

Kaspersky Administration Kit 8.0

KASPERSKY **lab**

MANUEL
D'ADMINISTRATEUR

VERSION DE L'APPLICATION: 8.0 CF2

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que ce document vous aidera dans votre travail et répondra à la plupart des problèmes émergents.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous un format quelconque et la diffusion, y compris la traduction, de n'importe quel document ne sont admises que par autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et à titre d'information.

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

Kaspersky Lab ne peut être tenu responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. Kaspersky Lab n'assume pas non plus de responsabilité en cas de dommages liés à l'utilisation de ces textes.

Ce document fait référence aux autres noms et aux marques déposés qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 14/10/2010

© 1997–2010 Kaspersky Lab ZAO. Tous droits réservés.

<http://www.kaspersky.fr>
<http://entreprise.kaspersky.fr>

Kaspersky Lab ZAO est propriétaire de tous les droits (Détenteur de droits), qu'ils soient exclusifs ou autres, au Kaspersky Administration Kit (le Logiciel).

EN CLIQUANT LA TOUCHE " ACCEPTER " DANS LA FENÊTRE DE LA LICENCE, VOUS CONSENTEZ À ÊTRE TENU PAR LES CONDITIONS DE CE CONTRAT. **CETTE ACTION EST SYMBOLIQUE DE VOTRE SIGNATURE ET PAR CELA VOUS CONSENTEZ À ÊTRE TENU PAR ET ÊTRE UNE PARTIE DE CE CONTRAT ET CONSENTEZ À CE QUE CE CONTRAT SOIT EXÉCUTOIRE DE LA MÊME FAÇON QU'UN CONTRAT NÉGOCIÉ ÉCRIT ET QUE VOUS AURIEZ SIGNÉ.** SI VOUS N'ÊTES PAS D'ACCORD SUR TOUTES LES CONDITIONS DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET N'INSTALLEZ PAS LE LOGICIEL.

Le logiciel peut être utilisé gratuitement uniquement à des fins administratives (y compris pour l'installation à distance, l'administration de la licence, la protection antivirus et la surveillance) pour tout autre produit de l'entreprise Kaspersky Lab décrit dans le guide de mise en œuvre (Implementation Guide) et uniquement par les utilisateurs de produits de l'entreprise Kaspersky Lab qui ont consenti aux conditions de la licence d'utilisateur final pour les produits de l'entreprise.

Les utilisateurs des produits de l'entreprise Kaspersky Lab qui ont consenti aux conditions de la licence d'utilisateur final des produits de l'entreprise ont droit à une assistance technique par le biais de l'Internet ou du service d'assistance téléphonique.

Service d'assistance technique : <http://support.kaspersky.com>

Vous ne devez ni émuler, cloner, louer, prêter, concéder, vendre, modifier, décompiler ou appliquer l'ingénierie inverse au logiciel ou désassembler ou créer des produits dérivés fondés sur le logiciel ou sur toute portion lui appartenant à l'exception unique d'un droit sans dérogation possible vous étant accordé par la législation en vigueur.

LE LOGICIEL EST FOURNI " EN L'ÉTAT " ET LE DÉTENTEUR DE DROITS NE FAIT AUCUNE DÉCLARATION ET NE CONCÈDE AUCUNE GARANTIE QUANT À SON UTILISATION OU À SON FONCTIONNEMENT. À L'EXCEPTION DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU OBLIGATION DONT L'ENVERGURE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE DÉTENTEUR DE DROITS ET SES PARTENAIRES NE CONCÈDENT AUCUNE GARANTIE, CONDITION, DÉCLARATION OU OBLIGATION (ÉNONCÉE OU IMPLICITE, QUE CE SOIT PAR LA LOI, LA COMMON LAW, LA COUTUME, L'USAGE OU AUTRE LÉGISLATION) EN CE QUI CONCERNE LES LITIGES, Y COMPRIS, ET SANS LIMITATION, LA NON VIOLATION DES DROITS DE TIERS, LA QUALITÉ MARCHANDE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU LES CONDITIONS D'APPLICATION DU PRODUIT À DES FINS PARTICULIÈRES. VOUS ACCEPTEZ TOUTE FAUTE, ET LE RISQUE INTÉGRAL QUANT AU FONCTIONNEMENT ET À VOTRE RESPONSABILITÉ DE CHOISIR LE LOGICIEL QUI CONVIENT POUR FOURNIR LES RÉSULTATS VOULUS ET QUANT À SON INSTALLATION, SON UTILISATION ET LES RÉSULTATS OBTENUS DU LOGICIEL. SANS LIMITER LES DISPOSITIONS QUI PRÉCÈDENT, LE DÉTENTEUR DE DROITS NE FAIT AUCUNE DÉCLARATION ET N'ACCORDE AUCUNE GARANTIE QUE LE LOGICIEL NE COMPORTERA PAS D'ERREUR NI NE SERA SANS COUPURES OU AUTRES PANNES OU QUE LE LOGICIEL REMPLIRA TOUTES OU CHACUNE DE VOS EXIGENCES, QU'ELLES SOIENT OU NON DÉVOILÉES AU DÉTENTEUR DE DROITS.

© 1997-2010 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et toute documentation l'accompagnant sont soumis au droit d'auteur et protégés par les lois sur le droit de reproduction et les lois internationales sur le droit d'auteur ainsi que par tout autre droit et traité de propriété intellectuelle.

CONTENU

A PROPOS DE CE MANUEL.....	6
Dans ce document.....	6
Conventions.....	7
SOURCES D'INFORMATIONS COMPLEMENTAIRES.....	8
Sources d'informations pour des recherches indépendantes.....	8
Discussion sur les applications de Kaspersky Lab dans le forum.....	9
Contacter le Groupe de rédaction de la documentation pour les utilisateurs.....	9
KASPERSKY ADMINISTRATION KIT.....	11
Nouveautés.....	12
Configuration logicielle et matérielle.....	13
INTERFACE DE L'APPLICATION.....	16
Configuration de l'interface.....	16
Fenêtre principale du programme.....	17
Arborescence de la console.....	18
Panneau des tâches.....	20
Panneau des résultats.....	23
Menu contextuel.....	26
LANCEMENT ET ARRET DE L'APPLICATION.....	27
NOTIONS PRINCIPALES.....	28
Serveur d'administration. Groupes d'administration.....	28
Hiérarchie des Serveurs d'administration.....	29
Poste client. Groupe.....	29
Poste de travail de l'administrateur.....	30
Plug-in d'administration de l'application.....	31
Stratégies, paramètres de l'application et tâches.....	31
Corrélation de la stratégie et des paramètres locaux de l'application.....	33
CONCEPTION DU FONCTIONNEMENT DE KASPERSKY ADMINISTRATION KIT.....	34
Déploiement du système de protection antivirus.....	34
Compatibilité avec le système Cisco Network Admission Control (NAC).....	34
Compatibilité avec Microsoft Network Access Protection (NAP).....	35
Création du système de gestion centralisée de la protection antivirus.....	35
Connexion des postes clients au Serveur d'administration.....	36
Connexion sécurisée au Serveur d'administration.....	37
Certificat du Serveur d'administration.....	37
Authentification du Serveur d'administration lors de l'utilisation de l'ordinateur.....	38
Authentification du Serveur lors de la connexion de la Console.....	38
Identification des postes clients sur le Serveur d'administration.....	38
Privilèges d'accès au Serveur d'administration et à ses objets.....	38
ADMINISTRATION DES ORDINATEURS DU RESEAU.....	41
Connexion au Serveur d'administration.....	41
Affectation des droits.....	42
Affichage des informations du réseau d'ordinateurs. Domaines, plages d'adresses IP et groupes Active Directory.....	43
Assistant de configuration initiale.....	45

Création, consultation et modification de la structure des groupes d'administration	45
Groupes	47
Postes clients.....	48
Serveurs d'administration secondaires	51
ADMINISTRATION A DISTANCE DES APPLICATIONS	54
Administration des stratégies.....	54
Paramètres locaux de l'application	58
Administration du fonctionnement de l'application	59
MISE A JOUR DES BASES ET DES MODULES D'APPLICATION.....	65
Téléchargement des mises à jour dans le référentiel du Serveur d'administration.....	65
Diffusion des mises à jour sur les postes clients	68
Récupération des mises à jour par les Serveurs secondaires et leurs postes clients.....	69
Diffusion des mises à jour à l'aide des agents de mise à jour	70
MAINTENANCE	72
Renouvellement de la licence.....	73
Quarantaine et dossier de sauvegarde.....	74
Journaux des événements. Requêtes d'événements	76
Rapports	80
Recherche d'un poste.....	83
Requêtes d'ordinateurs.....	85
Registre des applications.....	87
Contrôle de l'émergence d'épidémies de virus	88
Fichiers avec un traitement différé.....	91
Copie de sauvegarde et restauration des données du Serveur d'administration	91
CONTACTER LE SERVICE DU SUPPORT TECHNIQUE	93
GLOSSAIRE	94
KASPERSKY LAB.....	99
INFORMATIONS SUR LE CODE TIERS	100
Code de programme.....	100
BOOST 1.34.1	100
GSOAP 2.7.0D.....	101
LIBMSPACK 2004-03-08	106
MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86).....	115
MICROSOFT CORE XML SERVICES (MSXML) 6.0.....	115
MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8.....	115
MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3	116
MYSQL C API.....	116
OPENSSL 0.9.8L	116
STLPORT 4.6.2	117
UNZIP 5.52	118
VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES	118
WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2).....	119
ZLIB 1.2.3	119
Autre information	119
INDEX	120

A PROPOS DE CE MANUEL

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

DANS CETTE SECTION

Dans ce document	6
Conventions	7

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

- Sources d'informations complémentaires (à la page [8](#)). La section reprend les informations où vous pouvez obtenir des informations sur l'application, excepté l'ensemble de documents livrés avec l'application.
- Kaspersky Administration Kit (à la page [11](#)). La section contient des informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Administration Kit.
- Interface de l'application (à la page [16](#)). La section décrit les particularités générales de l'interface de l'application de Kaspersky Administration Kit.
- Lancement et arrêt de l'application (à la page [27](#)). La section décrit le mode de lancement de l'application Kaspersky Administration Kit.
- Notions principales (à la page [28](#)). La section contient les définitions détaillées des notions principales, concernant Kaspersky Administration Kit.
- Conception du fonctionnement de Kaspersky Administration Kit (à la page [34](#)). La section décrit les principes de base du fonctionnement de l'application, ainsi que les modes de résolution des tâches particulières.
- Administration des ordinateurs du réseau (à la page [41](#)). La section décrit les particularités d'utilisation de Kaspersky Administration Kit dans le cadre d'administration des ordinateurs du réseau.
- Administration à distance des applications (à la page [54](#)). La section décrit les moyens d'administration des applications à l'aide de Kaspersky Administration Kit.
- Mise à jour des bases et des modules d'application (à la page [65](#)). La section reprend les informations relatives à la mise à jour des bases des applications utilisées lors de l'analyse des objets infectés, à l'installation des mises à jour critiques des modules d'application, ainsi qu'à la mise à jour des versions des applications à l'aide de Kaspersky Administration Kit.
- Maintenance (à la page [72](#)). La section décrit les mesures à réaliser régulièrement sur la maintenance du réseau. Outre cela, cette section décrit la suite des fonctions qui facilitent la maintenance du réseau.
- Contacter le service du Support Technique (à la page [93](#)). La section décrit les règles des appels au service du Support Technique.
- Glossaire. La section reprend les termes utilisés dans ce document.
- Kaspersky Lab (à la page [99](#)). La section reprend les informations relatives à Kaspersky Lab.

- Les informations sur l'utilisation de code tiers. La section reprend les informations relatives au code tiers utilisé dans l'application.
- Index. Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

CONVENTIONS

Les conventions décrites dans le tableau ci-dessous sont utilisées dans le document.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La mise à jour, c'est ...	Les nouveaux termes sont en italique.
ALT+F4	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches.
Activer	Les noms des éléments de l'interface sont en caractères mi-gras : les champs de saisie, les commandes du menu, les boutons.
➡ <i>Pour planifier une tâche, procédez comme suit :</i>	Les phrases d'introduction sont en italique.
help	Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux.
<adresse IP de votre ordinateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable à chaque fois. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS COMPLEMENTAIRES

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

Kaspersky Lab offre de nombreuses sources d'informations sur l'application. Vous pouvez choisir celle qui vous convient le mieux en fonction de l'urgence et de la gravité de la question.

DANS CETTE SECTION

Sources d'informations pour des recherches indépendantes	8
Discussion sur les applications de Kaspersky Lab dans le forum	9
Contacteur le Groupe de rédaction de la documentation pour les utilisateurs	9

SOURCES D'INFORMATIONS POUR DES RECHERCHES INDEPENDANTES

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

- page consacrée à l'application sur le site Web de Kaspersky Lab ;
- page consacrée à l'application sur le site Web du service du Support Technique (dans la Base de connaissances) ;
- système d'aide électronique ;
- documentation.

Page sur le site Web de Kaspersky Lab

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

Cette page fournit des informations générales sur l'application, ses possibilités et ses particularités.

Page sur le site Web du service du Support Technique (Base de connaissances)

http://support.kaspersky.com/fr/remote_adm

Cette page propose des articles publiés par les experts du service du Support Technique.

Ces articles contiennent des informations utiles, des recommandations et les réponses aux questions les plus souvent posées sur l'achat, l'installation et l'utilisation de Kaspersky Administration Kit. Ils sont regroupés par thèmes tels que "Manipulation des fichiers clés", "Mise à jour des bases" ou "Résolution des problèmes". Les articles peuvent répondre à des questions concernant non seulement Kaspersky Administration Kit, mais également d'autres logiciels de Kaspersky Lab. Ils peuvent aussi contenir des informations sur le service du Support Technique dans son ensemble.

Système d'aide électronique

Une aide complète est livrée avec l'application.

Celle-ci propose une description détaillée des fonctions proposées par l'application.

Pour ouvrir l'aide, sélectionnez l'élément **Rubriques de l'aide** dans le menu **Aide** de la console.

Si vous avez des questions sur une fenêtre en particulier de l'application, vous pouvez consulter l'aide contextuelle.

Pour ouvrir l'aide contextuelle, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse, ou sur la touche **F1** du clavier.

Documentation

La documentation qui accompagne cette application contient la majorité des informations indispensables pour son utilisation. Elle contient des documents suivants :

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

Ces documents sont en format PDF et sont livrés avec le Kaspersky Administration Kit.

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

Les informations sur l'interface de l'application d'administration (API) Kaspersky Administration Kit s'affichent dans le fichier klakaut.chm situé dans le dossier d'installation de l'application.

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB DANS LE FORUM

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

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

CONTACTER LE GROUPE DE REDACTION DE LA DOCUMENTATION POUR LES UTILISATEURS

Si vous avez des questions concernant la documentation, ou vous y avez trouvé une erreur, ou vous voulez laisser un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs.

En passant au lien **Envoyer des commentaires** situé en haut à droite de la fenêtre de l'aide, vous pouvez ouvrir la fenêtre du client de messagerie utilisé par défaut sur votre ordinateur. L'adresse du groupe de rédaction de la documentation – docfeedback@kaspersky.com sera indiquée dans la fenêtre ouverte, et dans le sujet du message – "Kaspersky Help Feedback: Kaspersky Administration Kit". Sans modifier le sujet du message, écrivez votre commentaire et envoyez le message.

KASPERSKY ADMINISTRATION KIT

Le logiciel est proposé gratuitement avec toutes les applications de Kaspersky Lab de la suite Kaspersky Open Space Security (version vendue en boîte). Il peut également être téléchargé depuis le site de Kaspersky Lab (<http://www.kaspersky.fr>).

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

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

A l'aide de cette application, l'administrateur peut :

- Former une structure des groupes d'administration qui assure la protection antivirus de la société. Les groupes d'administration permettent d'administrer la sélection d'ordinateurs comme un tout unique.
- Effectuer l'installation à distance et la désinstallation des applications de la protection antivirus de l'entreprise.
- Effectuer l'administration à distance centralisée des applications de la protection antivirus.
- Recevoir et diffuser de façon centralisée sur les ordinateurs les mises à jour des bases et des modules de programme des applications antivirales.
- Recevoir les notifications sur les événements critiques dans le fonctionnement des applications de la protection antivirus.
- Recevoir les statistiques et les rapports de fonctionnement des applications de la protection antivirus.
- Administrer les licences de toutes les applications antivirales installées.
- Travailler de façon centralisée avec les objets, placés en quarantaine ou dans le dossier de sauvegarde par les applications antivirales, aussi qu'avec les objets dont le traitement est différé.
- Travailler avec les applications d'autres fabricants dans le réseau.

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

- **Serveur d'administration** : est un entrepôt centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau local de la société et un outil efficace de gestion de ces applications.
- **Agent d'administration** : coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant est unique pour toutes les applications Windows de la gamme des produits Kaspersky Open Space Security. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky Lab fonctionnant sur Novell ou Unix.
- **Console d'administration** : fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur et de l'Agent. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console).

DANS CETTE SECTION

Nouveautés	12
Configuration logicielle et matérielle	13

NOUVEAUTES

Modifications apportées dans la version 8.0 de Kaspersky Administration Kit par rapport à la version 6.0 de Kaspersky Administration Kit :

- Mode d'installation simplifiée.
- Possibilité d'afficher plusieurs comptes dans la tâche d'installation à distance.
- Le fichier de distribution Microsoft SQL Express 2005 fait partie de l'application : son installation s'effectue automatiquement dans le cas d'une sélection de l'installation standard.
- Ajout de la possibilité de surveillance SNMP des paramètres généraux de la protection antivirus du réseau de l'entreprise.
- La possibilité de création du paquet autonome d'installation pour les applications de Kaspersky Lab est ajoutée.
- L'interface utilisateur de l'application est remaniée considérablement : panneau des résultats, types de rapports, barres d'informations (cf. section "Fenêtre principale de l'application" à la page [17](#)).
- Le mécanisme de collecte des informations sur les applications installées sur les postes clients est ajouté (registre des applications).
- Le système des privilèges d'accès est remanié et élargi.
- Ajout du support des technologies Microsoft NAP.
- Ajout de la possibilité de permutation des clients nomades entre les Serveurs d'administration.
- Elargissement des critères de permutation des clients entre les stratégies mobiles et normales.
- Les possibilités de déplacement automatique des ordinateurs dans les groupes d'administration sont élargies.
- La possibilité de création des groupes d'administration à la base de la structure Active Directory est ajoutée.
- Les nouveaux rapports sont ajoutés, maintenant il est possible d'ajouter vos propres systèmes de compte, les informations affichées dans les rapports sont élargies.
- Ajout de la possibilité d'exporter les rapports dans les fichiers en format PDF et XML (Microsoft Excel).
- Ajout de la possibilité de collecter des données détaillées lors d'une construction de rapports généraux.
- Réalisation du mécanisme de mise en cache des informations pour la construction des rapports généraux, qui contiennent les données des Serveurs d'administration secondaires.
- Le support de deux ensembles des colonnes dans la Console d'administration est ajouté, ainsi que l'ensemble des colonnes est élargie (cf. page [23](#)).
- Les nouvelles colonnes pour la liste des ordinateurs sont ajoutées : "Redémarrage", "Description de l'état", "Version de l'Agent d'administration", "Version de la protection", "Version des bases", "Heure de l'activation".
- Ajout de nouveaux critères, à l'aide desquels les états des ordinateurs sont formés.
- Des nouvelles sélections d'ordinateurs, formés par défaut, sont ajoutées ; la possibilité de création des sélections d'ordinateurs à l'aide des données des Serveurs d'administration secondaires est ajoutée.
- La possibilité de gestion de la liste des notes de l'administrateur est ajoutée.
- La possibilité de visionnage des sessions et des contacts d'utilisateurs disponibles sur l'ordinateur est ajoutée.

- L'interface graphique pour l'utilitaire de sauvegarde et de restauration des données est ajoutée.
- Les fichiers des stratégies et des tâches de groupes se propagent à l'aide d'une diffusion d'adresses IP multiples.
- Le paramètre Wake On Lan est en accès libre pour les postes clients situés dans les sous-réseaux et différents du sous-réseau du Serveur d'administration, et dans le cas du lancement manuel de la tâche.
- Vous pouvez définir les paramètres de redémarrage pour les postes clients dans les configurations de la tâche d'installation à distance.
- Le mécanisme de restriction du nombre des notifications envoyées en unité de temps est modifié : maintenant, les restrictions sont comptées indépendamment pour chaque type d'événements.
- La possibilité de recherche de groupes et de Serveurs d'administration secondaires selon la hiérarchie des Serveurs est ajoutée.
- Elargissement des statistiques des agents de mises à jour.
- La tâche de suppression des applications étrangères permet maintenant de supprimer plusieurs applications à la fois.
- Elaboration de l'utilitaire de préparation de l'installation à distance des ordinateurs.
- Réalisation du mécanisme d'obtention des mises à jour nécessaires à l'application directement après la création de son paquet d'installation.
- Lors de l'obtention des mises à jour, les applications déjà connectées aux Serveurs d'administration secondaires sont prises en compte.
- Instauration du classement des erreurs possibles du sous-système de l'installation à distance de l'application, ajout des conseils de résolution des problèmes types.
- Ajout du mécanisme d'application automatique des mises à jour des modules pour les composants du système d'administration.

CONFIGURATION LOGICIELLE ET MATERIELLE

Serveur d'administration

- Configuration logicielle :
 - Microsoft Data Access Components (MDAC) de version 2.8 ou supérieure ou Windows DAC 6.0.
 - Système de gestion des bases de données : Microsoft SQL Express 2005, Microsoft SQL Express 2008 R2, Microsoft SQL Express 2008 R2 ; Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 ou MySQL Enterprise.
 - Microsoft Windows Server 2003 et supérieur ; Microsoft Windows Server 2003 x64 et supérieur ; Microsoft Windows Server 2008 ; Microsoft Windows Server 2008 déployé en mode Server Core ; Microsoft Windows Server 2008 x64 avec Service Pack 1 et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows Server 2008 R2 ; Microsoft Windows Server 2008 R2 déployé en mode Server Core ; Microsoft Windows XP Professional avec Service Pack 2 et supérieur ; Microsoft Windows XP Professional x64 et supérieur ; Microsoft Windows Vista x64 avec Service Pack 1 et supérieur, Microsoft Windows Vista x64 avec Service Pack 1 et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows 7.
- Configuration matérielle :

- Processeur avec 1 GHz ou plus ;
- 512 Mo de mémoire vive ;
- 1 Go d'espace disque disponible.

Console d'administration Kaspersky

- Configuration logicielle :
 - Système d'exploitation Windows.

La version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration.
 - Microsoft Management Console version 2.0 et supérieure.
 - Lors du fonctionnement sous Microsoft Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 ou Windows Vista : la présence du navigateur installé Microsoft Internet Explorer 7.0 ou suivant.
 - L'utilisation sous Microsoft Windows 7 requiert Microsoft Internet Explorer 8.0 ou suivant.
- Configuration matérielle :
 - Pendant le fonctionnement sous le système d'exploitation 32 bits :
 - Processeur avec 1 GHz ou plus ;
 - 512 Mo de mémoire vive ;
 - 1 Go d'espace disque disponible.
 - Pendant le fonctionnement sous le système d'exploitation 64 bits :
 - Processeur avec 1.4 GHz ou plus ;
 - 512 Mo de mémoire vive ;
 - 1 Go d'espace disque disponible.

Agent d'administration et agent de mises à jour

- Configuration logicielle :
 - Système d'exploitation :
 - Windows.

La version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration.
 - Linux.
 - Mac OS.
- Configuration matérielle :
 - Pendant le fonctionnement sous le système d'exploitation 32 bits :

- Processeur avec 1 GHz ou plus ;
- 512 Mo de mémoire vive ;
- Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.
- Pendant le fonctionnement sous le système d'exploitation 64 bits :
 - Processeur avec 1.4 GHz ou plus ;
 - 512 Mo de mémoire vive ;
 - Espace disque disponible : 32 Mo pour l'Agent d'administration, 500 Mo pour l'agent de mises à jour.

INTERFACE DE L'APPLICATION

La consultation, la création, la modification et la configuration des groupes d'administration, l'administration centralisée du fonctionnement de toutes les applications de Kaspersky Lab installées sur les postes clients sont exécutées depuis le poste administrateur. La Console d'administration assure l'interface d'administration. Elle représente un outil autonome centralisé, intégré dans Microsoft Management Console (MMC), c'est pourquoi l'interface Kaspersky Administration Kit est standard pour MMC.

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

Pour travailler localement avec les postes clients, l'application prévoit la possibilité d'installer une connexion à distance avec l'ordinateur par la Console d'administration à l'aide de l'application standard Microsoft Windows **Connexion en cours au poste de travail distant**.

Afin d'utiliser cette possibilité, il est nécessaire d'autoriser la connexion à distance au poste de travail sur le poste client.

DANS CETTE SECTION

Configuration de l'interface.....	16
Fenêtre principale du programme	17
Arborescence de la console	18
Panneau des tâches	20
Panneau des résultats.....	23
Menu contextuel.....	26

CONFIGURATION DE L'INTERFACE

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

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

1. Dans l'arborescence de la console, passez à l'entrée du Serveur d'administration.
2. Passez au menu **Vue** → **Configuration de l'interface**. Cela entraîne l'ouverture de la fenêtre du même nom (cf. ill. ci-après).

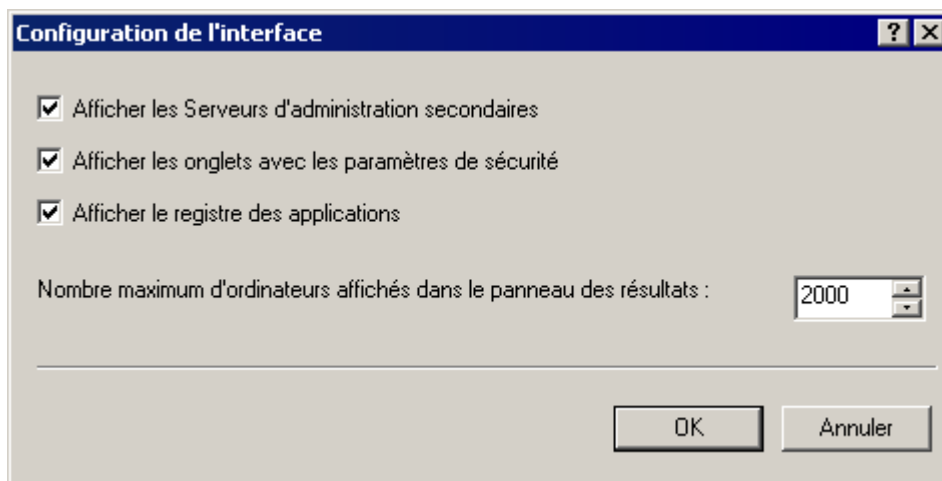


Illustration 1. Affichage des propriétés du groupe. Fenêtre **Configuration de l'interface**

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

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

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

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

FENETRE PRINCIPALE DU PROGRAMME

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

Le menu assure la gestion des fenêtres et offre l'accès au système d'informations. Le point du menu **Action** reprend les commandes du menu contextuel pour l'objet de l'arborescence de la console.

L'ensemble des boutons de la barre d'outils assure un accès direct à certains points du menu principal. Le contenu de la barre d'outils change selon la section actuelle ou pour le dossier de l'arborescence de la console.

La barre de consultation reflète l'étendue des noms de **Kaspersky Administration Kit** dans l'arborescence de la console (cf. section "Arborescence de la console" à la page [18](#)).

La zone d'informations du menu contextuel peut être représentée par la barre des tâches, la barre des résultats ou par leurs combinaisons. Pour certains dossiers de l'arborescence de la console, la zone d'informations a deux types de présentations : étendue et standard. Passer d'un type à l'autre est accessible par les onglets du même nom.

La barre des tâches (cf. page [20](#)) contient un ou plusieurs onglets avec des liens d'accès rapide aux opérations principales, envisagées pour l'objet sélectionné dans l'arborescence de la console.

La barre des résultats (cf. page 23) représente la liste des éléments de l'objet sélectionné dans l'arborescence de la console ou l'ensemble des zones d'information. Cela peut être la liste des ordinateurs dans les groupes, la liste des rapports, des requêtes d'événements ou d'ordinateurs.

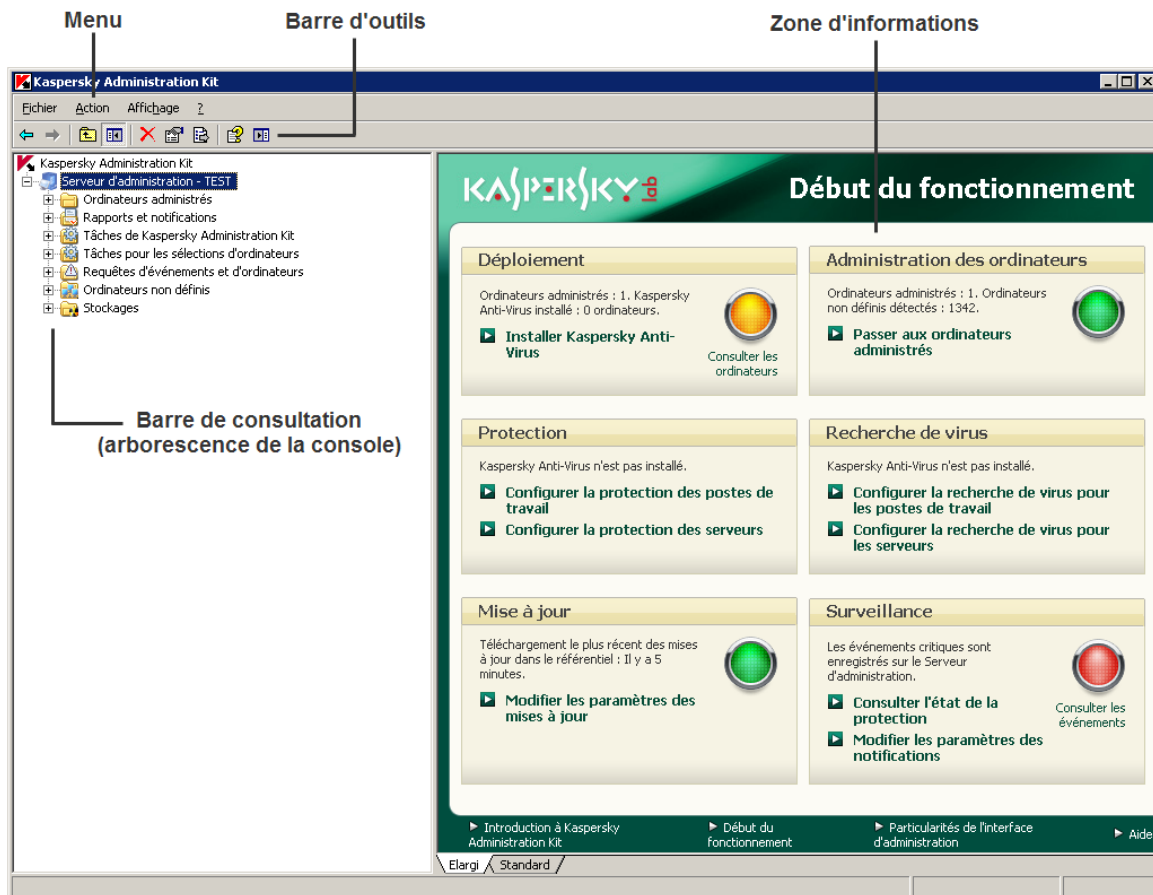


Illustration 2. Fenêtre principale de Kaspersky Administration Kit

ARBORESCENCE DE LA CONSOLE

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

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

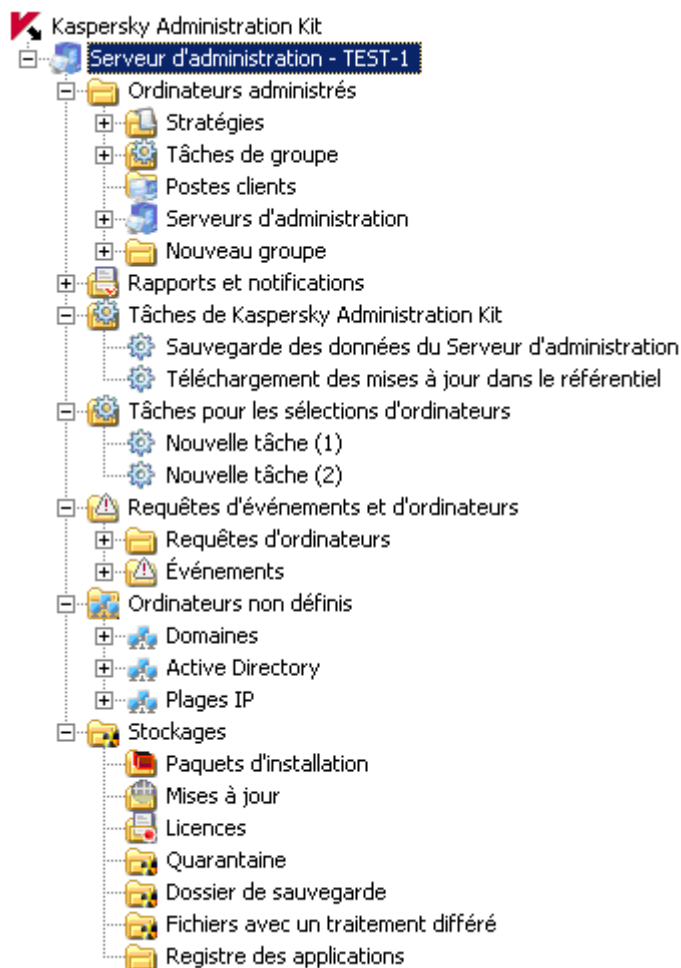


Illustration 3. Arborescence de la console

La section **Serveur d'administration : <Nom de l'ordinateur>** est un conteneur et reflète la structure du Serveur d'administration indiqué. Le conteneur **Serveur d'administration – <Nom de l'ordinateur>** inclut les dossiers suivants :

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

Le dossier **Ordinateurs administrés** est conçu pour conserver, refléter, configurer et modifier la structure des groupes d'administration, les stratégies de groupe et les tâches de groupe. Ce dossier reprend les sous-dossiers **Stratégies**, **Tâches de groupe**, **Postes clients** et **Serveurs d'administration**. Exactement la même structure des dossiers est créée pour chaque groupe d'administration particulier dans l'arborescence de la console.

Le dossier **Tâches de Kaspersky Administration Kit** contient l'ensemble de tâches, définies pour le Serveur d'administration. Il existe trois types de tâches du Serveur d'administration : l'envoi automatique des rapports, la sauvegarde et le téléchargement de la mise à jour par le Serveur d'administration.

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

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

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

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

Le dossier **Ordinateurs non définis** est conçu pour afficher le réseau d'ordinateurs où le Serveur d'administration est installé. Le Serveur d'administration obtient les informations relatives à la structure du réseau et aux ordinateurs qui en font partie lors des requêtes fréquentes adressées au réseau Windows, aux sous-réseaux IP ou Active Directory créés dans le réseau informatique de l'entreprise. Les résultats des sondages sont affichés dans la barre des résultats des sous-dossiers correspondants : **Domaines**, **Plages IP** et **Active Directory**.

Le dossier **Stockages** permet de manipuler les objets utilisés pour la surveillance de l'état des postes client et les entretenir. Les données suivantes le composent :

- **Paquets d'installation** : contient la liste des paquets d'installation qui peuvent être utilisés pour l'installation à distance des applications sur les postes clients.
- **Mises à jour** : contient la liste des mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les postes client.
- **Licences** : contient la liste des licences installées sur les postes clients.
- **Quarantaine** : contient la liste des objets placés par les applications antivirus dans les dossiers de quarantaine des postes client.
- **Dossier de sauvegarde** : contient la liste des copies de sauvegarde des objets placés dans le dossier de sauvegarde.
- **Fichiers avec un traitement différé** : contient la liste des fichiers pour lesquels les applications antivirus ont décidé le traitement ultérieur.
- **Registre des applications** : contient la liste des applications installées sur les postes clients sur lesquels l'Agent d'administration est installé.

PANNEAU DES TACHES

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

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

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

Il peut exister plusieurs panneaux des tâches pour une section ou pour un dossier. Ils se présentent alors sous la forme d'onglets, dont le titre figure dans la partie supérieure de la zone d'informations.

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

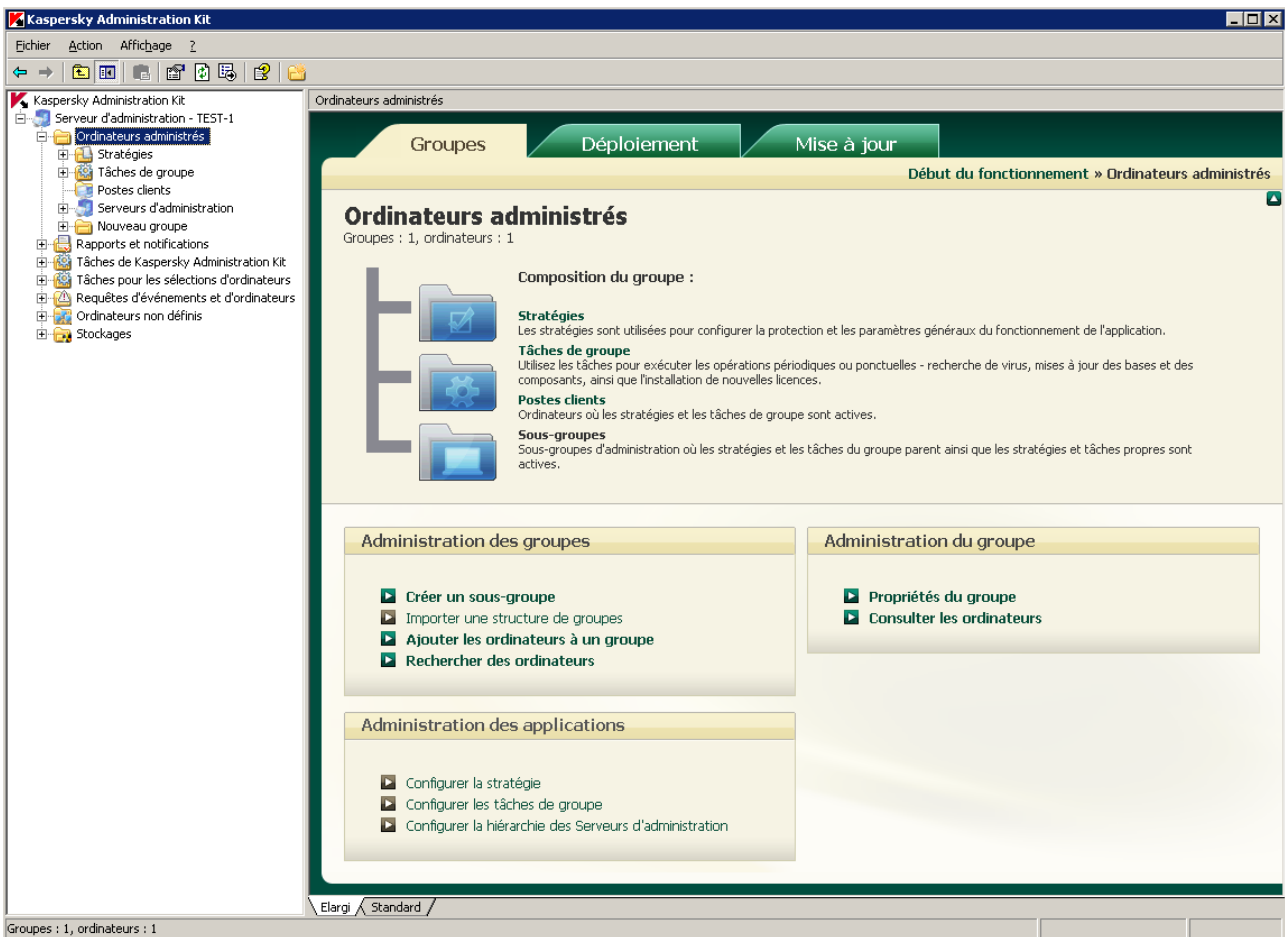


Illustration 4. Panneau des tâches

Pour certains objets de l'arborescence de la console, les informations récapitulatives sur l'objet peuvent être affichées dans la barre des tâches. Par exemple, les données statistiques lors de la sélection du dossier Rapports et notifications (cf. ill. ci-après). Dans ce cas, le panneau des tâches remplit la même fonction que le panneau des résultats (cf. page 23).

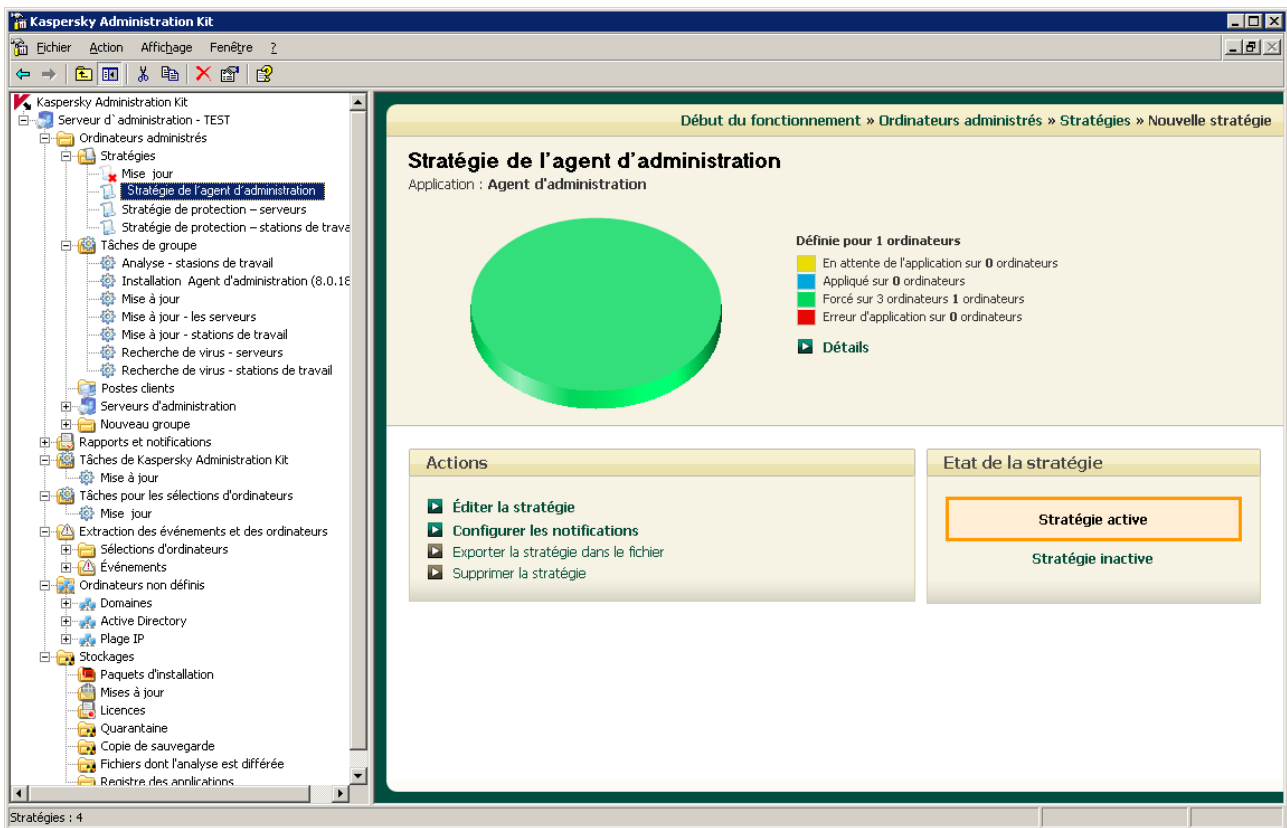


Illustration 5. Panneau des tâches remplissant la fonction du panneau des résultats

Pour certains dossiers qui ne possèdent pas la barre élargie des tâches, une barre standard des tâches est prévue. Cette barre est représentée par deux onglets en bas de la barre : <Nom de dossier> et Standard. En cas de sélection de l'onglet <Nom de dossier>, l'ensemble de liens est présenté dans la partie gauche de la barre (cf. ill. ci-après). Tout comme les liens du panneau des tâches étendu, les liens du panneau des tâches standard permettent d'exécuter les opérations, de consulter les propriétés d'un dossier ou de les modifier.

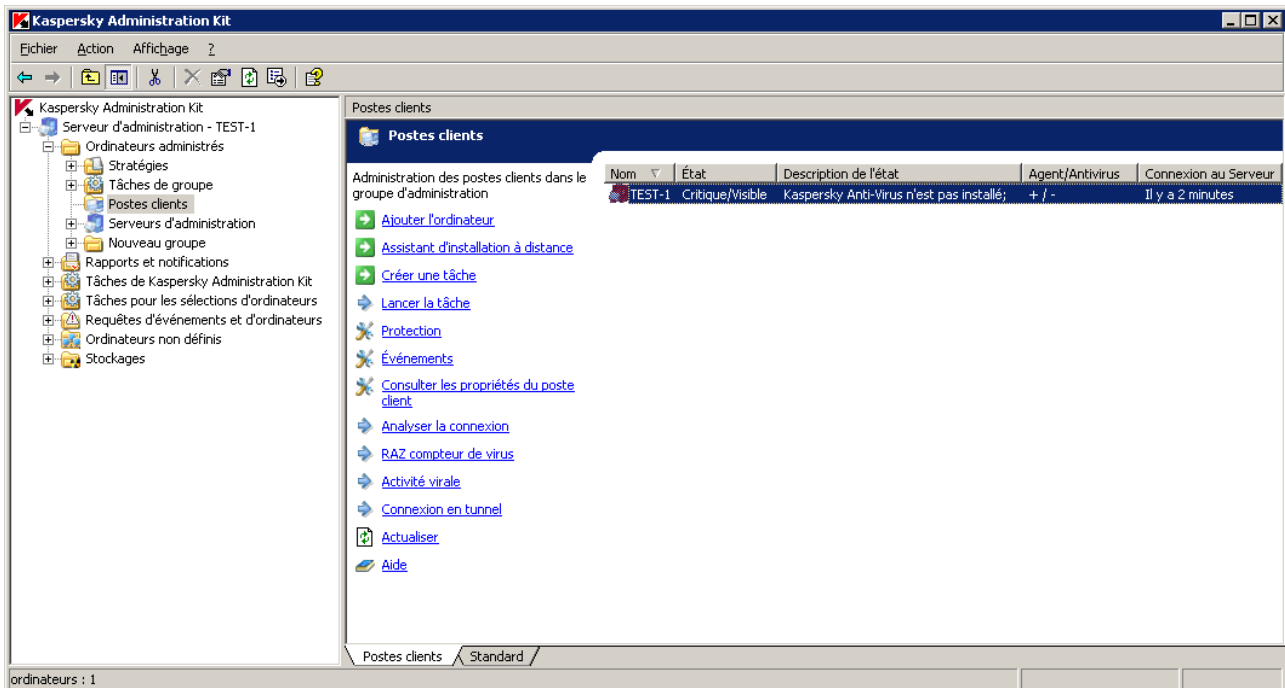


Illustration 6. Panneau des tâches standard pour le dossier **Postes clients**

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

PANNEAU DES RESULTATS

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

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

Le panneau élargi des résultats est prévu pour les rapports créés. Il contient les diagrammes, ainsi que les informations récapitulatives et détaillées présentées sous forme des tableaux (cf. ill. ci-après).

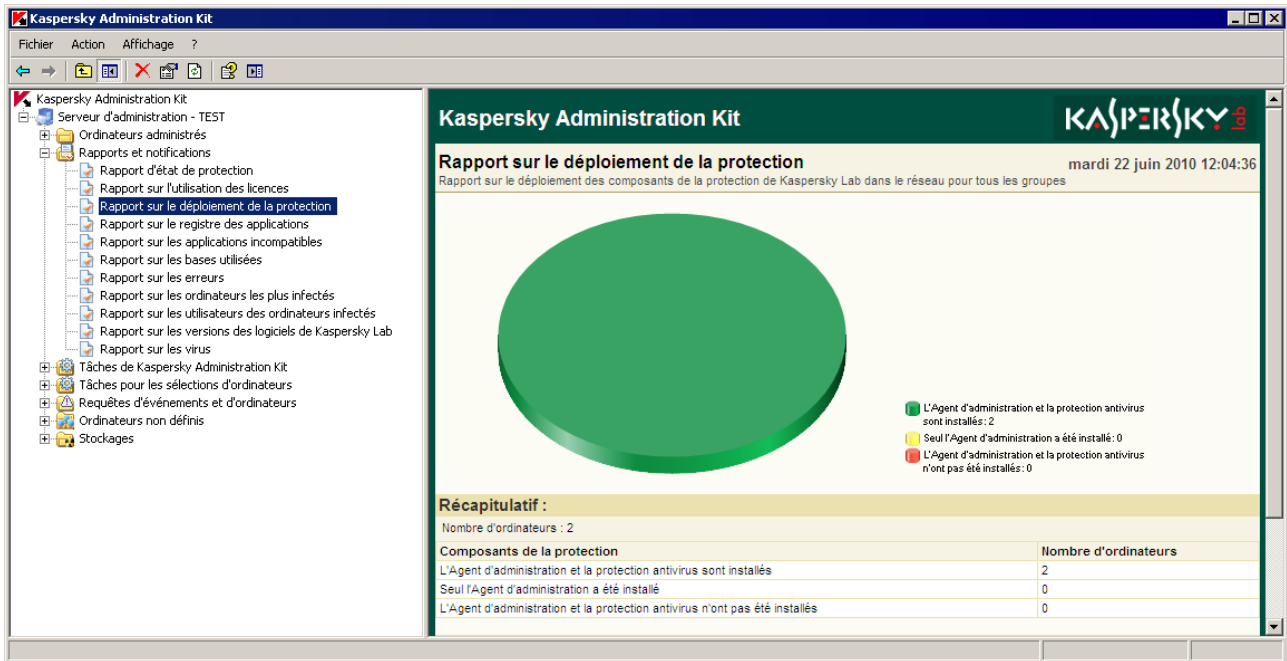







Illustration 7. Panneau des résultats. Rapport de déploiement

Le panneau des résultats élargi peut être composé de plusieurs pages (cf. ill. ci-après), dont chacune d'entre elles contient l'ensemble des panneaux d'informations.

Les données des panneaux d'informations peuvent être représentées sous forme de tableaux ou de diagrammes (camemberts ou barres). L'administrateur peut modifier la sélection des pages et des panneaux d'information, ainsi que la composition des données et le mode de représentation :

- Pour modifier la liste de pages, cliquez sur le bouton  situé dans le coin supérieur droit de cet onglet.
- Vous pouvez configurer la composition de la page à l'aide du bouton  situé à côté du nom de la page et définir les paramètres requis dans la fenêtre qui s'ouvre.
- Pour définir les paramètres de représentation d'un panneau d'information en particulier, cliquez sur le bouton  situé à côté du nom du panneau.
- Il est possible de déployer et de réduire les panneaux à l'aide des boutons  et .

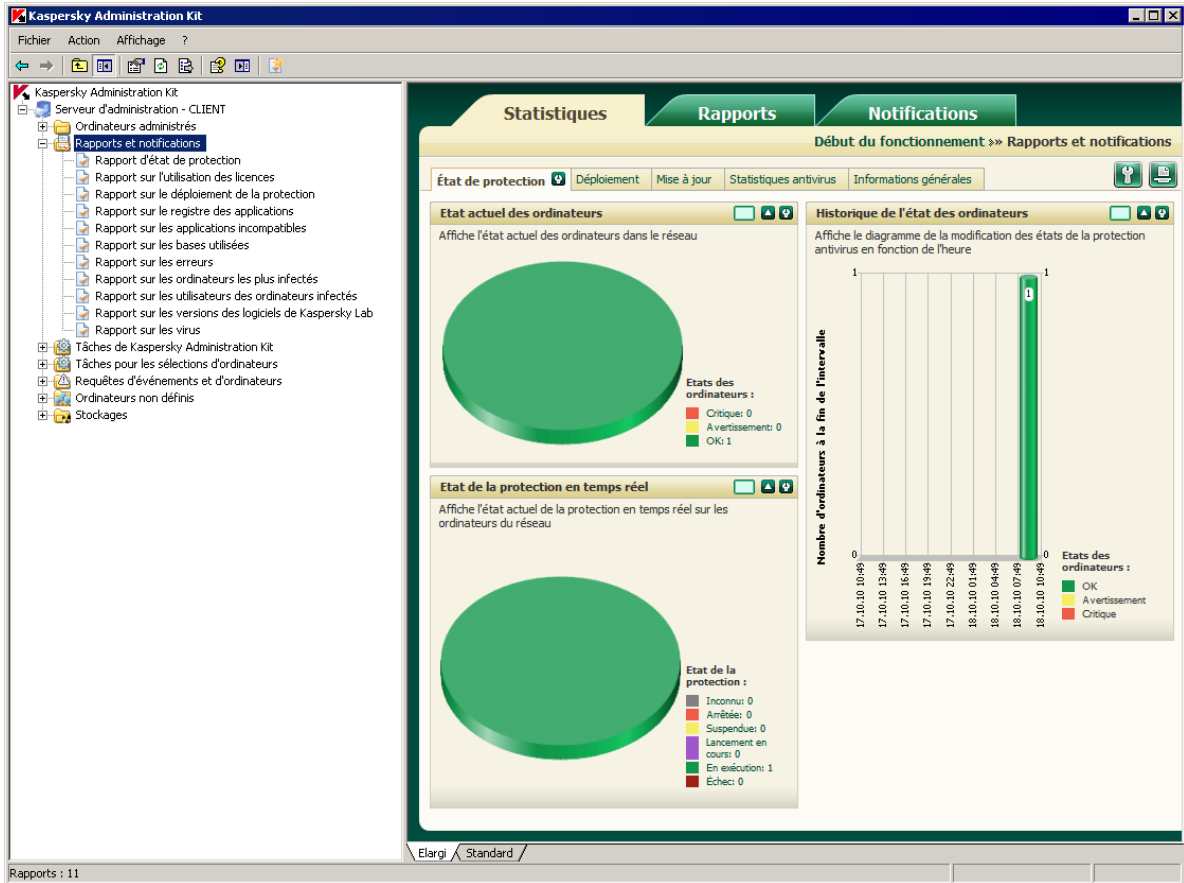


Illustration 8. Panneau des résultats contenant des volets d'informations

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

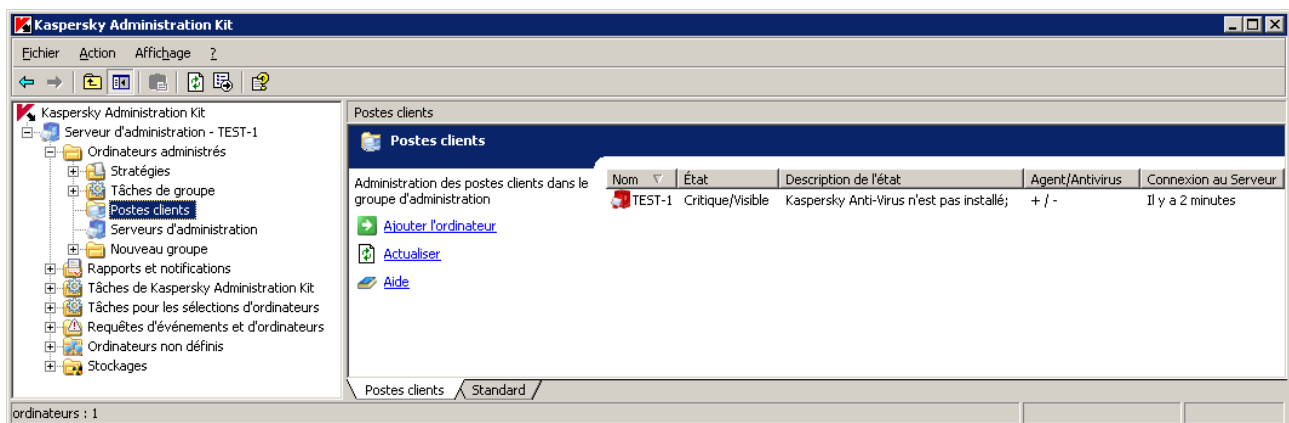



Illustration 9. Panneau des résultats standard

Dans Kaspersky Administration Kit l'information dans le panneau des résultats (par exemple : les états des ordinateurs, statistiques, journaux) n'est pas actualisée automatiquement. Vous pouvez actualiser les données dans le panneau des résultats en cliquant sur la touche **F5**, en sélectionnant dans le menu contextuel le point **Actualiser** ou en cliquant sur

 situé dans la barre d'outils.

MENU CONTEXTUEL

Dans l'arborescence de la console, chaque catégorie d'objets de l'espace des noms **Kaspersky Administration Kit** possède son propre menu contextuel. Outre les commandes standards du menu contextuel de MMC, on retrouve les commandes qui permettent de réaliser les opérations sur cet objet. La liste des objets et des commandes supplémentaires du menu contextuel qui peuvent être exécutées est reprise dans l'aide.

Le panneau des résultats de chaque élément de l'objet sélectionné dans l'arborescence possède également un menu contextuel dont les commandes permettent la réalisation d'opérations sur les éléments. Les principaux types d'éléments et les commandes supplémentaires associées figurent dans l'aide.

LANCEMENT ET ARRET DE L'APPLICATION

Kaspersky Administration Kit est lancé automatiquement lors du lancement du Serveur d'administration.

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

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

NOTIONS PRINCIPALES

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

DANS CETTE SECTION

Serveur d'administration. Groupes d'administration	28
Hiérarchie des Serveurs d'administration	29
Poste client. Groupe.....	29
Poste de travail de l'administrateur	30
Plug-in d'administration de l'application.....	31
Stratégies, paramètres de l'application et tâches.....	31
Corrélation de la stratégie et des paramètres locaux de l'application.....	33

SERVEUR D'ADMINISTRATION. GROUPES D'ADMINISTRATION

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

On appellera les ordinateurs sur lesquels le composant Serveur d'administration est installé les Serveurs d'administration.

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

Le Serveur d'administration s'installe sur l'ordinateur en qualité de service avec la sélection d'attributs suivante :

- sous le nom de Kaspersky Administration Server ;
- avec lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte **Système local** ou le compte utilisateur selon la sélection effectuée lors de l'installation du composant.

Les fonctions du Serveur d'administration, notamment le composant Serveur d'administration installé, se composent des points suivants :

- sauvegarde de la structure des groupes d'administration ;
- sauvegarde de la copie des informations de configuration des postes clients ;
- organisation des référentiels de distribution des applications de Kaspersky Lab ;
- installation à distance des applications sur les ordinateurs et leur désinstallation ;

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

HIERARCHIE DES SERVEURS D'ADMINISTRATION

Les Serveurs d'administration peuvent développer une hiérarchie du type "serveur principal – serveur secondaire". Chaque Serveur d'administration peut avoir plusieurs Serveurs secondaires comme sur un seul niveau de hiérarchie, ainsi que sur des niveaux imbriqués. Le niveau d'intégration des Serveurs secondaires n'est pas limité. De plus, les postes clients de tous les Serveurs secondaires feront partie des groupes d'administration du Serveur principal. De cette façon, les participants du réseau informatique indépendants peuvent être administrés par différents Serveurs d'administration qui, à leur tour, sont administrés par le Serveur principal.

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

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

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

POSTE CLIENT. GROUPE

L'interaction entre le Serveur d'administration et les ordinateurs s'opère par l'Agent d'administration. Par cela, on entend les points suivants :

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

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

Ce composant s'installe sur l'ordinateur en qualité de service avec la sélection d'attributs suivante :

- sous le nom de Kaspersky Network Agent ;
- avec lancement automatique lors du démarrage du système d'exploitation ;
- avec le compte **Système local**.

Le plug-in pour le fonctionnement avec Cisco NAC s'installe sur l'ordinateur conjointement avec l'Agent d'administration. Ce plug-in fonctionne dans le cas où l'application Cisco Trust Agent est installée sur l'ordinateur. Les paramètres de collaboration avec Cisco NAC sont indiqués dans les propriétés du Serveur d'administration.

En collaboration avec Cisco NAC, le Serveur d'administration joue le rôle d'un serveur standard des stratégies (Posture Validation Server), que l'administrateur peut utiliser pour autoriser ou interdire l'accès à un ordinateur du réseau (en fonction des conditions de la protection antivirus).

Nous appellerons *client du serveur d'administration* (ou tout simplement *poste client*) l'ordinateur, le serveur ou le poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky Lab.

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

Groupe d'administration (ci-après *groupe*) : c'est l'ensemble des postes clients, réunis selon un critère dans le but d'administrer les ordinateurs en tant que groupe unique. Pour tous les postes clients dans le groupe, les points suivants sont installés :

- les paramètres uniques de fonctionnement des applications, à l'aide *des stratégies de groupe* ;
- un mode unique de fonctionnement des applications, grâce à la création de tâches de groupe (des fonctions de l'application) avec l'ensemble établi des paramètres (par exemple : création et installation du paquet *d'installation* unique, mise à jour des bases et des modules d'applications, analyse de l'ordinateur à la demande et protection en temps réel).

Le poste client peut être inclus dans un seul groupe d'administration.

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

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

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

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

Le poste administrateur n'est pas un objet du groupe d'administration, mais toutefois, il peut être inclus dans le groupe en tant que poste client. Aucune restriction n'est imposée sur le nombre de postes administrateurs. Les postes

administrateurs peuvent coïncider pour différents Serveurs d'administration, chacun peut administrer les groupes d'administration de n'importe quel Serveur d'administration dans la structure du réseau de l'entreprise.

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

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

L'interface pour gérer le fonctionnement de l'application concrète par la Console d'administration est présentée par un composant spécialisé : *plug-in d'administration de l'application*. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Administration Kit. Le plug-in d'administration est spécifique à chaque application. Il est installé sur le poste administrateur et représente l'ensemble de boîtes de dialogues (interface) pour créer et rédiger les points suivants :

- les stratégies de l'application ;
- les paramètres de l'application ;
- les paramètres des tâches réalisées par l'application.

Le plug-in d'administration assure les points suivants :

- la fourniture des renseignements sur les tâches réalisées par l'application ;
- la fourniture des renseignements sur les événements générés par l'application ;
- la prestation des fonctions pour la Console d'administration de l'affichage des informations reçues des postes clients sur les événements et les statistiques de fonctionnement de l'application.

STRATEGIES, PARAMETRES DE L'APPLICATION ET TACHES

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

L'ensemble des paramètres de fonctionnement de l'application lors de son exécution correspond à une tâche. L'ensemble des paramètres de fonctionnement de l'application, unique pour tous les types de ses tâches, compose les *paramètres de l'application*. Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches, constituent les *paramètres de la tâche*. Les paramètres de l'application et les paramètres de la tâche ne se croisent pas.

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

Nous appellerons *paramètres locaux de l'application* les paramètres de l'application qui sont définis pour le poste client particulier par l'interface locale, ou à distance par la Console d'administration.

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

La stratégie : il s'agit de l'ensemble des paramètres de fonctionnement de l'application dans le groupe. La stratégie ne définit pas tous les paramètres de l'application.

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

Chaque paramètre, présenté dans la stratégie, a pour attribut : le "cadenas" qui affiche, s'il est interdit de modifier le paramètre dans les stratégies du niveau intégré de la hiérarchie (pour les groupes intégrés et pour les Serveurs d'administration secondaires). Il en est de même pour les paramètres des tâches et les paramètres locaux de l'application. Si dans la stratégie, le "cadenas" est placé pour le paramètre, il sera impossible de prédéfinir sa valeur (cf. section "Corrélation de stratégie et des paramètres locaux de l'application" à la page [33](#)). La case décochée **Hériter des paramètres de la stratégie de niveau supérieur** annule l'action du "cadenas" pour les stratégies héritées.

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

Il y a la possibilité d'activer la stratégie qui n'est pas active, selon l'événement. Cela permet, par exemple, d'installer des paramètres plus stricts de la protection antivirus dans les périodes de l'épidémie de virus.

Vous pouvez aussi former la stratégie pour les utilisateurs nomades. Elle va entrer en vigueur lorsque l'ordinateur est déconnecté du réseau de l'entreprise.

Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre pour l'application peut être créée dans chaque groupe.

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

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

- *la tâche de groupe* : tâche qui définit les paramètres de fonctionnement de l'application installés sur les ordinateurs et inclus dans le groupe d'administration ;
- *la tâche locale* : tâche pour un ordinateur individuel ;
- *la tâche pour la sélection d'ordinateurs* : tâche pour la sélection aléatoire d'ordinateurs, qu'ils soient ou non compris dans le groupe d'administration ;
- *la tâche de Kaspersky Administration Kit* : tâche qui est définie directement pour le Serveur d'administration.

Une tâche de groupe peut être définie pour un groupe, même si l'application de Kaspersky Lab n'est pas installée sur tous les postes clients du groupe. Dans ce cas, la tâche de groupe s'exécute uniquement pour les ordinateurs sur lesquels l'application est installée.

Les sous-groupes et les Serveurs d'administration secondaires héritent des tâches de groupe des niveaux plus élevés de la hiérarchie. La tâche, définie pour le groupe, sera exécutée non seulement sur les postes clients inclus dans ce groupe, mais aussi sur les postes clients inclus dans les sous-groupes et dans les Serveurs d'administration secondaires aux niveaux suivants de la hiérarchie.

Les tâches, créées pour le poste client de manière locale, seront exécutées uniquement pour cet ordinateur. Lors de la synchronisation du client avec le Serveur d'administration, les tâches locales seront ajoutées à la liste des tâches formées pour le poste client.

Puisque les paramètres de fonctionnement de l'application sont définis par la stratégie, les paramètres qui ne sont pas interdits peuvent être redéfinis, ainsi que les paramètres qui peuvent être installés uniquement pour l'exemplaire concret de la tâche. Par exemple, pour la tâche d'analyse du disque, il s'agit du nom du disque, des masques des fichiers analysés, etc.

La tâche peut être lancée automatiquement (selon la programmation) ou manuellement. Les résultats de l'exécution de la tâche sont enregistrés sur le Serveur d'administration et de manière locale. L'administrateur peut recevoir des notifications sur l'exécution de telle ou telle tâche, ainsi que parcourir les rapports détaillés.

Les informations sur les stratégies, les paramètres de l'application, les paramètres des tâches pour les sélections d'ordinateurs et les tâches de groupe sont enregistrées sur le Serveur et diffusées sur les postes clients lors de la synchronisation. Avec cela, les modifications locales (réalisées sur les postes clients et autorisées par la stratégie) sont à leur tour enregistrées dans les données du Serveur d'administration. En outre, la liste des applications qui fonctionnent sur le client est actualisée, ainsi que leur état et la liste des tâches formées.

CORRELATION DE LA STRATEGIE ET DES PARAMETRES LOCAUX DE L'APPLICATION

A l'aide des stratégies, les mêmes valeurs des paramètres de fonctionnement de l'application peuvent être installées pour tous les ordinateurs inclus dans le groupe.

Vous pouvez redéfinir les valeurs des paramètres définies par la stratégie pour les ordinateurs individuels dans le groupe à l'aide des paramètres locaux de l'application. Avec cela, vous pouvez établir les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie (le paramètre n'est pas fermé par le "cadenas").

La valeur utilisée par l'application sur le poste client (cf. ill. ci-dessous) est définie par la présence du "cadenas" dans le paramètre de la stratégie :

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

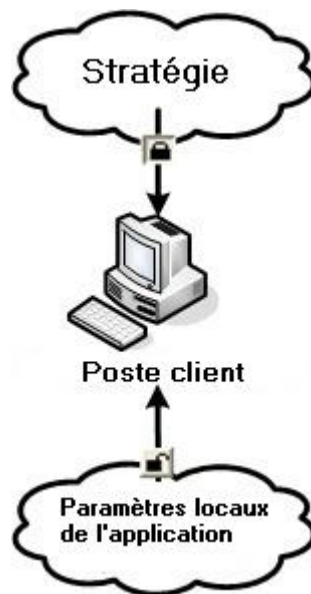


Illustration 10. Stratégie et paramètres locaux de l'application

De cette façon, lorsque la tâche est en exécution sur un poste client, l'application utilise les paramètres définis selon deux manières différentes :

- par les paramètres de la tâche et les paramètres locaux de l'application, si l'interdiction de modifier le paramètre n'était pas établie dans la stratégie ;
- par la stratégie du groupe, si l'interdiction de modifier le paramètre était établie dans la stratégie.

Les paramètres locaux de l'application sont modifiés après la première utilisation de la stratégie conformément aux paramètres de la stratégie.

CONCEPTION DU FONCTIONNEMENT DE KASPERSKY ADMINISTRATION KIT

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

DANS CETTE SECTION

Déploiement du système de protection antivirus	34
Compatibilité avec le système Cisco Network Admission Control (NAC)	34
Compatibilité avec Microsoft Network Access Protection (NAP)	35
Création du système de gestion centralisée de la protection antivirus	35
Connexion des postes clients au Serveur d'administration	36
Connexion sécurisée au Serveur d'administration	37
Identification des postes clients sur le Serveur d'administration	38
Privilèges d'accès au Serveur d'administration et à ses objets	38

DEPLOIEMENT DU SYSTEME DE PROTECTION ANTIVIRUS

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

- Grâce à l'installation à distance centralisée des applications sur les postes clients. Avec cela, l'installation des applications et la connexion au système d'administration à distance centralisé s'opèrent automatiquement, ne demandent aucune intervention de l'administrateur et permettent d'installer le logiciel antivirus sur n'importe quel nombre de postes clients.
- Grâce à l'installation locale des applications sur chaque poste client. Dans ce cas, l'installation des composants requis sur les postes clients et sur le poste administrateur s'opère manuellement. Les paramètres de connexion des clients au Serveur seront définis lors de l'installation de l'Agent d'administration. Cette option de déploiement est utilisée dans le cas où il n'est pas possible d'exécuter une installation à distance centralisée.

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

COMPATIBILITE AVEC LE SYSTEME CISCO NETWORK ADMISSION CONTROL (NAC)

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

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

COMPATIBILITE AVEC MICROSOFT NETWORK ACCESS PROTECTION (NAP)

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

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

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

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

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

CREATION DU SYSTEME DE GESTION CENTRALISEE DE LA PROTECTION ANTIVIRUS

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

1. Sélectionner dans le réseau les parties isolées et définir quel nombre de Serveurs d'administration il est nécessaire d'installer.
2. Définir quels ordinateurs sur le réseau de l'entreprise exécuteront les fonctions du Serveur d'administration principal et des Serveurs secondaires, et lesquels auront les fonctions de postes administrateurs et de postes clients. Tous les ordinateurs sur lesquels il est supposé d'installer les applications de Kaspersky Lab doivent devenir des postes clients.
3. Décider selon quel critère le groupement des postes clients sera exécuté et définir la hiérarchie des groupes.
4. Sélectionner quel type de déploiement du système de protection antivirus sera utilisé : une installation à distance ou locale.

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

1. Installer le Serveur d'administration sur les ordinateurs inclus dans le réseau de l'entreprise.
2. Installer la Console d'administration sur les ordinateurs depuis lesquels la gestion sera exécutée.

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

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

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

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

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

Toutes les applications de Kaspersky Lab dont la gestion est accessible par Kaspersky Administration Kit ne peuvent pas être installées à distance sur les postes clients. Consultez les informations détaillées à ce sujet dans les manuels des applications correspondantes.

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

Pour compléter, configurez les applications installées par la définition et l'application des stratégies de groupes (cf. section "Administration des stratégies" à la page [54](#)) et la création des tâches nécessaires (cf. section "Paramètres locaux de l'application" à la page [58](#)).

L'application offre la possibilité de créer un système de gestion centralisée de protection antivirus avec les paramètres minimums à l'aide de l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale" à la page [45](#)). La structure des groupes d'administration, identique à la structure de domaine du réseau Windows, est alors créée. Et le système de protection antivirus se forme, en utilisant Kaspersky Anti-Virus for Windows Workstations version 6.0 MP4.

Après avoir créé la structure des dossiers du Serveur d'administration, l'installation et la configuration de la protection antivirus, il est recommandé aux administrateurs de réaliser les mesures du service du réseau (cf. section "Maintenance" à la page [72](#)).

CONNEXION DES POSTES CLIENTS AU SERVEUR D'ADMINISTRATION

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

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

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

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

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

Les informations sur un événement sont envoyées sur le Serveur tout de suite après qu'il a eu lieu.

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

La synchronisation peut être manuellement exécutée par l'administrateur à l'aide de la commande **Synchroniser** du menu contextuel (cf. section "Menu contextuel" à la page [26](#)) du poste client. Dans ce cas, le mode auxiliaire de connexion est utilisé. Le Serveur initie la connexion dans ce mode. Pour ce faire, le port UDP s'ouvre sur le poste client. Le Serveur envoie une demande de connexion sur le port UDP. En réponse, l'analyse des privilèges du Serveur à une connexion au client est exécutée (à la signature numérique du Serveur d'administration), et dans le cas de leur existence, une connexion est exécutée.

Le deuxième mode de connexion est également utilisé lors d'un appel aux données du client sur le Serveur : pour recevoir des informations actuelles sur l'état des applications, des tâches et des statistiques du fonctionnement des applications.

CONNEXION SECURISEE AU SERVEUR D'ADMINISTRATION

L'échange des informations entre les postes clients et le Serveur d'administration, ainsi que la connexion de la Console au Serveur d'administration peuvent être exécutées en utilisant le protocole SSL (Secure Socket Layer). Il permet d'identifier les parties coopérantes, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérantes et le cryptage des données par clés ouvertes sont à la base du protocole SSL, utilisé au cours de la connexion sécurisée.

DANS CETTE SECTION

Certificat du Serveur d'administration.....	37
Authentification du Serveur d'administration lors de l'utilisation de l'ordinateur.....	38
Authentification du Serveur lors de la connexion de la Console.....	38

CERTIFICAT DU SERVEUR D'ADMINISTRATION

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

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

Le certificat du Serveur d'administration n'est créé qu'une seule fois, à l'installation. Il est recommandé de le sauvegarder à l'aide de l'assistant d'installation. Dans le cas où le certificat du Serveur d'administration serait perdu, il est nécessaire pour le restaurer de réinstaller le composant du serveur d'administration et de restaurer les données (cf. section "Copie de sauvegarde et restauration des données du Serveur d'administration" à la page [91](#)).

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

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

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

Selon la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée au cours des connexions ultérieures.

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

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

AUTHENTIFICATION DU SERVEUR LORS DE LA CONNEXION DE LA CONSOLE

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

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

IDENTIFICATION DES POSTES CLIENTS SUR LE SERVEUR D'ADMINISTRATION

L'identification des postes clients se réalise sur la base des noms des postes clients. Le nom d'un poste client est unique parmi tous les noms d'ordinateurs connectés au Serveur d'administration.

Le nom du poste client est transmis au Serveur d'administration, soit lors du sondage du réseau Windows et de la détection d'un nouvel ordinateur dans ce réseau, soit lors de la première connexion de l'Agent d'administration installé sur le poste client. Par défaut, le nom concorde avec le nom du réseau Windows (nom NetBIOS). Si un poste client est déjà enregistré avec ce nom sur le Serveur d'administration, alors un numéro d'ordre sera ajouté à la fin du nom du nouveau poste client, par exemple : <Nom>-1, <Nom>-2, etc. Sous ce nom, le poste client sera inclus dans le groupe d'administration.

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

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

- **Complète** - reprend toutes les autorisations (cf. ci-après).

- **Lecture** – consultation des paramètres des objets de Kaspersky Administration Kit sans privilèges d'exécution des opérations, de création de nouveaux objets et de modification des objets existants.
- **Ecriture** – modification des paramètres des objets de Kaspersky Administration Kit, ainsi que la création de nouveaux objets sans privilèges d'exécution des opérations sur les objets.
- **Exécution** – exécution des opérations sur les objets de Kaspersky Administration Kit sans privilèges de création de nouveaux objets et modification des objets existants.
- **Modification des privilèges d'accès** - attribution des droits d'accès aux fonctions de Kaspersky Administration Kit aux utilisateurs et aux groupes d'utilisateurs.
- **Modification des paramètres d'enregistrement des événements.**
- **Modification des paramètres d'envoi des notifications.**
- **Installation à distance des applications de Kaspersky Lab.**
- **Installation à distance d'autres applications** - préparation des paquets d'installation et installation à distance sur les postes clients des applications des éditeurs tiers ou des applications de Kaspersky Lab.
- **Modification des paramètres de la hiérarchie des Serveurs d'administration.**
- **Sauvegarde du contenu des listes de réseau** - copie des fichiers du dossier de sauvegarde, quarantaine et fichiers à réparation différée des postes clients sur l'ordinateur, où la Console d'administration est installée.
- **Création des tunnels** - création de connexion en tunnel entre l'ordinateur (avec la Console d'administration installée) et le poste client.

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

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

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

Tous les privilèges sont accordés au groupe **KLAdmins** et au groupe **KLOperators** : les privilèges sur **Lecture** et **Exécution**. Il est impossible de modifier l'ensemble des privilèges accordés au groupe **KLAdmins**.

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

La consultation des groupes **KLAdmins** et **KLOperators** et l'insertion des modifications nécessaires sont réalisées à l'aide des méthodes traditionnelles d'administration de Windows : **Administration** → **Utilisateurs locaux et groupes**.

Outre les utilisateurs du groupe **KLAdmins**, les privilèges d'administrateur sont accordés aux personnes suivantes :

- les administrateurs du domaine, dont les ordinateurs sont inclus dans ce groupe d'administration de ce Serveur ;
- les administrateurs locaux des ordinateurs, sur lesquels le Serveur d'administration est installé.

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

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

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

Les privilèges des utilisateurs (cf. section "Affectation de droits" à la page [42](#)) dans l'application Kaspersky Administration Kit sont établis selon l'authentification d'utilisateurs de Windows.

Après l'installation de l'application, l'administrateur de Kaspersky Administration Kit peut réaliser les points suivants :

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

ADMINISTRATION DES ORDINATEURS DU RESEAU

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

- Serveurs d'administration (cf. section "Connexion au Serveur d'administration" à la page [41](#)) et leur hiérarchie (cf. section "Serveurs d'administration secondaires" à la page [51](#)) ;
- Privilèges d'accès au Serveur d'administration (cf. section "Affectation de droits" à la page [42](#)) ;
- Composition et hiérarchie des groupes d'administration (cf. section "Création, consultation et modification de la structure du groupe d'administration" à la page [45](#)).

DANS CETTE SECTION

Connexion au Serveur d'administration.....	41
Affectation des droits.....	42
Affichage des informations du réseau d'ordinateurs. Domaines, plages d'adresses IP et groupes Active Directory.....	43
Assistant de configuration initiale	45
Création, consultation et modification de la structure des groupes d'administration	45

CONNEXION AU SERVEUR D'ADMINISTRATION

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

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

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

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

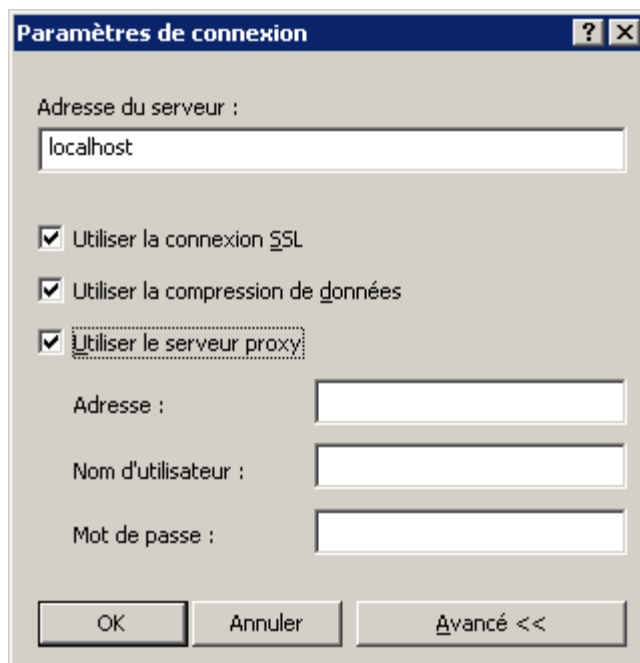


Illustration 11. Etablissement de la connexion au Serveur d'administration

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

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

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

AFFECTATION DES DROITS

Une fois que le Serveur d'administration a été installé, les utilisateurs appartenant aux groupes (cf. section "Privilèges d'accès au Serveur d'administration et à ses objets" à la page [38](#)) **KLAdmins** et **KLOperators** jouissent des privilèges de connexion au Serveur et d'utilisation de celui-ci.

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

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

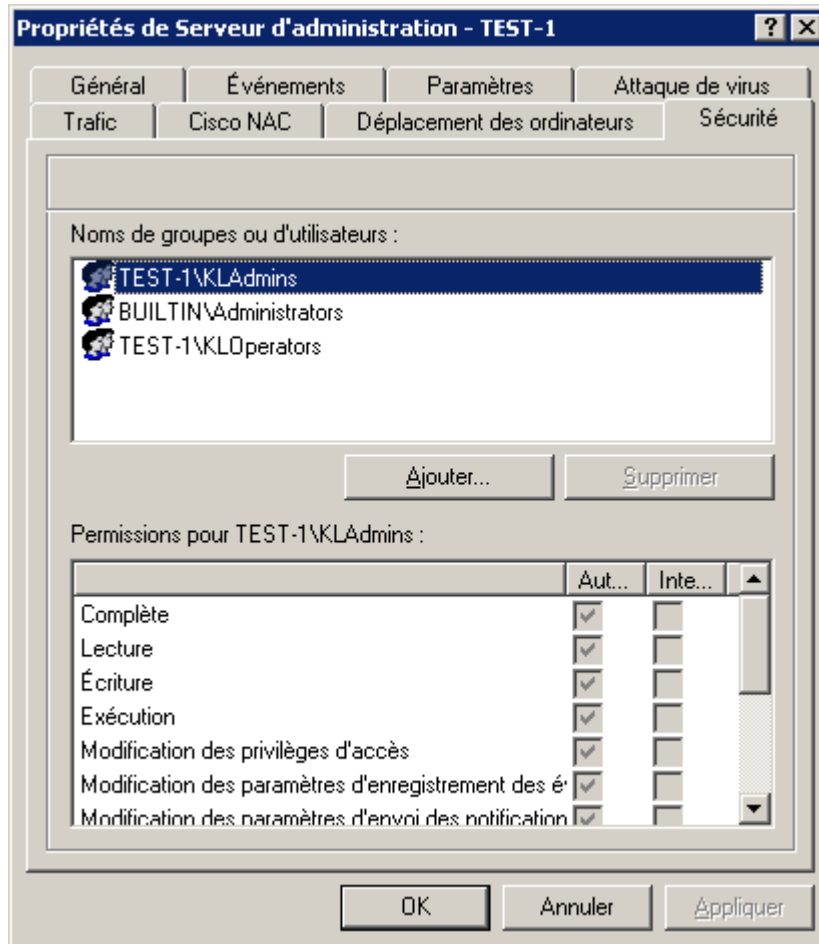


Illustration 12. Attribution des privilèges d'accès au Serveur d'administration

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

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

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

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

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

- **Domaines.**
- **Active Directory.**

- **Plages IP.**

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

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

La représentation des ordinateurs dans le dossier **Plages IP** repose sur la structure des plages IP créés sur le réseau. La structure du dossier **Plages IP** peut être composée par l'administrateur en créant des plages IP et en modifiant des paramètres existants.

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

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

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

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

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

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

Pour consulter ou modifier les paramètres de sondage du réseau Windows, cliquez sur le lien **Modifier les paramètres du sondage** situé dans le groupe **Sondage du réseau Microsoft** des tâches du dossier **Ordinateurs non définis**.

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

Pour consulter et modifier le sondage des groupes Active Directory, cliquez sur le lien **Modifier les paramètres du sondage** situé dans le groupe **Sondage Active Directory** dans le panneau des tâches du dossier **Ordinateurs non définis**.

- *Sondage des plages IP.* Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP et rassemble toutes les informations sur les ordinateurs appartenant à l'intervalle.

Pour consulter ou modifier les paramètres de sondage des plages IP, cliquez sur le lien **Modifier les paramètres du sondage** situé dans le groupe **Sondage des plages IP** des tâches du dossier **Ordinateurs non définis**.

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

Le dossier **Ordinateurs non définis** du Serveur d'administration principal reprend, entre autres, les ordinateurs faisant partie du réseau informatique auquel appartient le Serveur d'administration secondaire.

ASSISTANT DE CONFIGURATION INITIALE

L'application Kaspersky Administration Kit offre la possibilité de configurer uniquement un ensemble minimum de paramètres indispensables à l'établissement d'un système d'administration centralisée de la protection contre les virus. Il s'agit de l'Assistant de configuration initiale. L'Assistant de configuration initiale permettra de créer :

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

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

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

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

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

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

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

- Lors de la création de chaque groupe, les sous-dossiers **Serveurs d'administration**, **Stratégies**, **Tâches de groupe** et **Postes clients** sont créés automatiquement pour le stockage d'information et l'utilisation des Serveurs d'administration secondaires, des stratégies et des tâches du groupe sélectionné.

Lorsqu'un poste client est intégré à un groupe, les informations à son sujet sont reprises dans un tableau dans le panneau des résultats du sous-dossier **Postes clients**.

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

Les manipulations sur les objets du dossier **Ordinateurs administrés** s'opèrent à l'aide des commandes du menu contextuel (cf. section "Menu contextuel" à la page 26) et des liens dans le panneau des tâches.

Si la structure des groupes d'administration est identique à la structure des domaines et des groupes de travail du réseau Windows, vous pouvez utiliser l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale" à la page 45).

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

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

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

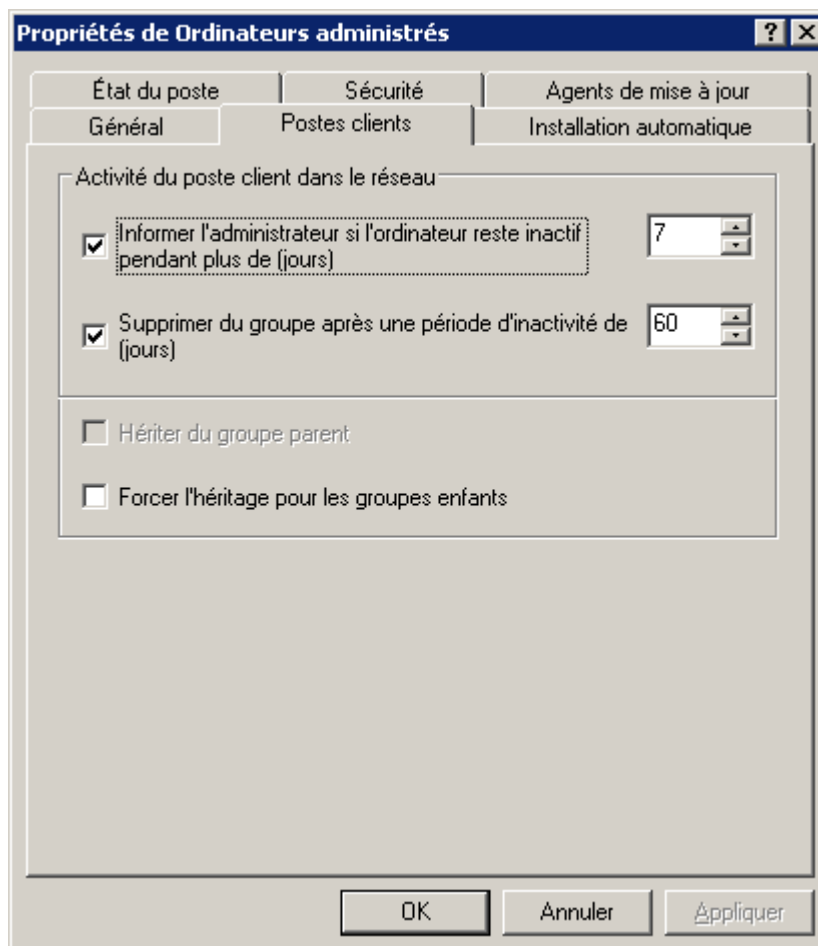


Illustration 13. Affichage des propriétés du groupe

Pour obtenir des informations sur des postes clients en particulier, vous pouvez utiliser la fonction de recherche de postes (cf. section "Recherche d'un poste" à la page [83](#)) sur le réseau de l'entreprise sur la base de critères définis. La recherche peut être réalisée sur la base d'informations relatives aux Serveurs d'administration secondaires. Pour rechercher les informations relatives à des ordinateurs dans un dossier en particulier de l'arborescence de la console, pour les enregistrer et pour les afficher, utilisez la fonction de création de sélections (cf. section "Sélections d'ordinateurs" à la page [85](#)).

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

- ajouter à la composition d'un groupe d'administration le nombre aléatoire de groupes de n'importe quel niveau (les Serveurs d'administration secondaires et les sous-groupes qui forment le niveau hiérarchique suivant peuvent être ajoutés au groupe) ;
- définir les applications de Kaspersky Lab qui seront installées automatiquement sur tout nouveau poste client ajouté au groupe ;
- ajouter au groupe des postes clients ;
- modifier la hiérarchie des objets des groupes d'administration en déplaçant des postes clients individuels ou des groupes entiers dans d'autres groupes ;
- supprimer d'un groupe les sous-groupes et les postes clients ;
- ajouter des Serveurs d'administration secondaires dans le but de réduire la charge sur le Serveur principal, de réduire le trafic interne et d'accroître la fiabilité du système d'administration à distance ;
- déplacer les postes clients des groupes d'administration d'un Serveur vers les groupes d'un autre.

DANS CETTE SECTION

Groupes	47
Postes clients	48
Serveurs d'administration secondaires.....	51

GROUPES

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

- **Stratégies.**
- **Tâches de groupe.**
- **Postes clients.**
- **Serveurs d'administration** dans le groupe qui vous intéresse.

La présence ou l'absence de ce dossier dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur. Afin de configurer l'affichage de ce dossier, passez au menu **Vue** → **Configuration de l'interface** et cochez la case sur la ligne Afficher les Serveurs d'administration secondaires.

Le dossier est rempli lors de la définition des stratégies du groupe, lors de la création de tâches de groupe ou de Serveurs secondaires.

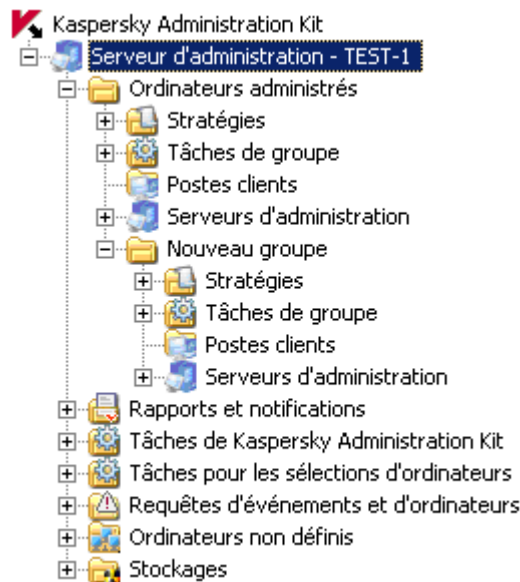


Illustration 14. Affichage de la structure des dossiers du Serveur d'administration

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

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

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

Le groupe est déplacé avec tous les sous-groupes, les Serveurs d'administration secondaires, les postes clients, les stratégies et les tâches de groupe. Tous les paramètres correspondant à sa nouvelle position dans la hiérarchie des groupes d'administration lui seront appliqués.

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

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

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

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

POSTES CLIENTS

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

Le serveur d'administration placera cet ordinateur dans le dossier **Ordinateurs non définis**, d'où vous allez pouvoir le déplacer dans le groupe qui vous est nécessaire.

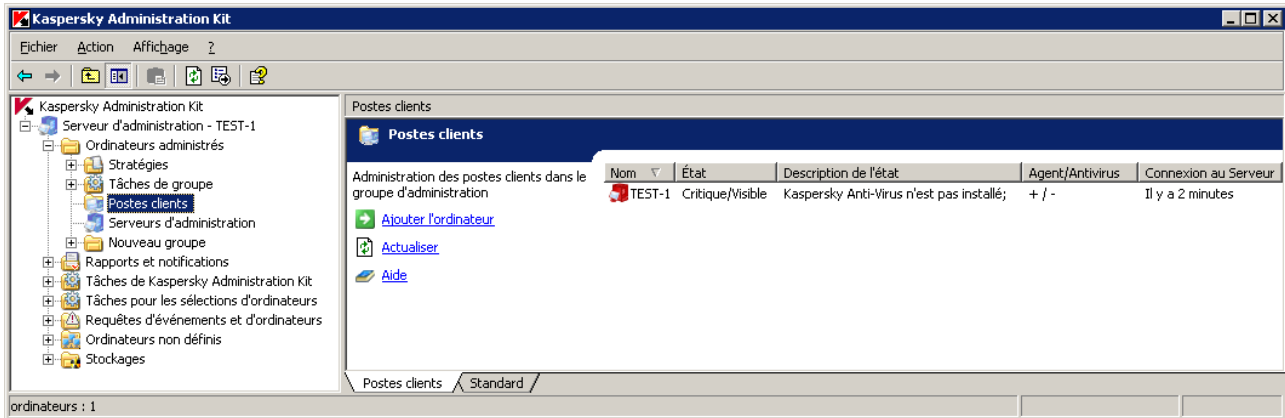


Illustration 15. Postes clients dans le groupe

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

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

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

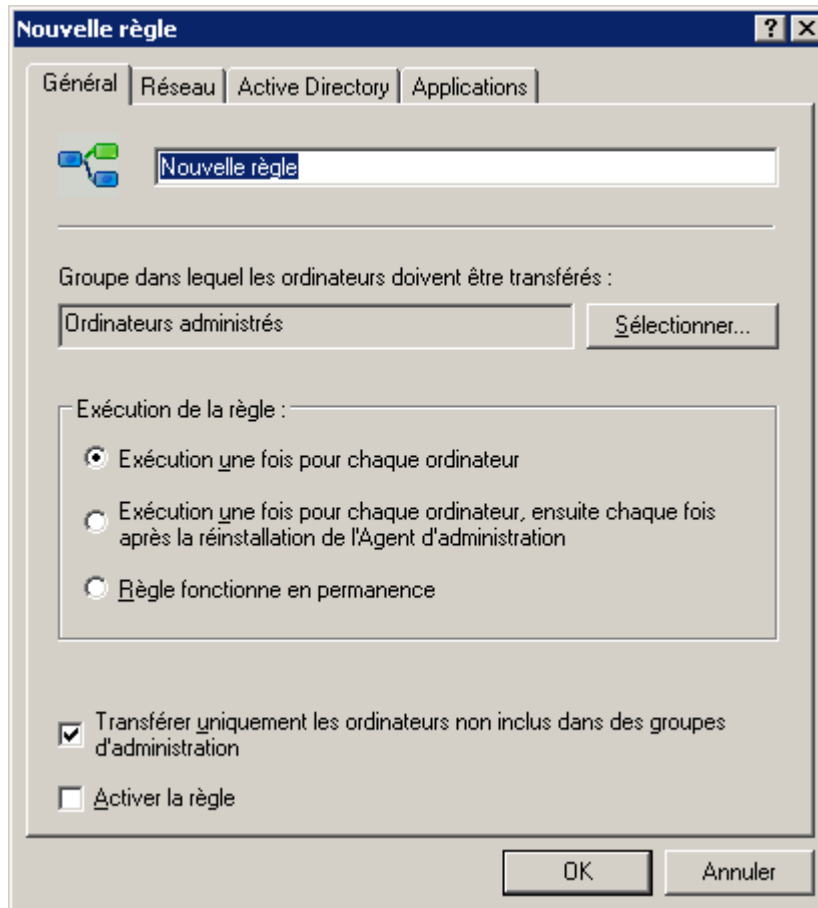


Illustration 16. Configuration de l'ajout automatique des nouveaux ordinateurs dans le groupe

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

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

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

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

SERVEURS D'ADMINISTRATION SECONDAIRES

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

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

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

➡ Pour ajouter un Serveur secondaire,

utilisez l'option **Créer** → **Serveur d'administration** pour l'objet du **Serveur d'administration** dans le groupe qui vous intéresse.

Avec cela l'Assistant d'ajout de Serveur secondaire se lance. A la suite de cela, cet assistant exécute les opérations suivantes :

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

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

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

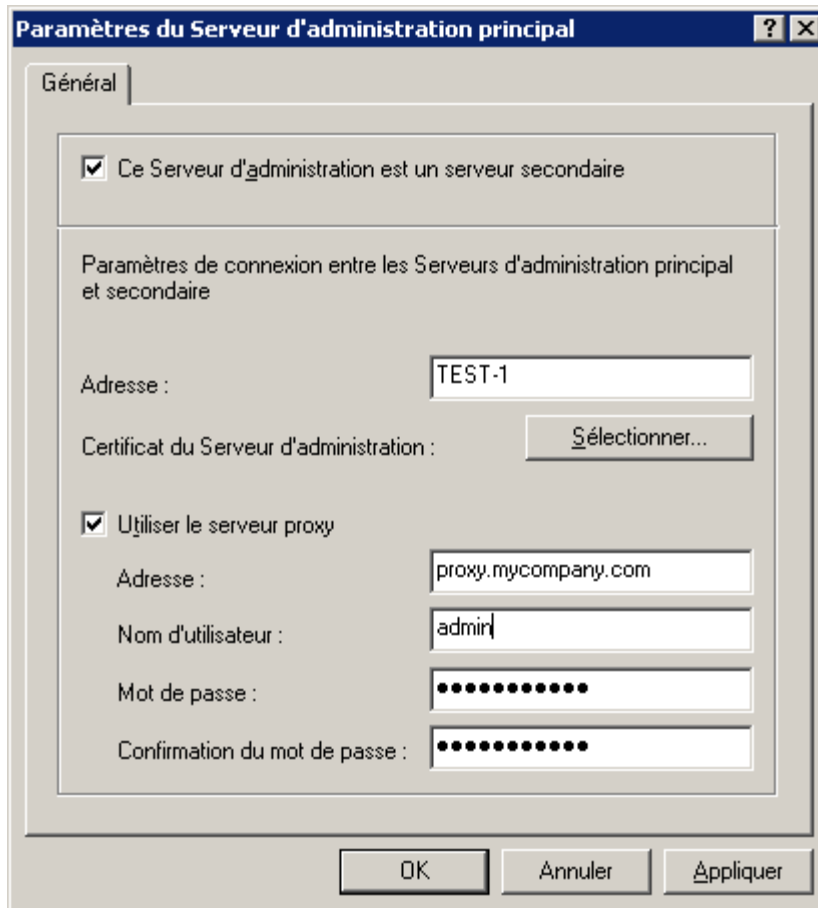








Illustration 17. Configuration dans le Serveur principal des infos du Serveur secondaire

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

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

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

- L'icône  (icône normale de la stratégie : ) apparaît à côté du nom de la stratégie obtenue du Serveur d'administration principal.
- Les valeurs des paramètres des stratégies héritées ne peuvent pas être modifiées sur le Serveur secondaire.
- Les paramètres dont la modification est impossible dans la stratégie héritée (icône ) ne peuvent être modifiés dans toutes les stratégies de l'application sur le Serveur secondaire et utilisent les valeurs définies dans la stratégie héritée.
- Les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie héritée, peuvent être changées (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page [33](#)) dans les stratégies du Serveur secondaire (icône ) . Si le paramètre n'est pas "verrouillé" dans la stratégie du Serveur secondaire, il pourra également être modifié (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page [33](#)) dans les paramètres de l'application et dans les paramètres de la tâche.

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

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

La mise à jour des postes clients du Serveur d'administration secondaire (cf. section "Récupération des mises à jour par les Serveurs secondaires et leurs postes clients" à la page [69](#)) peut être configurée de telle sorte que dès la réception des mises à jour par le Serveur principal, une tâche de réception des mises à jour par le Serveur secondaire sera lancée automatiquement. Après son exécution réussie, les tâches de mise à jour des applications sur les postes clients du Serveur secondaire seront exécutées.

ADMINISTRATION A DISTANCE DES APPLICATIONS

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

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

- l'administration des paramètres de l'application par la définition de stratégies (cf. section "Administration des stratégies" à la page [54](#)) et la modification des paramètres locaux des applications (cf. section "Paramètres locaux de l'application" à la page [58](#)) ;
- la création et l'exécution de tâches (cf. section "Administration du fonctionnement de l'application" à la page [59](#)).

DANS CETTE SECTION

Administration des stratégies	54
Paramètres locaux de l'application.....	58
Administration du fonctionnement de l'application.....	59

ADMINISTRATION DES STRATEGIES

La création de stratégies pour l'application n'est possible que si le poste de travail de l'administrateur est doté du module externe d'administration de l'application.

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

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

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

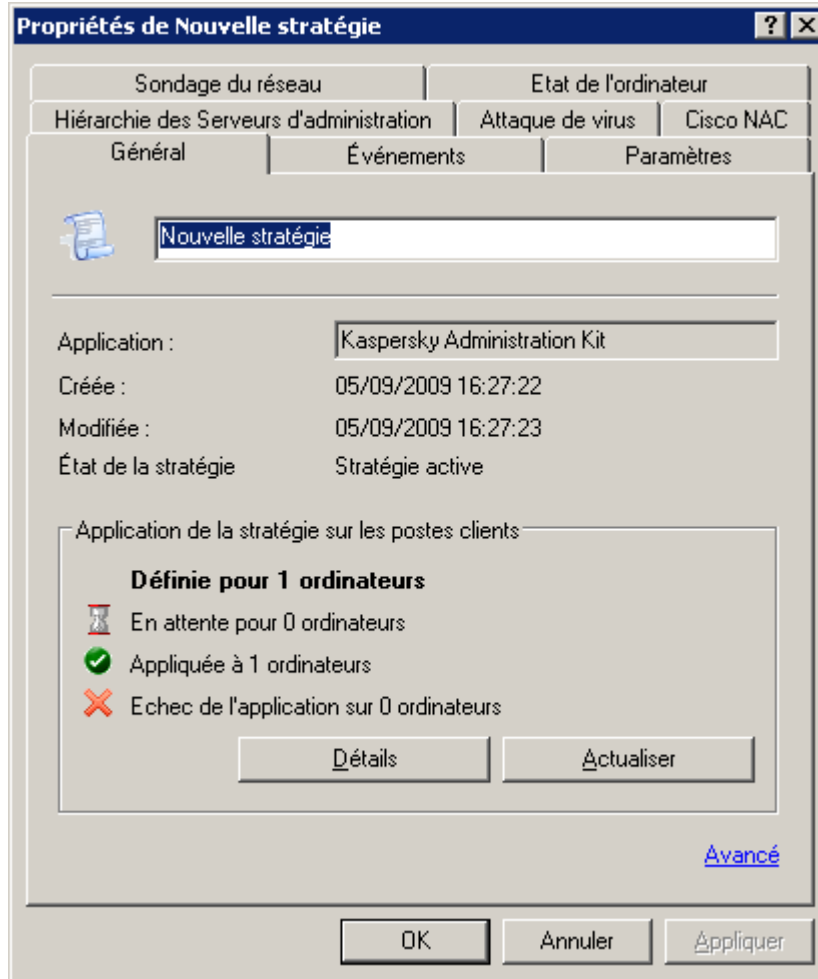





Illustration 18. Fenêtre des propriétés de la stratégie

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

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

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

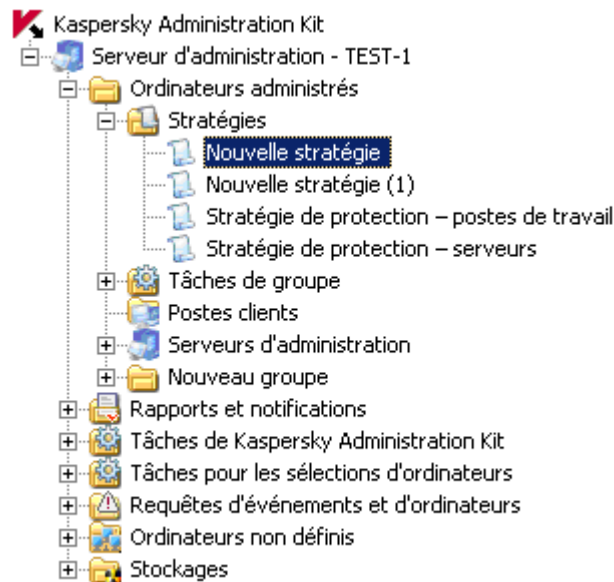


Illustration 19. Affichage de la liste des stratégies

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

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

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

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

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

Les résultats d'application de la stratégie sont affichés dans la fenêtre des propriétés de la stratégie.

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

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

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

L'application d'une stratégie se déroule de la manière suivante. Si des tâches résidentes (tâches de protection en temps réel) sont exécutées sur le poste client, elles sont poursuivies avec les nouvelles valeurs des paramètres sans interruption. Les tâches exécutées périodiquement (analyse à la demande, mise à jour des bases de l'application) maintiennent les anciennes valeurs. Le lancement suivant sera réalisé avec des paramètres modifiés. Les valeurs des

paramètres de fonctionnement de l'application définis après l'application de la stratégie peuvent être affichées par la Console d'administration dans la fenêtre des propriétés d'un poste client concret.

Dans la structure hiérarchique des Serveurs d'administration, les Serveurs secondaires obtiennent les stratégies du Serveur d'administration principal et les diffusent vers les postes clients. Quand le mode d'héritage est activé, les paramètres de la stratégie peuvent être modifiés sur le Serveur d'administration principal. Ensuite, les Serveurs d'administration secondaires modifient comme il se doit leurs stratégies et les diffusent vers les postes clients connectés.

En cas de perte de la connexion entre les Serveurs principal et secondaire, la stratégie sur le Serveur secondaire continue de fonctionner selon les paramètres précédents. Les paramètres modifiés dans la stratégie sur le Serveur d'administration principal sont propagés vers le Serveur secondaire une fois que la connexion a été rétablie.

Lorsque le mode d'héritage est désactivé, les paramètres de la stratégie peuvent être modifiés sur le Serveur secondaire indépendamment du Serveur principal.

En cas de déconnexion entre le Serveur d'administration et le poste client, la stratégie pour les utilisateurs nomades (si elle a été définie) entre en vigueur sur le poste client, ou la stratégie continue de fonctionner selon les paramètres précédents jusqu'au rétablissement de la connexion.

Les résultats de la diffusion de la stratégie sur les Serveurs d'administration secondaires figurent dans la fenêtre des propriétés de la stratégie sur le Serveur d'administration principal.

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

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

PARAMETRES LOCAUX DE L'APPLICATION

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

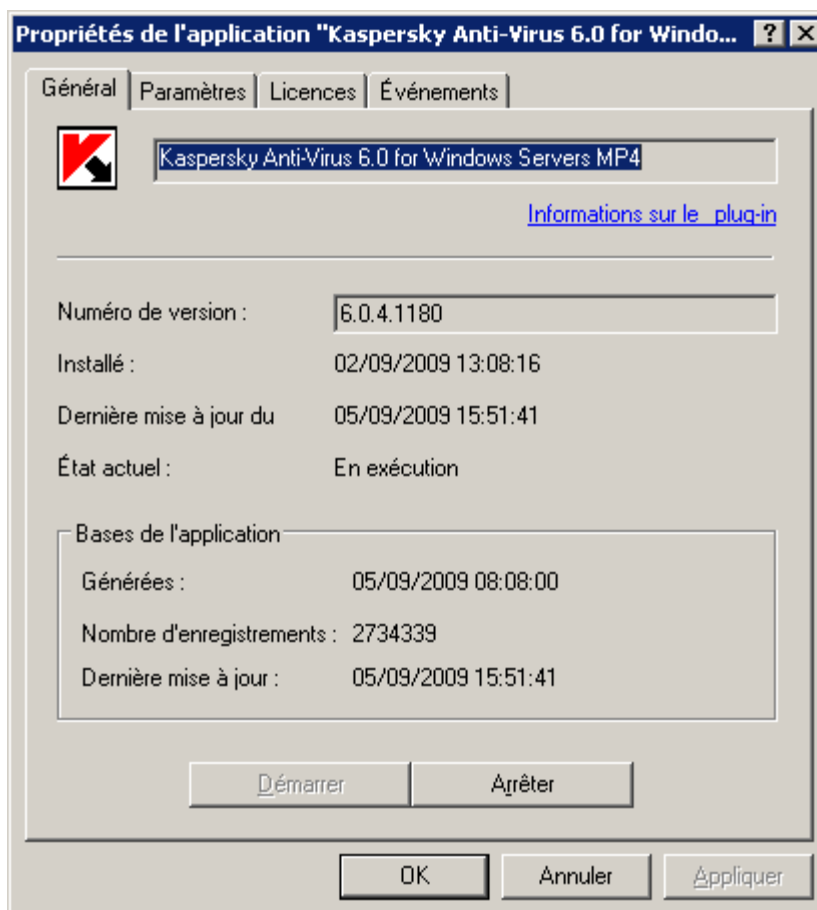


Illustration 20. Affichage des propriétés d'un poste client. Onglet **Général**

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

La sélection des paramètres locaux est propre à chaque application de Kaspersky Lab. Vous trouverez une description détaillée dans les Manuels pour chaque application.

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

ADMINISTRATION DU FONCTIONNEMENT DE L'APPLICATION

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

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

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

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

La création des tâches pour l'application est possible uniquement si le poste de travail de l'administrateur est doté du module externe d'administration de l'application.

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

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

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

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

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

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

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

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

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

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

Les tâches du Serveur d'administration sont placées dans le dossier de l'arborescence de la console de **Tâches de Kaspersky Administration Kit**. Pour créer une tâche du Serveur d'administration, ouvrez le dossier **Tâches de Kaspersky Administration Kit** dans l'arborescence de la console et utilisez la commande **Générer → Tâche**.

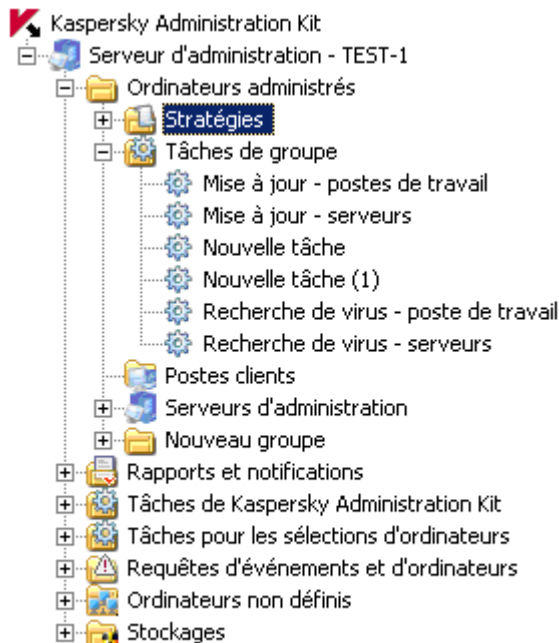


Illustration 21. Tâches de groupe

La fenêtre des propriétés d'un poste client affiche la liste des tâches locales sur celui-ci.

➡ Pour consulter la liste des tâches locales, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Postes clients** du groupe contenant l'ordinateur requis.
2. Sélectionnez l'ordinateur dans la liste reprise dans le panneau des résultats.
3. Ouvrez la fenêtre des propriétés de l'ordinateur à l'onglet **Tâches**, qui reprend la liste des tâches locales pour l'ordinateur sélectionné. Pour ce faire, cliquez sur le lien **Consulter les propriétés du poste client** situé à gauche de la liste des ordinateurs dans le panneau des résultats ou choisissez l'option **Propriétés** dans le menu contextuel de l'ordinateur sélectionné.

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

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

Les paramètres de fonctionnement de l'application lors de l'exécution des tâches sur chaque poste client sont définis conformément à la stratégie de groupe (cf. section "Corrélation de stratégie et de paramètres locaux de l'application" à la page 33), aux paramètres de la tâche et aux paramètres de cette application sur le poste client.

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

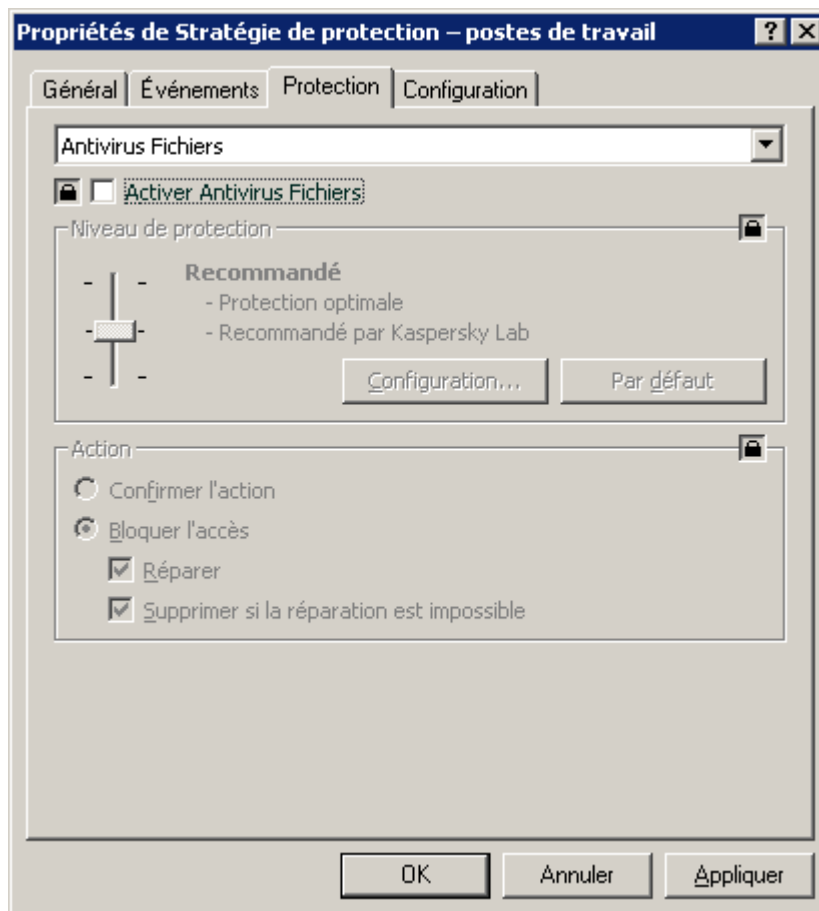


Illustration 22. Paramètres de la tâche ne pouvant pas être modifiés dans la stratégie

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

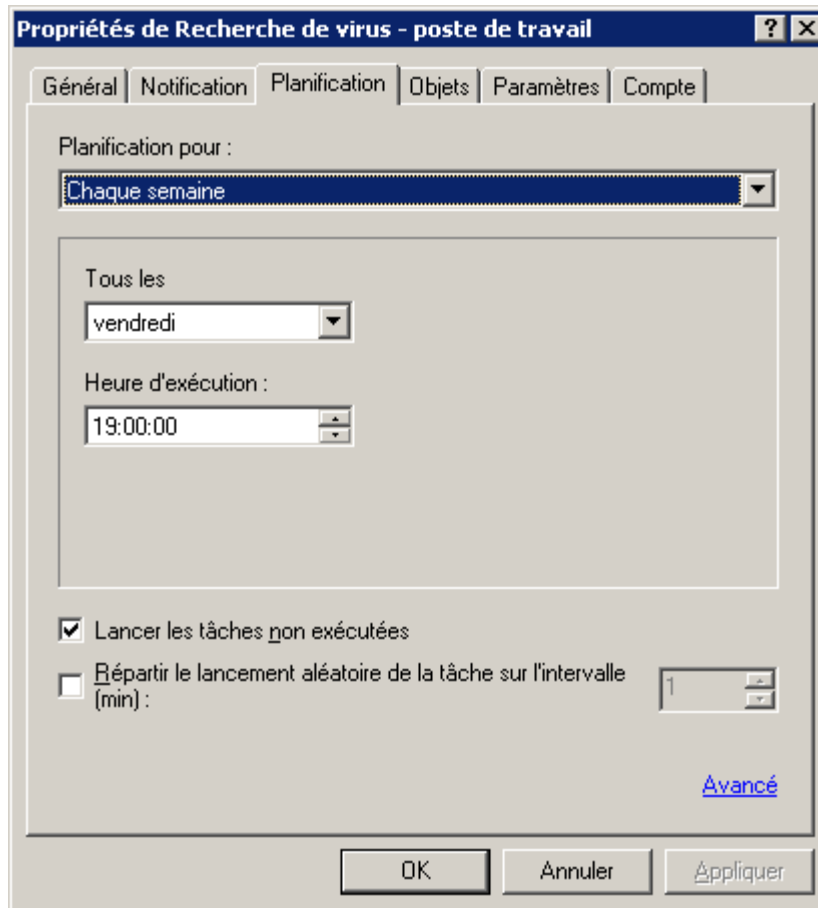


Illustration 23. Modification des propriétés de tâche. Onglet **Planification**

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

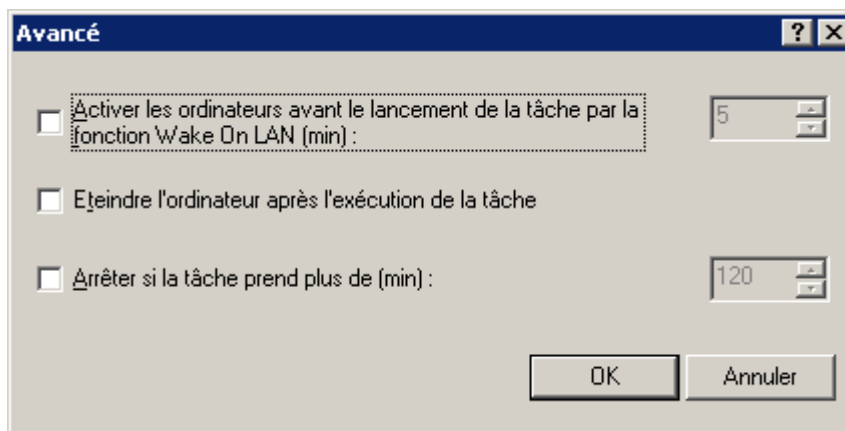


Illustration 24. Activation du démarrage automatique du système d'exploitation

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

La durée d'exécution de la tâche peut être limitée. Dans ce cas, la tâche s'arrêtera dès que l'intervalle défini dans les paramètres sera écoulé. Il est possible de désactiver le lancement des tâches programmées. Les tâches ne sont pas supprimées, mais elles ne seront tout simplement pas exécutées.

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

Les tâches ne sont lancées sur un poste client que dans le cas où l'application correspondante est en lancée. Si l'application est désactivée, toutes les tâches courantes sont annulées.

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

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

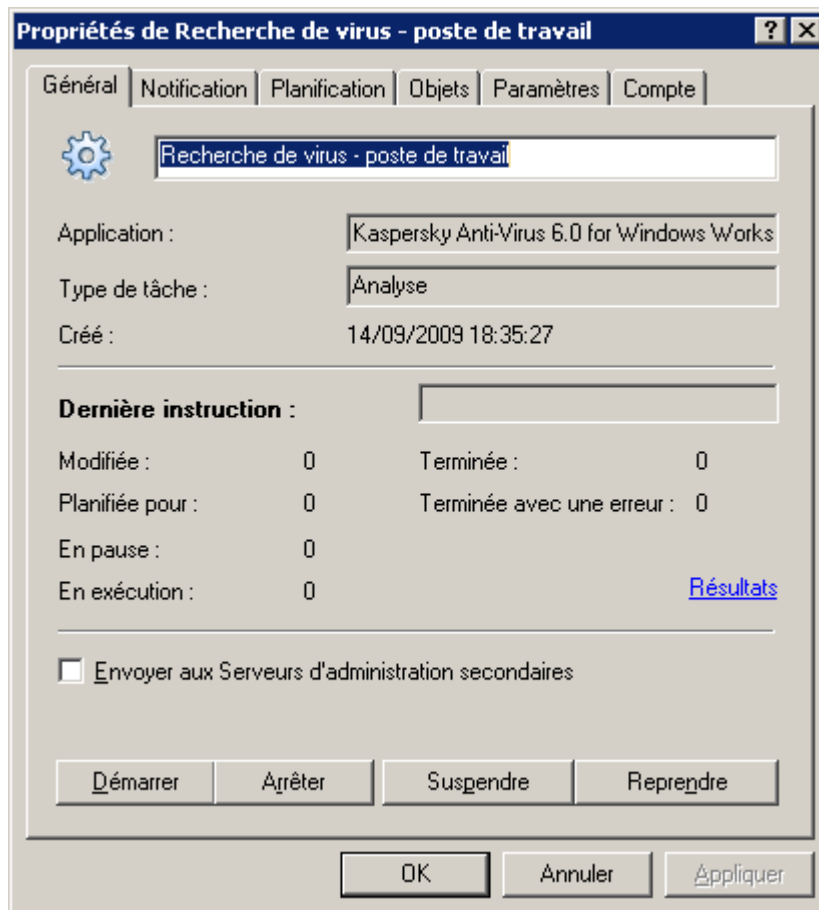


Illustration 25. Modification des propriétés de la tâche. Onglet **Général**

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

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

Les résultats de la diffusion de la tâche de groupe vers les Serveurs d'administration secondaire figurent dans la fenêtre **Résultats de l'exécution de la tâche**. Vous pouvez ouvrir cette fenêtre à l'aide du lien **Résultats**, sous l'onglet **Général** de la fenêtre des propriétés de la tâche de groupe du Serveur d'administration.

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

MISE A JOUR DES BASES ET DES MODULES D'APPLICATION

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

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

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

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

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

DANS CETTE SECTION

Téléchargement des mises à jour dans le référentiel du Serveur d'administration	65
Diffusion des mises à jour sur les postes clients	68
Récupération des mises à jour par les Serveurs secondaires et leurs postes clients	69
Diffusion des mises à jour à l'aide des agents de mise à jour	70

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

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

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

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

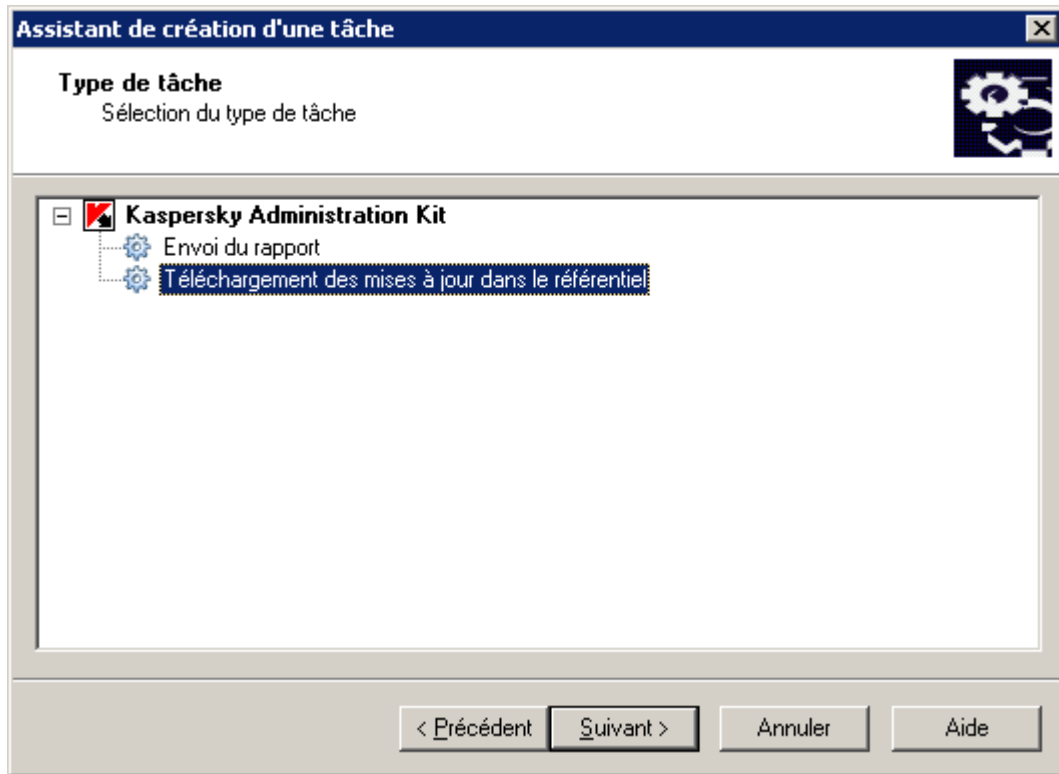


Illustration 26. Création d'une tâche de téléchargement des mises à jour dans le référentiel

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

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

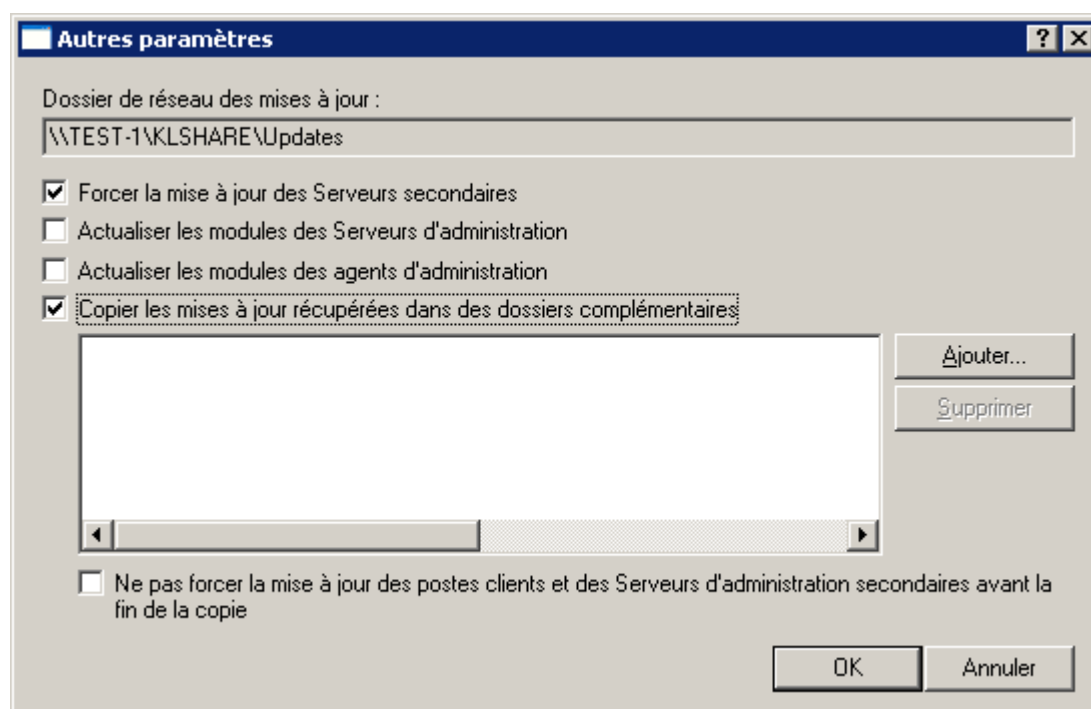


Illustration 27. Configuration d'autres paramètres de la tâche

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

Depuis le dossier partagé, les mises à jour seront diffusées vers les postes clients (cf. section "Diffusion des mises à jour sur les postes clients" à la page 68) et les Serveurs d'administration secondaires (cf. section "Récupération des mises à jour par les Serveurs secondaires et leurs postes clients" à la page 69).

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

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

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

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

Consultez les informations sur les mises à jour reçues dans l'arborescence de la console, dans le dossier **Stockages** → **Mises à jour**. La liste des mises à jour figure dans le panneau des résultats (cf. ill. ci-après).

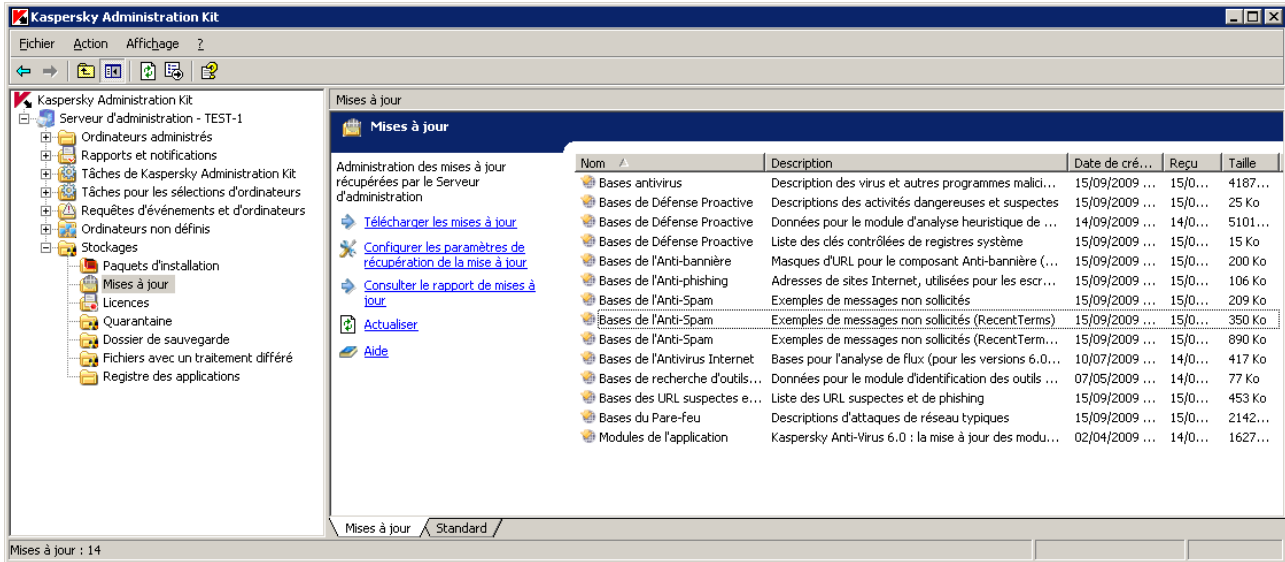


Illustration 28. Affichage des mises à jour reçues

DIFFUSION DES MISES A JOUR SUR LES POSTES CLIENTS

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

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

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

La création des tâches de mise à jour pour les applications est décrite en détails dans les Manuels pour ces applications.

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

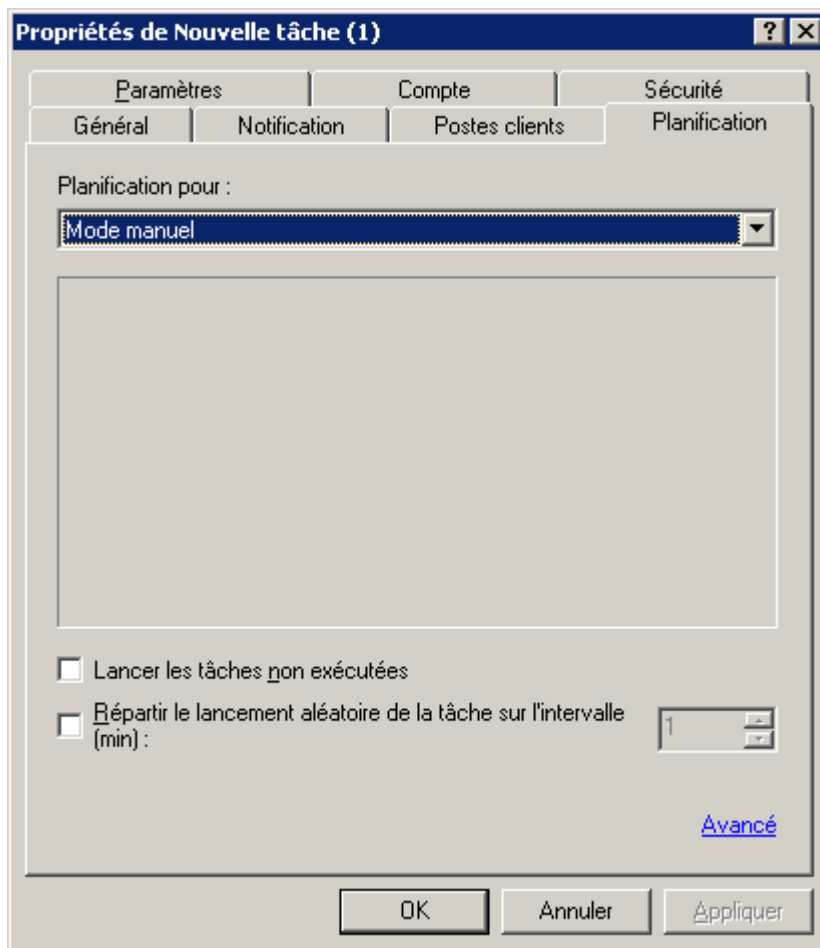


Illustration 29. Planification d'une tâche de mise à jour

Pour diminuer la charge des Serveurs d'administration, il est conseillé d'utiliser les agents de mise à jour (cf. section "Diffusion des mises à jour à l'aide des agents de mise à jour" à la page 70) qui permettra la diffusion des mises à jour dans les limites du groupe d'administration. En cas de diffusion d'adresses IP multiples, les agents de mise à jour diffusent également les paramètres des stratégies et des tâches.

RECUPERATION DES MISES A JOUR PAR LES SERVEURS SECONDAIRES ET LEURS POSTES CLIENTS

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

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

1. Créer une tâche de réception des mises à jour pour chaque Serveur d'administration secondaire.
2. Dans les paramètres de la tâche de réception des mises à jour pour les Serveurs secondaires, sélectionnez **Serveur d'administration principal** (cf. ill. ci-après) en guise de source des mises à jour.

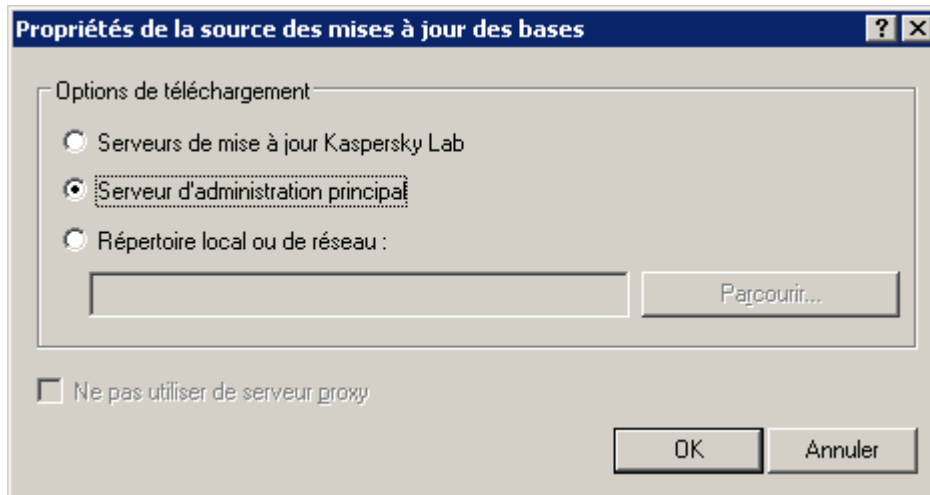


Illustration 30. Mise à jour depuis le Serveur d'administration principal

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

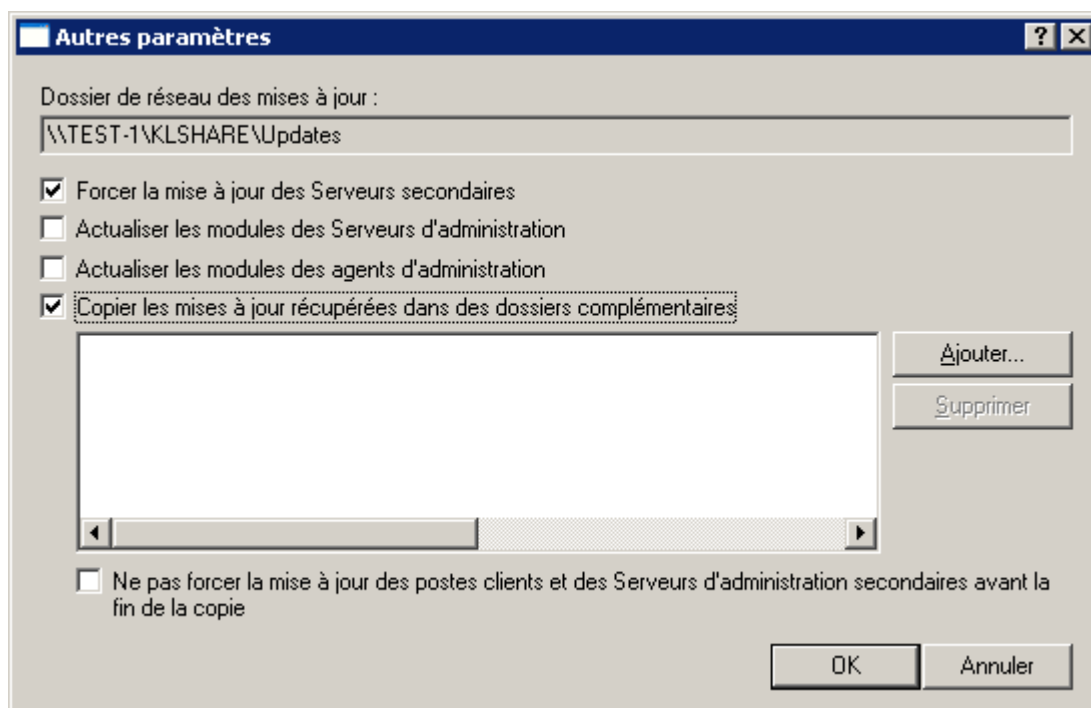


Illustration 31. Configuration d'autres paramètres de la tâche

4. Déterminer les agents de mises à jour (cf. section "Diffusion des mises à jour à l'aide des agents de mise à jour" à la page 70) dans les limites des groupes d'administration.

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

Pour diffuser les mises à jour vers les postes clients du groupe, il est possible d'utiliser les agents de mise à jour, à savoir les ordinateurs qui jouent le rôle du centre intermédiaire de diffusion des mises à jour et des paquets d'installation

dans les limites du groupe d'administration. Ils reçoivent les mises à jour depuis le Serveur d'administration et les placent dans le dossier désigné lors de l'installation de l'application. Le dossier peut être modifié dans les propriétés de l'agent de mise à jour. Seules les mises à jour requises dans les limites du groupe sont copiées. Par la suite, les postes clients du groupe contactent les agents pour les mises à jour.

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

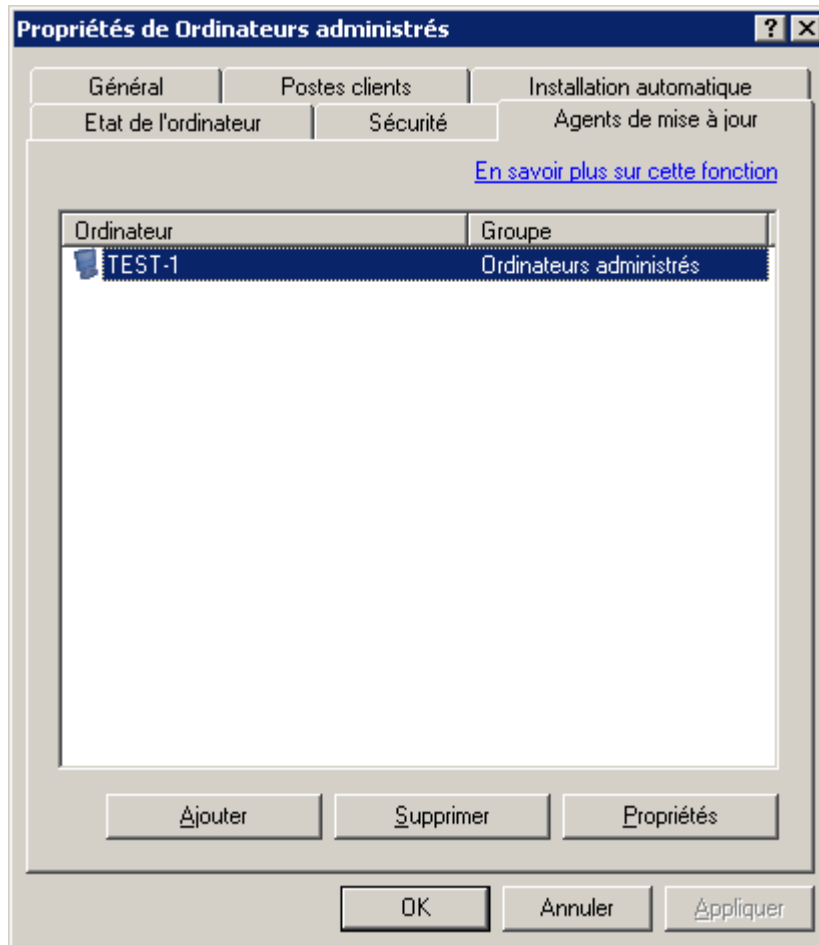


Illustration 32. Création de la liste des agents de mise à jour

MAINTENANCE

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

- Créer et consulter périodiquement les rapports de fonctionnement des applications sur les postes clients (cf. section "Rapports" à la page [80](#)).
- Lire les notifications envoyées depuis les postes clients et le Serveur d'administration.

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

- Actualiser en temps opportuns (cf. section "Mise à jour des bases et des modules de l'application" à la page [65](#)) les bases de l'application et les modules logiciels des applications installées sur les postes clients.
- Surveiller la taille des bases de données pour le stockage des informations en provenance des postes clients concernant le fonctionnement des applications et l'existence de l'espace suffisant sur le Serveur d'administration.
- Ajouter opportunément les nouveaux ordinateurs du réseau de l'entreprise aux groupes d'administration et y installer les applications antivirus requises.
- Réaliser à intervalles réguliers une copie de sauvegarde des données du système d'administration (cf. section "Copie de sauvegarde et restauration des données du Serveur d'administration" à la page [91](#)).
- Surveiller l'état des licences des applications installées sur le réseau et, le cas échéant, les renouveler (cf. section "Renouvellement de la licence" à la page [73](#)).
- Consulter les informations relatives aux événements du Serveur d'administration et des applications qu'il gère (cf. section "Journaux des événements. Requêtes d'événements" à la page [76](#)).
- Surveiller l'état de la quarantaine (cf. section "Quarantaine et sauvegarde" à la page [74](#)) et les informations relatives aux fichiers dont l'analyse a été différée (cf. section "Fichiers avec un traitement différé" à la page [91](#)).
- Si cela est nécessaire, effectuer des actions avec les objets sur les postes clients depuis le poste administrateur. Par exemple, réparer des fichiers infectés sur l'ordinateur.

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

- recherche d'ordinateurs, de groupes d'administration et de Serveurs d'administration secondaires selon des paramètres définis (cf. section "Recherche d'un poste" à la page [83](#)) ;
- tenue d'un registre des applications (cf. section "Registre des applications" à la page [87](#)) ;
- contrôle de l'émergence d'épidémies de virus (cf. page [88](#)).

DANS CETTE SECTION

Renouvellement de la licence	73
Quarantaine et dossier de sauvegarde	74
Journaux des événements. Requêtes d'événements.....	76
Rapports.....	80
Recherche d'un poste	83
Requêtes d'ordinateurs	85
Registre des applications	87
Contrôle de l'émergence d'épidémies de virus.....	88
Fichiers avec un traitement différé	91
Copie de sauvegarde et restauration des données du Serveur d'administration	91

RENOUVELLEMENT DE LA LICENCE

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

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

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

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

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

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

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

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

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

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

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

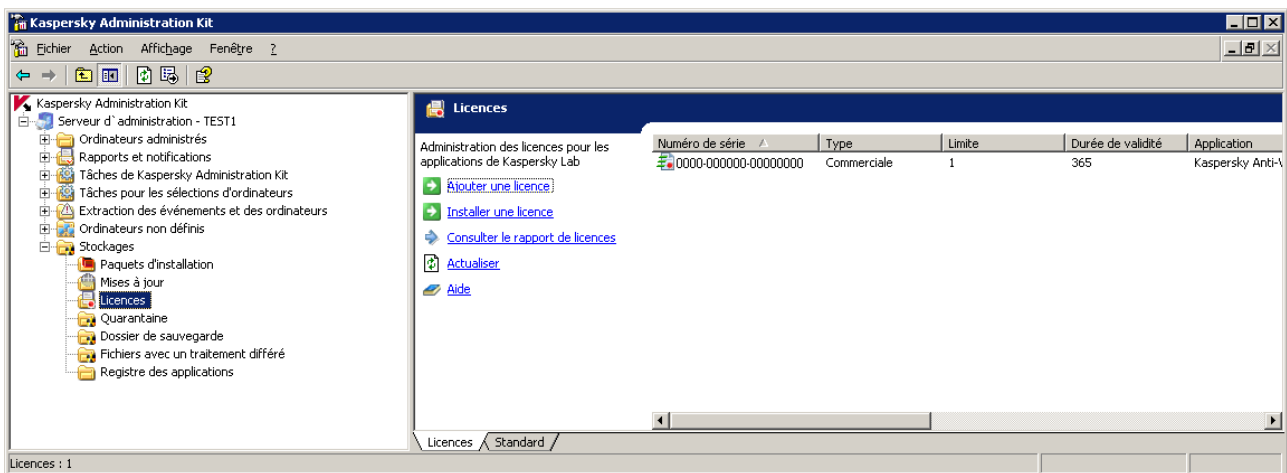


Illustration 33. Licences

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

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

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

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

QUARANTAINE ET DOSSIER DE SAUVEGARDE

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

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

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

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

► Pour activer la fonction d'administration à distance des objets des stockages locaux,

il faut cocher les cases dans le bloc **Informez le Serveur d'administration** (cf. ill. ci-après) dans la stratégie de l'application :

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

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

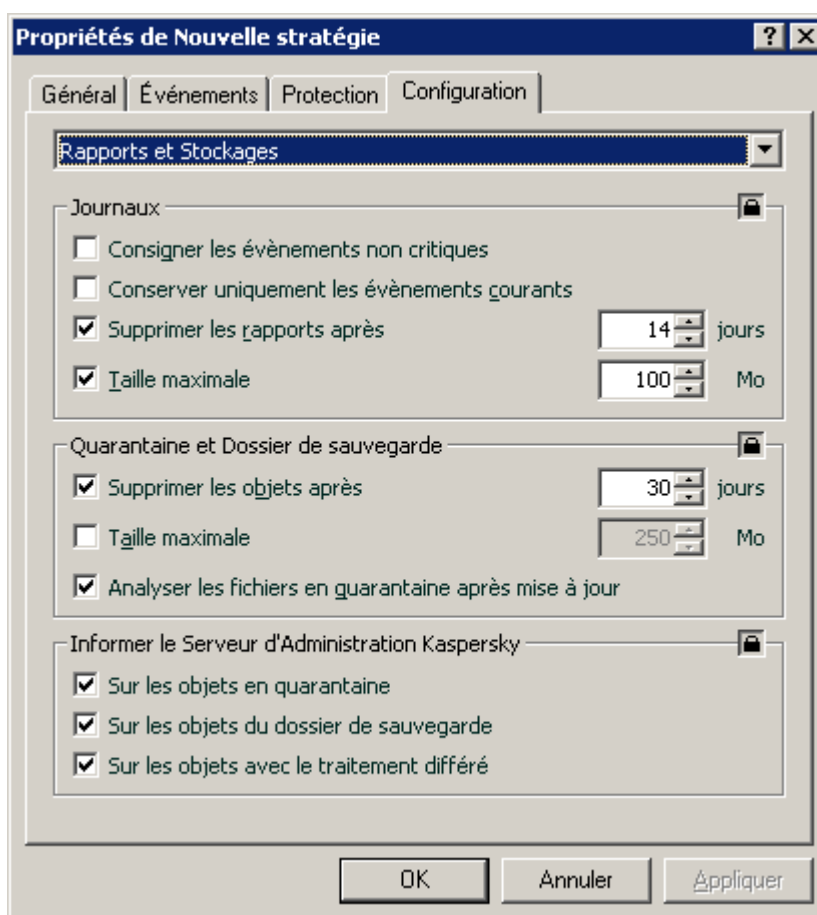


Illustration 34. Configuration des stockages distants

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

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

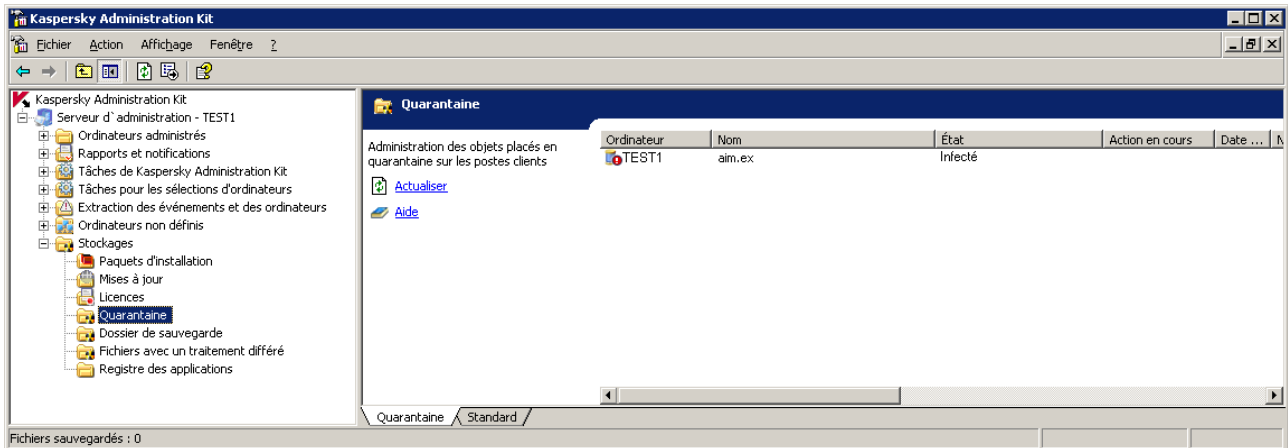


Illustration 35. Affichage du contenu du stockage

JOURNAUX DES EVENEMENTS. REQUETES D'EVENEMENTS

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

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

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

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

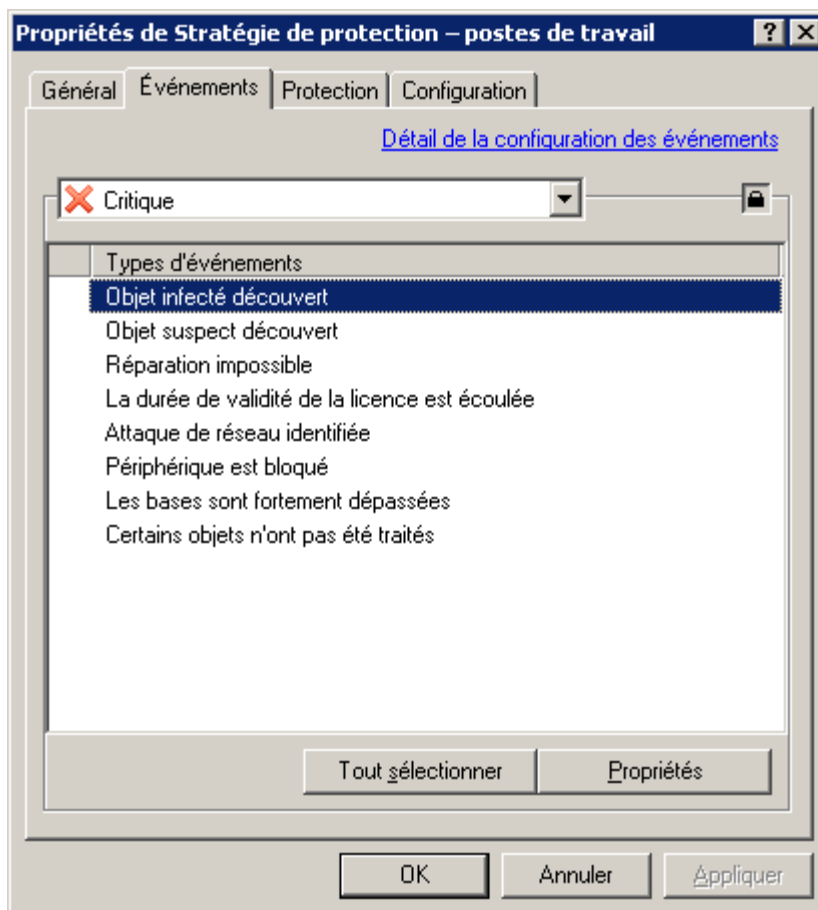


Illustration 36. Modification d'une stratégie. Onglet **Événements**

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

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

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

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

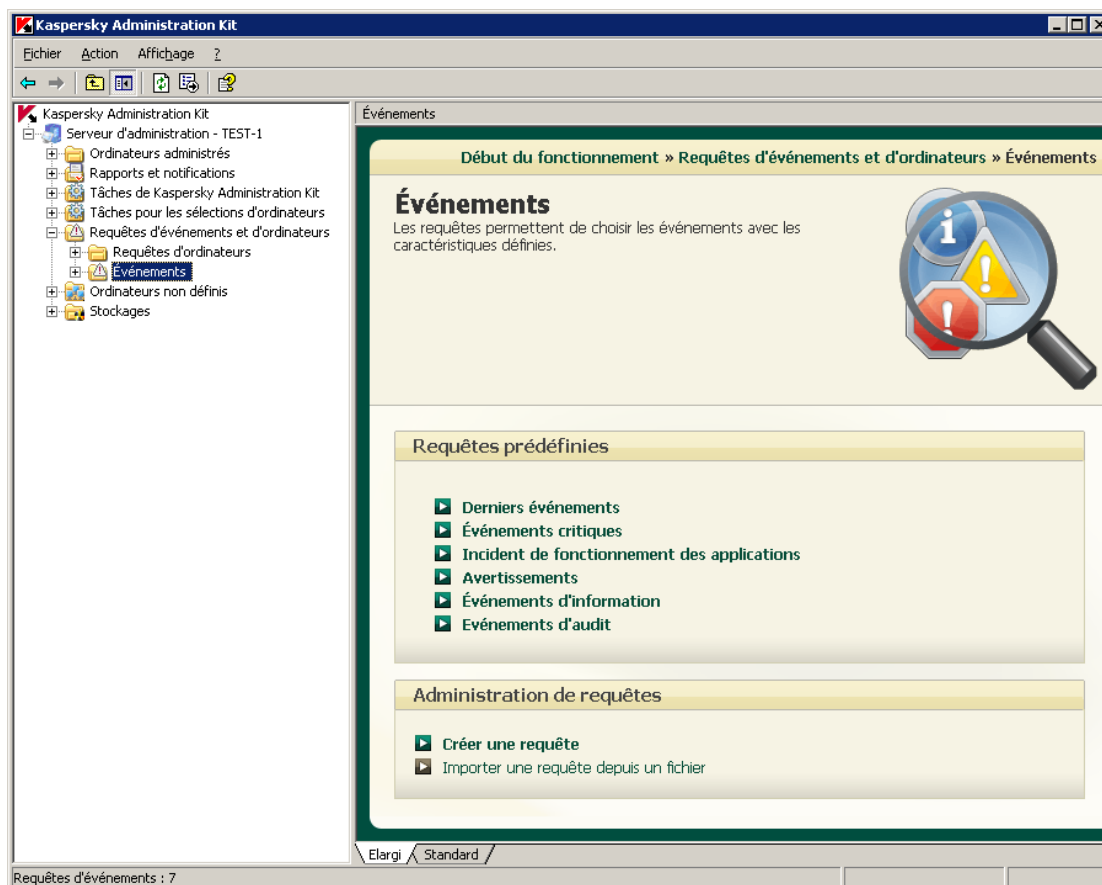


Illustration 37. Affichage des informations du journal des événements de Kaspersky Administration Kit

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

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

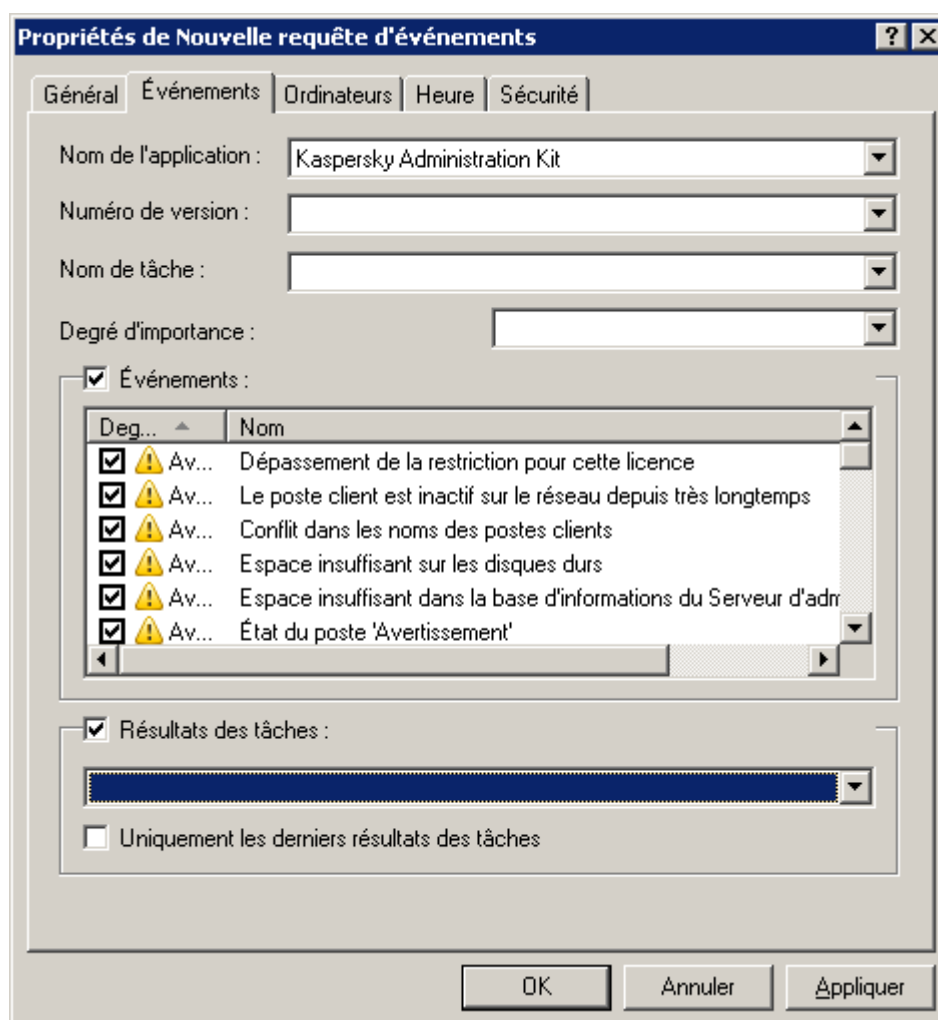


Illustration 38. Configuration d'une requête d'événements. Onglet **Événements**

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

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

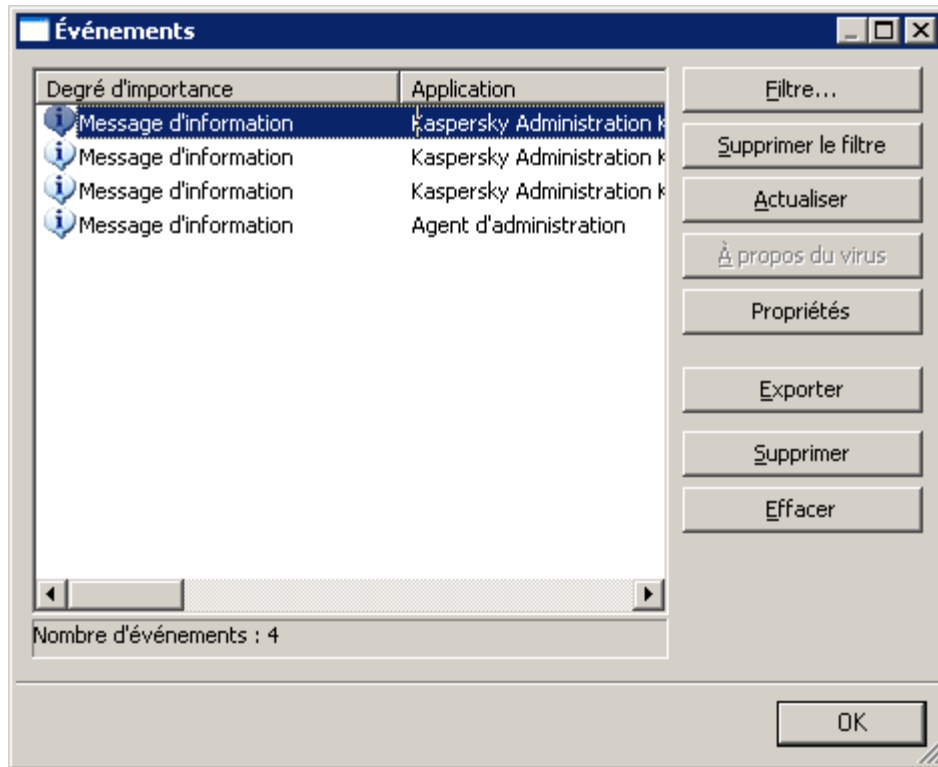


Illustration 39. Affichage des événements entreposés sur le Serveur d'administration

RAPPORTS

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

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

Il existe des rapports pour les objets suivant :

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

Les rapports de type suivant sont prévus :

- **Etat de protection :**
 - Le **Rapport d'état de protection** contient des informations sur les postes clients qui ne jouissent pas d'une protection antivirus suffisante.
 - Le **Rapport sur les erreurs** contient des informations sur les erreurs (refus de fonctionnement) enregistrées durant le fonctionnement des applications installées sur les postes clients.

- Le **Rapport sur les événements** contient la liste des événements des applications pour le groupe sélectionné. La liste reprend uniquement les événements indiqués lors de la création du rapport.
- Le **Rapport sur le fonctionnement des agents de mise à jour** contient les statistiques de fonctionnement des agents de mise à jour dans le cadre des groupes d'administration sélectionnés.
- Le **Rapport sur les Serveurs d'administration secondaires** contient les informations sur les Serveurs d'administration secondaires inclus dans les groupes d'administration sélectionnés.
- **Déploiement :**
 - Le **Rapport sur l'utilisation des licences** contient des informations sur l'état des licences utilisées par les applications et sur le respect des restrictions qu'elles imposent.
 - Le **Rapport sur les versions des logiciels de Kaspersky Lab** reprend les informations sur les versions des applications antivirus de Kaspersky Lab installées sur les postes clients.
 - Le **Rapport sur les applications incompatibles** contient des informations sur les applications antivirus d'autres éditeurs installés sur les postes clients ou sur les applications de Kaspersky Lab qui ne sont pas compatibles avec l'administration par Kaspersky Administration Kit.
 - Le **Rapport sur le déploiement de la protection** contient une liste des ordinateurs dans le réseau et les informations sur les applications antivirus qui y sont installées.
- **Mise à jour :**
 - Le **Rapport sur les bases utilisées** contient les informations sur les versions des bases utilisées par les applications.
 - Le **Rapport sur les versions des mises à jour des modules logiciels des applications de Kaspersky Lab** contient les informations de synthèse sur les versions des mises à jour des modules logiciels installés, le nombre de mises à jour installées, ainsi que le nombre d'ordinateurs ou de groupes, où l'installation a eu lieu.
- **Statistiques antivirus :**
 - Le **Rapport sur les virus** reprend les informations relatives aux résultats de l'analyse antivirus des postes clients.
 - Le **Rapport sur les ordinateurs les plus infectés** contient les informations sur les postes clients dont l'analyse s'est soldée par le plus grand nombre d'objets suspects découverts.
 - Le **Rapport d'attaques réseau** reprend les informations relatives aux attaques de réseau enregistrées sur les postes clients.
 - Le **Rapport sur les applications pour la protection des postes de travail et des serveurs de fichiers** contient les informations détaillées sur les logiciels antivirus installés pour la protection des postes de travail et des serveurs de fichiers, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.
 - Le **Rapport sur les applications pour la protection des systèmes de messagerie** contient les informations détaillées sur les logiciels antivirus installés pour la protection des systèmes de messagerie, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.
 - Le **Rapport sur les applications antivirus pour la protection des passerelles** contient les informations détaillées sur les logiciels antivirus installés pour la protection du périmètre, ainsi que les informations sur les objets infectés découverts par les applications de ce type et les actions entreprises.
 - Le **Rapport de synthèse sur les types d'application** contient les informations sur les types de logiciels antivirus installés sur les postes clients, ainsi que les informations sur les objets infectés découverts par ces applications et les actions associées.

- Le **Rapport d'utilisateurs des ordinateurs infectés** contient l'information relative aux utilisateurs du réseau, dont les ordinateurs ont par le plus grand nombre des objets suspects découverts.
- **Autres :**
 - Le **Rapport sur le registre des applications** contient les informations sur toutes les applications installées sur les postes clients des groupes d'administration.
 - Le **Rapport sur les notes de l'administrateur** reprend la liste des remarques de l'administrateur enregistrées dans le groupe pendant l'intervalle indiqué.

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

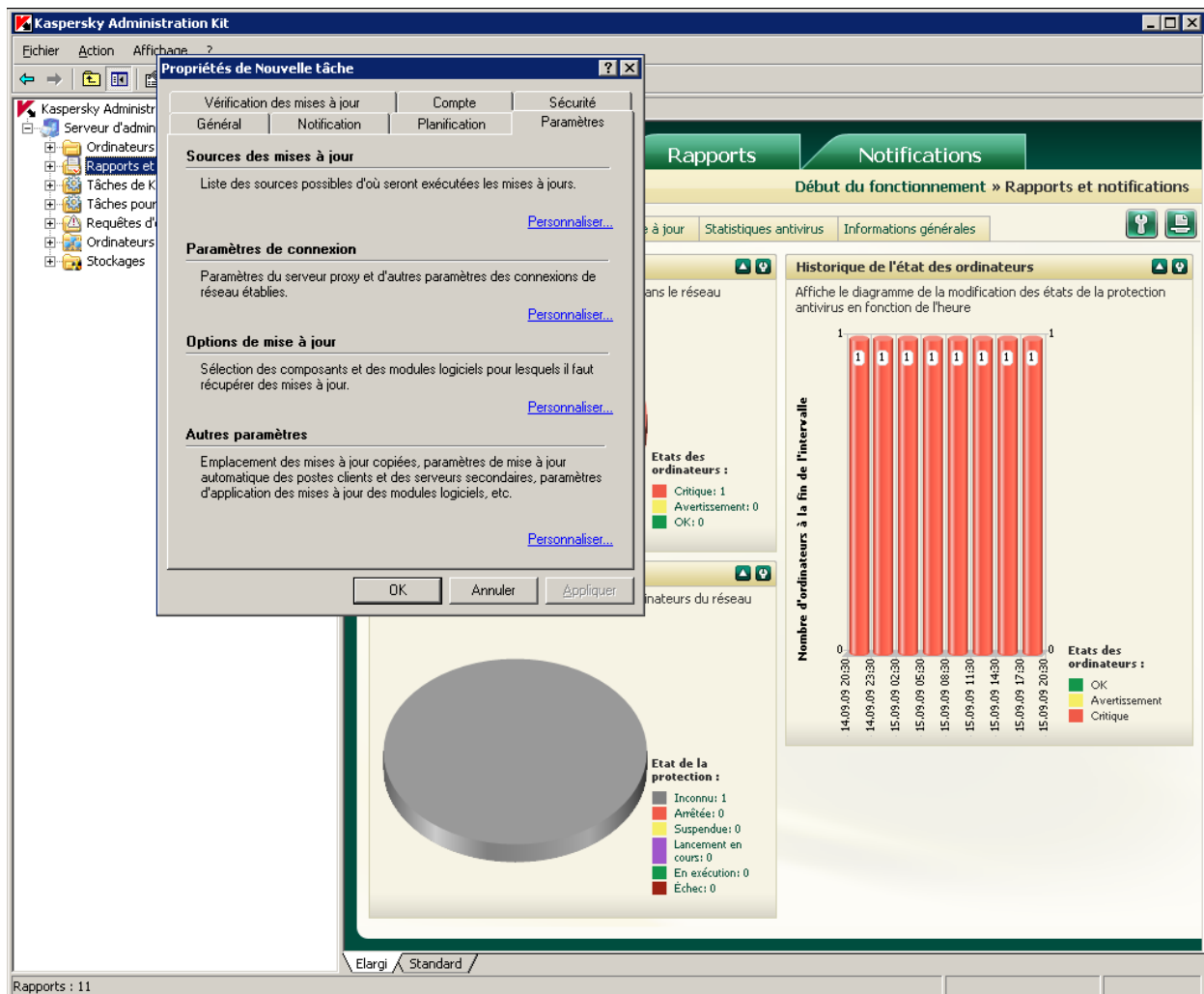


Illustration 40. Affichage de la liste des rapports

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

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

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

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

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

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

RECHERCHE D'UN POSTE

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

La fonction de recherche permet de trouver :

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

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

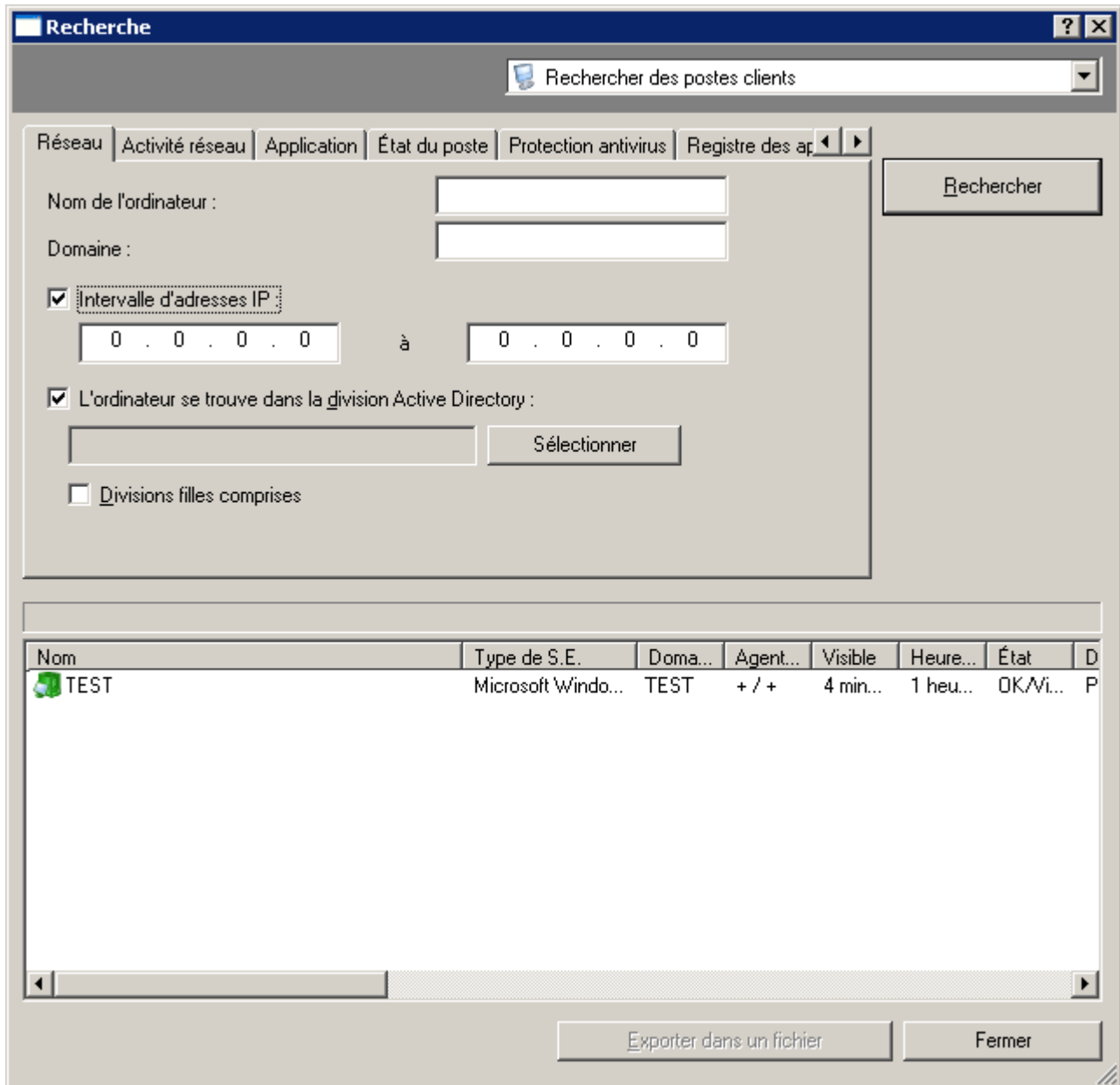


Illustration 41. Recherche d'un poste. Onglet **Réseau**

Les résultats suivants seront proposés en fonction de la section ou du dossier pour lequel la recherche est lancée :

- **Ordinateurs administrés** ou n'importe quel sous-dossier : la recherche des ordinateurs connectés au Serveur d'administration qui gère le groupe sélectionné.

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

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

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

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

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

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

La recherche donnera les résultats suivants :

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

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

REQUETES D'ORDINATEURS

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

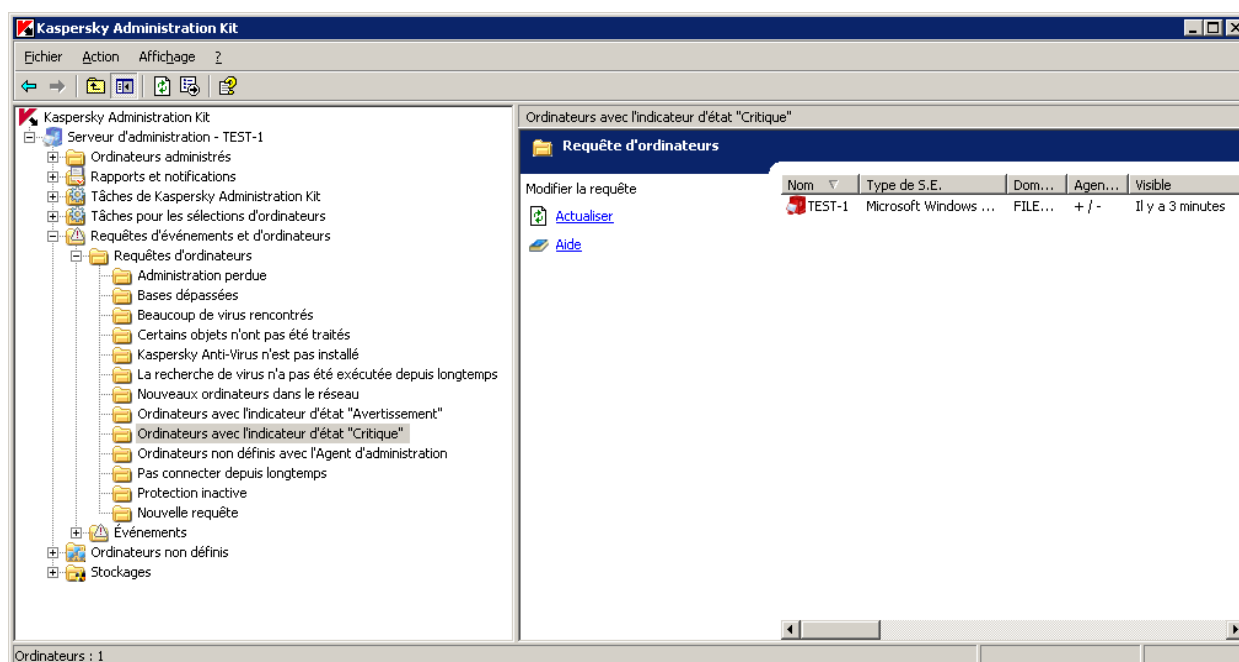


Illustration 42. Requêtes d'ordinateurs

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

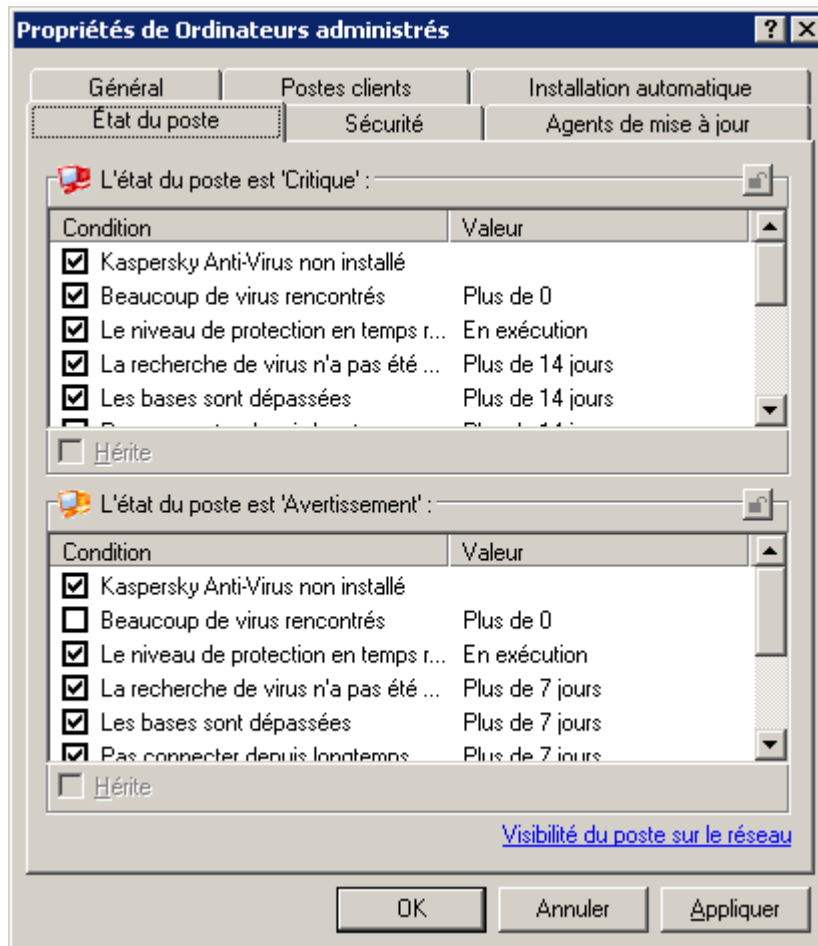


Illustration 43. La configuration de diagnostic de l'état du poste client

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

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

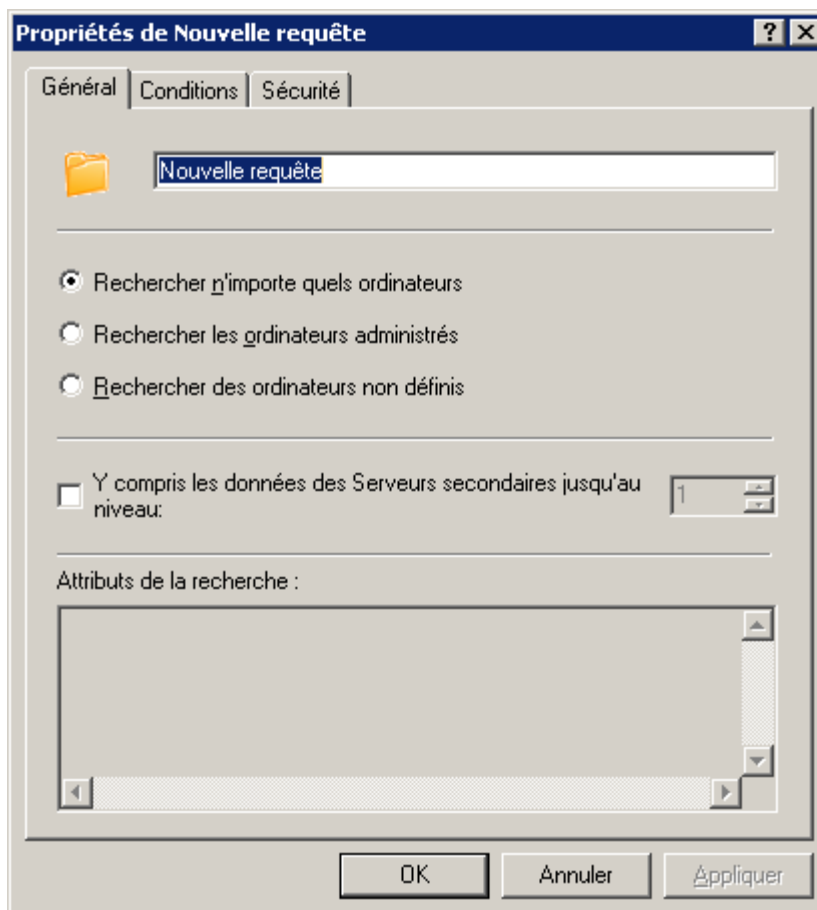


Illustration 44. Configuration de la requête d'ordinateurs.

REGISTRE DES APPLICATIONS

La présence ou l'absence de ce dossier dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur. Afin de configurer l'affichage de ce dossier, passez au menu **Vue** → **Configuration de l'interface** et cochez la case sur la ligne **Afficher le registre des applications**.

➤ Pour consulter le registre des applications installées sur les postes du réseau,

ouvrez le dossier **Stockages** → **Registre des applications**.

Les informations relatives aux applications proviennent du registre des postes clients du réseau local et sont présentées dans un tableau contenant les champs suivants :

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

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

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

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

CONTROLE DE L'EMERGENCE D'EPIDEMIES DE VIRUS

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

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

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

L'événement peut être fixé pour plusieurs types d'applications.

➤ *Pour enclencher le mécanisme d'identification des attaques de virus,*

cochez les cases situées à côté des types d'applications requis :

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

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

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

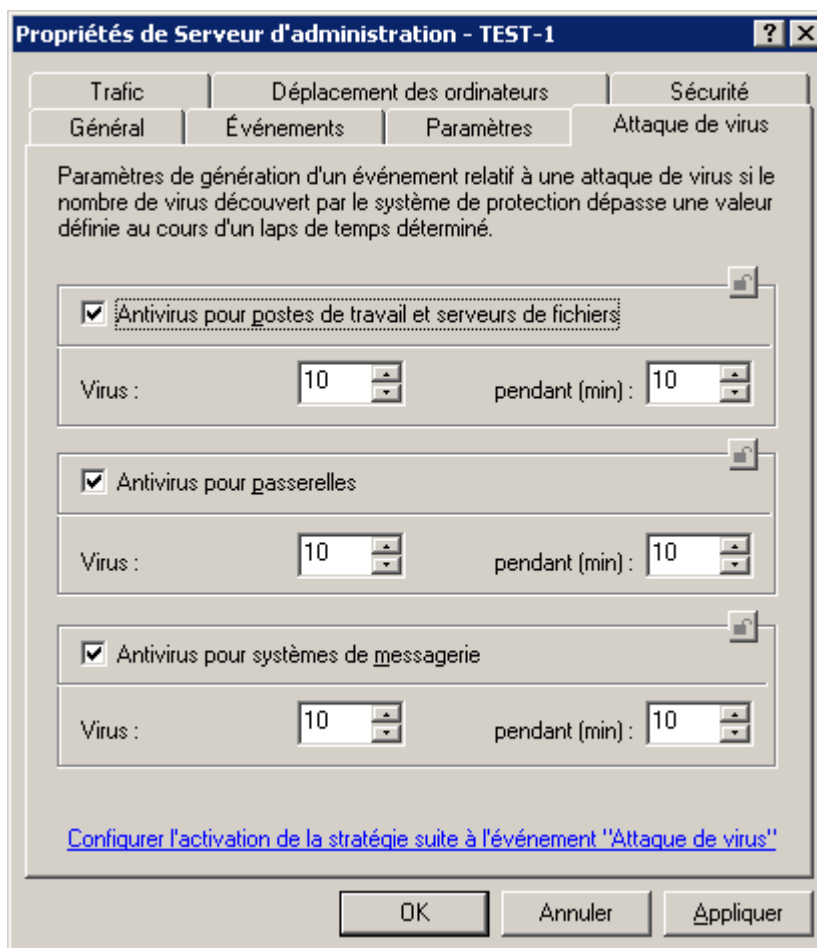


Illustration 45. Affichage des propriétés du Serveur d'administration. Onglet **Attaque de virus**

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

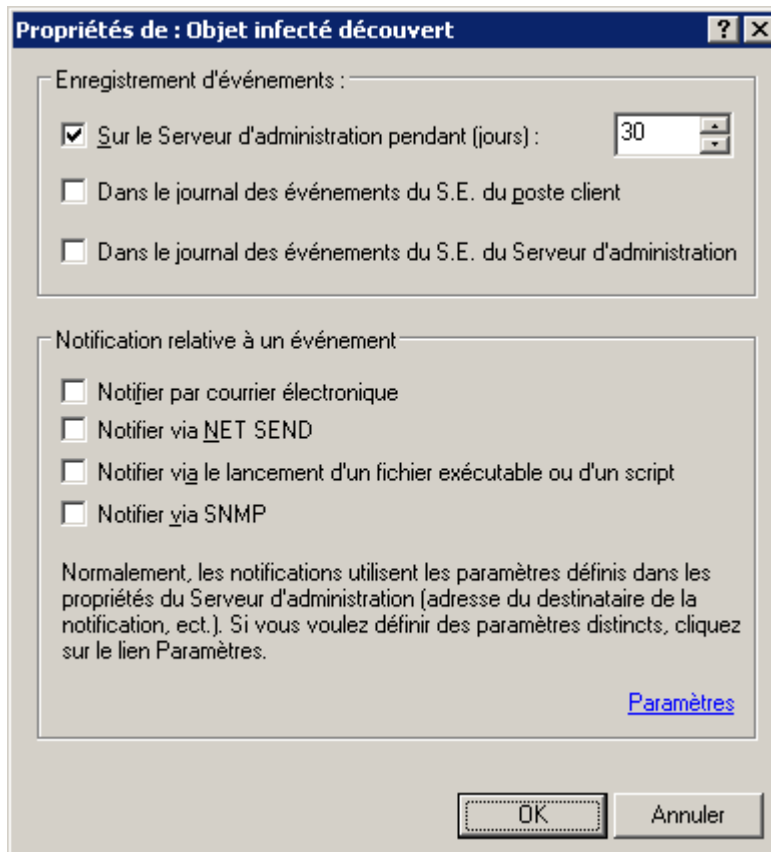


Illustration 46. Configuration de l'enregistrement de l'événement

L'ordre de notification sur l'événement **Attaque de virus** est défini sur le Serveur d'administration dans la fenêtre des propriétés de l'événement dans le groupe **Notification relative à un événement** (cf. ill. ci-après).

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

Sous le titre **Virus découvert**, les informations en provenance des postes clients du Serveur d'administration principal sont prises en compte. L'événement **Attaque de virus** est configuré individuellement pour chaque Serveur secondaire.

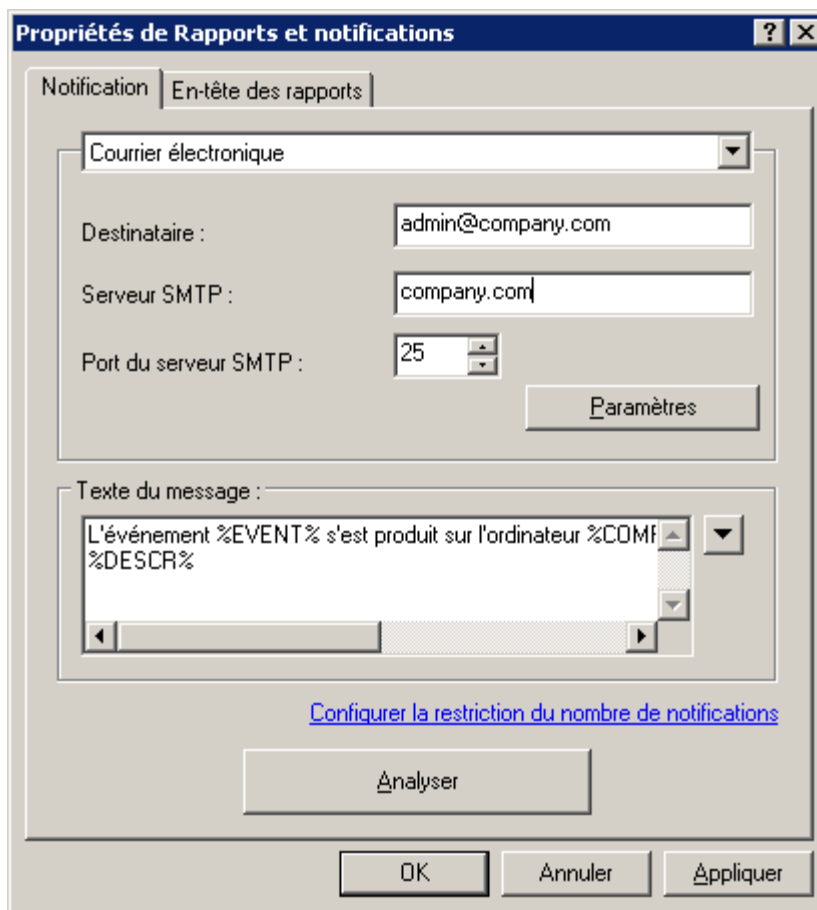


Illustration 47. Modification des paramètres de notification par courrier électronique

FICHIERS AVEC UN TRAITEMENT DIFFERE

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

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

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

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

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

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

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

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

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

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

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

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

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

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

Les experts du service du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application qui ne sont pas traitées dans l'aide. En cas d'infection de votre ordinateur, ils vous aideront à éliminer dans la mesure du possible les programmes malveillants, ainsi qu'à surmonter leurs effets.

Avant de contacter le service du Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique (<http://support.kaspersky.com/fr/support/rules>).

Formulaire de soumission de demande du Support Technique

Vous pouvez poser vos questions aux experts du Support Technique en remplissant le formulaire en ligne du Helpdesk (<http://support.kaspersky.ru/helpdesk.html?LANG=fr>).

Vous pouvez envoyer votre demande en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une demande électronique, vous devez indiquer votre **numéro client** obtenu lors de l'enregistrement sur le site Web du service du Support Technique et le **mot de passe**.

Si vous n'êtes pas un utilisateur enregistré des applications de Kaspersky Lab, remplissez le formulaire d'enregistrement (<https://support.kaspersky.com/ru/personalcabinet?LANG=fr>). Lors de l'enregistrement, indiquez *le code d'activation* de l'application ou *le fichier de licence*.

L'opérateur du service du Support Technique vous enverra sa réponse dans votre Espace personnel (<https://support.kaspersky.com/ru/personalcabinet?LANG=fr>) ainsi qu'à l'adresse électronique que vous avez indiquée dans votre demande.

Dans le formulaire en ligne de demande, décrivez le problème rencontré avec le plus de détails possible. Dans les champs obligatoires, indiquez :

- **Type de la demande.** Les questions le plus souvent posées par les utilisateurs sont regroupées par thème ; par exemple "Problème d'installation/de suppression d'un logiciel" ou "Problème de recherche/de suppression de virus". Si vous ne trouvez pas le sujet qui vous concerne, sélectionnez "Question générale".
- **Nom et version de l'application.**
- **Texte de la demande.** Décrivez le problème rencontré avec le plus de détails possible.
- **Numéro de client et mot de passe.** Saisissez le numéro de client et le mot de passe que vous avez reçu lors de l'enregistrement sur le site Web du service du Support Technique.
- **Adresse électronique.** Les experts du service du Support Technique vous enverront la réponse à votre question.

Support Technique par téléphone

Si le problème est urgent, vous pouvez toujours appeler le Support Technique local de Kaspersky Lab. Si vous contactez le Support Technique français (<http://partners.kaspersky.fr>) ou international (<http://support.kaspersky.com/fr/support/international>) veuillez fournir les informations (<http://support.kaspersky.com/fr/support/details>) concernant votre ordinateur. Ceci aidera nos experts à vous venir en aide le plus rapidement possible.

GLOSSAIRE

A

ADMINISTRATEUR DE KASPERSKY ADMINISTRATION KIT

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

ADMINISTRATION CENTRALISEE DE L'APPLICATION

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

ADMINISTRATION DIRECTE DE L'APPLICATION

Administration de l'application par l'interface locale.

AGENT D'ADMINISTRATION

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

AGENT DE MISE A JOUR

Ordinateur qui joue le rôle d'intermédiaire entre le centre de diffusion des mises à jour et des paquets d'installation dans les limites du groupe d'administration.

APPLICATION INCOMPATIBLE

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui n'est pas compatible avec l'administration par Kaspersky Administration Kit.

B

BASES

Bases de données créées par les experts de Kaspersky Lab et qui contiennent une description détaillée de toutes les menaces connues à l'heure actuelle contre la sécurité informatique, ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces surgissent.

C

CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui sert à l'authentification du Serveur d'administration lors de la connexion de la Console d'administration et de l'échange d'informations avec les postes client. Le certificat du Serveur d'administration est créé lors de l'installation du Serveur d'administration et enregistré dans le sous-dossier Cert du dossier d'installation de l'application.

CLIENT DU SERVEUR D'ADMINISTRATION (POSTE CLIENT)

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

CONSOLE D'ADMINISTRATION KASPERSKY

Composant de l'application Kaspersky Administration Kit qui offre l'interface utilisateur pour les services d'administration du Serveur d'administration et de l'Agent d'administration.

D**DEGRE D'IMPORTANCE DE L'EVENEMENT**

Caractéristique de l'événement enregistré durant le fonctionnement de l'application de Kaspersky Lab. Il existe quatre niveaux de gravité :

Critique.

Erreur.

Avertissement.

Message d'information.

Les événements du même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

DOSSIER DE SAUVEGARDE

Dossier spécial prévu pour conserver les copies de sauvegarde des objets créés avant leur réparation ou leur suppression.

DUREE DE VALIDITE DE LA LICENCE

Période durant laquelle vous pouvez utiliser l'ensemble des fonctions de l'application de Kaspersky Lab. En règle générale, la licence est valide pendant une année calendaire à partir de la date de son installation. Une fois la durée de la licence écoulée, l'application n'est plus opérationnelle : vous ne pourrez plus actualiser les bases de l'application.

E**ETAT DE PROTECTION**

Etat actuel de la protection qui caractérise le niveau de la protection de l'ordinateur.

F**FICHER DE LICENCE**

Fichier possédant l'extension .key qui constitue votre "clé" personnelle indispensable à l'utilisation de l'application de Kaspersky Lab. Le fichier de licence est livré avec le logiciel si vous avez acheté ce dernier chez un revendeur de Kaspersky Lab. Il est envoyé par courrier électronique si vous avez acheté le logiciel en ligne.

G**GROUPE D'ADMINISTRATION**

Sélection d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion dans son ensemble. Le groupe peut se trouver à l'intérieur d'autres groupes. Il est possible de créer dans le groupe les stratégies de groupe pour chacune des applications installées et chacune des tâches de groupe créées.

I**INSTALLATION FORCEEE**

Méthode d'installation à distance des applications de Kaspersky Lab qui permet de réaliser l'installation à distance d'un logiciel sur des postes clients définis. Pour réussir la tâche à l'aide de la méthode de l'installation forcée, le compte utilisateur employé pour le lancement de la tâche doit jouir des privilèges d'exécution à distance des applications sur les postes clients. Cette méthode est recommandée pour l'installation des applications sur les ordinateurs tournant sous les

systèmes d'exploitation Microsoft NT/2000/2003/XP compatibles avec cette possibilité ou sur les ordinateurs tournant sous Microsoft Windows 98/Me sur lesquels l'Agent d'administration est installé.

INSTALLATION A DISTANCE

Installation des applications de Kaspersky Lab à l'aide des services offerts par l'application Kaspersky Administration Kit.

INSTALLATION A L'AIDE D'UN SCRIPT D'OUVERTURE DE SESSION

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer l'exécution de la tâche d'installation à distance à un compte utilisateur (ou plusieurs comptes) concret. Lorsque l'utilisateur s'enregistre dans le domaine, le système tente d'installer l'application sur le poste client depuis lequel l'utilisateur s'est enregistré. Cette méthode est recommandée pour l'installation des applications de la société sur les ordinateurs tournant sous Microsoft Windows 98/Me.

L

LICENCE ACTIVE

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

LICENCE COMPLEMENTAIRE

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

M

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application) reçus depuis les serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR DISPONIBLE

Paquet des mises à jour des modules de l'application Kaspersky Lab qui contient les mises à jour urgentes recueillies au cours d'un intervalle de temps et les modifications dans l'architecture de l'application.

O

OPERATEUR DE KASPERSKY ADMINISTRATION KIT

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

P

PAQUET D'INSTALLATION

Sélection de fichiers pour l'installation à distance de l'application Kaspersky Lab à l'aide du système d'administration à distance Kaspersky Administration Kit. Le paquet d'installation est créé sur la base des fichiers spéciaux avec les extensions .kpd et .kud, inclus dans le distributif de l'application, et contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut.

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs pour l'ensemble de ses types de tâches et responsables du fonctionnement de l'application dans son ensemble, par exemple, paramètres des performances de l'application, paramètres de génération des rapports, paramètres du dossier de sauvegarde.

PARAMETRES DE LA TACHE

Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches.

PLUG-IN D'ADMINISTRATION DE L'APPLICATION

Composant spécial, qui fait office d'interface pour l'administration du fonctionnement de l'application par la Console d'administration. Le plug-in d'administration est spécifique à chaque application. Il est repris dans toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Administration Kit.

POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Ordinateur sur lequel est installé le composant qui fait office d'interface pour l'administration de l'application. Pour les logiciels antivirus, il s'agit de la Console Anti-Virus, pour l'application Kaspersky Administration Kit, de la Console d'administration.

Depuis le poste de travail de l'administrateur, il est possible de réaliser la configuration et l'administration de la partie Serveur de l'administration, et pour Kaspersky Administration Kit, d'élaborer et d'administrer la protection antivirus centralisée du réseau de l'entreprise sur la base des applications de Kaspersky Lab.

R

RESTAURATION

Transfert de l'objet original depuis la quarantaine ou du dossier de sauvegarde vers l'emplacement, où se trouvait l'objet avant qu'il ne soit placé en quarantaine, supprimé ou réparé, ou vers tout autre emplacement désigné par l'utilisateur.

RESTAURATION DES DONNEES DU SERVEUR D'ADMINISTRATION

Il s'agit de la restauration des données du Serveur d'administration à l'aide d'un utilitaire de sauvegarde sur la base des informations présentes dans le dossier de sauvegarde. L'utilitaire permet de restaurer :

la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;

les données de configuration de la structure du groupe d'administration et des postes clients ;

le stockage des paquets d'installation des applications pour l'installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;

le certificat du Serveur d'administration.

S

SAUVEGARDE

Création d'une copie de sauvegarde d'un fichier avant sa suppression ou la réparation et placement de cette copie dans le dossier de sauvegarde avec la possibilité de le restaurer ultérieurement, par exemple en vue de l'analyser à l'aide des bases actualisées.

SAUVEGARDE DES DONNEES DU SERVEUR D'ADMINISTRATION

Copie des données du Serveur d'administration pour la sauvegarde et la restauration ultérieure, réalisée à l'aide de l'utilitaire de copie de sauvegarde. L'utilitaire permet d'enregistrer :

la base du Serveur d'administration (stratégie, tâches, paramètres d'application, événements enregistrés sur le Serveur d'administration) ;

les données de configuration de la structure du groupe d'administration et des postes clients ;

le stockage des paquets d'installation des applications pour l'installation à distance (contenu des dossiers Packages, Uninstall, Updates) ;

le certificat du Serveur d'administration.

SERVEUR D'ADMINISTRATION

Composant de l'application Kaspersky Administration Kit qui remplit la fonction d'enregistrement centralisé des informations sur les applications Kaspersky Lab installées sur le réseau local de la société, et d'un outil efficace de gestion de ces applications.

SERVEURS DE MISE A JOUR KASPERSKY LAB

Liste des serveurs HTTP et FTP de Kaspersky Lab depuis lesquels l'application copie les bases et les mises à jour des modules sur votre ordinateur.

SEUIL DE L'ACTIVITE DU VIRUS

Nombre maximum d'événements d'un certain type admis au cours d'un intervalle déterminé, dont le dépassement sera considéré comme une augmentation de l'activité du virus et l'apparition de la menace d'attaque de virus. Ces données peuvent être utiles en période d'épidémie et permettent à l'administrateur de réagir opportunément à la menace d'une attaque de virus.

STOCKAGE DES COPIES DE SAUVEGARDE

Dossier spécial pour la conservation des copies des données du Serveur d'administration, créées à l'aide de l'utilitaire de copie de sauvegarde.

STRATEGIE

Sélection des paramètres de fonctionnement de l'application dans le groupe d'administration en cas d'administration à l'aide de Kaspersky Administration Kit. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes. Une stratégie propre à chaque application peut être définie. La stratégie contient les paramètres de la configuration complète de toutes les fonctions de l'application.

T

TACHE

Fonctions exécutées par l'application de Kaspersky Lab qui se présente sous la forme d'une tâche, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

TACHE DE GROUPE

Tâche définie pour un groupe et exécutée sur tous les postes clients de ce groupe d'administration.

TACHE LOCALE

Tâche définie et exécutée sur un poste client particulier.

TACHE POUR UNE SELECTION D'ORDINATEURS

Tâche définie pour une sélection des postes clients parmi des groupes d'administration aléatoires et exécutée sur ceux-ci.

KASPERSKY LAB

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les chefs d'analyse antivirus de Kaspersky Lab siègent en tant que membres de la prestigieuse organisation pour la recherche antivirus en informatique (CARO – Computer Anti-virus Researcher's Organization).

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

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

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

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

Site officiel de Kaspersky Lab : <http://www.kaspersky.fr>

Encyclopédie de virus : <http://www.securelist.com/fr/>

Laboratoire Anti-Virus : newvirus@kaspersky.com
(uniquement pour l'envoi d'objets suspects archivés)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>
(pour les demandes auprès des experts en virus)

INFORMATIONS SUR LE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

DANS CETTE SECTION

Code de programme	100
Autre information	119

CODE DE PROGRAMME

Le code de programme développé par d'autres éditeurs a été utilisé pour créer l'application.

DANS CETTE SECTION

BOOST 1.34.1	100
GSOAP 2.7.0D	101
LIBMSPACK 2004-03-08	106
MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86)	115
MICROSOFT CORE XML SERVICES (MSXML) 6.0	115
MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8	115
MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3	116
MYSQL C API	116
OPENSSL 0.9.8L	116
STLPORT 4.6.2	117
UNZIP 5.52	118
VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES	118
WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2)	119
ZLIB 1.2.3	119

BOOST 1.34.1

Copyright (C) 2000-2003, Beman Dawes

GSOAP 2.7.0D

Copyright (C) 2000-2004, Robert A. van Engelen, Genivia, Inc

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

1 DEFINITIONS.

1.0.1.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

01/08/01. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code, or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2 SOURCE CODE LICENSE.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell ("offer to sell and import") the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royaltyfree, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell ("offer to sell and import") the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

3 DISTRIBUTION OBLIGATIONS.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License

including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the LargerWork as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum

extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6 VERSIONS OF THE LICENSE.

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED

LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ONLINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL

APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8 TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10 U.S. GOVERNMENT END USERS.

11 MISCELLANEOUS.

12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

EXHIBIT A.

"The contents of this file are subject to the gSOAP Public License Version 1.3 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.cs.fsu.edu/~engelen/soaplicense.html>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code of the gSOAP Software is: stdsoap.h, stdsoap2.h, stdsoap.c, stdsoap2.c, stdsoap.cpp, stdsoap2.cpp, soapcpp2.h, soapcpp2.c, soapcpp2 lex.l, soapcpp2 yacc.y, error2.h, error2.c, symbol2.c, init2.c, soapdoc2.html, and soapdoc2.pdf, httpget.h, httpget.c, stl.h, stldeque.h, stllist.h, stlvector.h, stlset.h.

The Initial Developer of the Original Code is Robert A. van Engelen. Portions created by Robert A. van Engelen are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contributor(s):

" ____ "

[Note: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

EXHIBIT B.

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001–2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

LIBMSPACK 2004-03-08

Copyright (C) 2003-2004, Stuart Caie

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do

these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original

author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that

any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary

General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the

entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a

portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for

writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and

therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be

linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative

work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by

all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus

excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our

decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO

WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN

WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

In addition to the provisions of the LGPL, you are permitted to use the library directly as part of your build process provided you meet all of the following conditions:

Any modifications to the existing libmspack source code are ALL published and distributed under the LGPL license.

You MUST NOT use function calls, structures or definitions unless they are defined in the public library interface, "mspack.h".

MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86)

Copyright (C) 2008, Microsoft Corporation

MICROSOFT CORE XML SERVICES (MSXML) 6.0

Copyright (C) 2008, Microsoft Corporation

MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8

Copyright (C) 2008, Microsoft Corporation

MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3

Copyright (C) 2007, Microsoft Corporation

MYSQL C API

Copyright (C) 1995-2008, MySQL AB

OPENSSL 0.9.8L

Copyright (C) 1998-2008, The OpenSSL Project

Copyright (C) 1995-1998, Eric A. Young (eay@cryptsoft.com), Tim J. Hudson (tjh@cryptsoft.com)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

STLPORT 4.6.2

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999, 2000, 2001, 2002, Boris Fomitchev

This software is being distributed under the following terms :

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies.

Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

UNZIP 5.52

Copyright (C) 1990-2005, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES

Copyright (C) 2004, Microsoft Corporation

WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2)

Copyright (C) 2008, Microsoft Corporation

ZLIB 1.2.3

ZLIB 1.2.3 Copyright (C) 1995-2005, Jean-loup Gailly, Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

AUTRE INFORMATION

La bibliothèque de programme "Agava-C", développée par OOO "R-Alpha", est utilisée pour vérifier une signature numérique.

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel.

INDEX

A

Administration	
affectation des droits	42
configuration initiale	45
connexion au Serveur d'administration	41
informations relatives au réseau	43
paramètres locaux	58
Administration de l'application	59
Arborescence de la console	18

C

Certificat du Serveur d'administration	37
--	----

D

Déploiement	34
Dossier de sauvegarde	74

G

Groupes d'administration	28
--------------------------------	----

J

Journal des événements	76
------------------------------	----

K

KASPERSKY LAB	99
---------------------	----

L

Licence	
active	73
renouvellement	73

M

Menu contextuel	26
Mise à jour	
diffusion	68, 70
réception	65

P

Panneau des résultats	23
Postes clients	29, 48

Q

Quarantaine et dossier de sauvegarde	74
--	----

R

Rapports	80
Recherche d'un poste	83
Registre des applications	87
Requêtes d'événements	76
Requêtes d'ordinateurs	85

S

Sauvegarde.....	91
Serveur d'administration.....	28
Serveur d'administration secondaire	51
Stratégies.....	31

T

Tâches	31
--------------	----