégie – voir **Stratégie de groupe**

Stratégie de groupe – Ensemble des paramètres d'application d'un groupe administratif contrôlé par le Kaspersky Administration Kit. Les stratégies de groupe peuvent être différentes pour chaque groupe. Les stratégies

de groupe sont spécifiques pour différentes applications. La stratégie détermine la configuration de tous les paramètres des applications.

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

T

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

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

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

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

V

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

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

ANNEXE C. KASPERSKY LAB

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

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Bénélux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

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

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les 3 heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

C.1. Autres produits Kaspersky Lab

Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

Kaspersky Anti-Virus® Personal Pro

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

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

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

Kaspersky® Anti-Hacker

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

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

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

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

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

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

Kaspersky® Personal Security Suite

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

Kaspersky® Personal Security Suite possède les fonctions suivantes :

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

Kaspersky® Security for PDA

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

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

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

Kaspersky Anti-Virus® Business Optimal

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

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale⁴ intégrale de :

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

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

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

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

⁴ En fonction du type de livraison

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

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky SMTP Gateway

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

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

Kaspersky Security® for Microsoft Exchange 2003

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

Kaspersky® Mail Gateway

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

C.2. Comment nous contacter

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

Support technique	Pour une assistance technique, adressez-vous à : http://www.kaspersky.com/supportinter.html
-------------------	--

Information générale	WWW : http://www.kaspersky.com http://www.viruslist.com E-mail : sales@kaspersky.com
-------------------------	---

ANNEXE D. CONTRAT DE LICENCE

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

L'ACQUISITION DE CE LOGICIEL VIA INTERNET A LA SUITE D'UN CLIC SUR LE BOUTON ACCEPTER SIGNIFIE QUE VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Support technique.

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

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

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

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

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

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

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

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

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

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

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

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

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

6. **Limite de garantie**

(i) Kaspersky Lab garantit que pour une durée de [90] jours suivant le téléchargement ou l'installation du logiciel, ce dernier fonctionnera correctement comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le logiciel et sa documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions ou d'erreurs.

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

(iv) La responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement au paragraphe (i), et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un représentant au cours de la période de garantie. Vous devrez fournir toutes les informations nécessaires au fournisseur pour remédier à tout problème éventuel.

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

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

7. Décharge de responsabilité

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

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

- (a) Perte de revenus ;
- (b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats) ;
- © Perte de moyens de paiement ;
- (d) Perte d'économies prévues ;
- (e) Perte de marché ;
- (f) Perte d'occasions commerciales ;
- (g) Perte d'image ;

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

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

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

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

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

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