

Kaspersky Administration Kit 8.0

KASPERSKY **lab**

MANUEL DE REFERENCE

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 : 15/10/2010

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

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

CONTENU

A PROPOS DE CE MANUEL.....	8
Dans ce document.....	8
Conventions.....	9
SOURCES D'INFORMATIONS COMPLEMENTAIRES.....	10
Sources d'informations pour des recherches indépendantes.....	10
Discussion sur les applications de Kaspersky Lab dans le forum.....	11
Contacter le Groupe de rédaction de la documentation pour les utilisateurs.....	11
LANCEMENT ET ARRET DE L'APPLICATION.....	13
ASSISTANT DE CONFIGURATION INITIALE.....	14
Etape 1. Ajout d'une licence.....	14
Etape 2. Sondage de réseau.....	17
Etape 3. Configuration des paramètres de notification.....	18
Etape 4. Configuration du système de protection antivirus.....	18
Etape 5. Téléchargement des mises à jour.....	20
Etape 6. Fin de l'Assistant.....	21
ADMINISTRATION DES SERVEURS D'ADMINISTRATION.....	22
Connexion au Serveur d'administration.....	22
Utilitaire de sélection du compte du service du Serveur d'administration (klsrvswch).....	24
Déconnexion du Serveur.....	25
Permutation entre les Serveurs.....	26
Ajout d'un Serveur à l'arborescence de la console.....	26
Affectation des droits pour travailler avec le Serveur.....	27
Suppression d'un Serveur de l'arborescence de console.....	29
Affichage et modification des paramètres du Serveur d'administration.....	29
Paramètres généraux du Serveur d'administration.....	30
Paramètres de traitement des événements.....	38
Les paramètres de formation de l'événement Attaque de virus.....	46
Règles générales de déplacement des ordinateurs.....	48
Configuration de la collaboration avec le système Cisco Network Admission Control (NAC).....	51
Règles de restriction du trafic.....	53
Serveurs d'administration secondaires.....	54
Ajout d'un Serveur secondaire.....	54
Configurer la connexion d'un Serveur secondaire au Serveur d'administration principal.....	55
Affichage des groupes d'administration du Serveur secondaire.....	56
Connexion au Serveur d'administration via Internet.....	57
ADMINISTRATION DES GROUPES D'ADMINISTRATION.....	58
Création, déplacement et suppression d'un groupe.....	58
Création de structure des groupes d'administration.....	60
Structure des groupes sur la base des domaines et des groupes de travail du réseau Windows.....	61
Structure des groupes sur la base d'Active Directory.....	63
Structure des groupes sur la base du contenu du fichier texte.....	65
Affichage des informations sur un groupe.....	67
Affichage et modification des paramètres du groupe.....	68
Paramètres généraux.....	68

Affectation des droits pour travailler avec un groupe	70
Conditions de définition de l'état du poste.....	71
Surveillance de l'activité des postes clients	72
Installation automatique d'applications sur des postes clients	74
Création de la liste des agents de mise à jour	75
ADMINISTRATION A DISTANCE DES APPLICATIONS.....	76
Administration des stratégies.....	76
Création d'une stratégie	76
Affichage de la stratégie héritée dans le panneau des résultats du groupe imbriqué	79
Affichage et modification des paramètres d'une stratégie.....	79
Activation d'une stratégie	84
Activation d'une stratégie lors d'un événement.....	85
Stratégie pour utilisateur nomade	85
Suppression d'une stratégie.....	87
Copie d'une stratégie	87
Configuration des paramètres de stratégie de l'Agent d'administration	88
Configuration des paramètres de la stratégie du Serveur d'administration	91
Exportation d'une stratégie	96
Importation d'une stratégie.....	97
Conversion des stratégies.....	97
Gérer les tâches	100
Tâches de Kaspersky Administration Kit.....	101
Tâches pour les sélections d'ordinateurs	101
Création d'une tâche de groupe.....	101
Création d'une tâche pour le Serveur d'administration.....	113
Création d'une tâche pour la sélection d'ordinateurs	114
Création d'une tâche locale.....	115
Affichage et modification des paramètres de tâche	117
Affichage d'une tâche de groupe héritée dans le panneau des résultats du groupe imbriqué	123
Démarrage automatique du système d'exploitation sur les postes clients avant le lancement d'une tâche	124
Arrêt de l'ordinateur après l'exécution de la tâche	124
Limitation de la durée d'exécution de la tâche	124
Exportation d'une tâche	124
Importation d'une tâche.....	125
Conversion des tâches	126
Démarrage et arrêt manuels des tâches.....	126
Suspension et reprise manuelles d'une tâche.....	126
Suivi et affichage des comptes-rendus d'activité des tâches	127
Affichage de l'historique des tâches entreposé sur le Serveur d'administration.....	128
Configuration du filtre d'événements pour la tâche de groupe	129
Configuration du filtre des événements du poste sélectionné.....	131
Annulation de la fonction de filtre	133
Paramètres locaux de l'application	133
Affichage des paramètres de l'application.....	134
Configuration des paramètres de l'Agent d'administration	137
POSTES CLIENTS	139
Ajout d'ordinateurs à un groupe.....	139
Affichage d'informations relatives au poste client	140

Affichage d'informations sur le système du poste client	144
Tâche de modification du Serveur d'administration	151
Tâche d'administration du poste client.....	154
Allumer le poste client.....	154
Eteindre le poste client.....	157
Redémarrage du poste client.....	160
Envoi du message à l'utilisateur du poste client	164
Connexion manuelle du poste client au Serveur d'administration. Utilitaire klmover.exe	167
Vérification de la connexion du poste client avec le Serveur d'administration	168
Vérification manuelle de la connexion du poste client au Serveur d'administration. Utilitaire klnagchk.exe....	168
Vérifier la connexion entre le poste client et le Serveur d'administration à l'aide de l'action Analyser la connexion.	169
Utilitaire du diagnostic à distance des postes clients (klactgui)	169
Activation et désactivation du traçage, téléchargement du fichier de traçage.....	170
Téléchargement des paramètres des applications.....	172
Téléchargement des journaux des événements	174
Lancement du diagnostic et téléchargement de ses résultats.....	175
Lancement, relancement et arrêt des applications.....	177
RAPPORTS ET NOTIFICATIONS	179
Créer le nouveau rapport.....	179
Affichage des statistiques	182
Création de la page de statistiques.....	183
Modification de l'ensemble des pages de statistiques.....	185
Création du volet d'information	186
Modification de l'ensemble des panneaux d'informations	190
Affichage et modification des modèles de rapport	191
Génération et affichage de rapports	197
Tâche de diffusion des rapports	200
Rapports d'hierarchie des Serveurs d'administration.....	204
Limitation du nombre d'entrées dans le rapport.....	205
Limite de notifications	207
Notifications	207
Notification par courrier électronique	208
Notifications via NET SEND.....	210
Notification à l'aide du fichier exécutable	211
EXTRACTION DES EVENEMENTS ET DES ORDINATEURS	214
Requêtes d'événements	214
Affichage du journal des événements de Kaspersky Administration Kit.....	214
Création d'une requête d'événements	215
Configuration d'une requête d'événements.....	216
Enregistrement d'informations sur les événements d'un fichier	221
Suppression d'événements.....	222
Requêtes d'ordinateurs.....	222
Affichage d'une requête d'ordinateurs.....	223
Création d'une requête d'ordinateurs	225
Configuration de la requête d'ordinateurs.	226
ORDINATEURS NON DEFINIS	234
Sondage de réseau	234

Affichage et modification des paramètres de sondage du réseau Windows	235
Affichage et modification des paramètres de sondage des groupes Active Directory	237
Affichage et modification des paramètres de sondage des plages IP	238
Affichage et modification des paramètres du domaine	239
Création de la plage IP	241
Affichage et modification des paramètres de plage IP	242
Affichage et modification des paramètres du groupe Active Directory	245
MISE A JOUR	246
Création d'une tâche de téléchargement des mises à jour dans le référentiel	246
Ajout d'une source de mises à jour	249
Configurer la connexion aux serveurs de mises à jour	252
Définition du contenu des mises à jour	254
Configuration d'autres paramètres de la tâche de mise à jour	256
Analyse des mises à jour récupérées	258
Affichage des mises à jour récupérées	261
Déploiement de mises à jour automatique	262
Déploiement de mises à jour vers les clients immédiatement après le téléchargement	262
Redistribution automatique des mises à jour sur les Serveurs secondaires	263
Installation automatique des mises à jour des modules logiciels	263
Constitution de la liste des agents de mise à jour et leur configuration	264
Tâche de récupération des mises à jour par les agents de mise à jour	267
ADMINISTRATION DES LICENCES	270
Affichage des informations sur les licences installées	270
Installation d'une licence	273
Lancement de l'Assistant d'installation de la licence	274
Création et affichage de rapports sur les licences	275
Réception de la licence par le code d'activation	275
Extension automatique de la licence	276
STOCKAGES	277
Paquets d'installation	277
Quarantaine	277
Consultation des propriétés de l'objet placé en quarantaine	278
Suppression d'un objet de la quarantaine	279
Analyse du dossier de quarantaine sur le poste client	279
Restaurer un objet de la quarantaine	280
Sauvegarde d'un objet de la quarantaine sur le disque	280
Dossier de sauvegarde	280
Affichage des propriétés de l'objet placé dans le dossier de sauvegarde	280
Suppression d'un objet depuis le dossier de sauvegarde	281
Restauration d'un objet depuis le dossier de sauvegarde	281
Sauvegarde d'un objet du dossier de sauvegarde sur le disque	282
Fichiers avec un traitement différé	282
Réparation de l'objet du dossier Fichiers avec un traitement différé	282
La sauvegarde de l'objet du fichier Fichiers avec un traitement différé sur le disque	282
Suppression d'un objet du dossier Fichiers avec un traitement différé	283
Registre des applications	283

POSSIBILITES COMPLEMENTAIRES	288
Suivi de l'état de la protection antivirus à l'aide d'informations du registre système	288
Utilisateurs nomades	289
Création du profil pour les utilisateurs nomades	290
Création de la règle de permutation de l'Agent d'administration	293
Ajout d'une condition dans la règle	294
Recherche	298
Recherche d'un poste	299
Recherche de groupes d'administration	307
Recherche de Serveurs d'administration secondaires	309
Copie de sauvegarde des données	311
Tâche de copie de sauvegarde des données	311
Utilitaire de copie de sauvegarde et de restauration des données (klbackup)	314
Mode interactif de création de copie de sauvegarde et de restauration des données	315
Mode non interactif de création de copie de sauvegarde et de restauration des données	316
Déplacement du Serveur d'administration sur un autre ordinateur	317
Suivi des épidémies de virus	318
Activation du mécanisme d'identification d'une attaque de virus	318
Changement de stratégie pour l'application lors de l'enregistrement de l'événement Attaque de virus	321
Automatisation du fonctionnement de Kaspersky Administration Kit (klakaut)	323
Outils externes	323
Configuration de l'interface	323
AIDE	325
Menu contextuel	325
Panneau des résultats	327
Etats des ordinateurs, des tâches et des stratégies	333
GLOSSAIRE	335
KASPERSKY LAB	340
INDEX	341

A PROPOS DE CE MANUEL

Ce document contient une description du rôle de Kaspersky Administration Kit et une description pas à pas de ses fonctions. Les notions principales et les détails généraux de fonctionnement avec l'application sont décrits dans le Manuel d'administrateur de Kaspersky Administration Kit.

DANS CETTE SECTION

Dans ce document	8
Conventions	9

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

- Sources d'informations complémentaires (à la page [10](#)). La section reprend les informations où vous pouvez obtenir des informations sur l'application, excepté l'ensemble de documents livrés avec l'application.
- Lancement et arrêt de l'application (à la page [13](#)). La section décrit le mode de lancement de l'application Kaspersky Administration Kit.
- Assistant de configuration initiale (cf. page [14](#)). La section décrit les étapes de l'Assistant de configuration initiale des paramètres utilisés pour construire le système de gestion de la protection antivirus à l'aide de Kaspersky Administration Kit.
- Administration des Serveurs d'administration (cf. page [22](#)). La section reprend les informations sur les opérations avec les Serveurs d'administration dans le cadre de l'application Kaspersky Administration Kit.
- Administration des groupes d'administration (cf. page [58](#)). La section représente la conception du fonctionnement de Kaspersky Administration Kit avec les groupes d'administration.
- Administration à distance des applications (à la page [76](#)). La section décrit les modes d'administration à distance des applications à l'aide de Kaspersky Administration Kit.
- Postes clients (cf. page [139](#)). La section reprend les informations sur l'administration des postes clients dans le cadre du fonctionnement avec Kaspersky Administration Kit.
- Rapports et notifications (cf. page [179](#)). La section décrit les particularités de gestion des rapports et des notifications dans l'application Kaspersky Administration Kit.
- Requêtes d'événements et d'ordinateurs (cf. page [214](#)). La section reprend les informations sur les modes d'observation du fonctionnement du système de protection antivirus à l'aide de Kaspersky Administration Kit.
- Ordinateurs non définis (cf. page [234](#)). La section décrit les particularités du fonctionnement avec les ordinateurs du réseau de l'entreprise qui ne font pas partie des groupes d'administration.
- Mise à jour (cf. page [246](#)). La section décrit les procédures des mises à jour des bases et des modules des applications administrées à l'aide de Kaspersky Administration Kit.
- Administration des licences (cf. page [270](#)). La section reprend les informations sur l'administration centralisée des licences à l'aide des services Kaspersky Administration Kit.
- Stockages (cf. page [277](#)). La section décrit la manipulation avec les objets utilisés pour la surveillance de l'état des postes client et les entretenir.

- Possibilités complémentaires (cf. page [288](#)). La section aborde les possibilités complémentaires de Kaspersky Administration Kit prévues pour étendre les fonctions d'administration centralisée des applications du réseau informatique.
- Aide (cf. page [325](#)). La section reprend les informations sur les éléments du menu contextuel des objets de la Console d'administration, des objets du panneau des résultats ainsi que des informations sur la valeur des états des objets du réseau et des groupes d'administration.
- Glossaire. La section reprend les termes utilisés dans ce document.
- Kaspersky Lab (à la page [340](#)). La section reprend les informations relatives à Kaspersky Lab.
- 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	10
Discussion sur les applications de Kaspersky Lab dans le forum	11
Contacteur le Groupe de rédaction de la documentation pour les utilisateurs	11

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.

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.

ASSISTANT DE CONFIGURATION INITIALE

L'Assistant permet de réaliser la configuration des paramètres minimum indispensables à la création d'un système d'administration centralisée de la protection contre les virus.

L'Assistant s'ouvre pour la première fois après la connexion au Serveur d'administration.

DANS CETTE SECTION

Etape 1. Ajout d'une licence	14
Etape 2. Sondage de réseau.....	17
Etape 3. Configuration des paramètres de notification.....	18
Etape 4. Configuration du système de protection antivirus	18
Etape 5. Téléchargement des mises à jour.....	20
Etape 6. Fin de l'Assistant.....	21

ÉTAPE 1. AJOUT D'UNE LICENCE

Cette étape vous permet de sélectionner le mode d'ajout d'une licence (cf. ill. ci-après) pour les applications que l'administrateur va administrer à l'aide de Kaspersky Administration Kit.

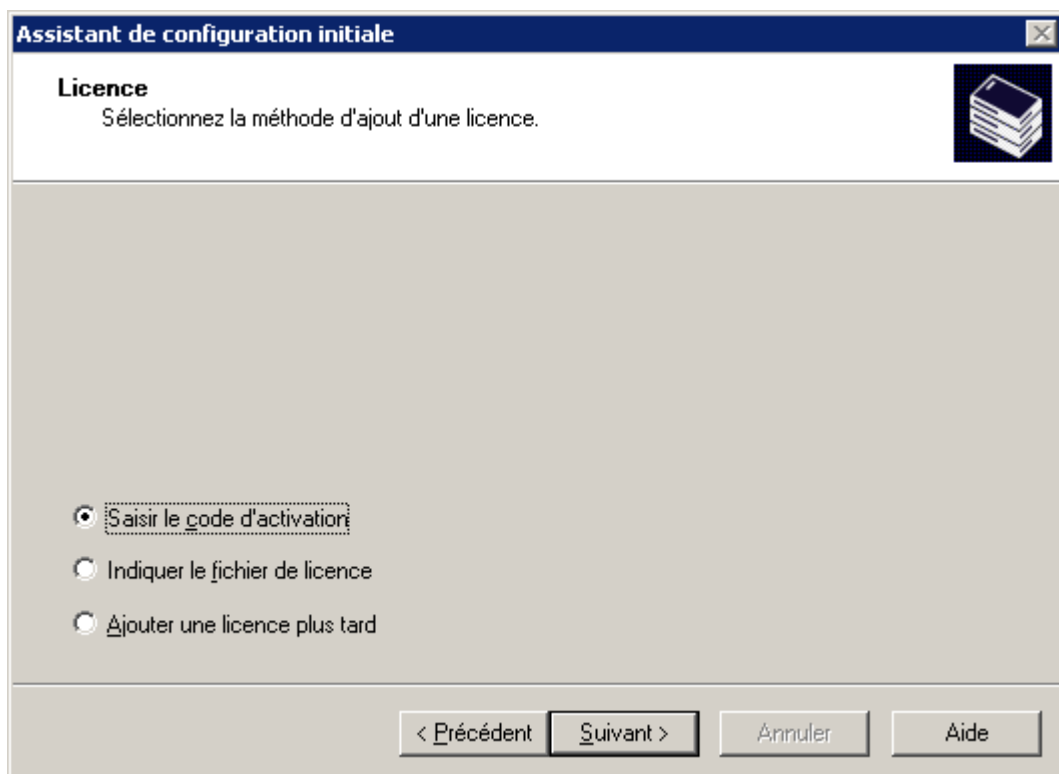
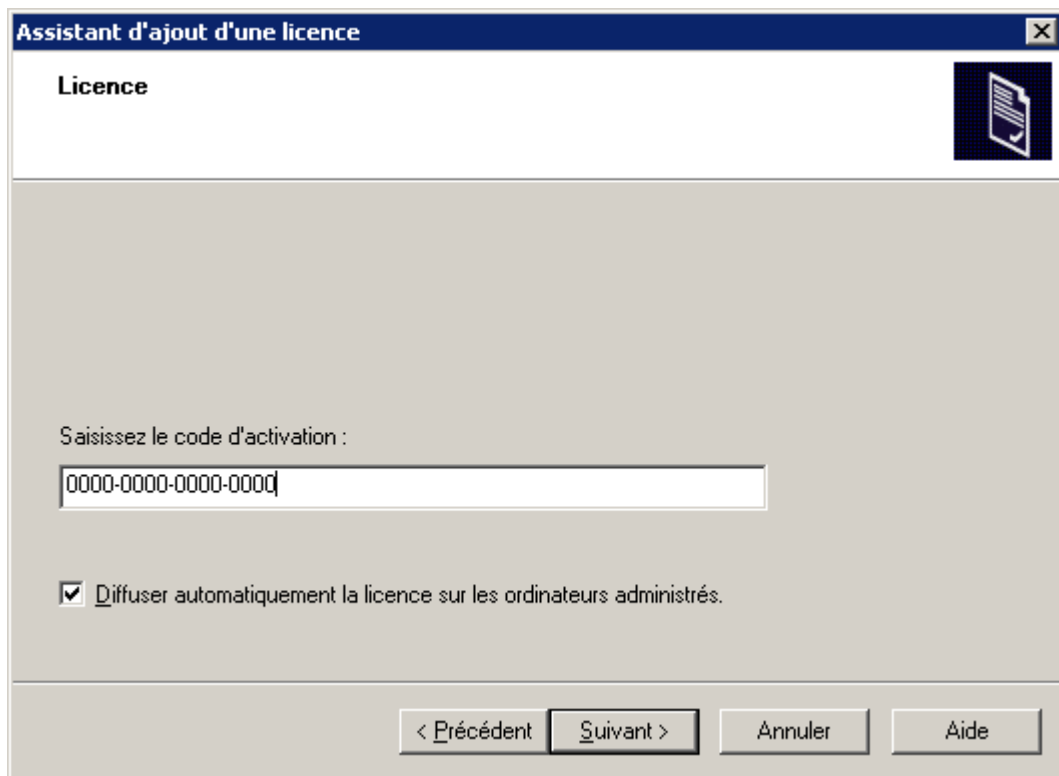


Illustration 1. Sélection du mode d'ajout d'une licence

Sélectionnez un des modes d'ajout d'une licence :

- **Saisir le code d'activation** : on vous proposera de saisir le code reçu lors de l'achat de la version commerciale de l'application (cf. ill. ci-après).



Assistant d'ajout d'une licence

Licence

Saisissez le code d'activation :

0000-0000-0000-0000

Diffuser automatiquement la licence sur les ordinateurs administrés.

< Précédent Suivant > Annuler Aide

Illustration 2. Insertion du code d'activation

Si vous voulez diffuser automatiquement la licence sur les ordinateurs dans les groupes d'administration, cochez la case dans le champ homonyme.

- **Indiquer le fichier de licence** : on vous proposera d'indiquer le fichier de licence (cf. ill. ci-après).

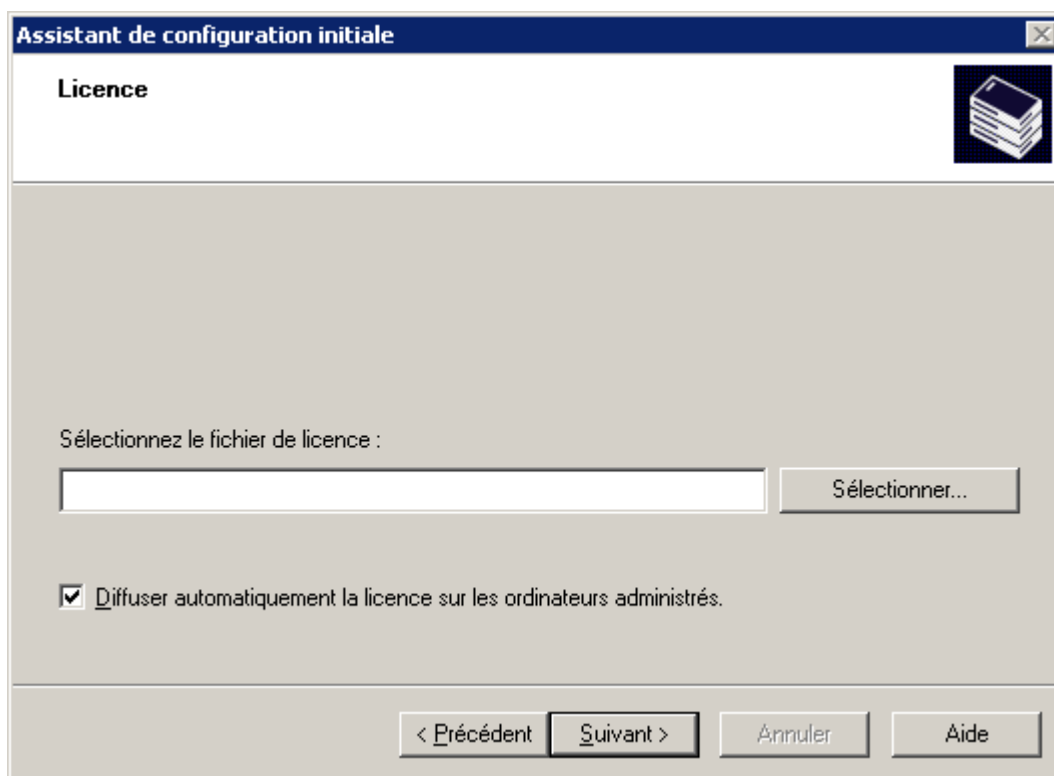


Illustration 3. Sélection du fichier de licence

Si vous voulez diffuser automatiquement la licence sur les ordinateurs dans les groupes d'administration, cochez la case dans le champ homonyme.

- **Ajouter une licence plus tard**. La licence peut être installée plus tard à l'aide de la tâche d'installation d'une licence (cf. section "Installation d'une licence" à la page [273](#)).

ÉTAPE 2. SONDAGE DE RESEAU

C'est pendant cette première étape qu'intervient le sondage du réseau et l'identification des ordinateurs (cf. ill. ci-après). Après le sondage, le groupe de service **Ordinateurs non définis** est créé, ainsi que la structure des dossiers Domaines, Active Directory et Plages IP qui en font partie. Les informations récupérées seront utilisées pour la création automatique du groupe d'administration.

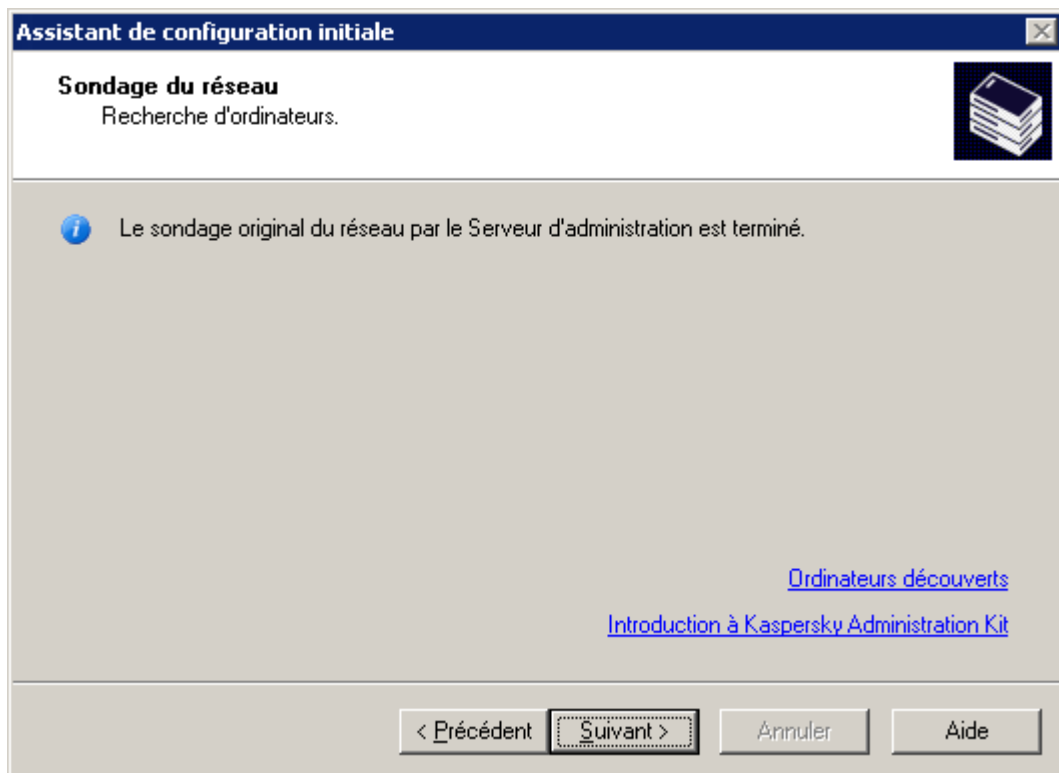


Illustration 4. Fenêtre de l'Assistant de démarrage rapide. Sondage du réseau

Pour afficher la structure du réseau d'ordinateurs, utilisez le lien **Ordinateurs découverts**. Grâce au lien **Introduction à Kaspersky Administration Kit**, vous pouvez découvrir les principales fonctions de Kaspersky Administration Kit.

ÉTAPE 3. CONFIGURATION DES PARAMETRES DE NOTIFICATION

Lors de l'étape suivante, il faut définir les paramètres d'envoi des notifications via courrier électronique pour les événements enregistrés lors du fonctionnement des applications de la société.

Illustration 5. Configuration des paramètres de diffusion des notifications

Si l'autorisation ESMTP est utilisée, cochez la case en regard de **Autorisation ESMTP requise** et remplissez les champs **Nom d'utilisateur**, **Mot de passe** et **Confirmation du mot de passe**. Ces paramètres seront utilisés comme paramètres par défaut pour les stratégies d'applications.

Pour vérifier les paramètres établis, cliquez sur le bouton **Analyser**. Cette action entraîne l'ouverture de la fenêtre d'envoi d'une notification d'essai. En cas d'erreur, des informations détaillées seront fournies.

ÉTAPE 4. CONFIGURATION DU SYSTEME DE PROTECTION ANTIVIRUS

Cette étape correspond à la configuration du système de protection antivirus (cf. ill. ci-après).

L'Assistant de démarrage rapide construit un système de protection antivirus pour les clients du groupe d'administration à l'aide de Kaspersky Anti-Virus pour Windows Workstations version 6.0 MP4. Dans ce cas, le Serveur d'administration crée une stratégie et définit un ensemble minimum de tâches pour le niveau supérieur de la hiérarchie de Kaspersky Anti-Virus pour Windows Workstations version 6.0 MP4. Il configure également une tâche pour récupérer les mises à jour et réaliser une copie de sauvegarde.

Les objets créés par l'Assistant apparaissent dans l'arborescence de la console :

- les stratégies pour les applications Kaspersky Anti-Virus for Windows Workstations et Kaspersky Anti-Virus for Windows Servers version 6.0 MP4 : dans le dossier **Stratégies** du groupe **Ordinateurs administrés** portant les

noms **Stratégie de protection – workstations** et **Stratégie de protection – serveurs** et les paramètres par défaut ;

- les tâches de mise à jour des bases pour les applications Kaspersky Anti-Virus for Windows Workstations et Kaspersky Anti-Virus for Windows Servers version 6.0 MP4 : dans le dossier **Tâches de groupe** du groupe **Ordinateurs administrés** portant les noms **Mise à jour - serveurs** et **Mise à jour - postes de travail** et les paramètres par défaut ;
- les tâches d'analyse à la demande pour les applications Kaspersky Anti-Virus for Windows Workstations et Kaspersky Anti-Virus for Windows Servers version 6.0 MP4 : dans le dossier **Tâches de groupe** du groupe **Ordinateurs administrés** portant les noms **Recherche de virus – postes de travail** et **Recherche de virus – serveurs** et les paramètres par défaut ;
- le téléchargement des mises à jour dans le stockage : dans le dossier **Tâches de Kaspersky Administration Kit** avec le nom **Téléchargement des mises à jour dans le référentiel** et des paramètres par défaut ;
- la tâche de copie de sauvegarde des données du serveur d'administration, dans le dossier **Tâches de Kaspersky Administration Kit** portant le nom **Sauvegarde des données du Serveur d'administration** et les paramètres par défaut.

Les stratégies de Kaspersky Anti-Virus for Windows Workstations version 6.0 MP4 ne sont pas créées si une stratégie pour cette application existe déjà dans le dossier **Ordinateurs administrés**. Si des tâches de groupe pour le groupe **Ordinateurs administrés** et **Téléchargement des mises à jour dans le référentiel** avec ces noms sont déjà créées, elles ne pourront pas non plus être créées.

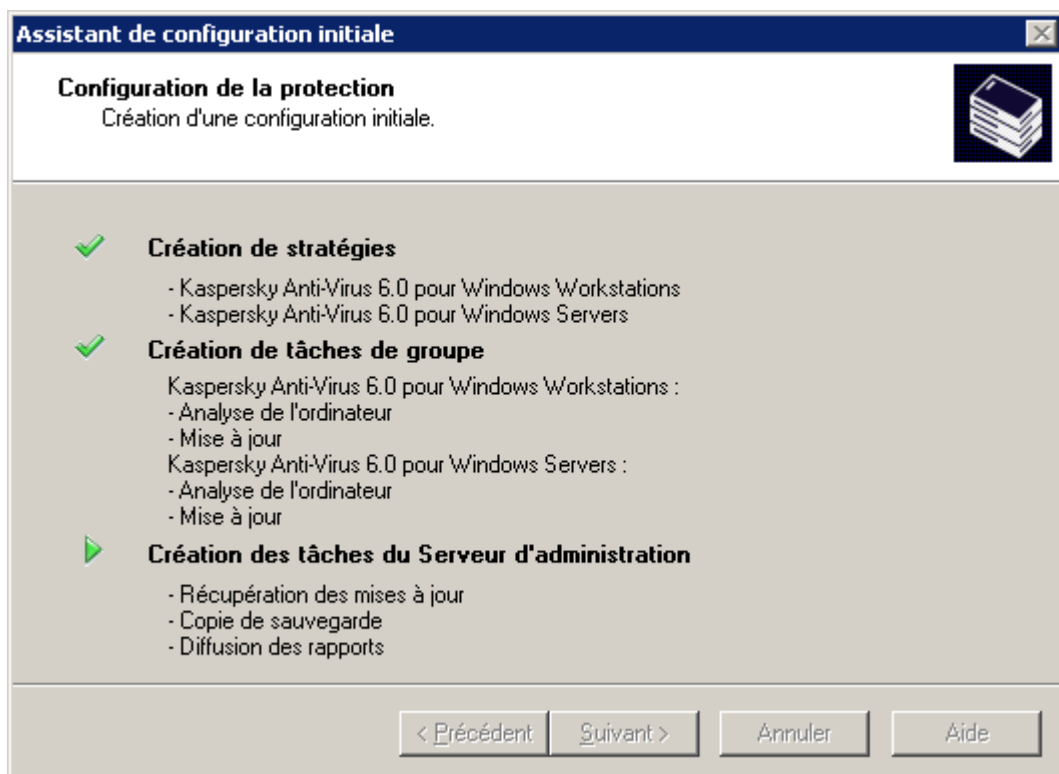


Illustration 6. Configuration du système de protection antivirus

La fenêtre de l'Assistant montre la progression de la création des tâches et des stratégies. En cas d'erreur, le message de circonstance sera affiché.

ETAPE 5. TELECHARGEMENT DES MISES A JOUR

Cette étape correspond au lancement du téléchargement des mises à jour par le Serveur d'administration : la liste des fichiers à télécharger est générée et ceux sont téléchargés (cf. ill. ci-après).

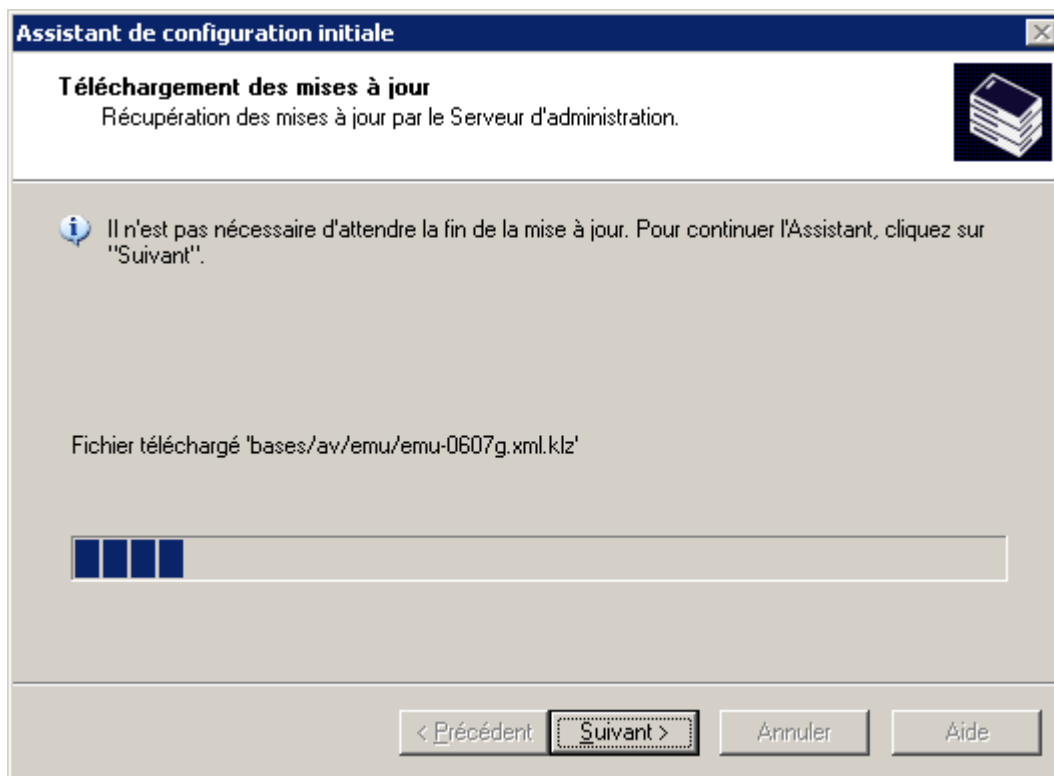


Illustration 7. Configuration du téléchargement des mises à jour

Il est possible de ne pas attendre la fin de la tâche de mise à jour. Les mises à jour poursuivront le téléchargement à l'aide de la tâche **Téléchargement des mises à jour dans le référentiel** (cf. section "**Définition du contenu des mises à jour**" à la page [254](#)).

ETAPE 6. FIN DE L'ASSISTANT

A la fin de l'Assistant de configuration initiale, vous serez invité à commencer le déploiement de la protection. Vous pouvez utiliser cet assistant pour installer l'Agent d'administration. Si vous ne souhaitez pas installer l'application immédiatement après la fin de l'Assistant de configuration initiale, décochez la case **Débuter le déploiement de la protection** (cf. ill. ci-après).

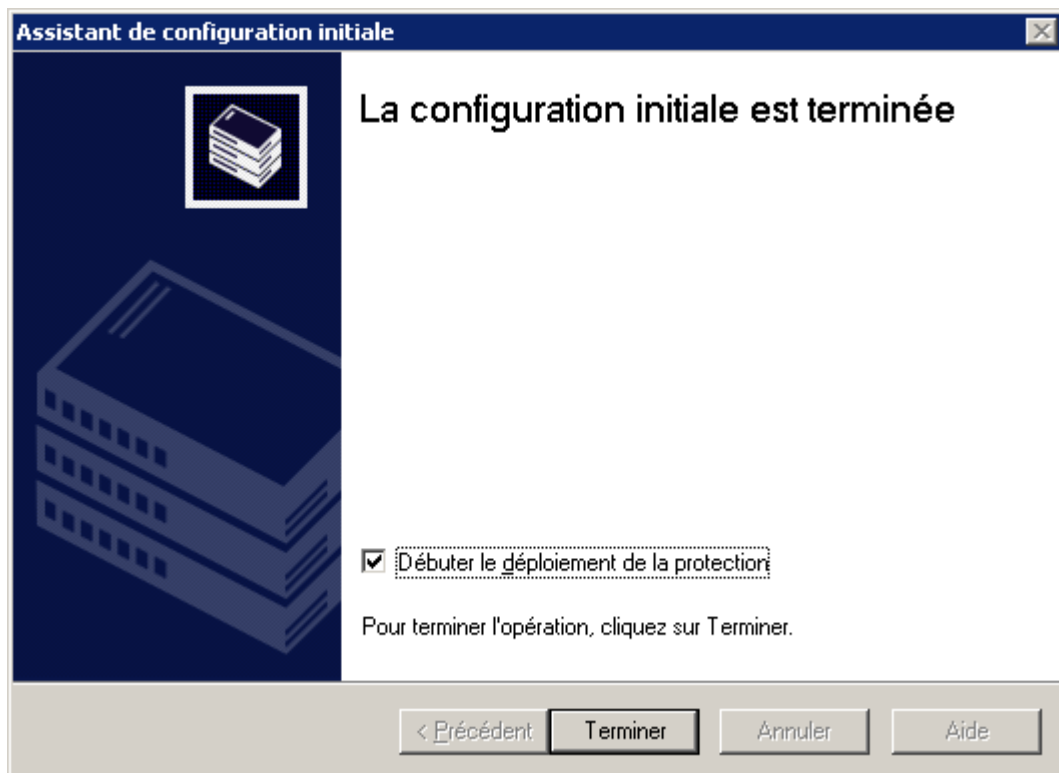


Illustration 8. Fin de l'Assistant de configuration initiale

Pour en savoir plus sur l'Assistant de déploiement, consultez le manuel de déploiement.

ADMINISTRATION DES SERVEURS D'ADMINISTRATION

Le Serveur d'administration est un ordinateur sur lequel est installé le composant **Serveur d'administration**. Il peut exister plusieurs Serveurs de ce genre dans le réseau d'une entreprise. Les opérations suivantes sont possibles avec les Serveurs d'administration :

- connexion/déconnexion ;
- ajout/suppression de l'arborescence de console ;
- connexion à un autre Serveur d'administration ;
- construction de la hiérarchie des Serveurs d'administration ;
- création et configuration des tâches de diffusion des rapports, de mise à jour et de copie de sauvegarde.

DANS CETTE SECTION

Connexion au Serveur d'administration.....	22
Utilitaire de sélection du compte du service du Serveur d'administration (klsrvswch).....	24
Déconnexion du Serveur.....	25
Permutation entre les Serveurs.....	26
Ajout d'un Serveur à l'arborescence de la console.....	26
Affectation des droits pour travailler avec le Serveur.....	27
Suppression d'un Serveur de l'arborescence de console.....	29
Affichage et modification des paramètres du Serveur d'administration.....	29
Serveurs d'administration secondaires.....	54
Connexion au Serveur d'administration via Internet.....	57

CONNEXION AU SERVEUR D'ADMINISTRATION

◆ *Pour se connecter au Serveur d'administration, procédez comme suit :*

Sélectionnez le Serveur d'administration souhaité dans l'arborescence de console.

Une tentative de connexion au Serveur d'administration est réalisée. S'il existe plusieurs Serveurs d'administration sur votre réseau, le programme se connectera au dernier Serveur utilisé lors d'une session précédente de Kaspersky Administration Kit. Lors du premier démarrage, l'application suppose que le Serveur d'administration et la Console d'administration se trouvent sur le même ordinateur. Par conséquent, le programme essaiera d'établir une connexion avec celui-ci.

Si le Serveur est introuvable, il faut indiquer le nom de Serveur manuellement dans la boîte de dialogue **Paramètres de connexion** (cf. ill. ci-après). Dans la zone **Adresse du serveur** indiquez l'adresse du Serveur indispensable. Vous pouvez indiquer l'adresse IP ou le nom de l'ordinateur dans le réseau Windows.

Pour vous connecter au serveur d'administration à travers un port différent du port par défaut, indiquez, dans le champ **Adresse du serveur** la valeur au format <Nom du serveur>:<Port>.

Illustration 9. Etablissement de la connexion au Serveur d'administration

En cliquant sur le bouton **Avancé**, vous pouvez afficher ou masquer les paramètres avancés de connexion suivants :

- **Utiliser la connexion SSL.** Cochez cette case pour échanger des données entre le Serveur d'administration et la Console d'administration via le protocole SSL. Enlevez la coche si vous ne voulez pas communiquer par SSL. Cependant, ceci pourrait compromettre la protection contre l'interception et la modification des données.
- **Utiliser la compression de données.** Cochez cette case pour accélérer la vitesse de transfert des données entre la Console d'administration et le Serveur grâce à la réduction du volume des données transmises et à la diminution de la charge sur le Serveur d'administration.

L'activation de ce paramètre peut entraîner une augmentation de la charge sur le processeur central de l'ordinateur où la Console d'administration est installée.

- **Utiliser le serveur proxy.** Cochez cette case pour vous connecter au Serveur d'administration à travers un proxy (cf. ill. ci-dessus). Dans le champ **Adresse** saisissez l'adresse pour la connexion au serveur proxy. Remplissez les champs **Nom d'utilisateur** et **Mot de passe** si l'authentification est requise pour accéder au serveur proxy.

Le système vérifie ensuite si l'utilisateur jouit des privilèges de connexion au Serveur d'administration et en cas d'utilisation du mode de connexion SSL, la Console d'administration authentifie le Serveur d'administration avant de contrôler les droits utilisateur.

Si vous reliez au Serveur pour la première fois ou si le certificat du Serveur dans cette session diffère de votre copie locale, le programme affiche une demande de connexion au Serveur et de réception d'un nouveau certificat (cf. ill. ci-après). Vous avez le choix parmi les options suivantes :

- **Je veux me connecter au Serveur et télécharger le certificat :** sélectionnez cette option pour vous connecter au serveur d'administration et recevoir automatiquement un nouveau certificat.
- **Je veux réessayer d'authentifier le Serveur d'administration à l'aide du certificat :** sélectionnez cette option pour indiquer manuellement l'emplacement du fichier de certification. Cliquez sur **Sélectionner** pour

indiquer le fichier de certification. Il possède l'extension .cer et se trouve sur le Serveur d'administration dans le dossier Cert du dossier d'installation de Kaspersky Administration Kit indiqué lors de l'installation de l'application. Le Serveur d'administration sera authentifié à nouveau en utilisant le certificat choisi.

Vous pouvez copier le fichier de certification dans un dossier partagé ou un périphérique externe de sauvegarde. Cette copie peut être utilisée pour configurer des paramètres d'accès au Serveur de la copie de ce fichier.

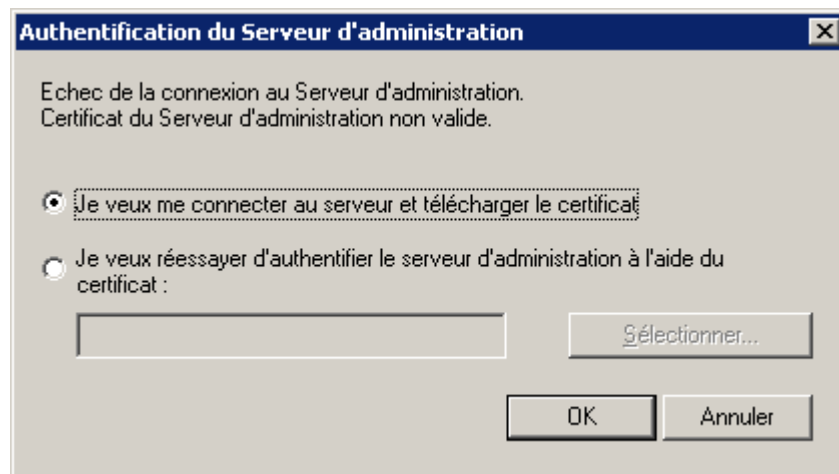


Illustration 10. Demande de confirmation de la connexion au Serveur d'administration

Les droits des utilisateurs sont vérifiés en utilisant le procédé d'authentification d'utilisateur de Windows. Si l'utilisateur n'est pas autorisé à accéder au Serveur d'administration, autrement dit, s'il ne dispose pas de privilèges d'opérateur (**KLOperators**) ou d'administrateur (**KLAdmins**) de Kaspersky Administration Kit, il sera invité à réaliser la procédure d'enregistrement pour accéder au Serveur d'administration (cf. ill. ci-après). Dans le format approprié, indiquez le compte d'utilisateur et le mot de passe disposant de privilèges d'opérateur ou d'administrateur de Kaspersky Administration Kit.



Illustration 11. Enregistrement d'un utilisateur pour accéder au Serveur d'administration

En cas de connexion réussie au Serveur d'administration, la structure des réseaux de ce Serveur et ses paramètres sont affichés dans l'arborescence de console.

UTILITAIRE DE SELECTION DU COMPTE DU SERVICE DU SERVEUR D'ADMINISTRATION (KLSRVSWCH)

En utilisant cet utilitaire, vous pouvez définir le compte pour lancer le Serveur d'administration comme un service sur cet

ordinateur (cf. ill. ci-après). En lançant l'utilitaire, sélectionnez l'une des deux options suivantes :

- **Compte du système local** : le Serveur d'administration est en cours d'exécution sous le compte et avec les privilèges *Compte du système local*.

Pour que Kaspersky Administration Kit fonctionne correctement, il faut que le compte possède les droits d'accès d'administrateur des ressources pour le placement de la base des informations du Serveur d'administration au démarrage du Serveur d'administration.

- **Compte d'utilisateur** : le Serveur d'administration sera lancé sous un compte utilisateur inclus dans le domaine. Dans ce cas, le Serveur d'administration initiera toutes les opérations avec les privilèges de ce compte. A l'aide du bouton **Rechercher** définissez l'utilisateur, dont le compte sera utilisé, et saisissez le mot de passe.

Si en tant que compte pour lancer le Serveur d'administration vous avez sélectionné le compte utilisateur du domaine, alors il vous sera proposé de définir cet utilisateur et de saisir le mot de passe pour son compte.

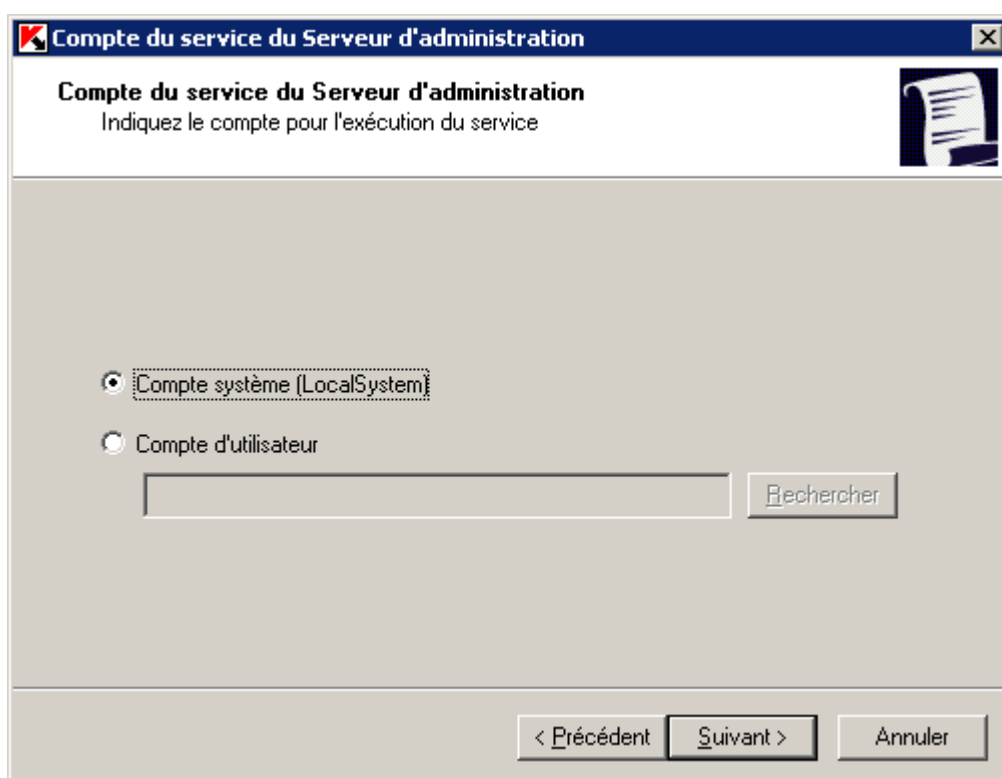


Illustration 12. Sélection d'un compte

En utilisant le serveur SQL en mode d'authentification de Windows, le compte utilisateur doit posséder l'accès aux bases de données. Le compte utilisateur doit posséder la base de données de Kaspersky Anti-Virus. Le schéma dbo doit être utilisé par défaut.

DECONNEXION DU SERVEUR

► Pour se déconnecter du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.
2. Ouvrez le menu contextuel.

- Sélectionnez la commande **Déconnecter du Serveur d'administration**.

PERMUTATION ENTRE LES SERVEURS

Si plusieurs Serveurs d'administration sont ajoutés dans l'arborescence de la console, alors vous pouvez se déplacer entre eux pour fonctionner avec eux.

➤ *Pour se connecter à un autre Serveur d'administration, procédez comme suit :*

- Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur requis.
- Ouvrez le menu contextuel et sélectionnez la commande **Connecter au Serveur d'administration**.

Dans la fenêtre **Paramètres de connexion** qui s'ouvre, saisissez le nom du Serveur avec lequel vous avez l'intention de travailler et définissez les paramètres de connexions au Serveur requis (cf. section "Connexion au Serveur d'administration" à la page [22](#)).

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

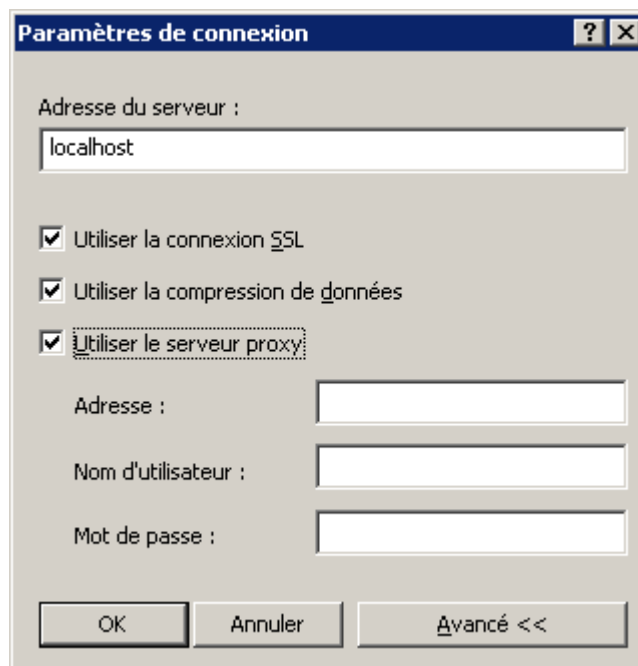


Illustration 13. Etablissement de la connexion au Serveur d'administration

- Cliquez sur le bouton **OK** pour terminer la permutation entre les Serveurs.

Si la connexion au Serveur réussit, le contenu de l'entrée correspondante est mis à jour.

AJOUT D'UN SERVEUR A L'ARBORESCENCE DE LA CONSOLE

➤ *Pour ajouter un nouveau Serveur d'administration à l'arborescence de la console, procédez comme suit :*

- Dans la fenêtre principale de Kaspersky Administration Kit, sélectionnez l'entrée **Kaspersky Administration Kit** dans l'arborescence de la console.

- Ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Serveur d'administration**.

Une nouvelle entrée appelée **Serveur d'administration - <nom de l'ordinateur> (Non connecté)** apparaîtra dans l'arborescence de console. Utilisez cette entrée pour la connecter à n'importe quel Serveur installé sur votre réseau des Serveurs d'administration.

AFFECTATION DES DROITS POUR TRAVAILLER AVEC LE SERVEUR

➔ Pour accorder des droits pour travailler sur un Serveur d'administration, procédez comme suit :

- Dans la fenêtre principale de Kaspersky Administration Kit, sélectionnez l'entrée dans l'arborescence de la console qui correspond au Serveur d'administration requis. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.
- Dans la fenêtre **Propriétés de Serveur d'administration – <Nom de l'ordinateur>** (cf. ill. ci-après) qui s'ouvre, choisissez l'onglet **Sécurité**.

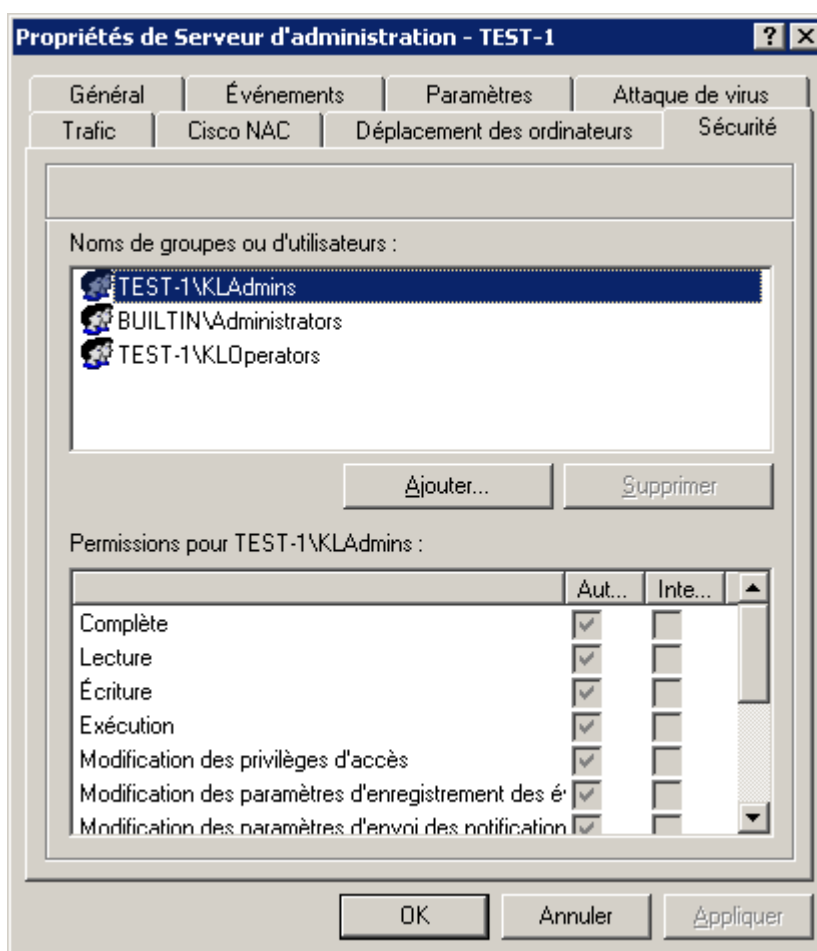


Illustration 14. Attribution des privilèges d'accès au Serveur d'administration

La présence ou l'absence de cet onglet est définie par les paramètres d'interface de l'utilisateur. Afin de configurer l'affichage de cet onglet, passez au menu **Vue** → **Configuration de l'interface** et cochez la case dans la ligne **Afficher les onglets avec les paramètres de sécurité**.

La partie supérieure de l'onglet reprend la liste des utilisateurs et des groupes des utilisateurs qui possèdent l'accès au

Serveur d'administration. La partie inférieure reprend les privilèges possibles :

- **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.

Pour se connecter au Serveur d'administration, l'utilisateur doit avoir l'autorisation sur la **Lecture**.

➔ Pour indiquer les privilèges sur le travail avec le Serveur, procédez comme suit :

1. Sélectionnez le groupe d'utilisateurs.
2. Dans la colonne **Autoriser** cochez les cases en regard des autorisations octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.
3. Dans la colonne **Interdire** cochez les cases en regard des autorisations qui ne peuvent être octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.

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

Pour supprimer le groupe ou l'utilisateur, il faut sélectionner l'objet dans la liste et cliquer sur le bouton **Supprimer**.

Il est impossible de supprimer le groupe d'administrateurs de Kaspersky Administration Kit (KLAdmins).

Pour appliquer le paramètre, il suffit de cliquer sur **Appliquer** ou **OK**.

SUPPRESSION D'UN SERVEUR DE L'ARBORESCENCE DE CONSOLE

➔ Pour supprimer un Serveur d'administration de l'arborescence de la console, procédez comme suit :

1. Sélectionnez l'entrée correspondant au Serveur d'administration à supprimer dans l'arborescence de console.
2. Ouvrez le menu contextuel.
3. Sélectionnez le point **Supprimer**.

AFFICHAGE ET MODIFICATION DES PARAMETRES DU SERVEUR D'ADMINISTRATION

Les liens du panneau des tâches du Serveur d'administration permettent de passer rapidement aux fonctions suivantes :

- installation de la protection antivirus ;
- organisation des groupes d'administration ;
- configuration des paramètres de mise à jour, de protection et d'analyse ;
- affichage des statistiques et configuration des notifications.

La fenêtre des propriétés du Serveur d'administration présente les paramètres de ce dernier et permet d'introduire les modifications requises.

➔ Pour ouvrir la fenêtre des propriétés du Serveur, procédez comme suit :

1. Sélectionnez le Serveur requis dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.

La fenêtre qui s'ouvre contient un ensemble d'onglets qui permettent d'afficher et de modifier les paramètres suivants du Serveur d'administration :

- connexion au Serveur d'administration (cf. section "Paramètres généraux du Serveur d'administration" à la page [30](#)) ;
- attribution de privilèges d'accès au Serveur (cf. section "Affectation des droits pour travailler avec le Serveur" à la page [27](#)) ;
- enregistrement des événements (cf. section "Paramètres de traitement des événements" à la page [38](#)) ;
- déplacement des ordinateurs (cf. section "Règles générales de déplacement des ordinateurs" à la page [48](#)) ;
- restriction du trafic pour des intervalles IP et des plages IP (cf. section "Règles de restriction du trafic" à la page [53](#)) ;
- formation de l'événement Attaque de virus (cf. section "Paramètres de formation de l'événement Attaque de virus" à la page [46](#)) ;
- configuration de la collaboration avec Cisco NAC (cf. section "Configuration de la collaboration avec le système Cisco Network Admission Control (NAC)" à la page [51](#)).

PARAMETRES GENERAUX DU SERVEUR D'ADMINISTRATION

Les paramètres généraux du Serveur d'administration peuvent être configurés sous les onglets **Général**, **Paramètres** et **Sécurité**.

Sur l'onglet **Général** (cf. ill. ci-après), vous retrouverez les informations suivantes :

- nom du composant (Serveur d'administration) et nom de l'hôte du réseau Windows sur lequel est installé le composant ;
- numéro de la version installée.

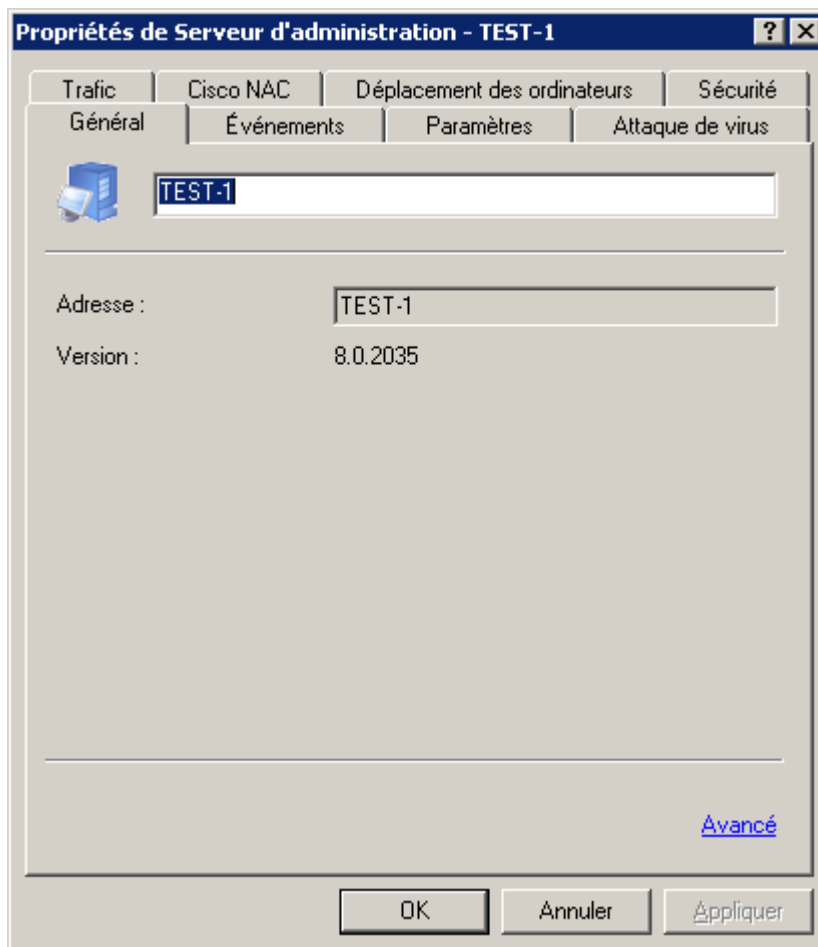


Illustration 15. Affichage des propriétés du Serveur d'administration. Onglet **Général**

Affichage des propriétés du Serveur d'administration. Onglet **Général**

Le lien **Avancé** ouvre une fenêtre qui reprend les informations suivantes (cf. ill. ci-après) :

- Chemin d'accès au dossier partagé de conservation des fichiers de l'installation à distance de l'application et le stockage des mises à jour copiées depuis la source sur le Serveur d'administration. Vous pouvez changer le chemin vers le dossier d'accès public à l'aide du bouton **Modifier**.

- Le lien **Statistiques de fonctionnement du Serveur d'administration** permet d'ouvrir la fenêtre des statistiques générales du Serveur d'administration.

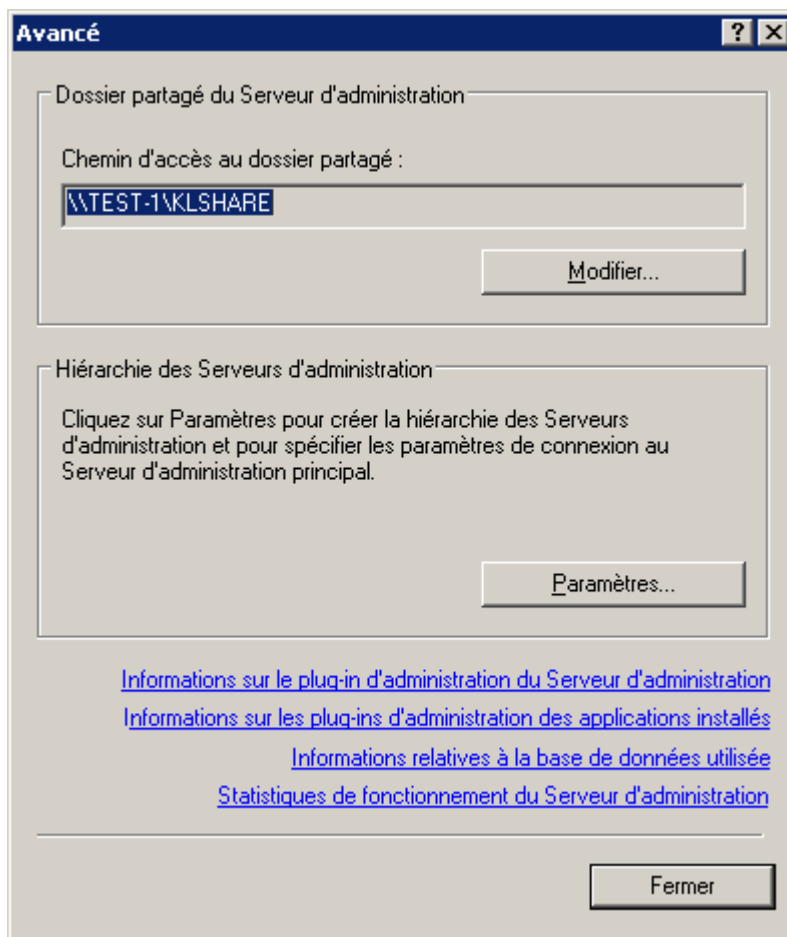


Illustration 16. Propriétés du Serveur d'administration. Fenêtre **Avancé**

- Le lien **Information sur le plugin du Serveur d'administration** permet d'ouvrir la fenêtre de consultation des propriétés du plug-in (cf. ill. ci-après). La fenêtre reprend les informations suivantes :
 - nom et chemin d'accès complet au fichier du plug-in d'administration ;
 - version de l'application ;
 - informations sur le fabricant (**Kaspersky Lab**) et sur le copyright ;

- date et heure de création du plug-in d'administration.

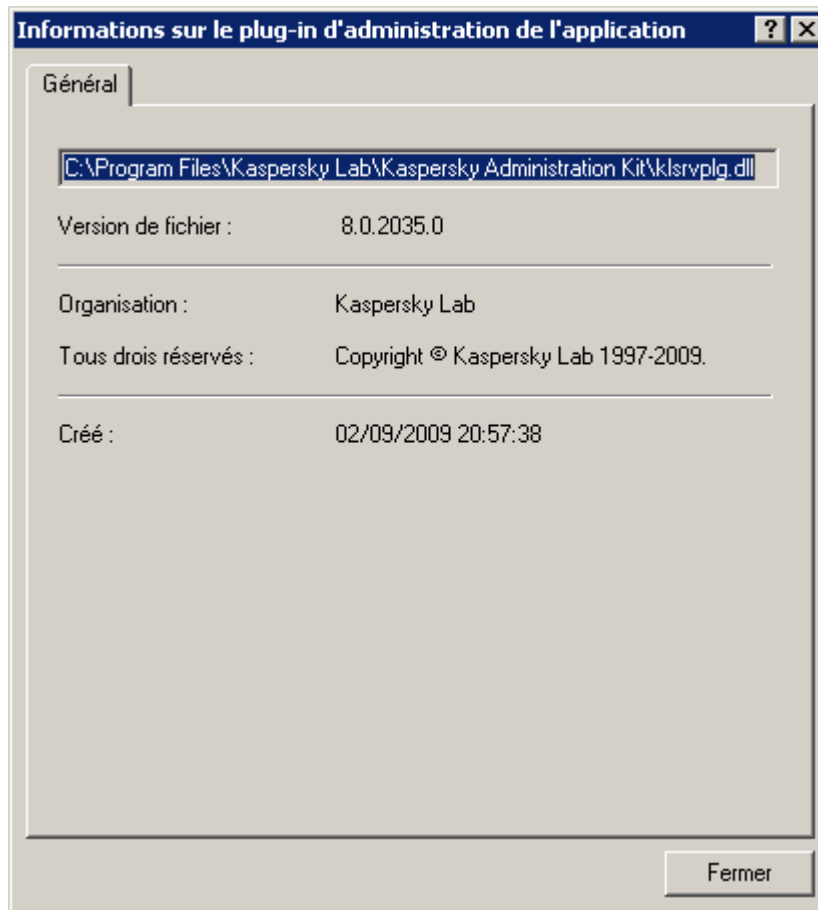


Illustration 17. Fenêtre de consultation des propriétés du plug-in d'administration de l'application

- Le lien **Informations sur les plug-ins d'administration des applications installés** permet d'ouvrir la fenêtre contenant la liste des logiciels installés sur le Serveur d'administration (cf. ill. ci-après). Chacun d'entre eux est accompagné du nom de l'application et de la version du logiciel. Cette fenêtre vous permet de consulter les informations détaillées sur le plug-in d'administration choisi de l'application, en cliquant sur le bouton **Information**.

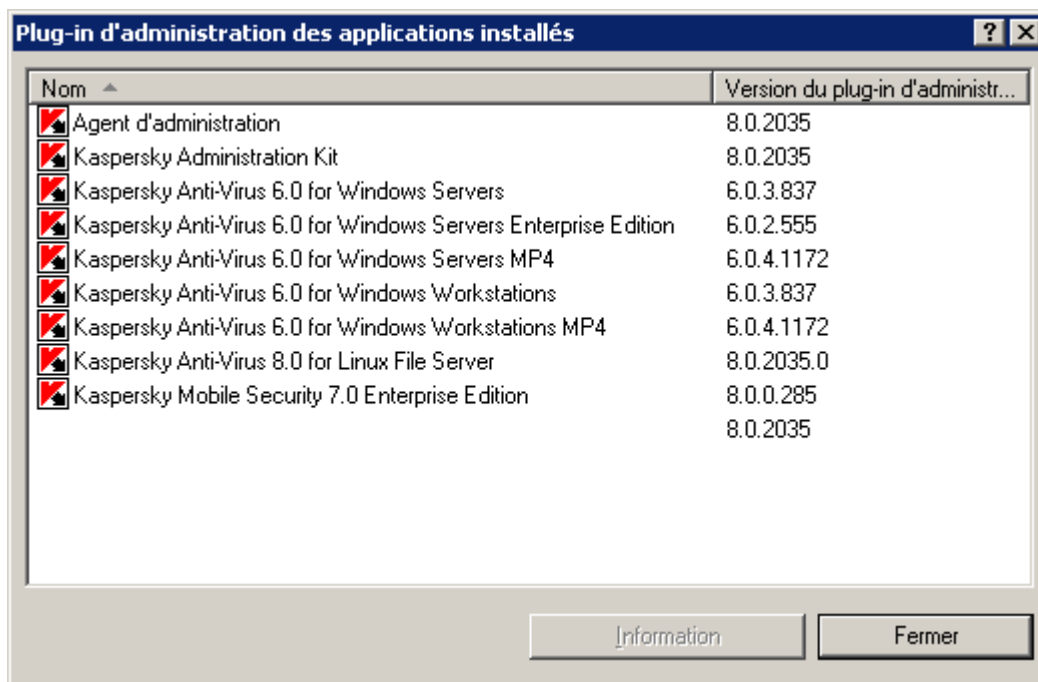


Illustration 18. Liste des logiciels d'administration des applications installés sur le Serveur d'administration

- Le lien **Informations relatives à la base de données utilisée** permet d'ouvrir la fenêtre des propriétés de la base de données utilisée (cf. ill. ci-après). Cette fenêtre reprend les informations suivantes :
 - le nom du serveur de bases de données utilisé ;
 - le nom de l'exemplaire de service du serveur de bases de données ;

- le nom de la base de données.

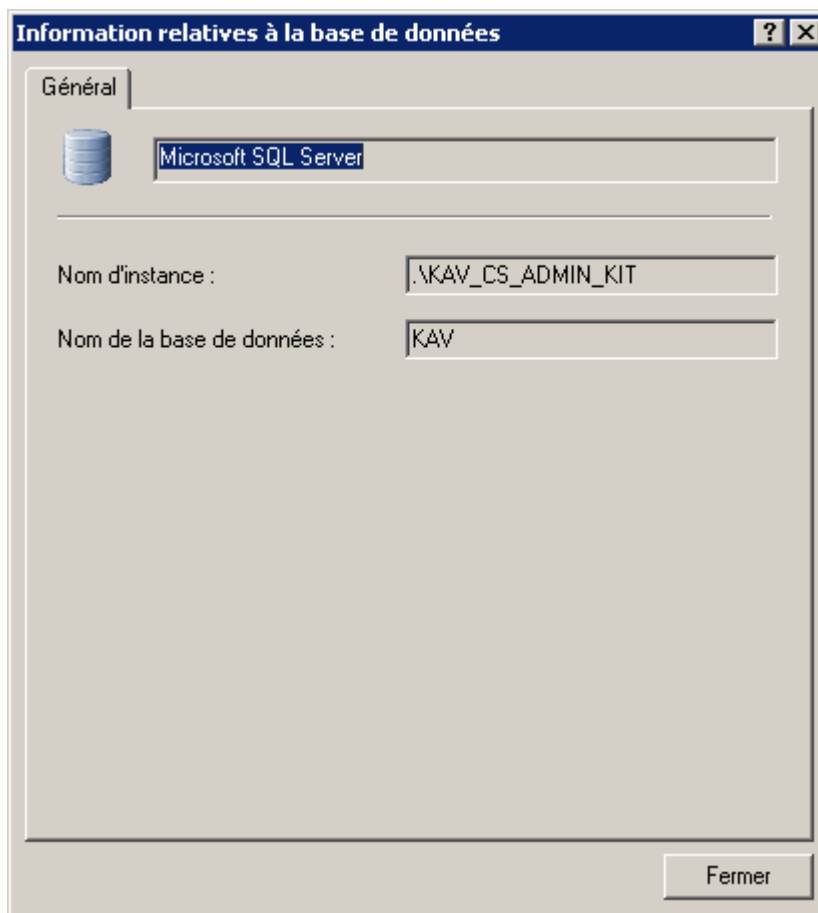


Illustration 19. Affichage d'informations sur la base de données

- En cliquant sur le bouton **Paramètres**, dans le groupe **Hiérarchie des Serveurs d'administration**, vous pouvez ouvrir la fenêtre de configuration de la hiérarchie des Serveurs d'administration (cf. ill. ci-après). Dans cette boîte de dialogue, vous pouvez :
 - indiquer si le Serveur d'administration est un Serveur secondaire en cochant la case **Ce Serveur d'administration est un serveur secondaire** ;
 - définir l'adresse du Serveur d'administration principal dans le champ **Adresse** ;
 - indiquer ou modifier le chemin d'accès au fichier du certificat du Serveur d'administration principal, en cliquant sur le bouton **Sélectionner** ;
 - définir les paramètres du serveur proxy pour se connecter au Serveur d'administration principal.

Si, dans la stratégie du Serveur d'administration, la case **Autoriser la modification de la hiérarchie des Serveurs d'administration secondaires** est décochée, ces paramètres sont en lecture seule.

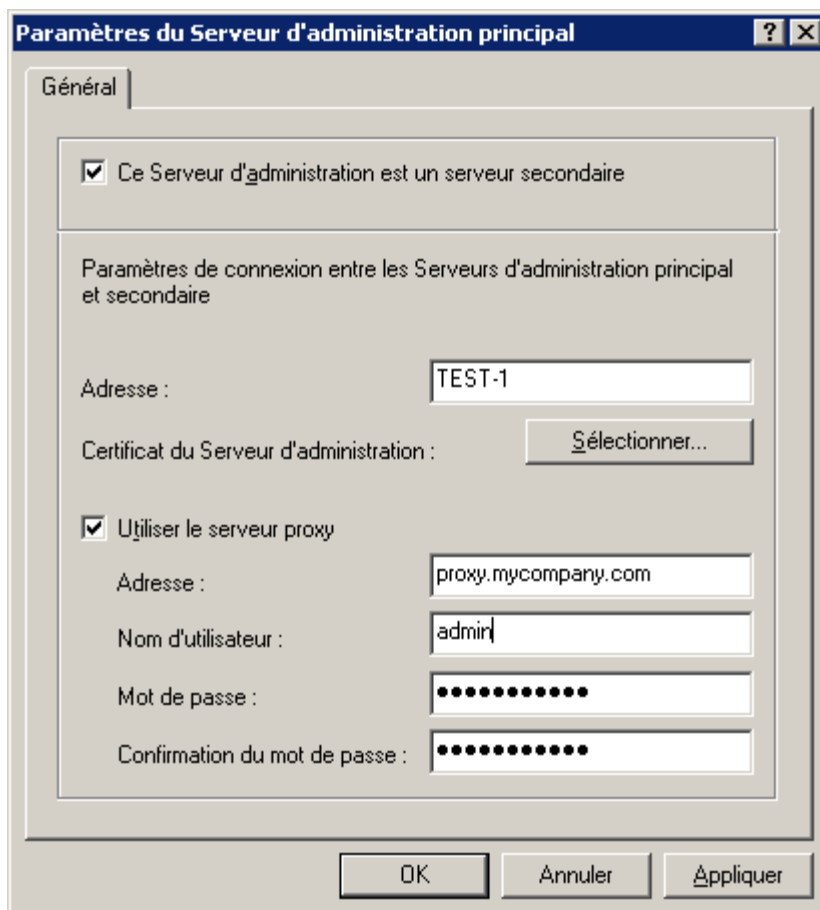


Illustration 20. Configuration dans le Serveur principal des infos du Serveur secondaire

Sur l'onglet **Paramètres** (cf. ill. ci-après) vous retrouverez les paramètres du Serveur d'administration. Le groupe **Paramètres de connexion au Serveur d'administration** contient les numéros des ports, à l'aide desquels les connexions suivantes sont réalisées :

- Connexion au Serveur d'administration. Le numéro de port par défaut est 14000. Si ce port est déjà en service, vous pouvez en changer.
- Connexion sécurisée avec le Serveur d'administration par le protocole SSL. Par défaut, il s'agit du port 13000.
- Connexion des appareils nomades au Serveur d'administration. Le numéro de port par défaut est 13292. Pour activer l'utilisation de ce port sur le Serveur d'administration, cochez la case **Ouvrir le port pour les périphériques mobiles**.

Vous pouvez également préciser dans le champ correspondant le nombre maximum d'événements qui seront conservés dans la base de données du Serveur d'administration.

Dans le groupe **Visibilité de l'ordinateur dans le réseau** dans le champ **Délai de visibilité de l'ordinateur (min.)** définissez la durée pendant laquelle l'hôte est considéré comme visible dans le réseau après une perte de la connexion au Serveur d'administration. Par défaut, l'intervalle est fixé à 60 minutes. A la fin de cette période, le Serveur d'administration considérera que l'hôte est inactif.

Le cas échéant, vous pouvez modifier les valeurs de ces paramètres.

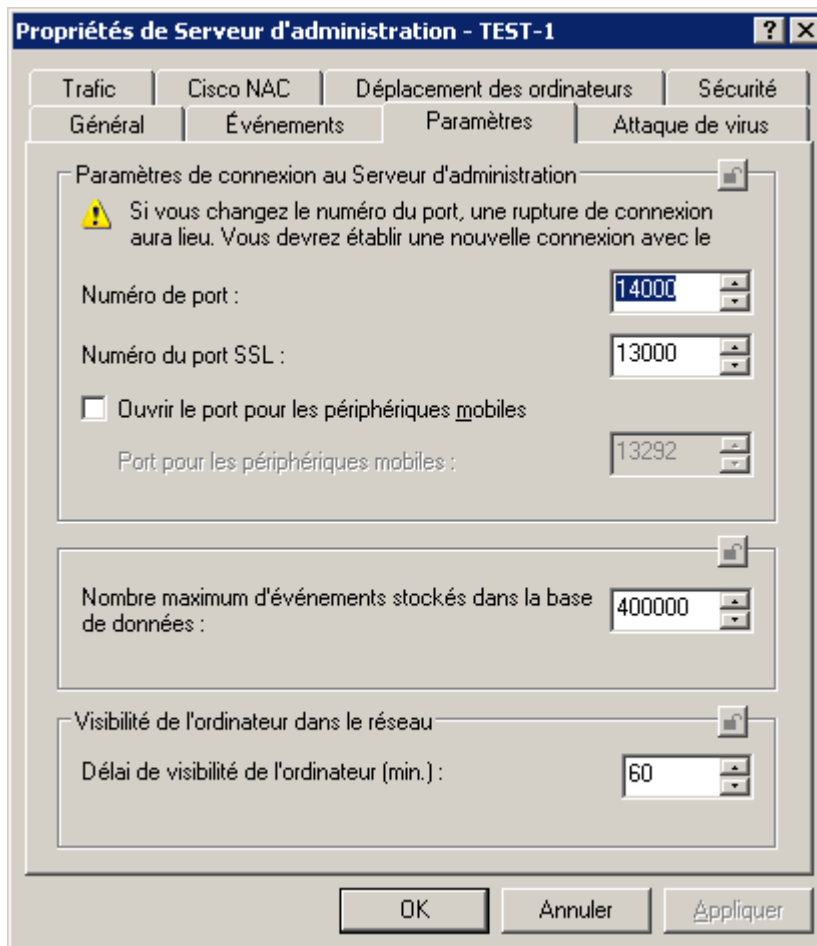


Illustration 21. Affichage des propriétés du Serveur d'administration. Onglet **Paramètres**

L'onglet **Sécurité** (cf. ill. ci-après) permet de configurer les privilèges d'accès au Serveur d'administration (cf. section "Affectation des droits pour travailler avec le Serveur" à la page 27).

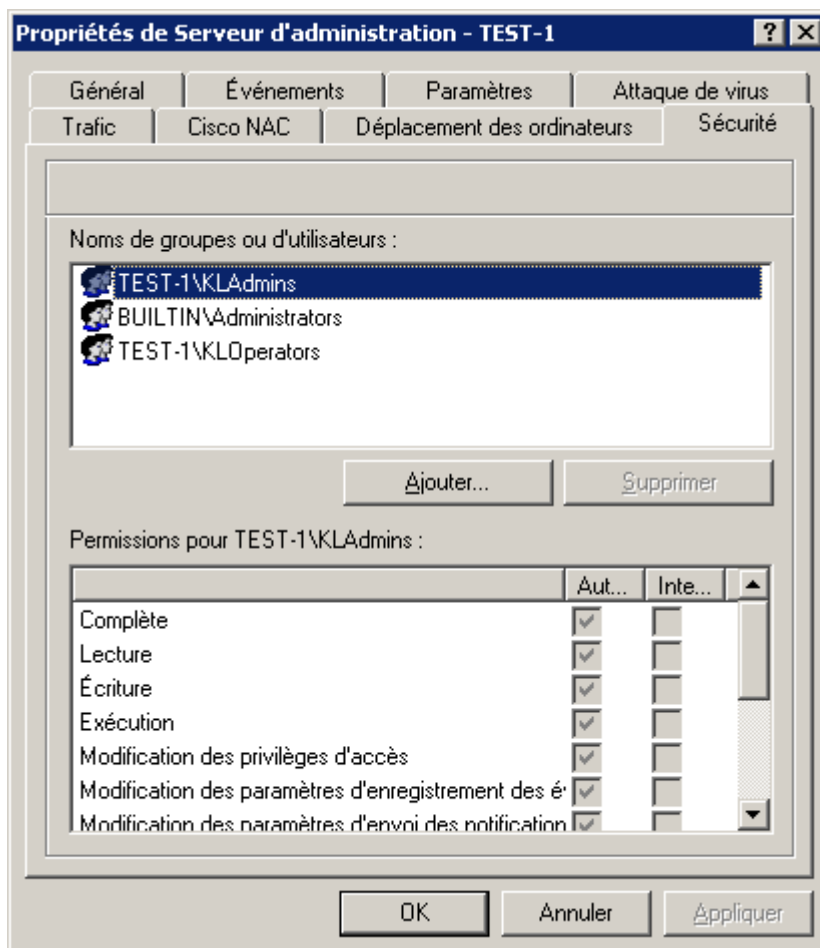


Illustration 22. Attribution des privilèges d'accès au Serveur d'administration

La présence ou l'absence de cet onglet est définie par les paramètres d'interface de l'utilisateur. Afin de configurer l'affichage de cet onglet, passez au menu **Vue** → **Configuration de l'interface** et cochez la case dans la ligne **Afficher les onglets avec les paramètres de sécurité**.

PARAMETRES DE TRAITEMENT DES EVENEMENTS

Les paramètres définissant les règles de traitement des événements dans le fonctionnement du Serveur d'administration sont présentés sous l'onglet **Événements** (cf. ill. ci-après).

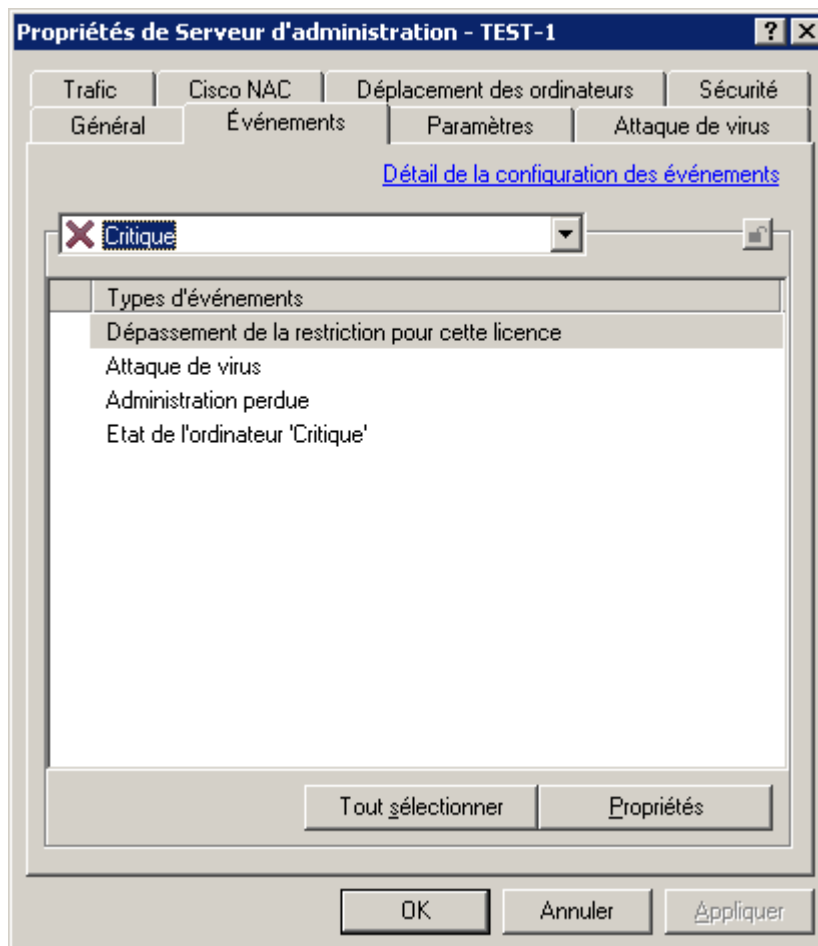


Illustration 23. Affichage des propriétés du Serveur d'administration. Onglet **Événements**

Les événements du Serveur d'administration, comme pour d'autres applications Kaspersky Lab contrôlées par Kaspersky Administration Kit, peuvent être rangés dans l'un des quatre degrés de gravité : **Critique**, **Erreur**, **Avertissement**, **Message d'information**.

Conformément au degré de leur importance, les événements sont classés d'une manière suivante :

- **Critique** :
 - Dépassement de la restriction de licences de la licence (par exemple, le nombre de postes clients sur lesquels la licence est installée est supérieur à la limite imposée par la licence).
 - Attaque de virus (l'activité virale dans les groupes d'administration dépasse la limite prédéfinie).
 - Connexion perdue avec le poste (impossible d'établir une connexion avec l'Agent d'administration installé sur le poste client).
 - Etat du poste *Critique* (un poste avec une configuration en état *Critique* a été détecté sur le réseau).
- **Erreur** :

- Plus d'espace disponible sur le disque (il ne reste plus d'espace libre sur le disque utilisé par le Serveur d'administration pour enregistrer ses données d'exploitation).
- Le dossier en accès public n'est pas disponible (le dossier partagé de mise à jour des bases et des modules des applications n'est pas disponible).
- La base de données du Serveur d'administration est indisponible.
- Il n'y a plus d'espace disponible dans la base de données du Serveur d'administration.
- Lors de la copie des mises à jour dans le dossier spécifié, l'erreur s'est produite.
- **Avertissement :**
 - Dépassement de la restriction pour cette licence.
 - La période d'inactivité de l'ordinateur a été trop longue.
 - Conflit dans les noms de postes clients (l'exclusivité des noms de clients à l'intérieur d'un niveau de hiérarchie a été violée).
 - Trop peu d'espace libre sur les disques durs.
 - Trop peu d'espace libre dans la base de données du Serveur d'administration.
 - Etat du poste *Avertissement* (un poste avec une configuration en état *Avertissement* a été détecté sur le réseau).
 - Déconnecté du Serveur principal.
 - Connexion avec le Serveur secondaire perdue.
 - Application incompatible installée.
- **Information :**
 - Plus de 90% de la limite pour cette licence ont été utilisés.
 - Trouvé nouvel poste client (un nouveau client a été trouvé pendant l'exploration du réseau).
 - Poste automatiquement ajouté au groupe (un nouveau poste client a été automatiquement inclus dans un groupe, conformément aux paramètres du groupe **Ordinateurs non définis**).
 - Un poste client n'a pas répondu pendant longtemps et a été enlevé du groupe.
 - Connexion avec le Serveur secondaire établie.
 - Connexion avec le Serveur principal établie.
 - L'application observée a été installée depuis le registre des applications.
 - Les mises à jour sont copiées dans le dossier spécifié.
 - Audit : Connexion au Serveur d'administration.
 - Audit : Objet modifié.
 - Audit : Etat de l'objet modifié.
 - Audit : Paramètres de groupe modifiés.

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

1. Dans la liste déroulante, sélectionnez le niveau de gravité de l'événement : **Critique, Erreur, Avertissement** ou **Message d'information**.
2. En fonction de la sélection, les événements correspondant au niveau de gravité choisi seront affichés dans la zone inférieure. La liste d'événements est propre à chaque application. Pour plus d'informations sur les événements, reportez-vous à la documentation de l'application. Sélectionnez les types d'événements dont les informations doivent être consignées à l'aide des touches **<Shift>** et **<Ctrl>**. Pour sélectionner tous les types d'événements, appuyez sur le bouton **Tout sélectionner**.
3. Pour les types d'événements sélectionnés, cliquez sur le bouton **Propriétés**.
4. Pour que les informations relatives aux événements soient consignées dans les journaux des événements, cochez les cases requises dans le groupe **Enregistrement d'événements** (cf. ill. ci-après) :

- **Sur le Serveur d'administration pendant (jours)** pour que le Serveur d'administration enregistre de manière centralisée les événements de l'application qui se produisent pour tous les clients du groupe. Dans le champ à droite, indiquez le nombre de jours pendant lesquels les enregistrements seront conservés. Après la fin de la période d'enregistrement indiquée, l'entrée correspondante à cet événement sera supprimée.

Vous pouvez examiner les comptes-rendus d'événement entreposés sur le Serveur d'administration à partir de la console du poste administrateur. Ces informations sont enregistrées dans le dossier **Evénements** de l'arborescence de console.

- **Dans le journal des événements du S.E. du poste client** pour que chaque client enregistre les événements en local, dans leur propre journal d'événement de Windows.
- **Dans le journal des événements du S.E. du Serveur d'administration** pour activer l'enregistrement de tous les événements des applications associés à tous les clients du groupe dans le journal d'événement de Windows, sur un ordinateur équipé du Serveur d'administration.

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

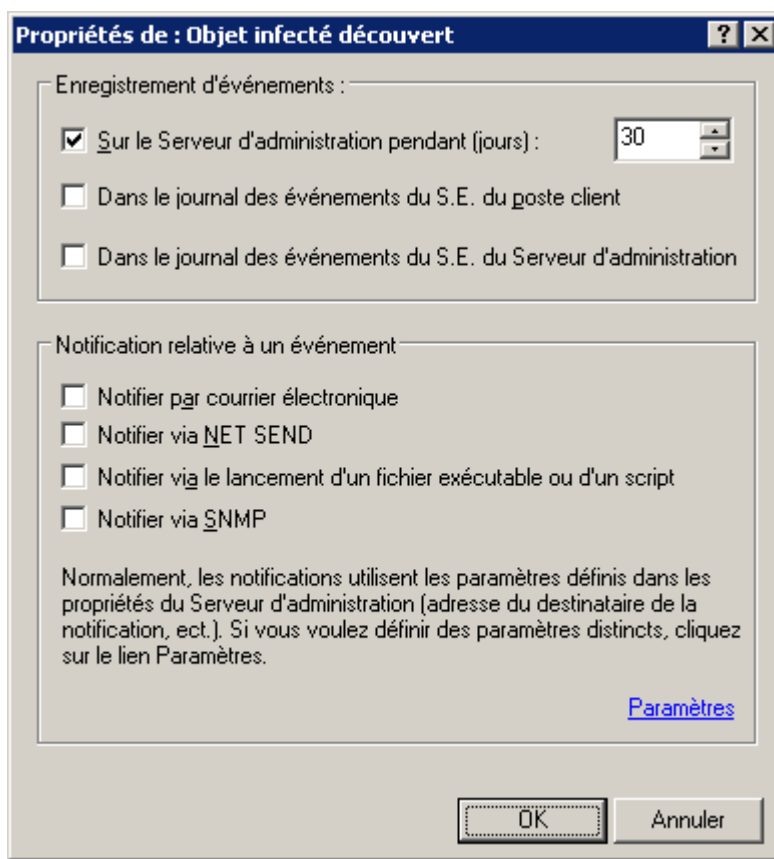


Illustration 24. Modification des propriétés des événements.

5. Pour activer la notification sur les événements sélectionnés par un mode quelconque, définissez le mode voulu en cochant la case souhaitée dans la section **Notification relative à un événement** :

- **Notifier par courrier électronique** ;
- **Notifier via NET SEND** ;

Notifications via NET SEND est inaccessible dans le système d'exploitation Microsoft Windows Vista et les versions plus récentes.

- **Notifier via le lancement d'un fichier exécutable ou d'un script** ;
- **Notifier via SNMP.**

La notification via SNMP est configurée directement dans l'application qui fonctionne avec SNMP.

Pour configurer les paramètres de notification, cliquez sur le lien **Paramètres** et dans la fenêtre qui s'ouvre (cf. ill. ci-après), définissez les valeurs des paramètres.

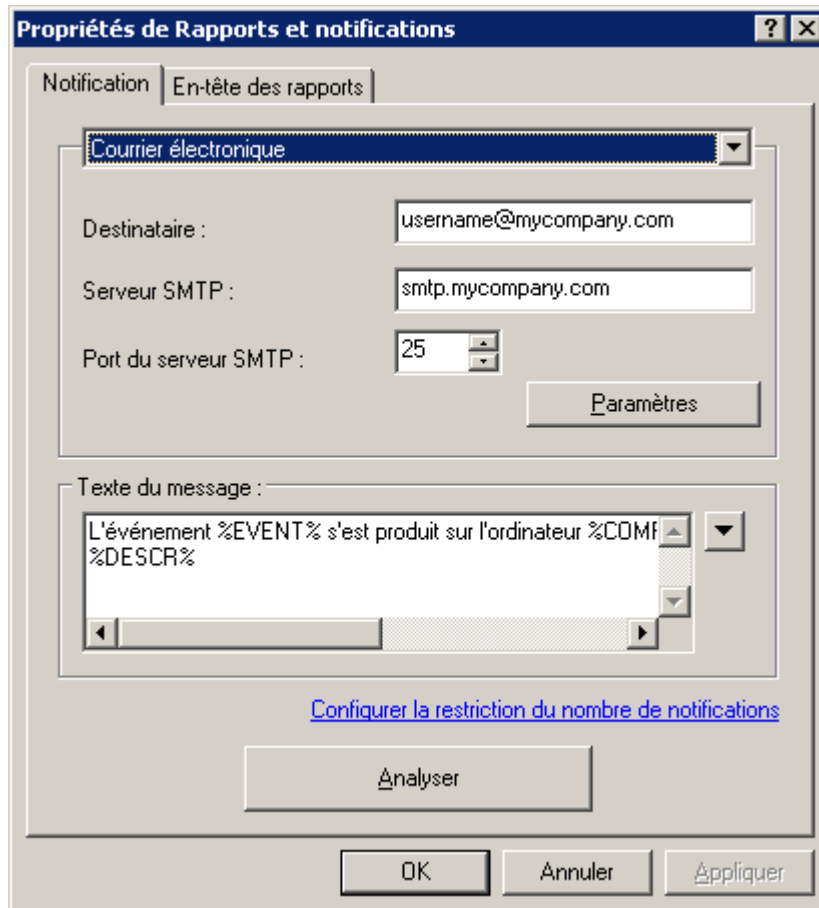


Illustration 25. Configuration des paramètres de notifications sur les événements

Dans la partie supérieure de la fenêtre, sélectionnez le mode de notification dont les paramètres doivent être modifiés. Si, dans ce groupe, la case **Appliquer les paramètres du Serveur d'administration** est cochée, les valeurs utilisées par défaut sont celles de l'onglet **Notification** des propriétés du Serveur d'administration. Pour modifier les paramètres de notification, décochez la case **Appliquer les paramètres du Serveur d'administration** et sélectionnez un des éléments suivants dans la liste déroulante :

- **Courrier électronique** (cf. ill. ci-dessus). Dans ce cas, saisissez les données suivantes :
 - dans la zone **Destinataire** - l'adresse de messagerie du destinataire. Vous pouvez indiquer plusieurs adresses séparées par une virgule ou un point-virgule ;
 - dans la zone **Serveur SMTP** - l'adresse du serveur de messagerie (vous pouvez utiliser une adresse IP ou le nom dans le réseau Windows) ;
 - dans la zone **Port du serveur SMTP** - le numéro de port du serveur SMTP (le numéro de port par défaut est 25) ;

- expéditeur et sujet du message de notification. Cliquez sur **Paramètres** et dans la boîte de dialogue affichée (cf. ill. ci-après), remplissez le champ **Objet**. Dans le champ bas de saisie indiquez l'adresse du courrier électronique, qui sera utilisée comme l'adresse d'expéditeur du message. Si le serveur SMTP nécessite une authentification, précisez **Nom d'utilisateur**, **Mot de passe** et **Confirmation** du mot de passe dans les zones correspondantes.

The screenshot shows a dialog box titled "Paramètres" with a standard Windows-style title bar (minimize, maximize, close buttons). The dialog contains the following elements:

- Objet :** A text input field containing "%EVENT%" and a dropdown arrow on the right.
- Autorisation ESMTMP requise**
- Nom d'utilisateur :** A text input field containing "user".
- Mot de passe :** A text input field with masked characters (dots).
- Confirmation du mot de passe :** A text input field with masked characters (dots).
- A paragraph of text: "L'adresse du courrier électronique de l'expéditeur. Si le paramètre n'est pas défini, l'adresse du destinataire sera utilisée. Attention : il est déconseillé d'indiquer une adresse de courrier électronique qui n'existe pas dans ce champ." Below this text is an empty text input field.
- At the bottom right, there are two buttons: "OK" and "Annuler".

Illustration 26. Définition des paramètres d'envoi des notifications. Expéditeur et objet des notifications

- **NET SEND** (cf. ill. ci-après). Dans ce cas, indiquez l'adresse des ordinateurs qui recevront les notifications par le réseau. Vous pouvez également utiliser une adresse IP ou le nom de l'ordinateur dans le réseau Windows. Vous pouvez écrire plus d'une adresse séparée par une virgule ou un point-virgule. Afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les ordinateurs le Messenger doit être lancé.

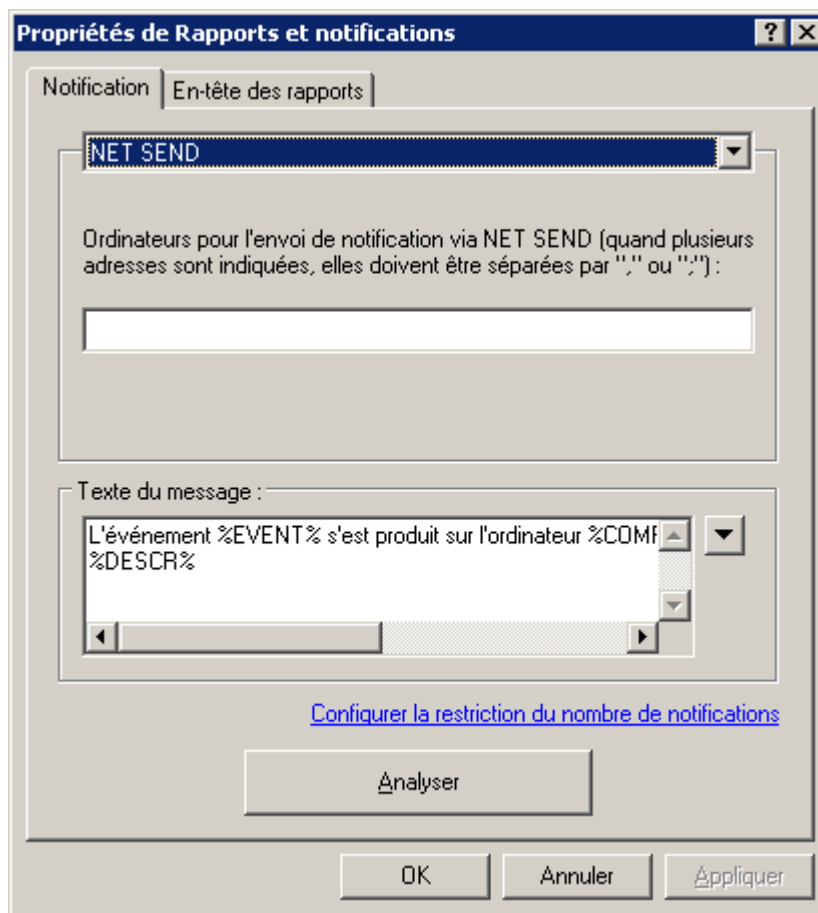


Illustration 27. Configuration de l'envoi des notifications. Envoi de notifications à l'aide de **NET SEND**

- **Fichier exécutable à lancer** (cf. ill. ci-après). Dans ce cas, appuyez sur le bouton **Sélectionner** pour indiquer le module exécutable à lancer lorsqu'un événement se produit.

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

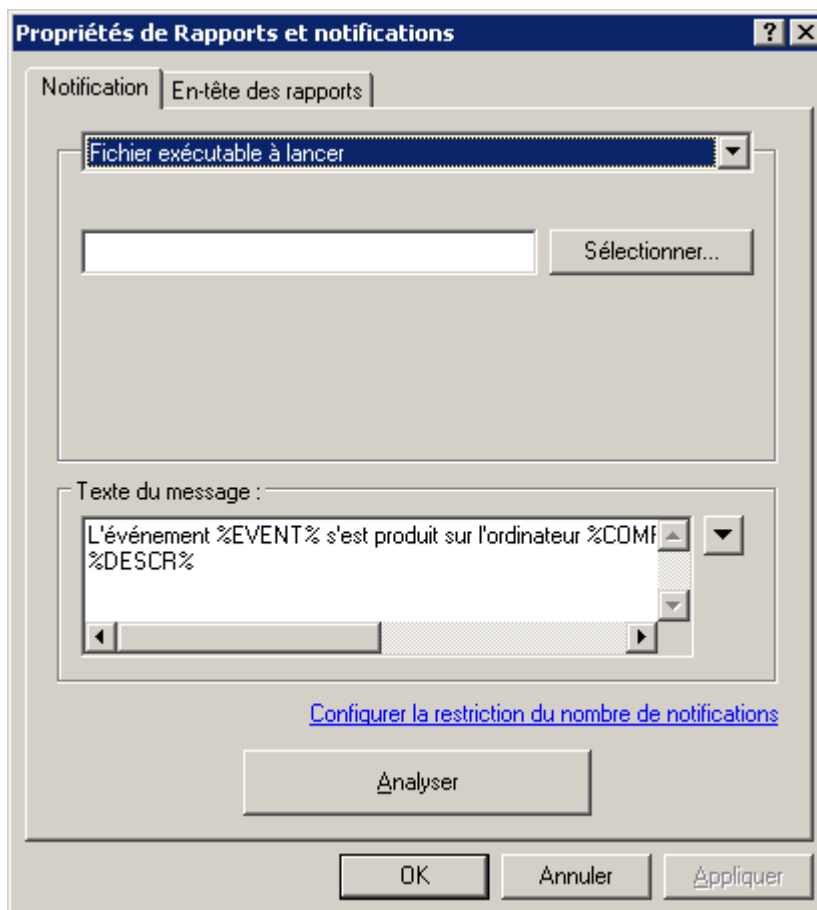


Illustration 28. Configuration de l'envoi des notifications. Envoi de notifications à l'aide d'un exécutable.

Dans la partie inférieure du bloc **Texte du message** (cf. ill. ci-après), écrivez le texte de la notification à envoyer. Si, dans ce groupe, la case **Appliquer les paramètres du Serveur d'administration** est cochée, le texte utilisé par défaut est celui de l'onglet **Notification** des propriétés du Serveur d'administration. Pour modifier le texte de la notification, décochez la case **Appliquer les paramètres du Serveur d'administration** et encodez un nouveau texte.

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

- **Degré d'importance de l'événement ;**
- **A partir de l'ordinateur ;**
- **Domaine ;**
- **Événement ;**
- **Description d'événement ;**
- **Heure ;**
- **Nom de tâche ;**
- **Application ;**

- **Numéro de version ;**
- **Adresse IP ;**
- **Adresse IP de la connexion.**

Pour vérifier les valeurs spécifiées dans l'onglet Paramètres, envoyez manuellement des messages de test. Pour ce faire, cliquez sur **Analyser**. Cette action entraîne l'ouverture de la fenêtre d'envoi d'une notification d'essai (cf. ill. ci-après). En cas d'erreur, des informations détaillées seront fournies.

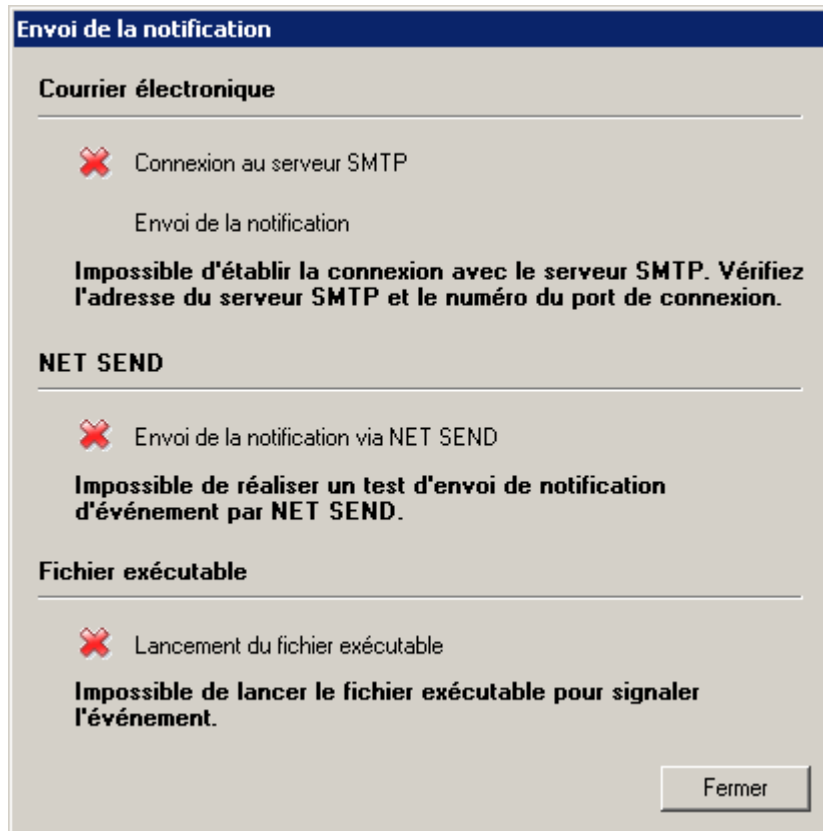


Illustration 29. Définition des paramètres d'envoi des notifications. Envoi d'une notification d'essai

LES PARAMETRES DE FORMATION DE L'EVENEMENT ATTAQUE DE VIRUS

Sur l'onglet **Attaque de virus** (cf. ill. ci-après), vous pouvez définir comme Critères d'envoi d'événements en cas d'**Attaque de virus**, le nombre maximum des virus détectés pendant un intervalle de temps spécifié. 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.

Cochez la case en regard des types d'application 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.

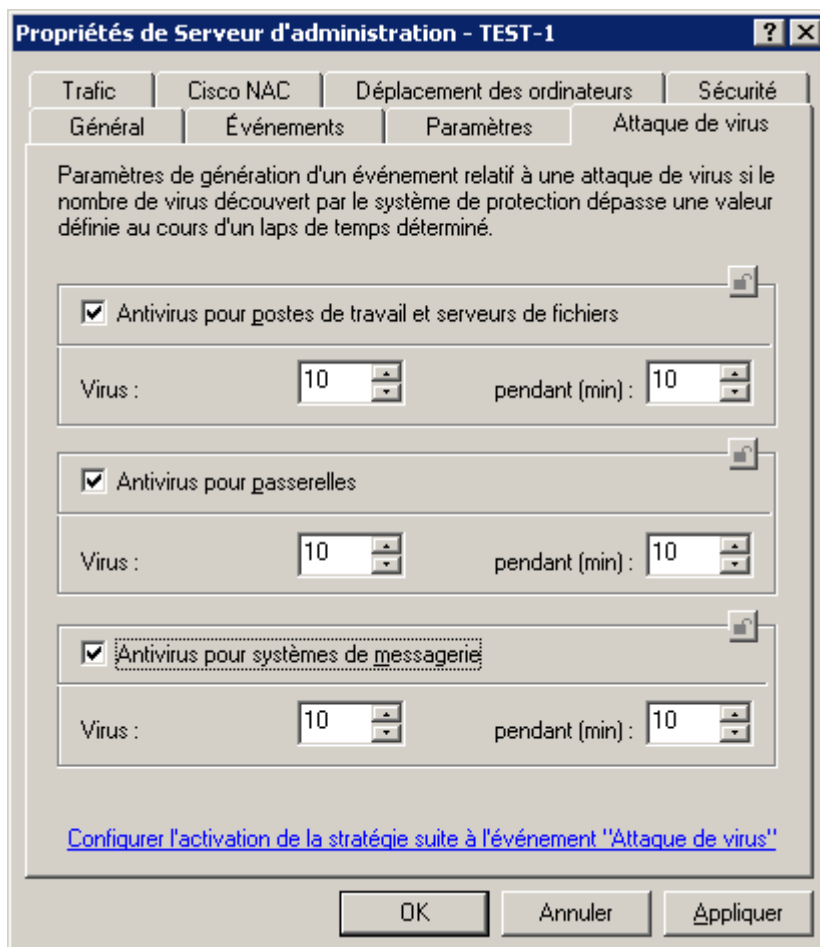


Illustration 30. Affichage des propriétés du Serveur d'administration. Onglet **Attaque de virus**

Cliquez sur le lien **Configurer l'activation de la stratégie suite à l'événement "Attaque de virus"** et ouvrez la fenêtre **Activation des stratégies** (cf. ill. ci-après) et composez la liste des stratégies, qui seront utilisés par les applications en guise de stratégies actives en cas d'un événement "Attaque de virus". Pour ce faire, utilisez les boutons **Ajouter** et **Supprimer**.

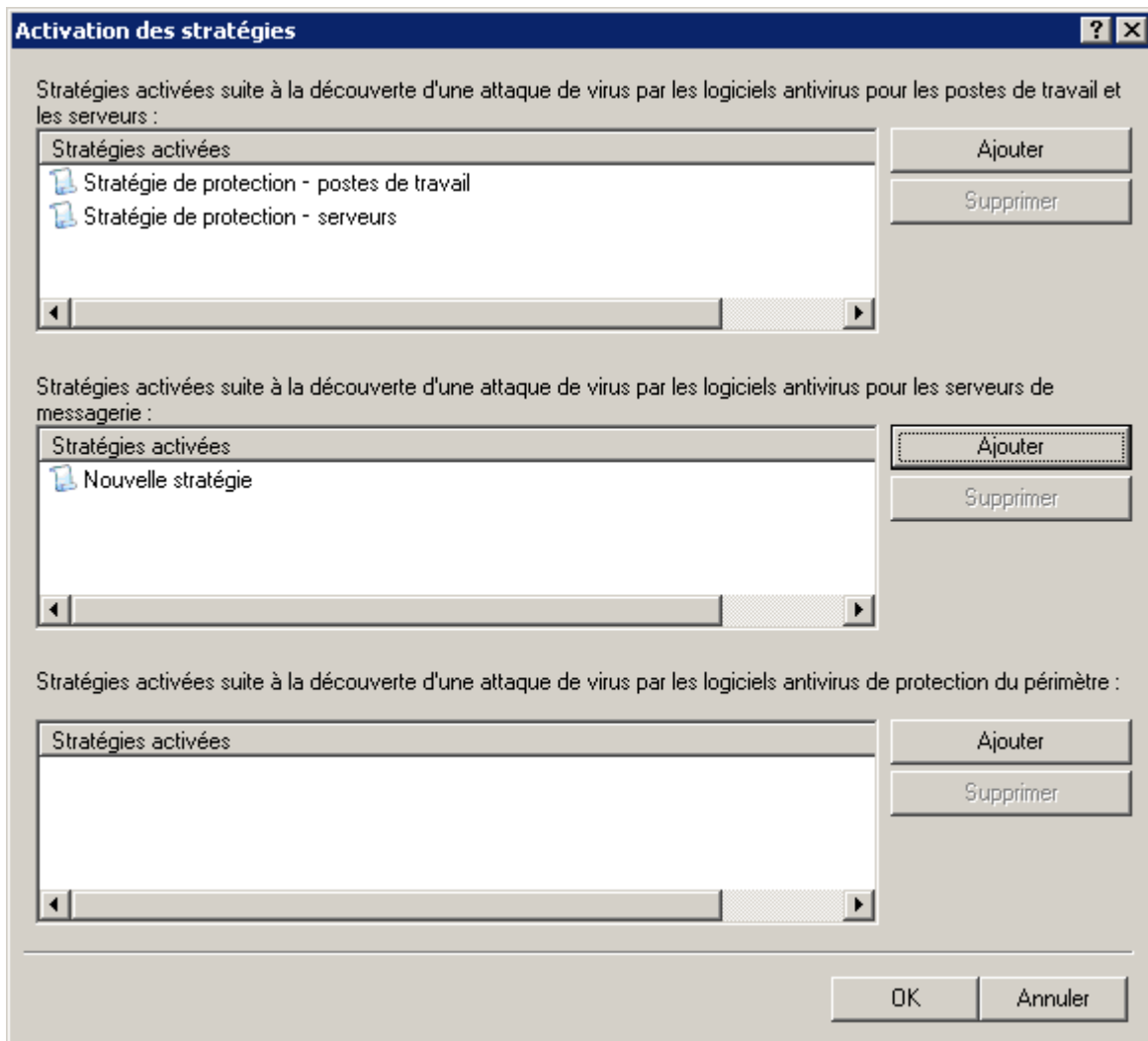


Illustration 31. Configuration de l'activation de la stratégie en cas de découverte d'une attaque de virus

REGLES GENERALES DE DEPLACEMENT DES ORDINATEURS

L'onglet **Déplacement des ordinateurs** (cf. ill. ci-après) vous permet de définir les règles de déplacement d'ordinateurs du réseau dans des groupes d'administration.

L'ordre d'application des règles du bloc **Liste des règles de transfert des ordinateurs** est défini par la priorité d'application des règles. Pour supprimer ou déplacer une règle dans la liste, utilisez les boutons situés à droite du groupe.

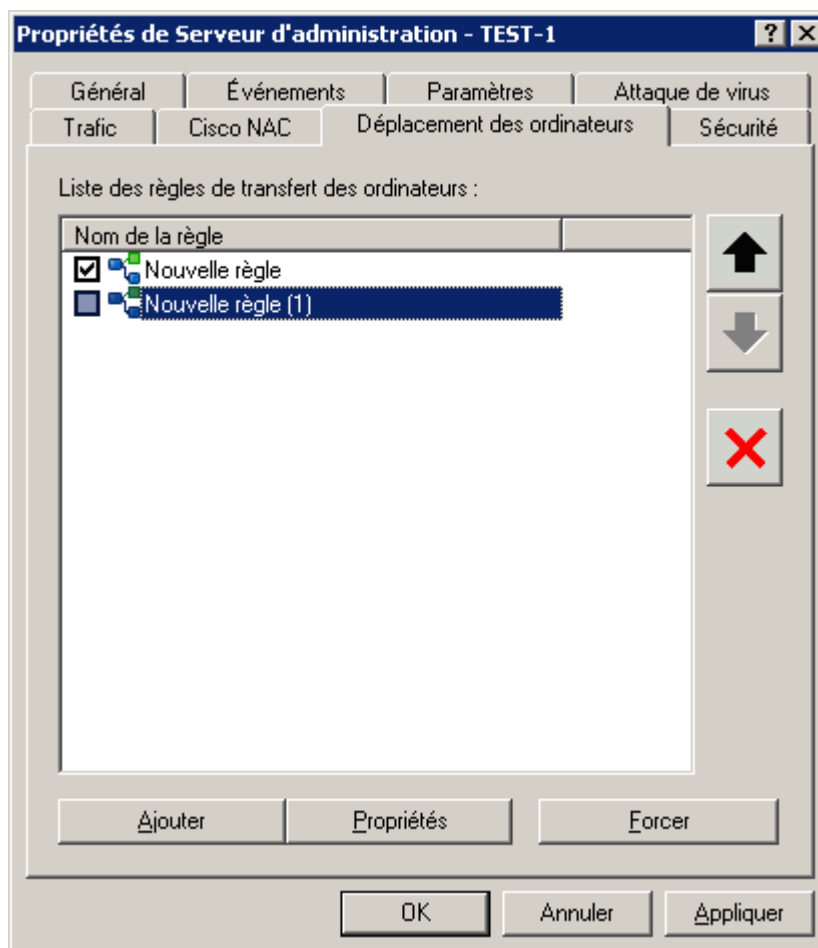


Illustration 32. Fenêtre des propriétés du Serveur d'administration. Onglet **Déplacement des ordinateurs**

Pour consulter ou modifier les paramètres de la règle existante, cliquez sur le bouton **Propriétés**.

Pour ajouter une page, cliquez sur **Ajouter**. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), définissez les valeurs des paramètres de la règle.

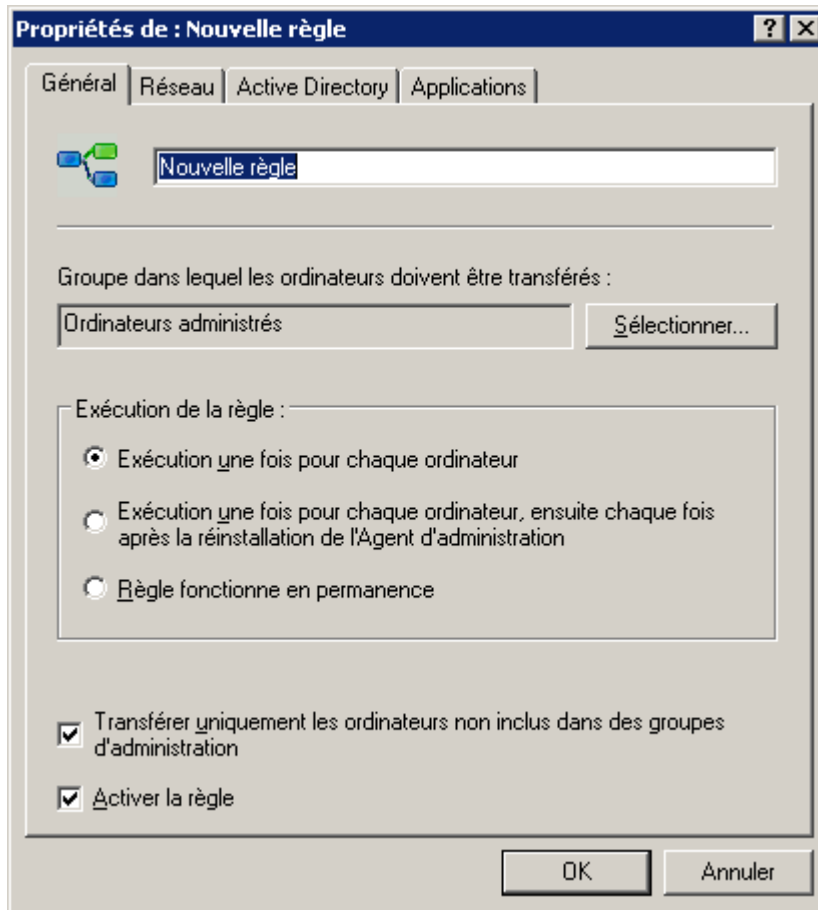


Illustration 33. Fenêtre des propriétés de la règle de déplacement des ordinateurs. Onglet **Général**

Sous l'onglet **Général**, indiquez les informations suivantes :

- le nom de la règle ;
- le groupe dans lequel les ordinateurs seront déplacés conformément à la règle ;
- l'ordre d'exécution des règles :
 - **Exécution une fois pour chaque ordinateur** : si la règle doit être appliquée une fois seulement pour chaque poste ;
 - **Exécution une fois pour chaque ordinateur, ensuite chaque fois après la réinstallation de l'Agent d'administration** ;
 - **Règle fonctionne en permanence.**

Cochez les cases suivantes sous cet onglet :

- **Transférer uniquement les postes non inclus dans des groupes d'administration** : si les ordinateurs qui se trouvent déjà dans un groupe d'administration quelconque ne doivent pas être déplacés dans un groupe conformément à la règle ;
- **Activer la règle** : pour que la règle soit appliquée durant le travail.

Sur l'onglet **Réseau**, définissez les critères que l'ordinateur doit remplir pour être déplacé dans le groupe d'administration

désigné :

- **Nom de l'ordinateur dans le réseau Windows.**
- **Domaine.**
- **Nom de domaine de l'ordinateur.**
- **Domaine DNS.**
- Si l'adresse IP de l'ordinateur doit figurer dans une plage IP définie, cochez la case **Intervalle d'adresses IP** et définissez les limites inférieure et supérieure de l'intervalle.
- Pour que l'**Adresse IP de connexion au serveur** soit prise en compte lors du traitement de l'ordinateur, cochez la case du même nom et définissez les limites supérieure et inférieure de l'intervalle auquel l'adresse IP de connexion doit appartenir.
- Cochez la case **L'ordinateur appartient à l'intervalle d'adresses IP** et à l'aide du bouton **Sélectionner** définissez la plage IP à laquelle doit appartenir l'ordinateur. La plage IP est sélectionnée dans la liste des plages contenues dans le dossier **Ordinateurs non définis** de l'arborescence de la console.

Sur l'onglet **Active Directory**, procédez comme suit :

- Si l'ordinateur doit appartenir à une unité définie Active Directory, cochez la case **Le poste se trouve dans l'unité d'organisation Active Directory** et à l'aide du bouton **Sélectionner**, indiquez le groupe Active Directory. Les sous-divisions Active Directory sont sélectionnées dans la liste des groupes du dossier **Ordinateurs non définis**.
- Pour le traitement des ordinateurs qui appartiennent à des sous-divisions filles, cochez la case **L'ordinateur est un membre du groupe Active Directory**.

Sur l'onglet **Applications** sélectionnez dans les listes déroulantes :

- le critère de présence de l'Agent d'administration sur l'ordinateur : **Installé** ou **Non installé** ;
- la version du système d'exploitation qui doit être installée sur l'ordinateur.

Pour les critères qui ne doivent pas être tenus en compte dans la règle, il faut désélectionner les cases qui leur correspondent et les champs doivent rester vides.

L'ordinateur est déplacé dans le groupe d'administration s'il répond à tous les critères définis dans la règle.

Pour modifier les règles créées, cliquez sur le bouton **OK**.

Si vous voulez forcer l'application d'une règle, indépendamment des règles de l'application, sélectionnez la règle requise puis cliquez **Forcer**.

Si le même ordinateur est sous l'influence de plusieurs des règles citées ci-dessus, alors la priorité sera accordée à la règle pour le groupe Active Directory, puis à celle pour la plage IP puis à celle pour le domaine.

CONFIGURATION DE LA COLLABORATION 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 configurer une collaboration entre les états Cisco NAC et les conditions de protection antivirus, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez le Serveur d'administration et dans son menu contextuel sélectionnez le point **Propriétés**. Ceci permet d'ouvrir la boîte de dialogue de configuration du Serveur. Dans cette fenêtre sélectionnez l'onglet **Cisco NAC** (cf. ill. ci-après).

Cet onglet est absent si le composant **Kaspersky Lab Cisco NAC Posture Validation Server** (cf. Manuel d'implantation de Kaspersky Administration Kit) n'a pas été installé conjointement avec le Serveur d'administration.

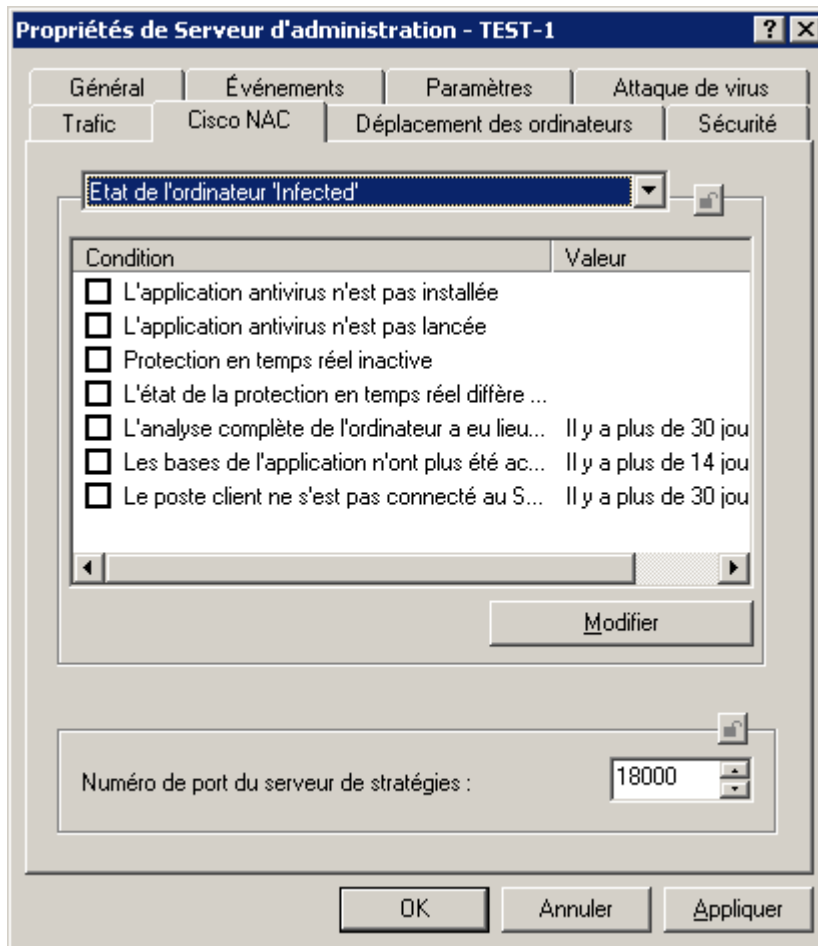


Illustration 34. Affichage des propriétés du Serveur d'administration. Onglet **Cisco NAC**

2. Sélectionnez un des états de l'ordinateur Cisco NAC dans la liste déroulante : *Healthy*, *Checkup*, *Quarantine* ou *Infecté*.
3. Dans le tableau en dessous, à l'aide des cases, indiquez les conditions de la protection antivirus qui correspondent à l'état. Le cas échéant modifiez les valeurs de seuil de ces conditions.

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. Il est possible, pour certaines conditions, de modifier la valeur limite. Pour ce faire, sélectionnez la condition requise dans la colonne **Condition** et, à l'aide du bouton **Modifier**, ouvrez la fenêtre de modification (cf. ill. ci-après).

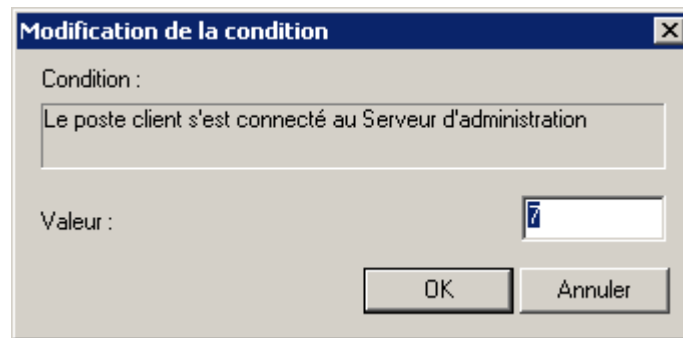


Illustration 35. Fenêtre **Modification de la condition**

4. Indiquez le numéro du port Postrure Validation Server, utilisé pour l'échange de données avec le serveur Cisco, dans le champ **Numéro de port du serveur de stratégies**. Le numéro de port par défaut est 18000.
5. Cliquez sur **OK** ou **Appliquer** pour terminer la configuration.

REGLES DE RESTRICTION DU TRAFIC

Pour réduire la charge du réseau, il est possible de limiter la vitesse de transfert des données sur le Serveur d'administration pour des plages IP ou des intervalles IP en particulier. Les valeurs limites admises ainsi que l'intervalle de temps durant lequel ces valeurs sont d'application sont définis dans les règles. La liste des règles figure sur l'onglet **Trafic** de la fenêtre des propriétés du Serveur d'administration.

► Pour ajouter une nouvelle règle, cliquez sur **Ajouter** et dans la fenêtre qui s'ouvre, définissez ses paramètres :

1. Dans le groupe **Plage d'adresses IP pour lesquelles il faut limiter le trafic**, sélectionnez le mode de définition du sous-réseau ou de la plage d'adresses :
 - **Définir l'intervalle IP à l'aide d'une adresse et d'un masque de sous-réseau** : en ce cas indiquez les paramètres de sous-réseau dans les champs **Adresse de sous-réseau** et **Masque de sous-réseau**.
 - **Définir l'intervalle IP à l'aide d'une &adresse de début et de fin** : en ce cas, définissez les limites de la plage dans les champs **Début** et **Fin**.
2. Dans le groupe **Restriction du trafic**, indiquez les informations suivantes :
 - L'intervalle de temps durant lequel la restriction du trafic sera d'application dans le champ **Période de temps** ;
 - La vitesse limite pour le transfert de données sur le Serveur d'administration dans le champ **Restriction (Ko/s)** ; cette restriction sera d'application durant l'intervalle défini dans le champ **Période de temps** ;
 - La valeur limite de vitesse de transfert des données en dehors de l'intervalle de temps dans le champ **Limiter le trafic le reste du temps (Ko/s)**, s'il faut limiter le trafic durant cette période.

Une fois que les paramètres auront été définis, la règle apparaîtra dans la liste. Le nom de la règle est créé automatiquement sur la base des données sur la création de la plage d'adresses IP.

En cas de modification des paramètres des limites de la plage d'adresses IP, de l'adresse ou du masque de sous-réseau dans les propriétés de la règle, le nom de la règle dans la liste change pour refléter les nouvelles valeurs.

Pour supprimer une règle, sélectionnez-la dans la liste et cliquez sur le bouton **Supprimer**.

Pour consulter ou modifier les paramètres d'une règle existante, sélectionnez la règle dans la liste puis cliquez sur le bouton **Propriétés**.

SERVEURS D'ADMINISTRATION SECONDAIRES

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.

AJOUT D'UN SERVEUR SECONDAIRE

➤ Pour ajouter un Serveur d'administration secondaire, procédez comme suit :

1. Sélectionnez dans le groupe d'administration l'entrée **Serveurs d'administration**, ouvrez le menu contextuel et cliquez sur **Générer** → **Serveur d'administration**. Cette action lance un Assistant. Suivez les instructions de l'Assistant.
2. Spécifiez l'adresse réseau du Serveur d'administration secondaire. Dans ce cas, le Serveur d'administration principal enverra une commande de connexion au Serveur secondaire et transmettra toutes les propriétés indispensables (adresse réseau du Serveur d'administration principal, certificat du Serveur d'administration principal).
3. Saisissez dans la fenêtre suivante le nom du Serveur d'administration secondaire. Le nouveau Serveur d'administration sera affiché sous ce nom dans le groupe d'administration. Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie.

Si l'adresse du Serveur a été saisie à l'étape précédente, alors le champ **Nom du Serveur d'administration secondaire** affichera la valeur suivante : **Serveur d'administration de <Nom du poste>**, où **<Nom du poste>** est le nom repris dans l'adresse et qui doit être ajouté en tant que Serveur secondaire.

4. Si précédemment l'adresse du Serveur d'administration n'a pas été indiquée, alors spécifiez le chemin d'accès au certificat du Serveur d'administration à l'aide du bouton **Sélectionner**.
5. Si vous avez indiqué l'adresse d'un Serveur secondaire préalablement, définissez les paramètres de connexion du Serveur d'administration secondaire au Serveur principal :
 - Indiquez l'adresse du Serveur d'administration principal. En guise d'adresse, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur dans le réseau Windows.
 - Si la connexion s'opère via un serveur proxy, configurez les paramètres de connexion dans le groupe **Paramètres du serveur proxy**.

Cochez la case **Utiliser le serveur proxy**. Dans le champ **Adresse** saisissez l'adresse du serveur proxy. Remplissez les champs **Nom d'utilisateur**, **Mot de passe** et **Confirmation du mot de passe** si l'authentification est requise pour accéder au serveur proxy.

Si l'adresse du Serveur secondaire n'a pas été indiquée, cette étape ne sera pas présentée.

6. Attendez la fin de l'exécution des opérations suivantes :
 - Connexion de la Console d'administration au Serveur secondaire.
 - Ajout des informations relatives au Serveur secondaire dans la base de données du Serveur d'administration principal.

Si précédemment l'adresse du Serveur d'administration a été indiquée, alors, en fonction de la demande, désignez les comptes utilisateurs (nom et mot de passe) jouissant des privilèges de connexion à l'ordinateur qui doit devenir un Serveur secondaire.

- Configuration des paramètres de connexion du Serveur secondaire au Serveur d'administration primaire.

Si l'adresse du Serveur secondaire n'a pas été indiquée, il faudra, après avoir quitté l'Assistant, réaliser manuellement les opérations suivantes :

- connecter la Console d'administration au Serveur secondaire ;
- configurer les paramètres de connexion du Serveur secondaire au Serveur principal.

7. Cliquez sur **Suivant**. L'exécution de l'opération est indiquée dans la fenêtre de l'Assistant. En cas d'erreur, le message de circonstance sera affiché.

8. Cliquez sur **Terminer** dans la dernière fenêtre de l'Assistant.

A la fin de l'Assistant, le Serveur d'administration principal ajoute les informations relatives au Serveur d'administration secondaire dans la base de données. L'icône et le nom du Serveur secondaire d'administration figurent dans le dossier **Serveurs d'administration** du groupe d'administration correspondant.

CONFIGURER LA CONNEXION D'UN SERVEUR SECONDAIRE AU SERVEUR D'ADMINISTRATION PRINCIPAL

➔ Pour configurer la connexion d'un Serveur secondaire au Serveur d'administration principal, procédez comme suit :

1. Ajoutez le Serveur d'administration secondaire à l'arborescence de la console (cf. section "Ajout d'un Serveur à l'arborescence de la console" à la page [26](#)) en tant que Serveur d'administration géré.
2. Sélectionnez le Serveur d'administration et à l'aide de la commande **Propriétés** du menu contextuel, ouvrez la fenêtre contenant ses propriétés.
3. Dans la fenêtre **Propriétés de Serveur d'administration <Nom de l'ordinateur>** qui s'ouvre, sous l'onglet **Général**, cliquez sur le lien **Avancé**. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Paramètres** dans le bloc **Hierarchie des Serveurs d'administration**.
4. Dans la fenêtre **Paramètres du Serveur d'administration principal** qui suit (cf. ill. ci-après), cochez la case **Ce Serveur d'administration est un Serveur secondaire**.

Ensuite, dans le groupe des paramètres indiquez ci-dessous :

- Adresse du Serveur d'administration principal. En guise d'adresse, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur dans le réseau Windows.
- Certificat du Serveur d'administration principal. Il est possible d'indiquer le chemin d'accès au fichier du certificat à l'aide du bouton **Sélectionner**.

Cochez la case **Utiliser le serveur proxy** si la connexion au Serveur d'administration s'opère via un serveur proxy. Dans le champ **Adresse** saisissez l'adresse pour la connexion au serveur proxy. Remplissez les champs **Nom d'utilisateur**, **Mot de passe** et **Confirmation** du mot de passe si l'authentification est requise pour accéder au serveur proxy.

5. Pour appliquer le paramètre, cliquez sur **OK** ou **Appliquer**.

Le Serveur d'administration secondaire se connecte au Serveur principal et en reçoit toutes les stratégies et tâches pour le groupe où est raccordé le Serveur secondaire. Par la suite, vous pourrez vous connecter au Serveur secondaire via le Serveur principal au départ du nœud **Serveurs d'administration**.

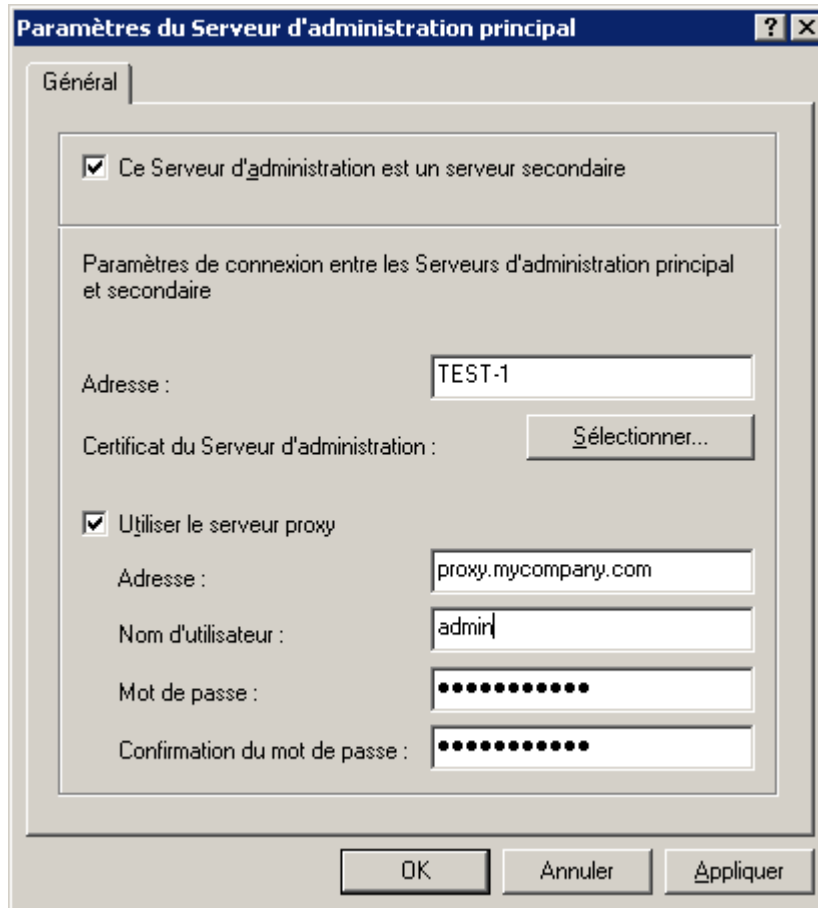


Illustration 36. Configuration dans le Serveur principal des infos du Serveur secondaire

AFFICHAGE DES GROUPES D'ADMINISTRATION DU SERVEUR SECONDAIRE





► Pour consulter les groupes d'administration du Serveur d'administration secondaire via le Serveur principal, connectez la console au Serveur secondaire :

1. Sélectionnez dans l'arborescence de la console du Serveur principal l'entrée **Serveurs d'administration** dans le groupe qui vous intéresse.
2. Dans l'entrée **Serveurs d'administration**, sélectionnez le Serveur secondaire requis.
3. Ouvrez le menu contextuel et sélectionnez la commande **Connecter au Serveur d'administration**.

La structure du groupe d'administration du Serveur d'administration secondaire apparaît dans la Console d'administration. Ensuite, vous pouvez consulter la structure des groupes (cf. section "Affichage des informations sur un groupe" à la page [67](#)).

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 apparaît à côté du nom de la stratégie reçue du Serveur d'administration principal (icône standard de stratégie –).

- Lorsque le mode d'héritage est activé, les valeurs des paramètres de la stratégie héritée 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 ils utilisent les valeurs définies dans la stratégie héritée.
- Les paramètres qui n'ont pas été "verrouillés" dans la stratégie héritée peuvent être modifiés dans les stratégies du Serveur secondaire (icône ). Si la modification du paramètre est possible dans la stratégie du Serveur secondaire, elle sera possible également dans les paramètres de l'application (cf. section "Affichage et modification des paramètres d'une stratégie" à la page [79](#)) et dans les paramètres de la tâche (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)).
- L'icône apparaît à côté du nom de la tâche de groupe reçue du Serveur d'administration principal  (icône standard de tâche – ).

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

Les tâches de Kaspersky Administration Kit et les tâches pour les sélections d'ordinateurs ne sont pas transmises aux Serveurs secondaires.

➔ Pour administrer le Serveur d'administration secondaire via la console du Serveur principal,

ajoutez l'ordinateur sur lequel le Serveur d'administration asservi est installé à l'arborescence de la console en tant que nouveau Serveur (cf. section "Ajout d'un Serveur secondaire" à la page [54](#)), et passez dans le nœud, correspondant à ce Serveur.

CONNEXION AU SERVEUR D'ADMINISTRATION VIA INTERNET

Pour la connexion au Serveur d'administration via Internet, il est nécessaire d'exécuter les exigences suivantes :

- Le Serveur d'administration dans l'office principal doit posséder l'adresse IP externe, et sur cette adresse les ports entrants 13000 et 14000 doivent être ouverts.
- L'adresse IP externe du Serveur d'administration principal doit être indiquée lors de l'installation de l'Agent d'administration sur les postes clients de l'office distant. Si pour l'installation, le paquet d'installation est utilisé, alors l'adresse IP est indiquée manuellement dans les propriétés de ce paquet sur l'onglet **Paramètres**.
- L'Agent d'administration doit être installé préalablement sur les ordinateurs de l'office distant.
- Pour administrer les applications et les tâches du poste client, dans les propriétés de ce poste sous l'onglet **Général**, l'administrateur doit cocher la case dans la ligne **Maintenir la connexion avec le Serveur d'administration**. Après avoir coché la case, il faut attendre la synchronisation avec le poste client distant. En même temps cette case peut être cochée chez pas plus de 100 postes clients.
- Pour accélérer l'exécution de la tâche sur le poste client, il est possible d'y ouvrir le port 15000. Dans ce cas pour lancer une tâche, le Serveur d'administration envoie un paquet spécial à l'Agent d'administration par le port 15000 sans attendre la synchronisation avec le poste client.

ADMINISTRATION DES GROUPES D'ADMINISTRATION

L'interaction entre le Serveur d'administration et les ordinateurs du réseau de l'entreprise (postes clients) s'opère via l'Agent d'administration. Ce composant doit être installé sur tous les ordinateurs où l'administration des applications de Kaspersky Lab va être réalisée à l'aide de Kaspersky Administration Kit.

Selon la structure de l'entreprise, les postes clients peuvent être rassemblés dans des groupes d'administration (groupes). Pour les postes clients dans les limites d'un groupe, il est possible de définir :

- des paramètres uniques de fonctionnement des applications à l'aide de stratégies ;
- un mode unique de fonctionnement des applications – grâce à la création de tâches de groupe.

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.

DANS CETTE SECTION

Création, déplacement et suppression d'un groupe	58
Création de structure des groupes d'administration	60
Affichage des informations sur un groupe	67
Affichage et modification des paramètres du groupe	68

CREATION, DEPLACEMENT ET SUPPRESSION D'UN GROUPE

➡ *Pour créer un groupe, procédez comme suite :*

1. Dans l'arborescence de la console, ouvrez le dossier **Ordinateurs administrés**.
2. Sélectionnez le dossier correspondant au groupe dans lequel le nouveau groupe doit être ajouté. Si vous créez un groupe à un niveau supérieur de la hiérarchie, sélectionnez le dossier **Ordinateurs administrés**.
3. Ouvrez le menu contextuel et choisissez l'option **Générer** → **Groupe** ou cliquez sur le lien **Créer un sous-groupe**, situé dans le panneau des tâches.
4. Dans la fenêtre qui s'ouvre, saisissez le nom du groupe (cf. ill. ci-après) puis cliquez sur le bouton **OK**.

Un nouveau dossier portant le nom attribué apparaîtra alors dans le dossier sélectionné du dossier **Ordinateurs administrés** de l'arborescence de la console. Ce dossier reprendra automatiquement les sous-dossiers **Stratégies**, **Tâches de groupe**, **Serveurs d'administration** et **Postes clients**. Ceux-ci sont peuplés au moment de la définition des stratégies du groupe, de la création de tâches de groupe et de l'ajout de Serveurs d'administration secondaires.

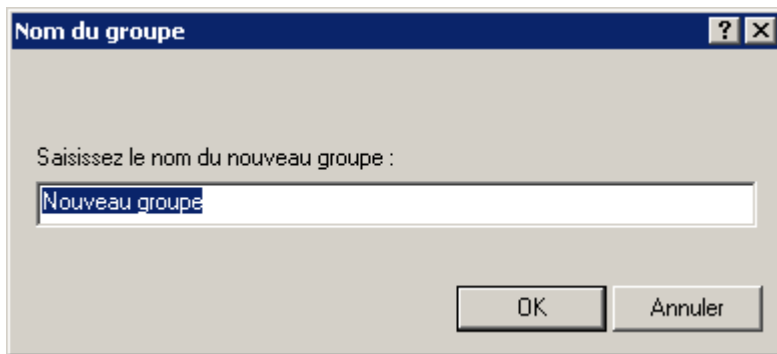


Illustration 37. Ajouter un nouveau groupe

- Pour modifier le nom d'un groupe, procédez comme suit :

Sélectionnez le dossier du groupe dans l'arborescence de la console, ouvrez le menu contextuel et sélectionnez la commande **Propriétés** ou cliquez sur le lien **Propriétés du groupe** dans le panneau des tâches. Sur l'onglet **Général** de la boîte de dialogue **Propriétés de <Nom du groupe>** (cf. ill. ci-après), modifiez le nom du groupe.

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

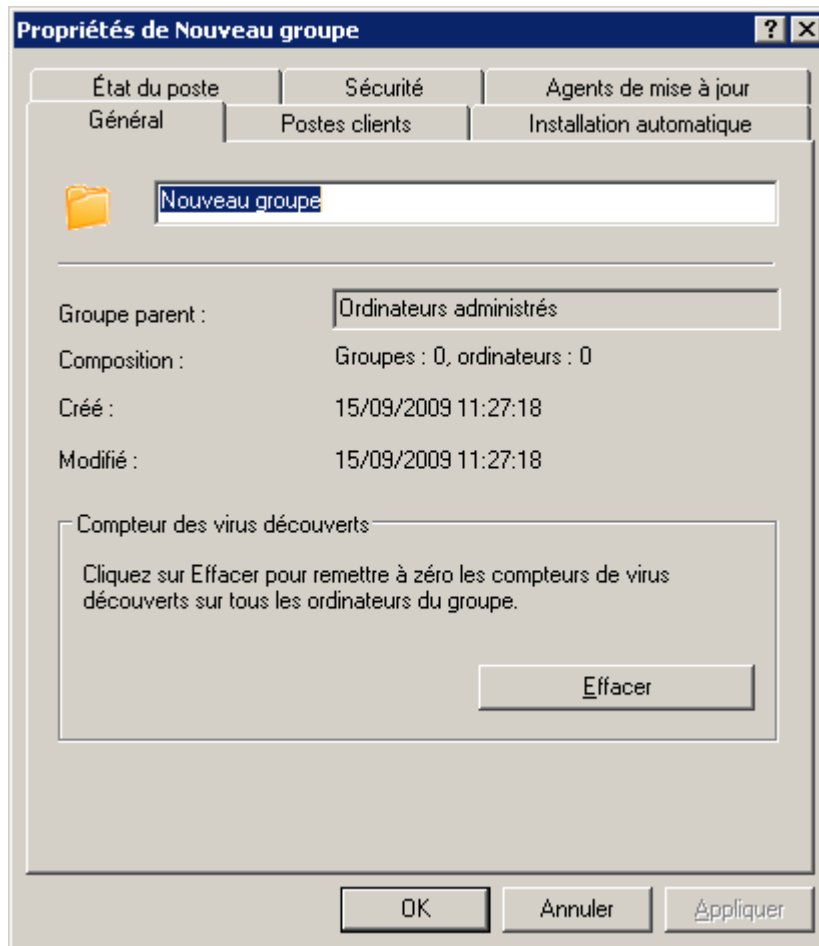


Illustration 38. Affichage des propriétés du groupe. Onglet **Général**

- Pour déplacer un groupe dans un autre dossier de l'arborescence de la console, procédez comme suit :

Sélectionnez le dossier à déplacer et utilisez les commandes standards du menu contextuel **Couper/Coller** ou déplacez-le à l'aide de la souris.

- Pour supprimer un groupe, procédez comme suit :

Sélectionnez le dossier du groupe dans l'arborescence de la console et cliquez sur la commande **Supprimer**.

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

CREATION DE STRUCTURE DES GROUPES D'ADMINISTRATION

Kaspersky Administration Kit offre la possibilité de former une structure des groupes d'administration sur la base de :

- Domaines et des groupes de travail du réseau Windows (cf. section "Structure des groupes sur la base des domaines et des groupes de travail du réseau Windows" à la page [61](#)).

- Active Directory (cf. section "Structure des groupes sur la base d'Active Directory" à la page 63).
- Contenu du fichier texte (cf. section "Structure des groupes sur la base du contenu du fichier texte" à la page 65).

Si un ordinateur n'est pas enregistré dans le groupe **Ordinateurs non définis** quand vous créez une structure de groupe (il est désactivé ou déconnecté du réseau), il ne sera pas ajouté au réseau de l'entreprise. L'utilisation de l'Assistant pour créer un réseau logique ne remet pas en cause sa cohérence.

La création d'une structure de groupe à l'aide de l'Assistant ne viole pas l'intégrité du réseau de l'entreprise : de nouveaux groupes sont ajoutés ; mais ils ne remplacent pas les groupes existants. Un poste client déjà affecté à un groupe existant ne sera pas ajouté une seconde fois, parce que le groupe **Ordinateurs non définis** n'affiche que les ordinateurs qui ne sont pas présents dans le réseau.

STRUCTURE DES GROUPES SUR LA BASE DES DOMAINES ET DES GROUPES DE TRAVAIL DU RESEAU WINDOWS

➤ Afin de créer la structure des groupes d'administration sur la base des domaines et des groupes de travail du réseau Windows, procédez comme suit :

1. Ouvrez le menu contextuel du dossier Ordinateurs administrés et sélectionnez le point Toutes les tâches © Créer la structure du groupe. L'Assistant pour créer une structure des groupes apparaît (cf. ill. ci-après). Cliquez sur Suivant.

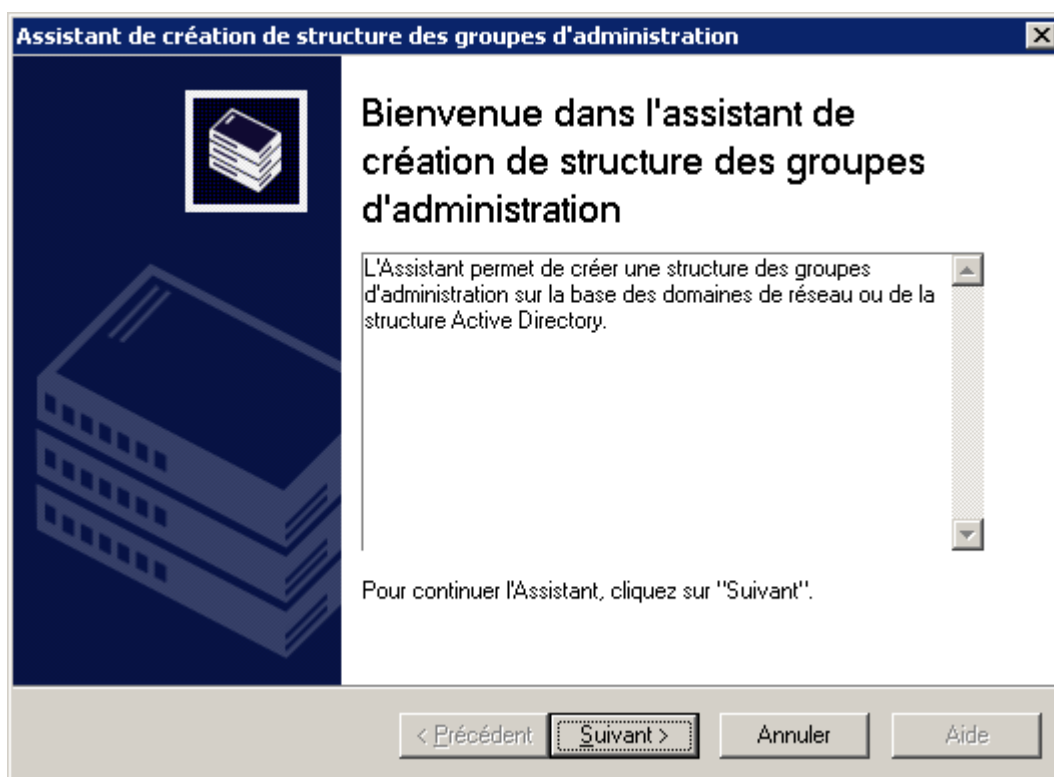


Illustration 39. Assistant de création de structure de groupe

2. Dans la fenêtre ouverte sélectionnez Domaines et groupes de travail du réseau Microsoft Windows (cf. ill. ci-après).

La structure sera créée sur la base des informations sur la structure des domaines du réseau Windows, reçus lors du dernier sondage et présentés dans le groupe Ordinateurs non définis. Cliquez sur Suivant.

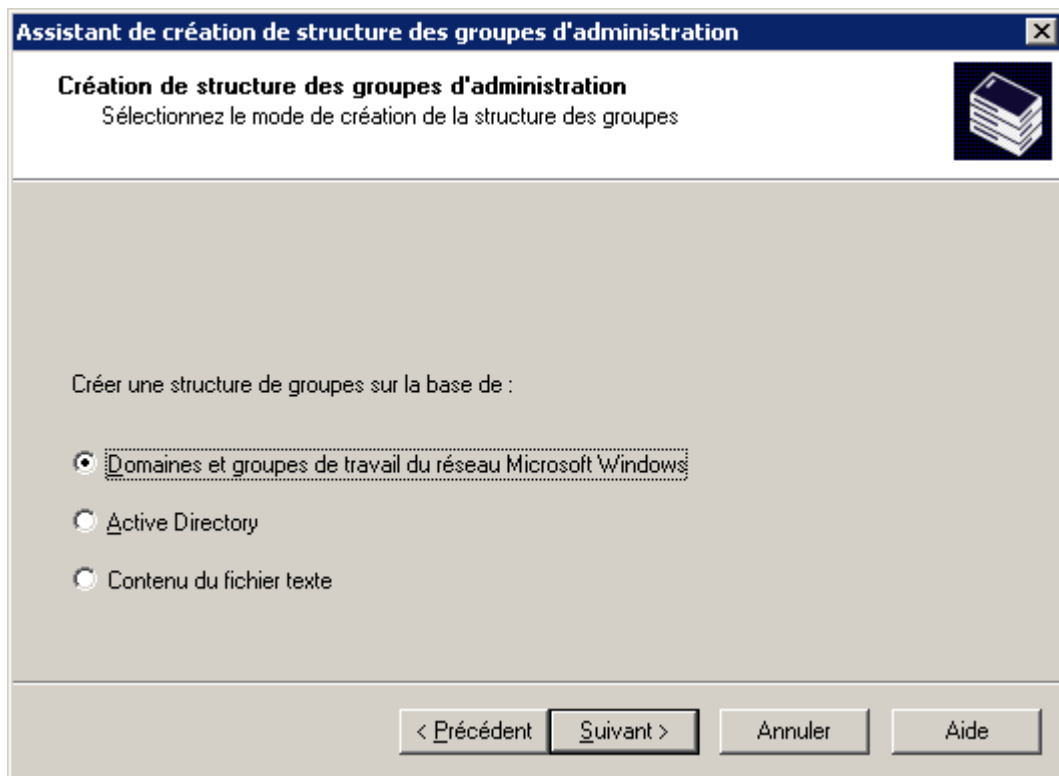


Illustration 40. Définir la création de groupe

3. Dans la fenêtre suivante sélectionnez le groupe et cliquez sur le bouton Parcourir, situé à côté du champ Groupe de destination.

Finalement une fenêtre s'ouvre qui contient l'hierarchie de groupes formés pour le Serveur d'administration. Pour sélectionner un groupe dans la liste des groupes déjà formés, il faut déployer l'entrée **Ordinateurs administrés**. Si ce groupe n'existe pas, pour créer un nouveau groupe, il faut cliquer sur le bouton **Créer un groupe**. Le groupe indiqué sera créé dans le groupe **Ordinateurs administrés**. Cliquez sur **Suivant**.

4. Dans la fenêtre suivante de l'assistant cliquez sur **Terminer**, afin de terminer la création de structure des groupes d'administration.

STRUCTURE DES GROUPES SUR LA BASE D'ACTIVE DIRECTORY

➤ Afin de créer la structure des groupes d'administration sur la base d'Active Directory, procédez comme suit :

1. Ouvrez le menu contextuel du dossier **Ordinateurs administrés** et sélectionnez le point **Toutes les tâches** → **Créer la structure du groupe**. L'Assistant pour créer une structure des groupes apparaît (cf. ill. ci-après). Cliquez sur **Suivant**.

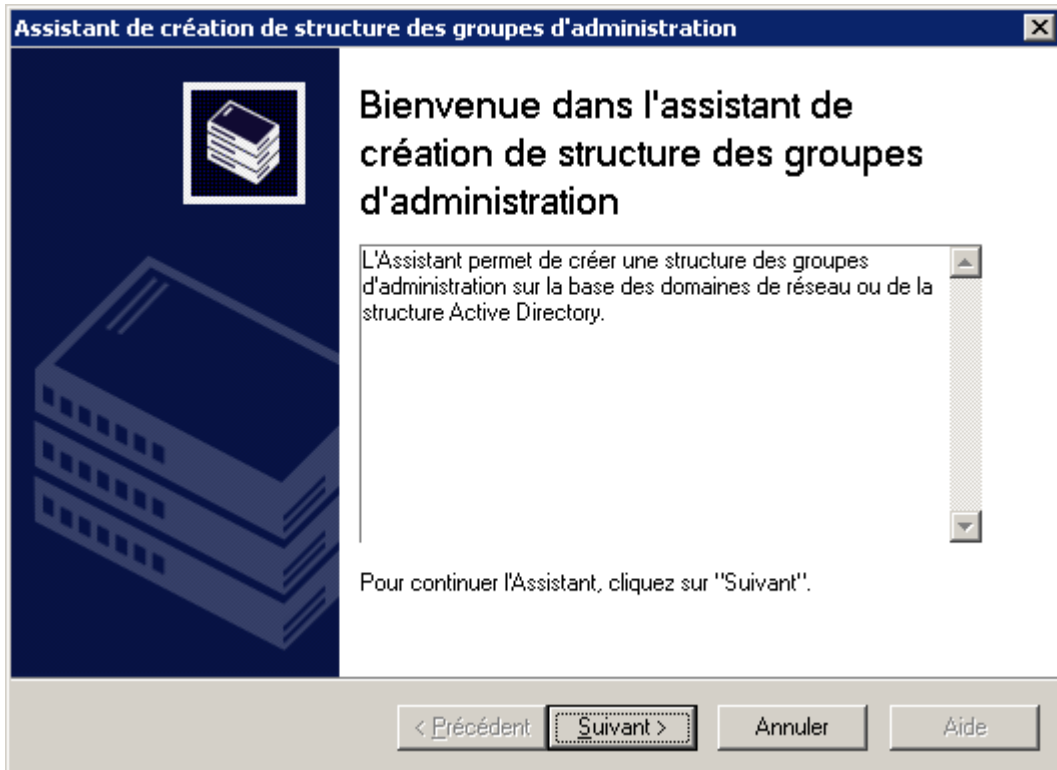


Illustration 41. Assistant de création de structure de groupe

2. Dans la fenêtre ouverte sélectionnez **Active Directory** (cf. ill. ci-après).

La structure sera créée sur la base des informations sur la structure des sous-divisions Active Directory, reçus lors du dernier sondage et présentés dans le groupe **Ordinateurs non définis**. Cliquez sur **Suivant**.

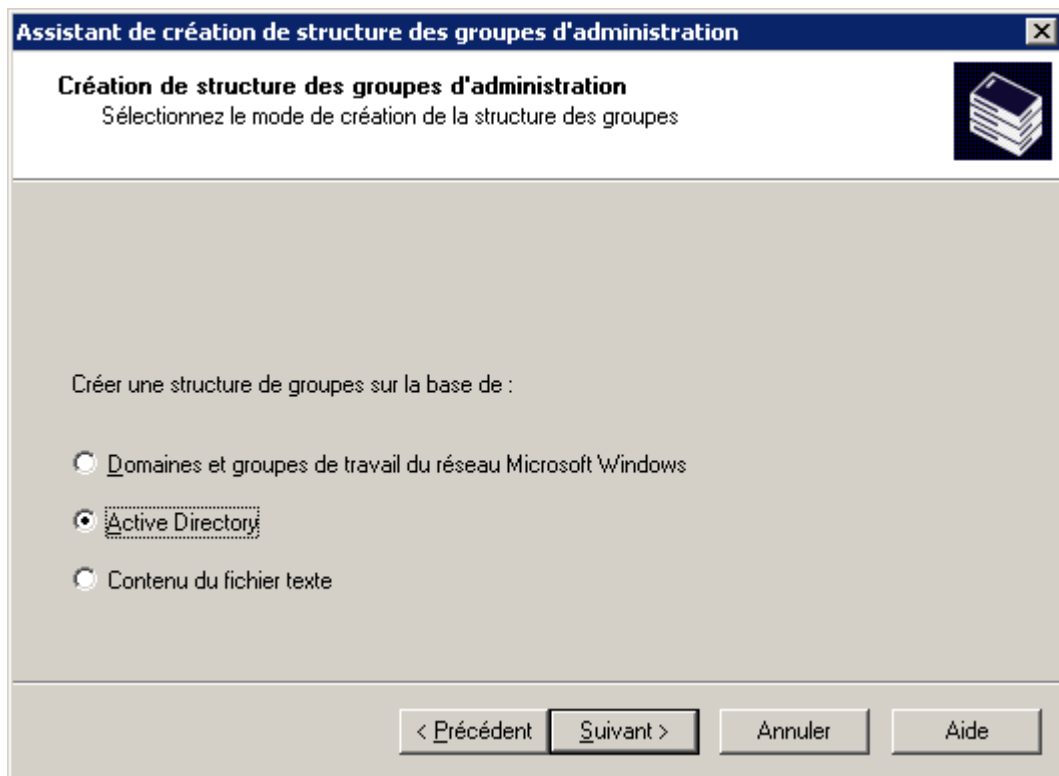


Illustration 42. Définir la création de groupe

3. Dans la fenêtre suivante sélectionnez le groupe et cliquez sur le bouton **Parcourir**, situé à côté du champ **Groupe de destination**. Finalement une fenêtre s'ouvre qui contient l'hierarchie de groupes formés pour le Serveur d'administration. Pour sélectionner un groupe dans la liste des groupes déjà formés, il faut déployer l'entrée **Ordinateurs administrés**. Si ce groupe n'existe pas, pour créer un nouveau groupe, il faut cliquer sur le bouton **Créer un groupe**. Le groupe indiqué sera créé dans le groupe **Ordinateurs administrés**. Sélectionnez une sous-division de départ d'Active Directory, en cliquant sur le bouton **Parcourir**, situé à côté du champ **La subdivision de base d'Active Directory**. Cliquez sur **Suivant**.
4. Dans la fenêtre suivante de l'assistant cliquez sur **Terminer**, afin de terminer la création de structure des groupes d'administration.

STRUCTURE DES GROUPES SUR LA BASE DU CONTENU DU FICHIER TEXTE

➔ Afin de créer la structure des groupes d'administration sur la base du contenu du fichier texte, procédez comme suit :

1. Ouvrez le menu contextuel du dossier **Ordinateurs administrés** et sélectionnez le point **Toutes les tâches** → **Créer la structure du groupe**. L'Assistant pour créer une structure des groupes apparaît (cf. ill. ci-après). Cliquez sur **Suivant**.

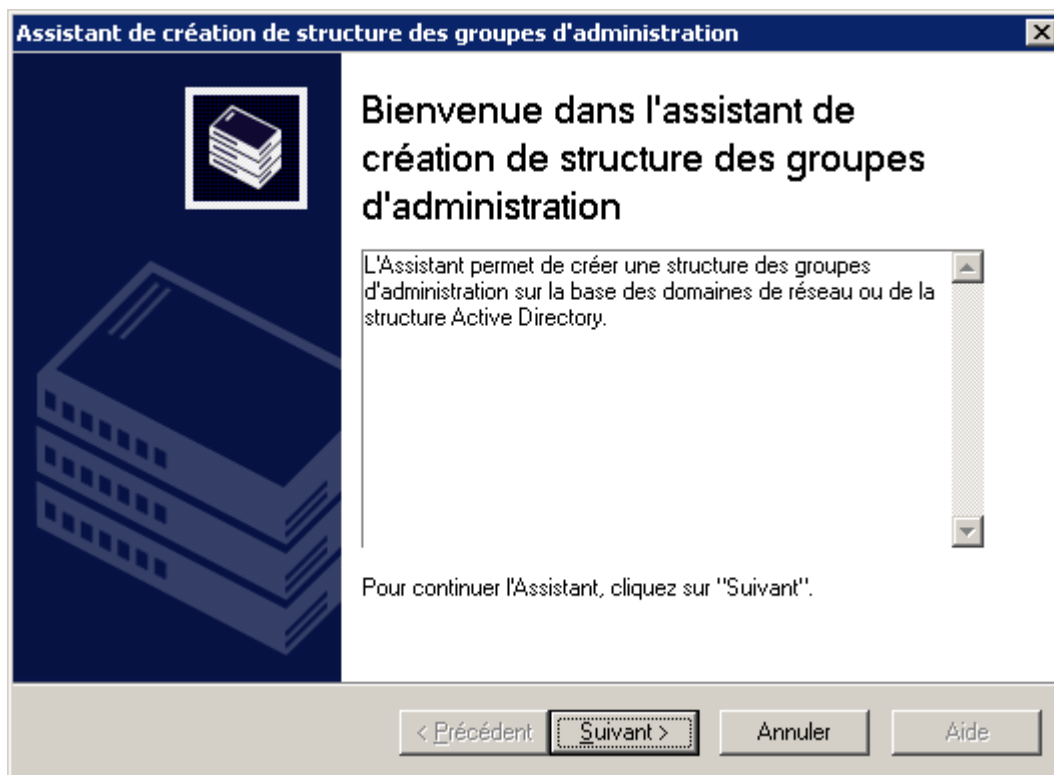


Illustration 43. Assistant de création de structure de groupe

2. Dans la fenêtre ouverte sélectionnez le point **Contenu du fichier texte** (cf. ill. ci-après).

La structure des groupes sera créée conformément au fichier texte, formé par l'administrateur. Dans le cas de sélection de cette option sur l'étape suivante sélectionnez le groupe, dans lequel les sous-groupes seront ajoutés, et indiquez le fichier texte qui contient la structure des groupes pour une formation.

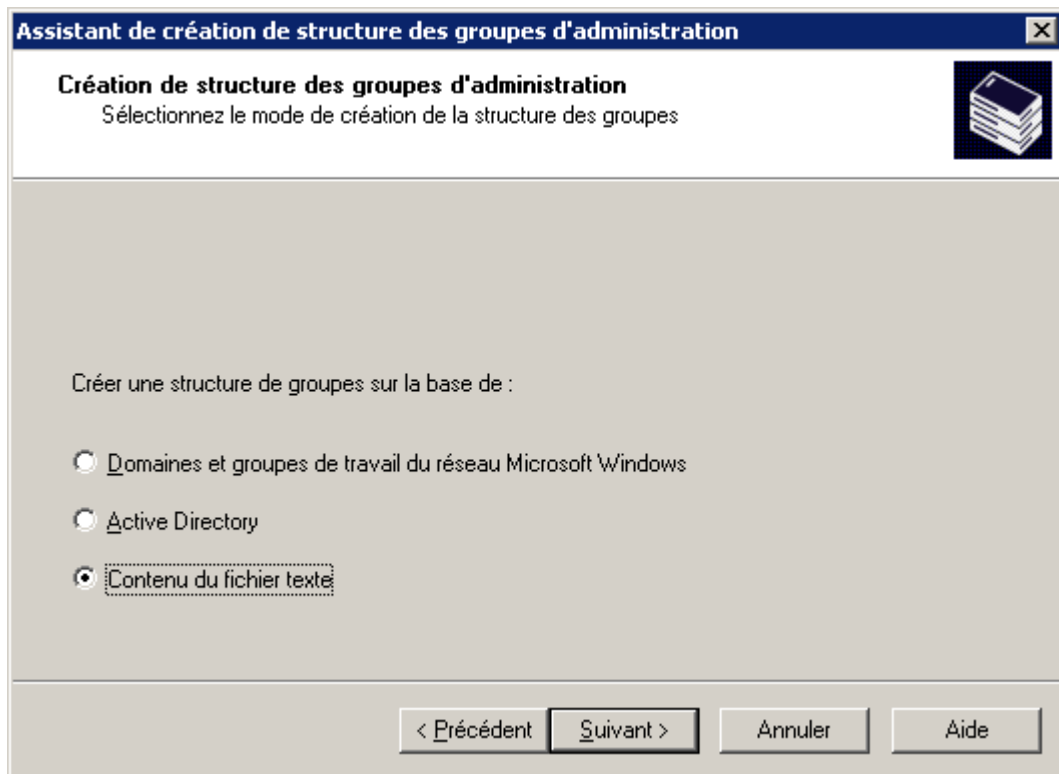


Illustration 44. Définir la création de groupe

3. Exécutez les actions suivantes dans la fenêtre suivante :

- Sélectionner le groupe et cliquez sur **Parcourir**, situé à côté du champ **Groupe de destination**. Finalement une fenêtre s'ouvre qui contient l'hierarchie de groupes formés pour le Serveur d'administration. Pour sélectionner un groupe dans la liste des groupes déjà formés, il faut déployer l'entrée **Ordinateurs administrés**. Si ce groupe n'existe pas, pour créer un nouveau groupe, il faut cliquer sur le bouton **Créer un groupe**. Le groupe indiqué sera créé dans le groupe **Ordinateurs administrés**.
- Indiquez le fichier, à base duquel l'hierarchie dans un groupe sera formée, définie dans le champ **Groupe de destination**. Pour ce faire, cliquez sur **Parcourir**, situé à côté du champ **Fichiers texte avec les noms des groupes**, et sélectionnez le fichier texte créé d'avance, formé selon les règles suivantes :
 - Le nom de chaque nouveau groupe doit commencer par une nouvelle ligne ; séparateur – traduction de la ligne. Les lignes vides lors d'une création sont ignorées.

Exemple :

Office 1

Office 2

Office 3

Trois groupes d'hierarchie du premier niveau seront formés dans le groupe de destination.

- Il faut indiquer le nom du groupe placé par une barre oblique (/).

Exemple :

Office 1/Subdivision 1/Section 1/Groupe 1

Quatre sous-groupes placés l'un dans l'autre seront formés dans le groupe de destination.

- Pour former quelques groupes placés du même niveau d'hierarchie, il faut indiquer "le chemin complet vers le groupe".

Exemple :

Office 1/Subdivision 1/Section 1

Office 2/Subdivision 2/Section 1

Office 3/Subdivision 3/Section 1

Office 1/Subdivision 4/Section 1

Dans le groupe de destination un groupe du premier niveau d'hierarchie "Office 1" sera formé. Il sera composé de quatre groupes placés du même niveau d'hierarchie "Subdivision 1", "Subdivision 2", "Subdivision 3", "Subdivision 4". Chaque groupe est composé d'encore un groupe "Section 1".

Cliquez sur **Suivant**.

4. Dans la fenêtre suivante de l'assistant cliquez sur **Terminer**, afin de terminer la création de structure des groupes d'administration.

AFFICHAGE DES INFORMATIONS SUR UN GROUPE

➔ Pour consulter les informations sur la structure d'un groupe, procédez comme suit :

1. Ouvrez le dossier **Ordinateurs administrés**.
2. Sélectionnez le dossier portant le nom du groupe qui vous intéresse.

La liste des objets présents dans ce groupe est affichée dans le panneau de détails (vous pouvez également développer le contenu du dossier dans l'arborescence de console) :

- Pour afficher les informations relatives aux stratégies de groupe, sélectionnez le dossier **Stratégies**.

Si des stratégies ont été définies pour le groupe, elles figureront dans l'arborescence de la console. Dans le cas contraire, le dossier sera vide.

- Pour afficher les informations sur les tâches de groupe, sélectionnez le dossier **Tâches de groupe**.

Si des tâches ont été définies pour le groupe, elles figureront dans l'arborescence de la console. Dans le cas contraire, le dossier sera vide.

- Pour travailler avec les Serveurs d'administration secondaires, sélectionnez le dossier **Serveurs d'administration**.

- Afin de travailler avec les grappes et matrices de serveurs sélectionnez le dossier **Grappes et matrices de serveurs**. Ce dossier s'affichera dans l'arborescence de la console uniquement dans le cas d'ajout de la grappe dans le réseau de l'entreprise.

Les points cités ci-dessus dépendent des paramètres de l'interface utilisateur.

- Pour consulter la liste des postes clients, sélectionnez le dossier **Postes clients**. La liste des postes clients figure dans le panneau des résultats.

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.

AFFICHAGE ET MODIFICATION DES PARAMETRES DU GROUPE

➤ Pour consulter ou modifier les paramètres du groupe, procédez comme suit :

1. Ouvrez le groupe **Ordinateurs administrés** dans l'arborescence de la console.
2. Sélectionnez le groupe requis.
3. Ouvrez le menu contextuel.
4. Sélectionnez le point **Propriétés**.

Cette action entraîne l'ouverture de la fenêtre des propriétés du groupe qui contient des onglets sur lesquels vous pouvez consulter et modifier les paramètres de la sécurité, de l'interaction avec les postes clients, définir l'interaction du Serveur d'administration avec les postes clients, indiquer une sélection de conditions qui déterminent l'état de l'ordinateur.

Pour ouvrir la fenêtre des propriétés du groupe, vous pouvez également cliquer sur le lien **Propriétés du groupe** situé dans le panneau des tâches du groupe.

PARAMETRES GENERAUX

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez consulter et modifier le nom des groupes. Le nom doit être unique dans les limites d'un même niveau de la hiérarchie de dossiers ou de groupes.

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

Cet onglet propose également les informations suivantes :

- **Groupe parent** : nom du groupe auquel appartient ce groupe (pour les groupes d'un niveau de hiérarchie supérieur, ce champ contient le nom du Serveur d'administration auquel se rapporte ce groupe).
- **Composition** : informations statistiques sur les structures de groupe – nombre de groupes imbriqués et le total des clients, y compris dans les groupes imbriqués.
- **Créé** : date de création du groupe.
- **Modifié** : date de dernière modification du nom ou des attributs du groupe (si le nom de groupe n'a pas changé, la valeur est <Inconnu>).

Le bouton **Effacer** de la rubrique **Compteur des virus découverts** permet de remettre à zéro le compteur des virus découverts pour tous les postes clients des ordinateurs du groupe.

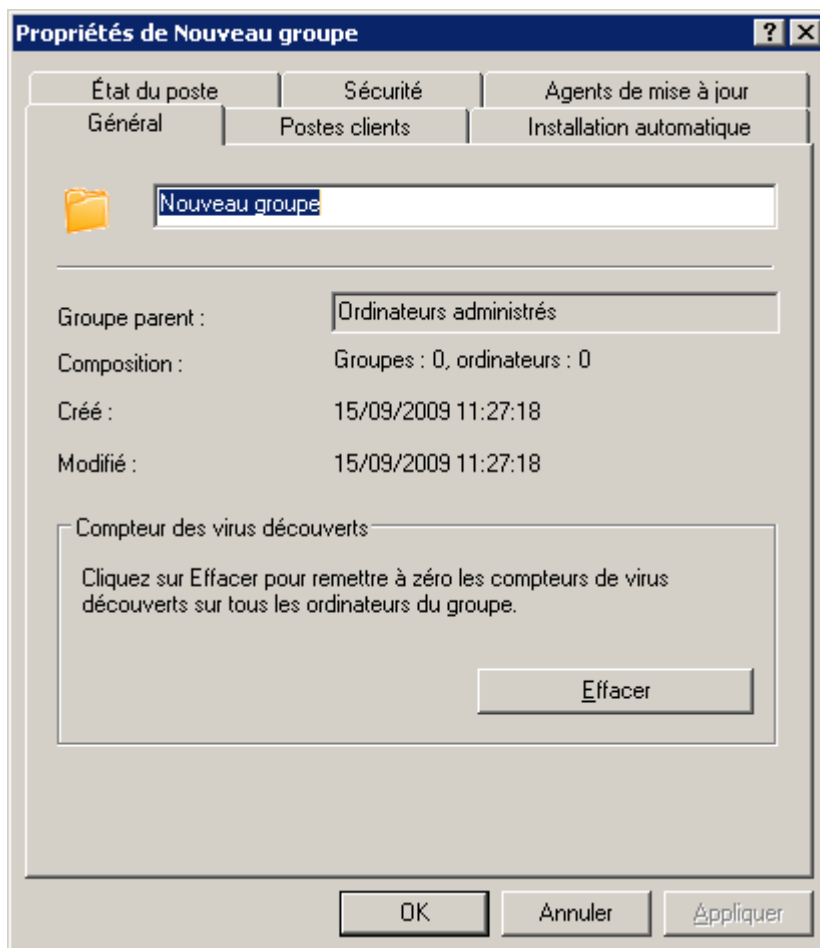


Illustration 45. Affichage des propriétés du groupe. Onglet **Général**

AFFECTATION DES DROITS POUR TRAVAILLER AVEC UN GROUPE

L'onglet **Sécurité** (cf. ill. ci-après) est prévu pour la configuration des privilèges d'accès au groupe d'administration.

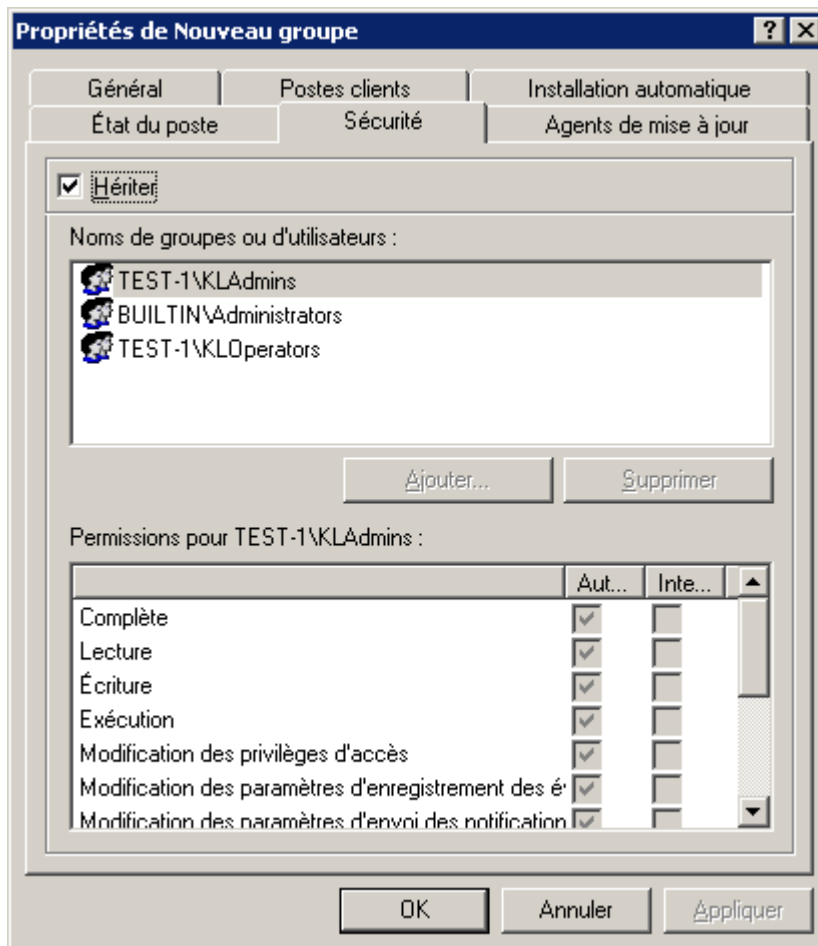


Illustration 46. Attribution de droits d'accès à un groupe d'administration

La présence ou l'absence de cet onglet est définie par les paramètres d'interface de l'utilisateur. Afin de configurer l'affichage de cet onglet, passez au menu **Vue** → **Configuration de l'interface** et cochez la case dans la ligne **Afficher les onglets avec les paramètres de sécurité**.

Par défaut, les droits d'utilisation d'un groupe sont hérités des propriétés du Serveur d'administration (cf. section "Affectation des droits pour travailler avec le Serveur²⁷" à la page), où l'on définit les privilèges de manipulation de tous les objets administrés par le Serveur. Afin de définir des privilèges d'accès à un groupe administratif différents de ceux définis dans les paramètres du Serveur d'administration, il faut décocher la case **Hériter**.

La partie supérieure de l'onglet reprend la liste des utilisateurs et des groupes des utilisateurs qui possèdent l'accès au Serveur d'administration. La partie inférieure reprend les privilèges possibles :

- **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.

➡ Pour indiquer les privilèges sur le travail avec le groupe, procédez comme suit :

1. Sélectionnez le groupe d'utilisateurs.
2. Dans la colonne **Autoriser** cochez les cases en regard des autorisations octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.
3. Dans la colonne **Interdire** cochez les cases en regard des autorisations qui ne peuvent être octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.

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

Pour supprimer le groupe ou l'utilisateur, il faut sélectionner l'objet dans la liste et cliquer sur le bouton **Supprimer**.

Il est impossible de supprimer le groupe d'administrateurs de Kaspersky Administration Kit (**KLAdmins**).

Pour appliquer le paramètre, il suffit de cliquer sur **Appliquer** ou **OK**.

CONDITIONS DE DEFINITION DE L'ETAT DU POSTE

Dans la fenêtre des propriétés du Serveur d'administration sur l'onglet **Etat du poste** (cf. ill. ci-après) définit les conditions dans lesquelles le client recevra un des deux états suivants : *Critique* ou *Avertissement*. Si le client ne satisfait à aucun des critères indiqués, il reçoit l'état *OK*.

Il est possible, pour certaines conditions, de modifier la valeur limite. Pour modifier la valeur, double cliquez sur une condition dans la colonne **Condition** pour ouvrir la boîte de dialogue d'édition.

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

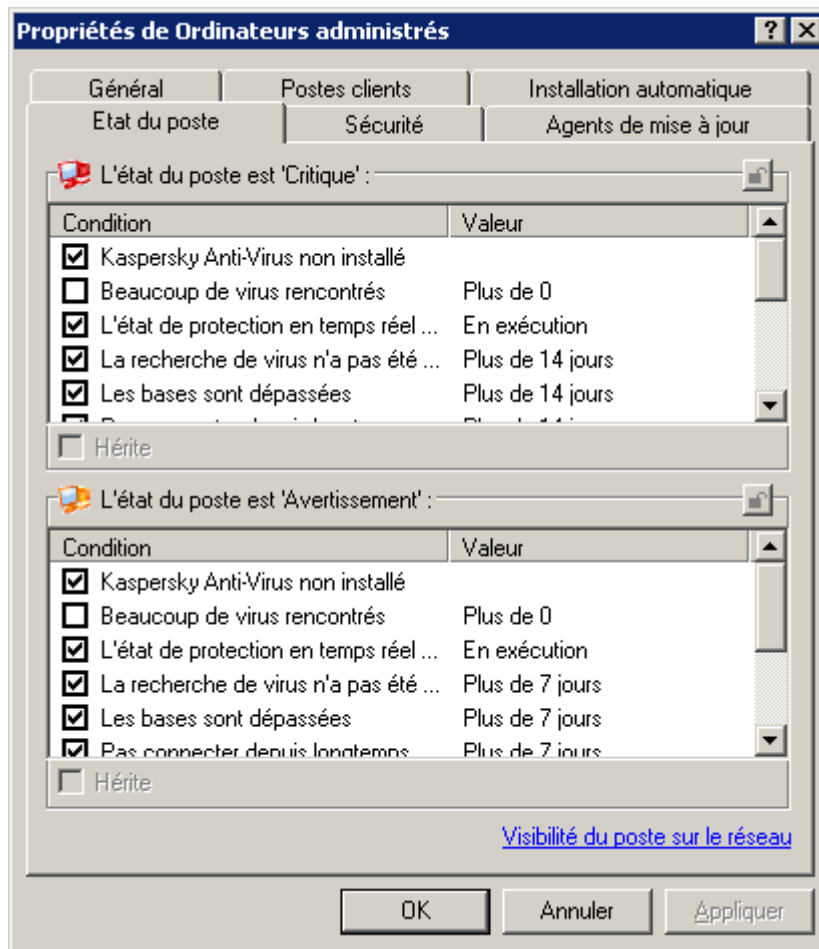


Illustration 47. La configuration de diagnostic de l'état du poste client

Si l'état du poste est OK, alors, par exemple dans le panneau des résultats de la fenêtre principale de l'application, son nom sera accompagné de l'icône . Si l'état du poste est *Avertissement*, il est accompagné de l'icône . Si son état est *Critique*, il sera accompagné de l'icône .

Les critères permettant de déterminer l'état du poste client sont définis dans les paramètres du groupe du niveau hiérarchique supérieur, et sont hérités par tous les groupes d'administration. Pour définir des critères distincts pour un groupe, désélectionnez la case **Hériter** et configurez les paramètres (pour le groupe du niveau supérieur de la hiérarchie, la case **Hériter** est inactive).

Le lien **Visibilité de l'ordinateur dans le réseau** ouvre la fenêtre **Visibilité de l'ordinateur**. Le champ **Délai de visibilité de l'ordinateur (min.)** reprend la durée pendant laquelle l'hôte est considéré comme visible dans le réseau après une perte de la connexion au Serveur d'administration. Par défaut, l'intervalle est fixé à 60 minutes. A la fin de cette période, le Serveur d'administration considérera que l'hôte est inactif. Le cas échéant, vous pouvez modifier la valeur de ce paramètre dans les propriétés de la stratégie de Kaspersky Administration Kit (cf. section "Configuration des paramètres de la stratégie du Serveur d'administration" à la page [91](#)).

SURVEILLANCE DE L'ACTIVITE DES POSTES CLIENTS

Dans la fenêtre des propriétés du groupe d'administration sur l'onglet **Postes clients** (cf. ill. ci-après) vous pourrez définir les paramètres suivants :

- Dans le bloc **Activité du poste client dans le réseau** définissez la réaction du serveur d'administration face à l'absence d'activité de réseau des clients de ce groupe pendant un certain temps :

- En cas d'exécution d'une action quelconque (par exemple, avertir les administrateurs de Kaspersky Administration Kit), cochez la case **Informez l'administrateur si l'ordinateur reste inactif pendant plus de (jours)** et précisez le nombre de jours dans le champ à droite. A la fin de cette période, le Serveur d'administration exécutera les actions requises.

Les notifications sont envoyées conformément aux paramètres définis dans les propriétés du Serveur d'administration (cf. section "Affichage et modification des paramètres du Serveur d'administration" à la page [29](#)).

- Si des clients doivent être supprimés du groupe, cochez la case **Supprimer du groupe après une période d'inactivité de (jours)** et précisez le nombre de jours dans le champ à droite. A la fin de cette période, le client sera supprimé automatiquement du groupe et placé dans le groupe **Ordinateurs non définis**.

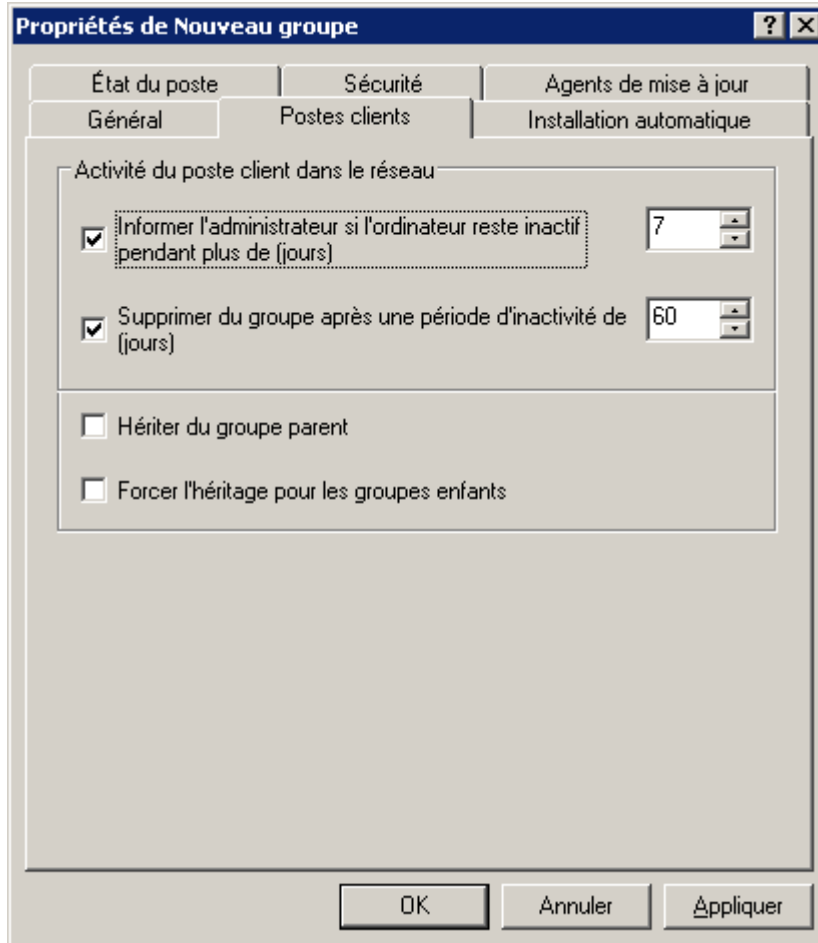


Illustration 48. Fenêtre des propriétés du groupe. Onglet **Postes clients**

- Indiquez les paramètres d'héritage de valeurs, que ceux définis sur cet onglet :
 - **Hériter du groupe parent**, pour que les valeurs établies soient héritées du groupe du niveau précédent d'hierarchie. Si cette case est cochée, alors les paramètres repris à l'onglet ne peuvent pas être modifiés.
 - **Forcer l'héritage pour les groupes enfants** – pour que les valeurs établies ne se diffusent pas sur les groupes intégrés. Si vous cochez cette case, dans les propriétés des groupes enfant les paramètres repris à l'onglet ne pourront pas être modifiés.

INSTALLATION AUTOMATIQUE D'APPLICATIONS SUR DES POSTES CLIENTS

Sous l'onglet Installation automatique vous pouvez définir les fichiers d'installation à utiliser pour l'installation automatique à distance des applications Kaspersky Lab sur les nouveaux clients qui viennent d'être intégrés au groupe. Pour utiliser un paquet d'installation, il suffit de cocher la case située en regard de son nom. Pour empêcher l'installation automatique de l'application, désélectionnez la case située en regard du nom du paquet d'installation. Par défaut, l'installation automatique des applications Kaspersky Lab est désactivée. Des tâches de groupe d'installation à distance portant le nom **Installation <Nom du fichier d'installation sélectionné>** seront créées pour tous les paquets d'installations sélectionnés. Vous pouvez les lancer manuellement.

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

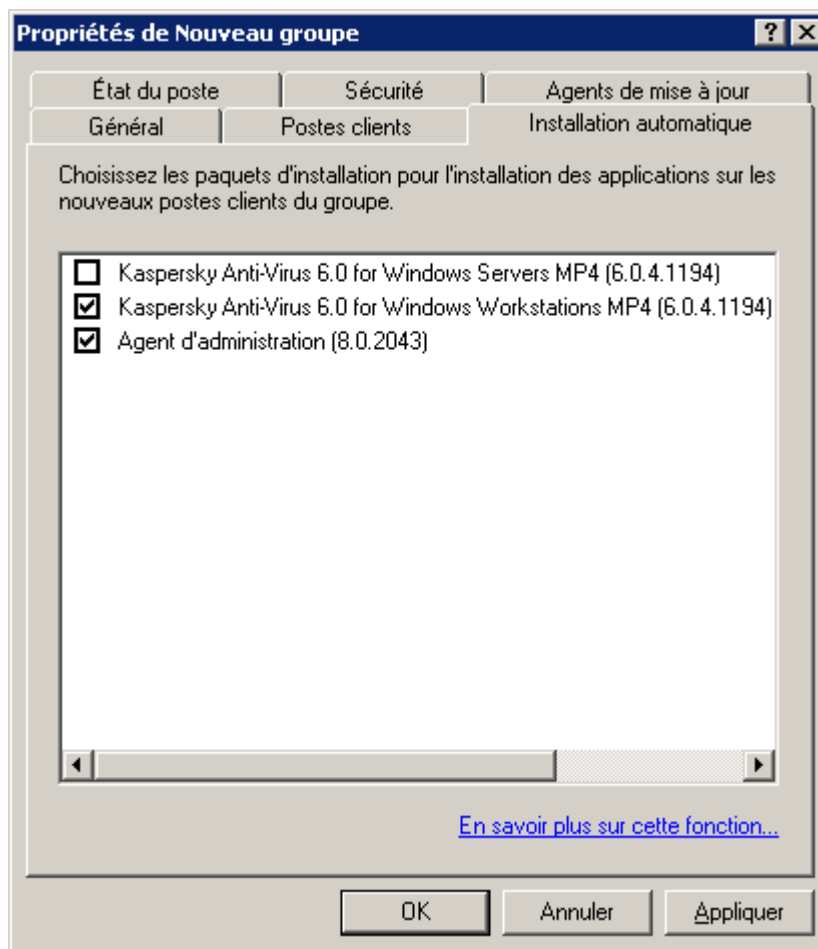


Illustration 49. Fenêtre des propriétés du groupe. Onglet **Installation automatique**

Si plusieurs paquets d'installation d'une seule application sont indiqués pour une installation automatique, alors la tâche d'installation sera uniquement créée pour la dernière version de l'application.

CREATION DE LA LISTE DES AGENTS DE MISE A JOUR

L'onglet **Agents de mise à jour** (cf. ill. ci-après) permet de composer la liste des ordinateurs (cf. section "Constitution de la liste des agents de mise à jour et leur configuration" à la page 264), à l'aide desquels les mises à jour, les paquets d'installation et les tâches et les stratégies de groupe sont diffusés dans les limites du groupe.

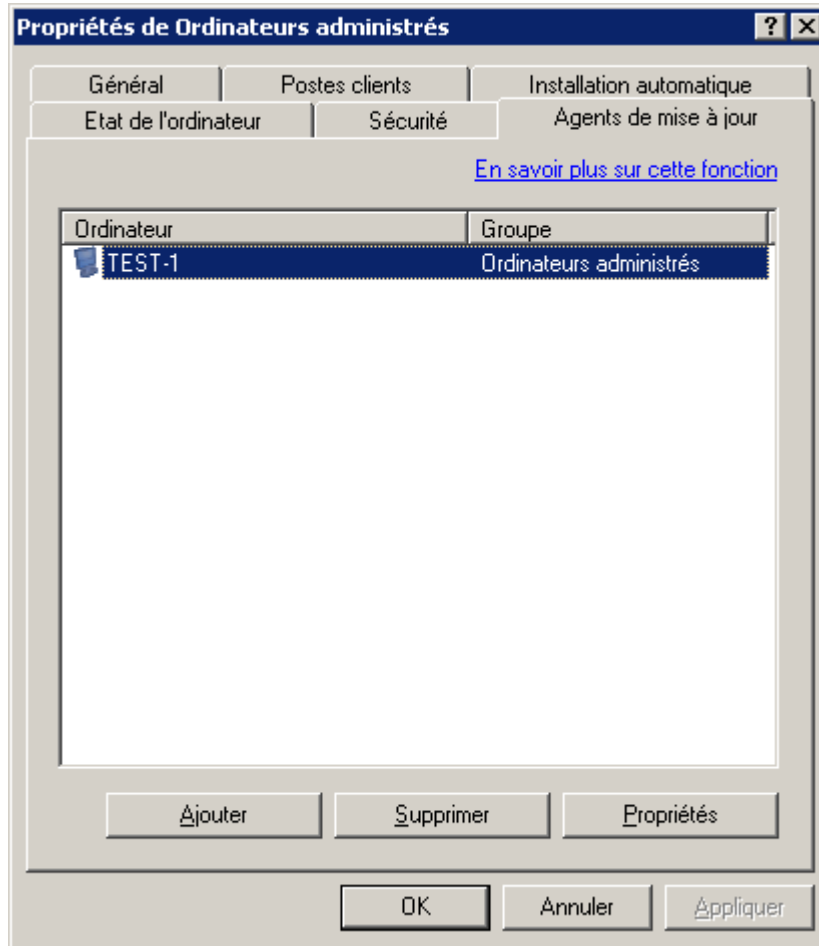


Illustration 50. Création de la liste des agents de mise à jour

ADMINISTRATION A DISTANCE DES APPLICATIONS

L'application Kaspersky Administration Kit permet d'administrer à distance les applications installées sur les ordinateurs des groupes d'administration et du réseau de l'entreprise. L'administration s'opère grâce à :

- la création de *stratégies* chargées de la configuration centralisée des paramètres de fonctionnement des applications installées sur les postes clients ;
- la création et l'exécution de *tâches* (cf. section "Administration des tâches" à la page [100](#)) prévues pour les groupes d'administration, le Serveur d'administration ou des groupes distincts d'ordinateurs ;
- la configuration des *paramètres locaux* des applications installées sur des ordinateurs distincts du réseau.

DANS CETTE SECTION

Administration des stratégies	76
Gérer les tâches.....	100
Paramètres locaux de l'application.....	133

ADMINISTRATION DES STRATEGIES

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

Les stratégies composées pour les applications dans le groupe apparaissent dans l'arborescence de la console dans le dossier correspondant. Une icône figure devant le nom de chaque stratégie et caractérise son état (cf. section "Etats des ordinateurs, des tâches et des stratégies" à la page [333](#)).

CREATION D'UNE STRATEGIE

➡ Pour créer une stratégie pour un groupe, procédez comme suit :

1. Dans l'arborescence de console, choisissez le groupe dans lequel vous allez créer une stratégie. Dans le dossier du groupe, sélectionnez le dossier **Stratégies**, ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Stratégie** ou cliquez sur le lien **Créer une stratégie** dans le panneau des tâches. Cette action lance un Assistant. Suivez les instructions de l'Assistant.

A l'aide des liens **Créer une stratégie de Kaspersky Anti-Virus pour Windows Workstations** et **Créer une stratégie de Kaspersky Anti-Virus pour Windows Servers**, situés dans le panneau des tâches, il est possible de créer des stratégies pour les applications correspondantes. Dans ce cas, il n'est pas nécessaire d'indiquer l'application dans l'assistant de configuration de stratégie.

2. Vous devez maintenant indiquer le nom et l'application cible de la stratégie.

La définition du nom se fait de manière standard. Si une stratégie de ce nom existe déjà, un **(1)** sera automatiquement ajouté à la fin du nouveau nom.

La sélection des applications s'opère (cf. ill. ci-après) dans la liste déroulante. La liste déroulante inclut toutes les applications de la société qui possèdent un plug-in de console installé sur le poste administrateur.

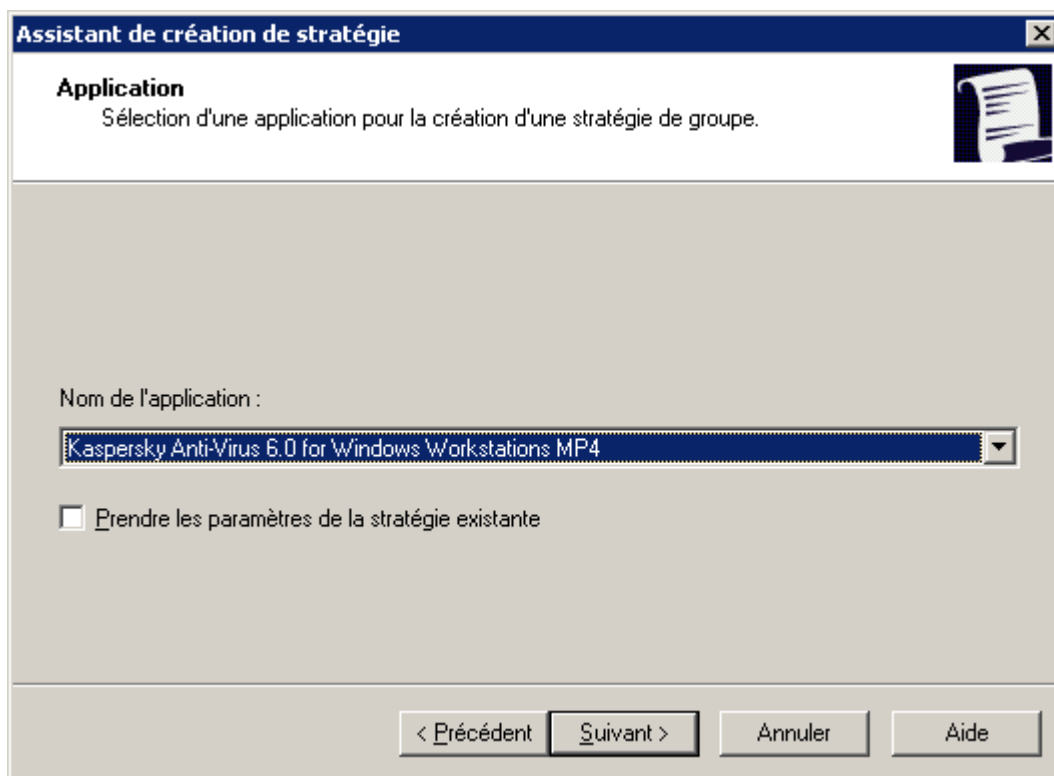


Illustration 51. Sélection de l'application pour la création d'une stratégie

3. Dans la fenêtre suivante de l'Assistant (cf. ill. ci-après), indiquez l'état de la stratégie. Vous avez le choix parmi les options suivantes :
 - **Stratégie active.** Dans ce cas, la stratégie créée sera la stratégie utilisée par l'application.
 - **Stratégie inactive.** Dans ce cas, la stratégie sera enregistrée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins (cf. section "Activation d'une stratégie" à la page [84](#)).
 - **Stratégie pour utilisateur nomade.** Cette stratégie sera activée lorsque l'ordinateur est déconnecté du réseau de l'entreprise. Ce type de stratégie est accessible pour Kaspersky Anti-Virus for Windows Workstations versions 6.0 MP3 ou supérieure.

Il est possible de créer de nombreuses stratégies pour une application, mais une seule d'entre elles peut être celle active. Lors de la création d'une nouvelle stratégie effective, la stratégie précédente devient inactive.

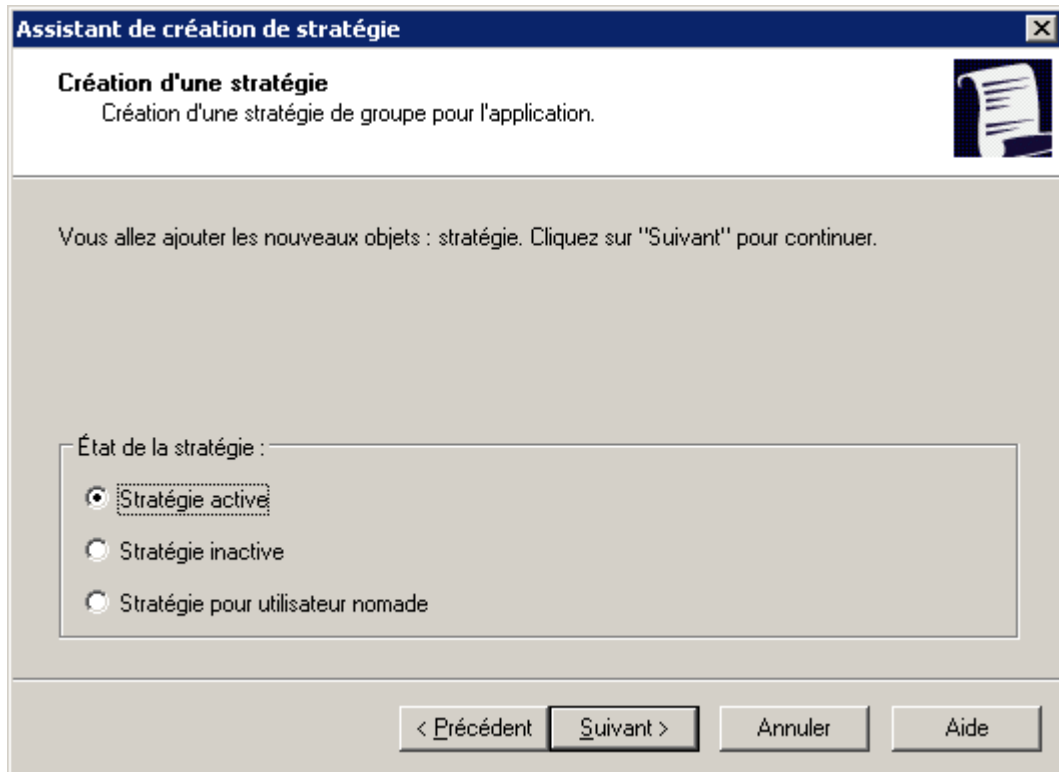




Illustration 52. Assistant de création de stratégie. Activation de la stratégie

- Vous devez ensuite considérer les paramètres généraux de la stratégie et configurer ceux de l'application sélectionnée (cf. ill. ci-après). Vous pouvez verrouiller les paramètres de stratégie des sous-groupes, des paramètres d'application, et des paramètres de tâche. Les paramètres de stratégie qui peuvent être verrouillés sont identifiés par l'icône . Cliquez sur cette icône avec le bouton gauche de la souris pour verrouiller un paramètre. L'icône deviendra .

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

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. Vous pouvez modifier la stratégie en l'éditant (cf. section "Affichage et modification des paramètres d'une stratégie" à la page [79](#)).

Vous trouverez une description détaillée de la configuration des stratégies pour chacune des applications dans les documentations respectives.

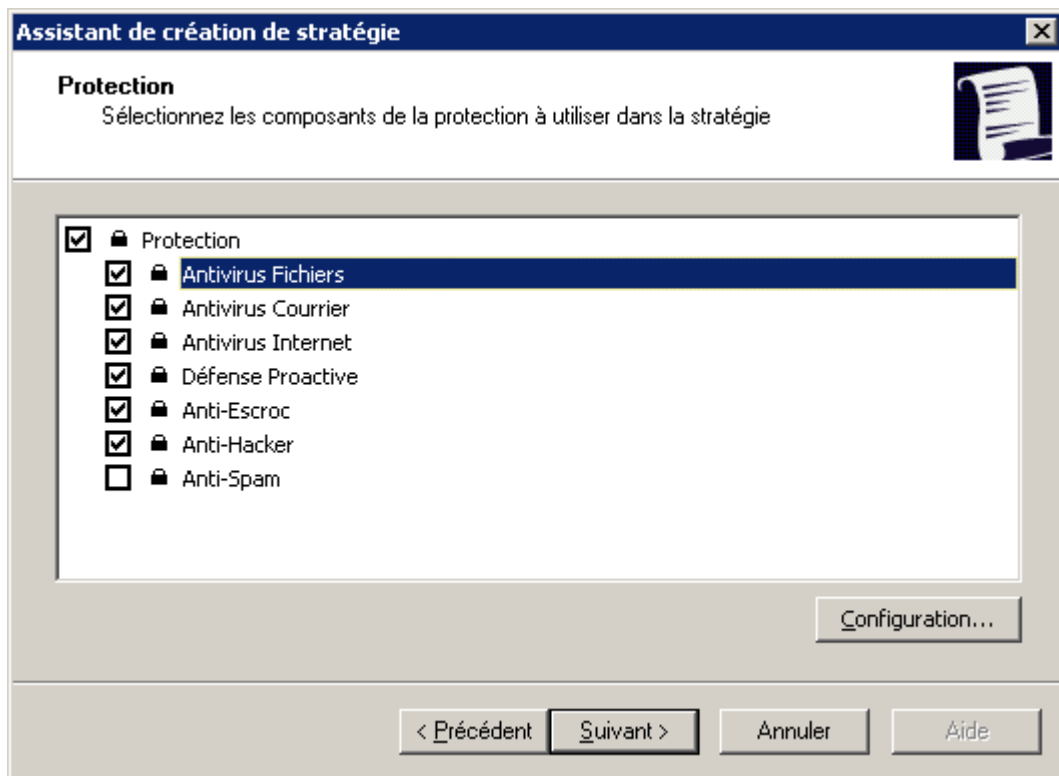


Illustration 53. Création d'une stratégie pour Kaspersky Anti-Virus for Windows Workstations


5. Cliquez sur **Terminer** dans la dernière fenêtre de l'Assistant.

Après avoir créé la stratégie sur les postes clients, les paramètres verrouillés (marqués d'un "cadenas" ) sont effectifs.

AFFICHAGE DE LA STRATEGIE HERITEE DANS LE PANNEAU DES RESULTATS DU GROUPE IMBRIQUE

➤ Pour que les stratégies héritées apparaissent dans le groupe imbriqué dans le dossier **Stratégies** procédez comme suit :

1. Sélectionnez le dossier **Stratégies** du dossier imbriqué dans l'arborescence de la console.
2. Ouvrez le menu contextuel, choisissez **Vue** et cochez la case **Stratégies héritées**.

Les stratégies héritées sont alors affichées dans l'arborescence de la console en regard de l'icône . Il est possible de visualiser les propriétés des stratégies héritées. Lorsque le mode d'héritage des paramètres est activé, la modification des stratégies héritées n'est possible que dans les groupes où elles ont été créées.

AFFICHAGE ET MODIFICATION DES PARAMETRES D'UNE STRATEGIE

➤ Pour afficher les valeurs des paramètres d'une stratégie ou pour les modifier, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Stratégies** du groupe d'administration qui vous intéresse.
2. Sélectionnez la stratégie requise.

3. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.

Pour passer rapidement à la fenêtre des propriétés de la stratégie, sélectionnez la stratégie dans l'arborescence de la console et cliquez sur le lien **Editer** la stratégie, dans le groupe **Actions** du panneau des tâches.

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

Sur l'onglet **Général** (cf. ill. ci-après), vous retrouverez les informations générales sur la stratégie :

- nom de stratégie ;
- nom de l'application pour laquelle la stratégie est créée (par exemple, Kaspersky Administration Kit) ;
- date et heure de création de la stratégie ;
- date et heure de la dernière modification des paramètres de la stratégie ;
- état de la stratégie ;
- informations sur les résultats de l'application de la stratégie.

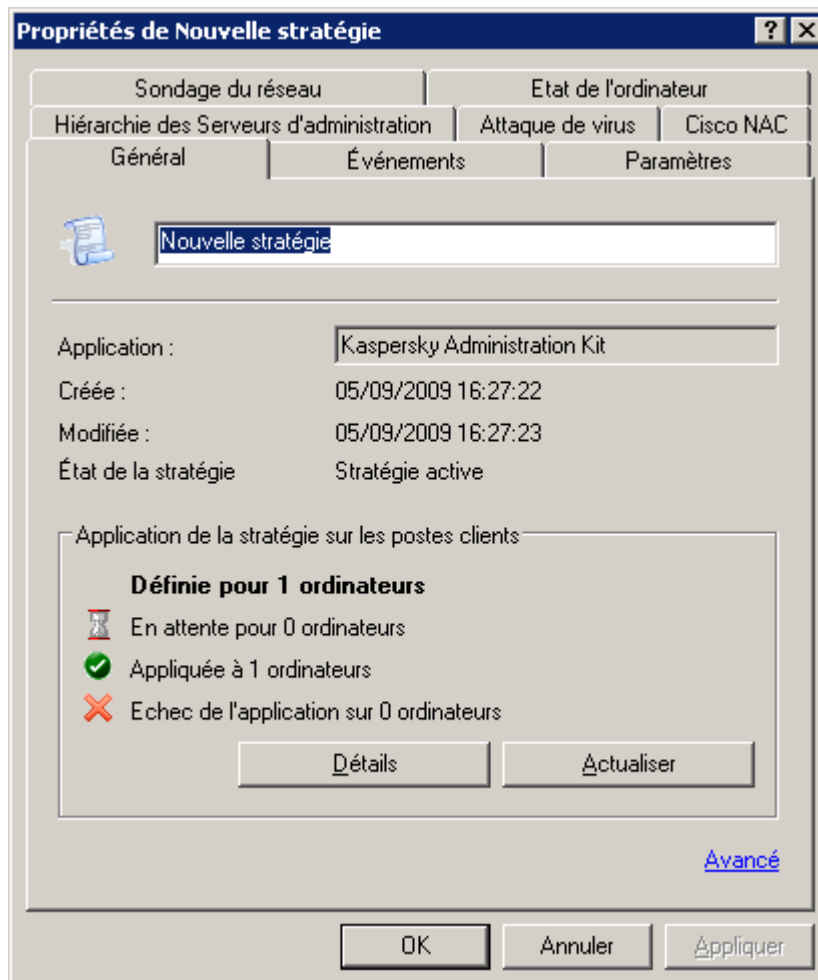


Illustration 54. Fenêtre des propriétés de la stratégie

Sur cet onglet, vous pouvez :

- renommer la stratégie ;

- afficher les résultats de l'application de la stratégie ;
- passer à la configuration des paramètres complémentaires à l'aide du lien **Avancé**.

Dans le groupe **Application de la stratégie sur les postes clients** vous trouverez également l'aide sur les résultats de l'application de la stratégie sur les postes clients du groupe. Le nombre d'ordinateurs est indiqué :

- ordinateurs pour lesquels la stratégie a été définie ;
- ordinateur sur lesquels la stratégie a été appliquée ;
- ordinateurs sur lesquels la stratégie n'a pu être appliquée.

Pour actualiser les informations sur les résultats de l'application de la stratégie, cliquez sur le bouton **Actualiser**.

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

- **Ordinateur** : nom du poste client.
- **Domaine** : nom du domaine auquel l'ordinateur appartient.
- **Etat** : état de la stratégie ; la colonne peut contenir une des valeurs suivantes :
 - *Modifiée* : les paramètres de cette stratégie ont été modifiés sur le serveur Administration Kit, mais n'ont pas encore été synchronisés avec les postes de travail ;
 - *Appliquée* : la stratégie pour une application sur cet ordinateur a été appliquée avec succès ;
 - *En attente* : la stratégie d'une application n'est pas encore appliquée sur cet ordinateur ;
 - *Echec* : l'application de la stratégie a échoué sur cet ordinateur (l'ordinateur a été arrêté, déconnecté, l'application ne s'exécute pas, ou n'a pas été installée).

- **Date** : date et heure de l'événement.

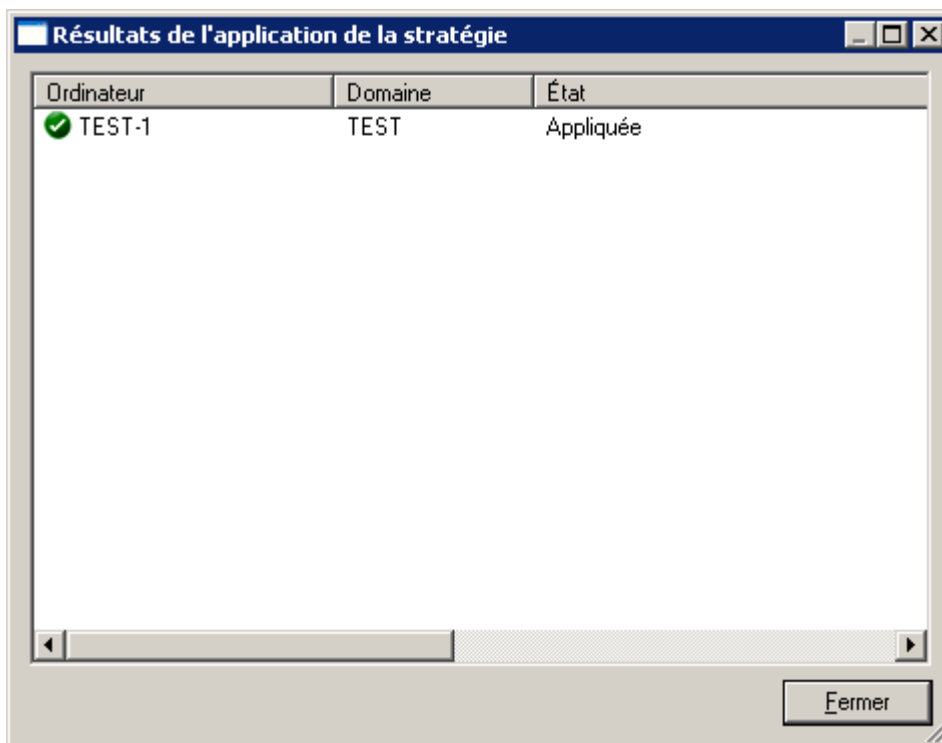


Illustration 55. Résultats de l'application de la stratégie sur les postes clients du groupe

La modification des paramètres locaux s'opère automatiquement en fonction des paramètres lors de la première application de la stratégie sur l'ordinateur client.

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.

Tout changement de stratégie réalisé sur un grand nombre de clients augmente considérablement la charge du Serveur d'administration ainsi que le volume du trafic réseau.

Pour passer à la configuration des paramètres complémentaires, cliquez sur le lien **Avancé**.

Pour définir l'état de la stratégie, sélectionnez une des options proposées dans le groupe **Etat** de la stratégie de la fenêtre qui s'ouvre (cf. ill. ci-après) :

- **Stratégie active** ;
- **Stratégie pour utilisateur nomade** ;
- **Stratégie inactive**.

Pour activer le mode d'héritage, ç.-à-d. pour interdire la modification dans les propriétés des paramètres de la stratégie héritée marqués par un verrou dans les propriétés de la stratégie héritée, cochez la case **Hériter des paramètres de la stratégie de niveau supérieur**. Pour désactiver le mode d'héritage, décochez la case **Hériter des paramètres de la stratégie de niveau supérieur**.

Pour imposer l'héritage des paramètres aux stratégies enfant, cochez la case en regard du point homonyme. Les actions suivantes seront exécutées après l'application des modifications dans la stratégie :

- les valeurs définies des paramètres seront diffusées dans la stratégie des groupes d'administration intégrés, dans les stratégies enfant ;

- la case **Hériter des paramètres de la stratégie de niveau supérieur** sera cochée dans les stratégies enfant ;
- les valeurs des paramètres des stratégies enfant ne pourront être modifiées tant que la case **Imposer l'héritage des paramètres aux stratégies enfant** sera cochée.

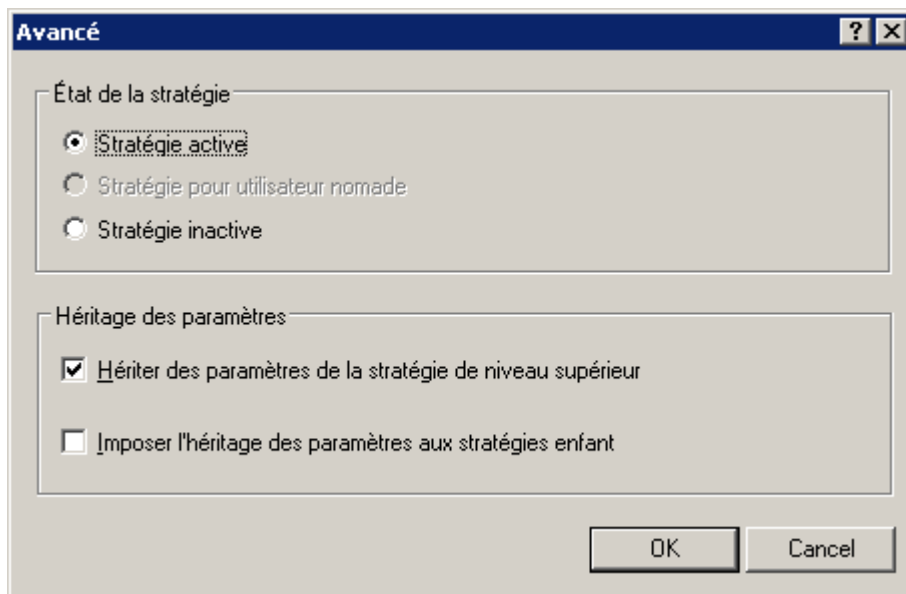


Illustration 56. Configuration des paramètres complémentaires de la stratégie

L'onglet **Événement** (cf. ill. ci-après) affiche les informations sur les événements se fixant lors du fonctionnement de l'application. Avec cela, les types des événements sont classés selon les niveaux d'importance.

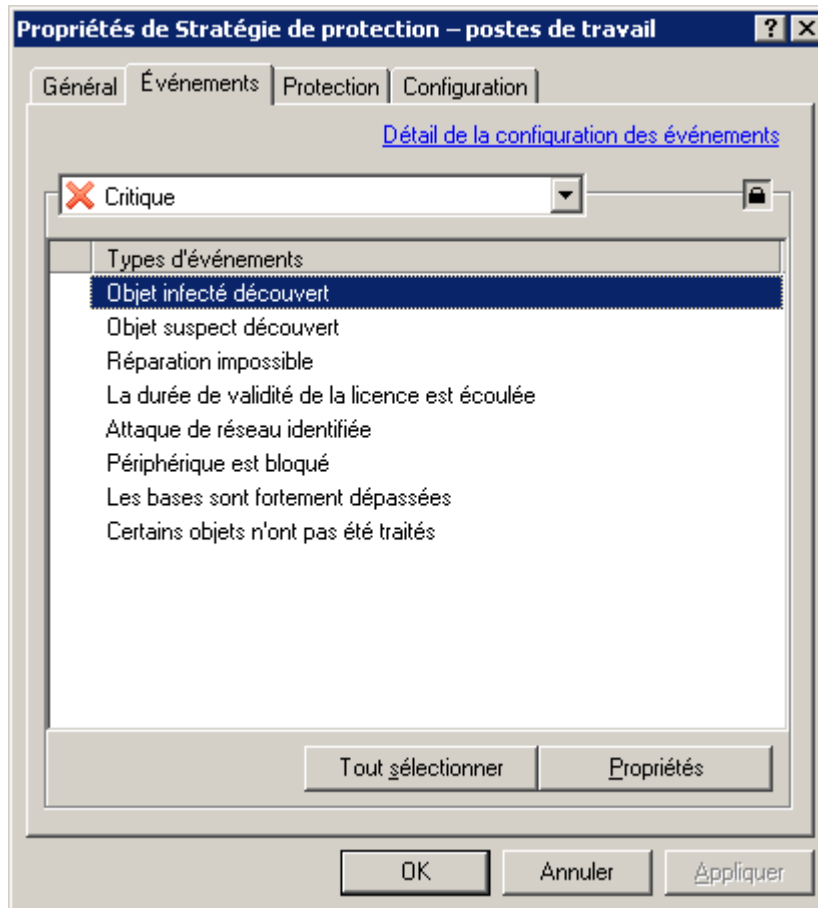


Illustration 57. Modification d'une stratégie. Onglet **Événements**

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

Les paramètres de l'onglet **Événements** dans les propriétés d'une stratégie doivent être configurés de la même manière que les paramètres de l'onglet **Événements** dans les propriétés du Serveur d'administration (cf. section "Paramètres généraux du Serveur d'administration" à la page [30](#)).

ACTIVATION D'UNE STRATEGIE

➤ Pour définir une stratégie active pour l'application, procédez comme suit :

1. Sélectionnez la stratégie requise dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés** ou cliquez sur le lien **Editer la stratégie**, situé dans le groupe **Actions** dans le panneau des tâches.
3. Dans la fenêtre de configuration de la stratégie de l'application sélectionnez **Propriétés de <Nom de stratégie>** et ouvrez l'onglet **Général** (cf. ill. ci-après).
4. A l'aide du lien **Avancé**, ouvrez la fenêtre de configuration complémentaire. Dans la section **Etat de la stratégie**, sélectionnez la valeur **Stratégie active**.

Pour désactiver la stratégie, sélectionnez l'option **Stratégie inactive**.

Pour changer rapidement l'état de la stratégie, cliquez sur les liens **Stratégie active** et **Stratégie inactive** dans le panneau des tâches de la stratégie sélectionnée.

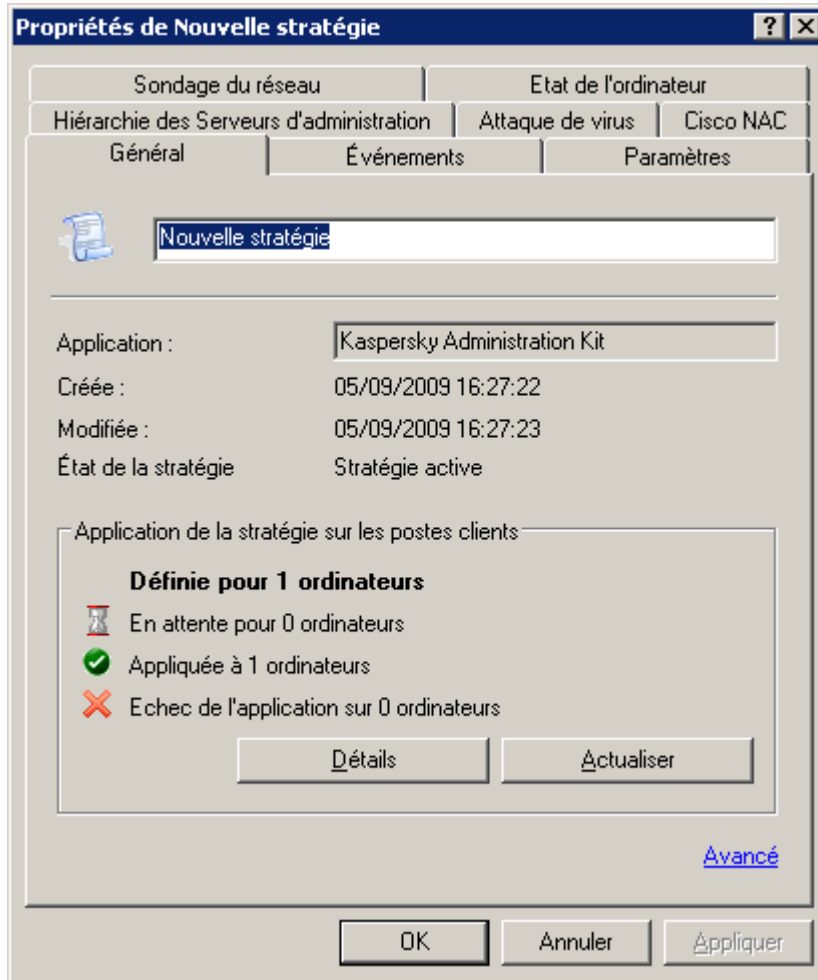


Illustration 58. Fenêtre des propriétés de la stratégie

ACTIVATION D'UNE STRATEGIE LORS D'UN EVENEMENT

- Pour activer une stratégie automatiquement lors de l'événement "Attaque de virus",

dans les propriétés du Serveur d'administration, dans la configuration des paramètres sous l'onglet **Attaques de virus**, la stratégie doit être reprise dans la liste correspondante (cf. section "Changement de stratégie pour l'application lors de l'enregistrement de l'événement Attaque de virus" à la page [321](#)).

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

STRATEGIE POUR UTILISATEUR NOMADE

Ce type de stratégie est accessible pour Kaspersky Anti-Virus for Windows Workstations versions 6.0 MP4.

- Pour configurer l'application d'une stratégie lorsque l'ordinateur est déconnecté du réseau de l'entreprise, procédez comme suit :
 1. Sélectionnez la stratégie requise dans l'arborescence de la console, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.
 2. Dans la fenêtre de configuration de la stratégie de l'application sélectionnez **Propriétés de <Nom de stratégie>** et sélectionnez l'onglet **Général** (cf. ill. ci-après).

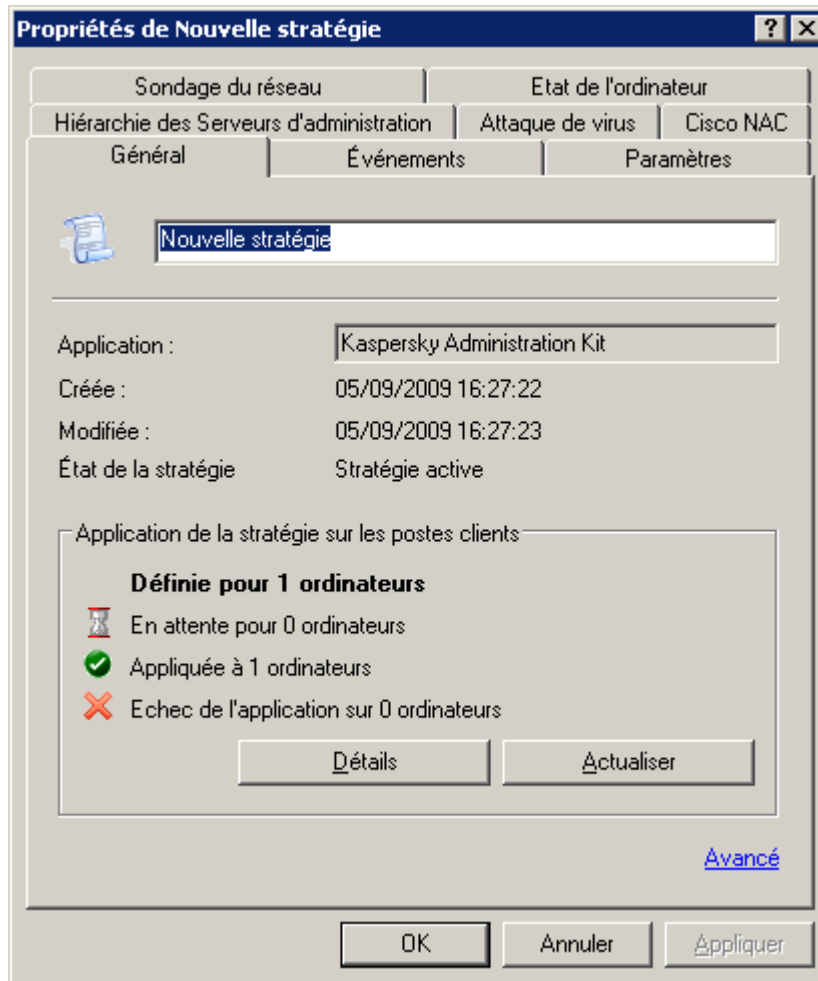


Illustration 59. Fenêtre des propriétés de la stratégie

3. A l'aide du lien **Avancé** ouvrez la fenêtre de configuration complémentaire (cf. ill. ci-après).

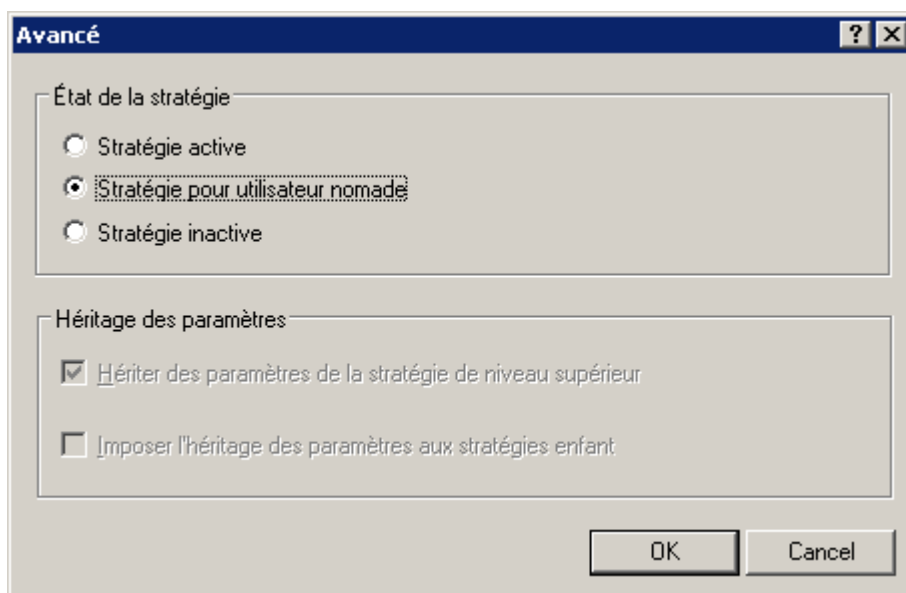


Illustration 60. Fenêtre de configuration des paramètres complémentaires de la stratégie

4. Dans le groupe **Etat de la stratégie**, sélectionnez la valeur **Stratégie pour utilisateur nomade**.

SUPPRESSION D'UNE STRATEGIE

- Pour supprimer une stratégie, procédez comme suit :

Sélectionnez la stratégie correspondante dans le dossier **Stratégies** de l'arborescence de la console et cliquez sur l'élément Supprimer du menu contextuel ou sur le lien Supprimer la stratégie situé dans le panneau des tâches.

COPIE D'UNE STRATEGIE

- Pour copier une stratégie, procédez comme suit :

1. Sélectionnez la stratégie correspondante dans le dossier **Stratégies**, dans le panneau des résultats et utilisez la commande **Copier** du menu contextuel.
2. Passez au dossier **Stratégies** du groupe requis (ou restez dans le même dossier) et utilisez la commande **Insérer** du menu contextuel.

Une stratégie active devient inactive lors de la copie. Le cas échéant, vous pouvez en faire une stratégie active (cf. section "Activation d'une stratégie" à la page [84](#)).

La stratégie est copiée avec tous les paramètres et elle est diffusée sur tous les ordinateurs du groupe où elle a été déplacée. Si vous copiez la stratégie dans le même dossier, le suffixe **_1** est ajouté automatiquement à son nom.

CONFIGURATION DES PARAMETRES DE STRATEGIE DE L'AGENT D'ADMINISTRATION

Lors de la création d'une stratégie pour l'Agent d'administration, vous pouvez définir dans la fenêtre **Paramètres** (cf. ill. ci-après) les paramètres suivants :

- Dans le groupe **Taille de la file d'attente d'événements** dans le champ **Taille maximum de la file d'attente d'événements (Mo)** définissez l'espace maximum sur le disque, que la file d'attente d'événements peut occuper.
- Dans le groupe **Mot de passe de désinstallation de l'application** cliquez sur le bouton **Modifier** et saisissez le mot de passe. Il devra être fourni lors de la désinstallation à distance de l'Agent d'administration.

Illustration 61. Création d'une stratégie pour l'Agent d'administration. Fenêtre **Paramètres**

Dans la fenêtre **Stockages** indiquez les paramètres du système de collecte d'informations relatives aux applications installées sur les ordinateurs du groupe. Pour que les informations relatives aux applications apparaissent dans le registre des applications (cf. section "Registre des applications" à la page 283), cochez la case **Informations relatives aux applications installées**. Pour que les informations relatives aux objets placés dans la sauvegarde par les applications de la version 6.0 MP3 apparaissent dans le dossier **Stockages** dans les sous-dossiers correspondants, cochez les cases **Objets de la quarantaine** et **Objets du dossier de sauvegarde**.

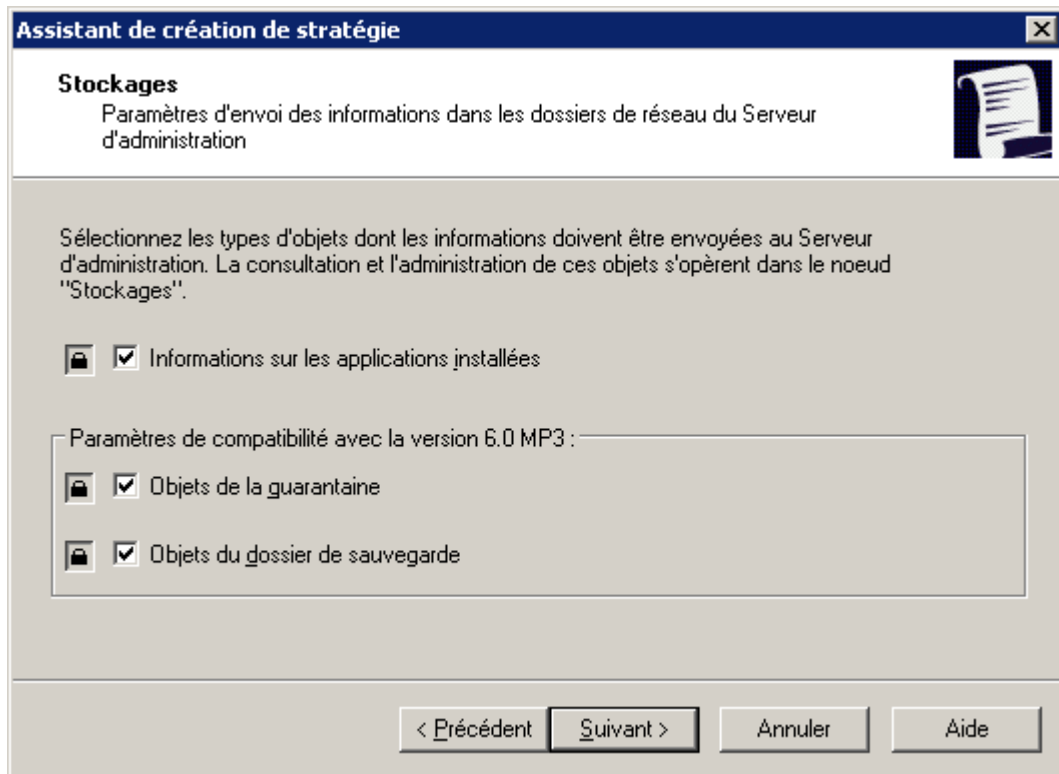


Illustration 62. Création d'une stratégie pour l'Agent d'administration. Fenêtre **Stockages**

Dans la fenêtre **Réseau** (cf. ill. ci-après) vous pouvez définir les paramètres de connexion au Serveur d'administration.

Dans le champ **Connexion au Serveur d'administration** :

- Définissez l'intervalle (en minutes) de synchronisation des données de l'hôte et du Serveur d'administration dans le champ **Période de synchronisation (min.)**.
- Cochez la case **Utiliser la connexion SSL** si vous souhaitez que la connexion soit réalisée via un port sécurisé (à l'aide du protocole SSL).
- Cochez la case **Compression du trafic réseau** afin d'accélérer la vitesse de transfert des données de l'Agent d'administration grâce à la réduction du volume des informations et à la diminution de la charge sur le Serveur d'administration.

L'activation de ce paramètre peut entraîner une augmentation de la charge du processeur central de l'hôte.

Dans la section **Port de l'Agent d'administration**, autorisez la connexion de l'hôte au Serveur d'administration via le port UDP et définissez le numéro du port. Afin d'ouvrir une connexion via le port UDP, cochez la case **Utiliser le port UDP** et saisissez le numéro du port dans le champ **Numéro de port UDP**. Par défaut, il s'agit du port 15000. Le cas échéant, vous pouvez le modifier. Seules des valeurs décimales sont admises.

Assistant de création de stratégie

Réseau
Configuration des paramètres de connexion de l'Agent d'administration au Serveur d'administration.

Connexion au Serveur d'administration

Période de synchronisation (min) : 15

Utiliser la connexion SSL

Compression du trafic réseau

Port de l'agent d'administration

Utiliser le port UDP

Numéro de port UDP : 15000

< Précédent Suivant > Annuler Aide

Illustration 63. Création d'une stratégie pour l'Agent d'administration. Fenêtre **Réseau**

Lors de la modification d'une stratégie pour l'Agent d'administration, vous pouvez modifier les paramètres sur les onglets **Général**, **Événements**, **Paramètres**, **Stockages** et **Réseau**.

En plus des paramètres définis dans l'Assistant de création d'une stratégie, l'onglet **Réseau** (cf. ill. ci-après), il est aussi possible de cocher la case **Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**. Cela permet d'ajouter le port UDP, indispensable au bon fonctionnement de l'Agent d'administration, dans la liste des exceptions du pare-feu Microsoft Windows.

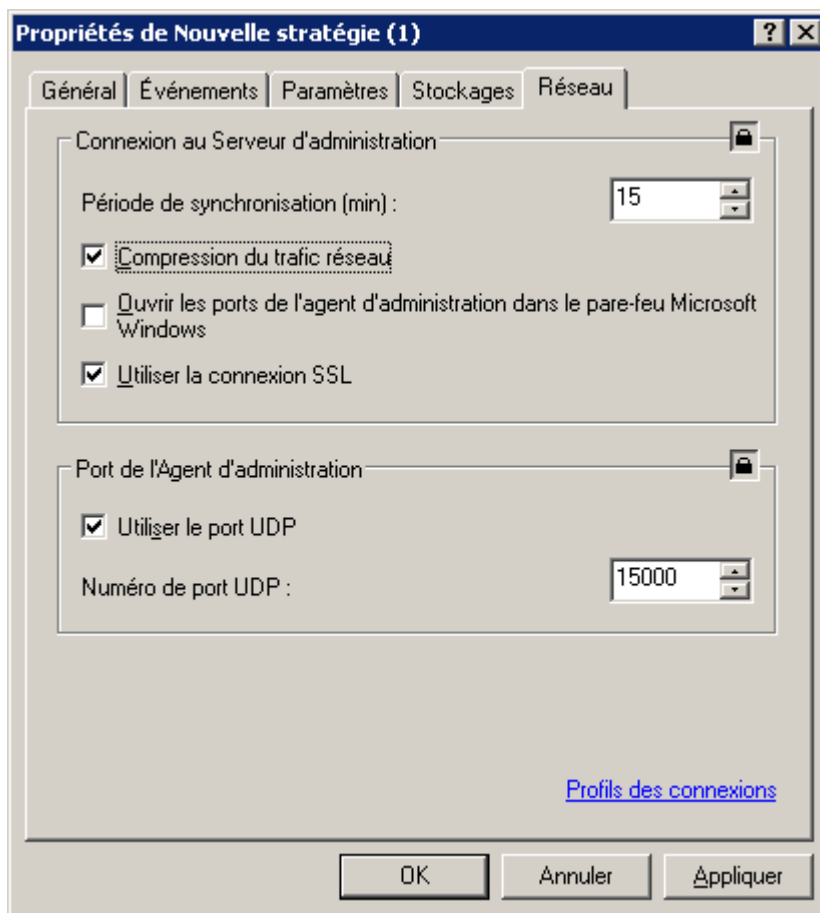


Illustration 64. Modification d'une stratégie pour l'Agent d'administration. Onglet **Réseau**

CONFIGURATION DES PARAMETRES DE LA STRATEGIE DU SERVEUR D'ADMINISTRATION

Lors de la création d'une stratégie pour le Serveur d'administration, sélectionnez Kaspersky Administration Kit dans la fenêtre de sélection des applications. Ensuite, dans la fenêtre **Paramètres** (cf. ill. ci-après) vous pouvez configurer les paramètres généraux du Serveur d'administration.

Dans le champ **Paramètres de connexion au Serveur d'administration** :

- numéro de port utilisé pour se connecter au Serveur d'administration. Par défaut, il s'agit du port 14000. Vous pouvez le modifier s'il est occupé ;
- numéro du port utilisé pour établir une connexion sécurisée avec le Serveur d'administration via le protocole SSL. Par défaut, il s'agit du port 13000.

Dans le champ **Nombre maximum d'événements stockés dans la base de données**, indiquez la valeur souhaitée. Par défaut, ce nombre est limité à 400 000.

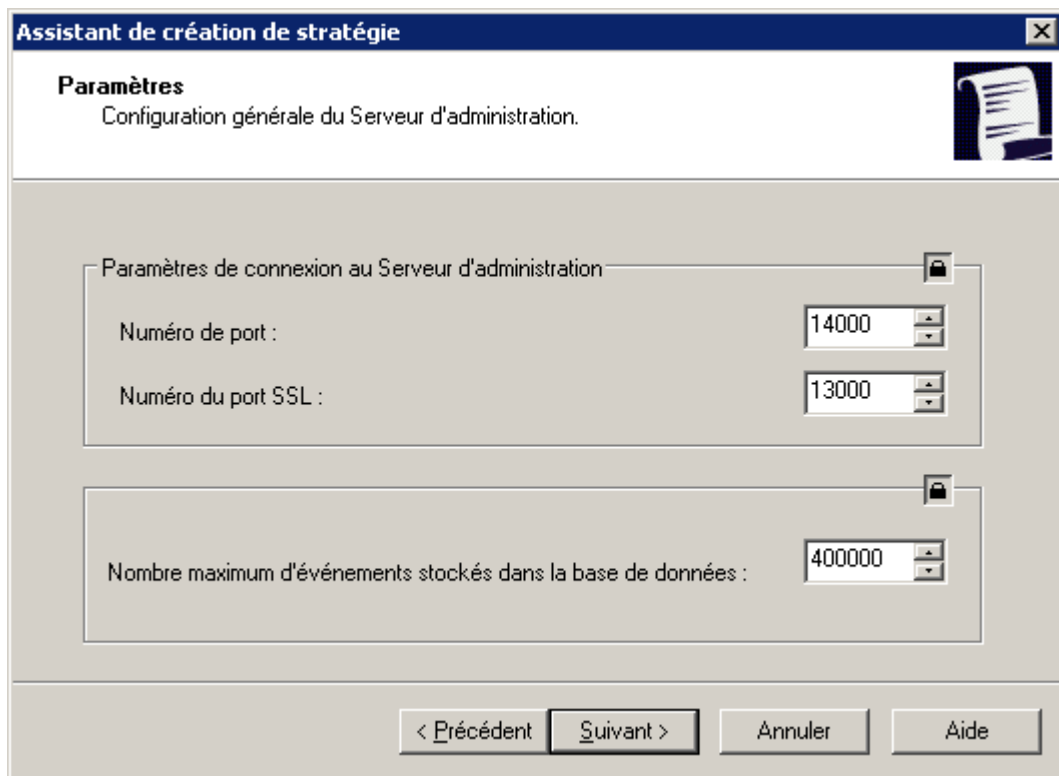


Illustration 65. Création d'une stratégie pour le Serveur d'administration. Fenêtre **Paramètres**

Dans la fenêtre **Sondage du réseau** (cf. ill. ci-après) vous pouvez définir les paramètres d'actualisation des informations relatives à la structure du réseau :

- Pour activer le sondage automatique, cochez la case **Autoriser le sondage** dans le groupe **Réseau Windows**.
- Pour activer le sondage automatique des plages IP, dans le groupe **Plages IP** cochez la case **Autoriser le sondage**. Le Serveur d'administration sondera des plages selon la fréquence définie dans le champ **Période de sondage (min)**. Celle-ci est établie par défaut à 420 minutes.

- Pour activer le sondage automatique du réseau conformément à la structure Active Directory, cochez la case **Autoriser le sondage** dans le groupe **Active Directory**.

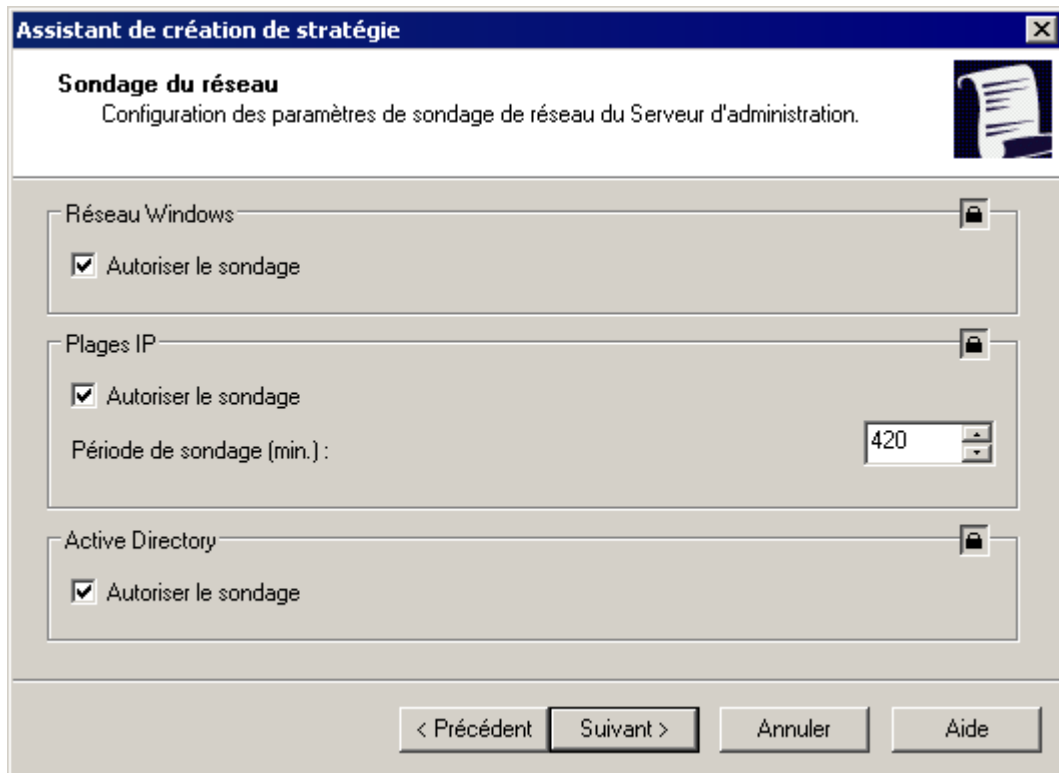


Illustration 66. Création d'une stratégie pour le Serveur d'administration. Fenêtre **Sondage du réseau**

Il est possible de modifier d'autres paramètres que ceux définis à l'étape de création de la stratégie.

Vous pouvez préciser dans le champ **Délai de visibilité de l'ordinateur (min.)** de l'onglet **Paramètres** (cf. ill. ci-après) la durée pendant laquelle l'hôte est considéré comme visible dans le réseau après une perte de la connexion au serveur d'administration. Par défaut, l'intervalle est fixé à 60 minutes. A la fin de cette période, le Serveur d'administration considérera que l'hôte est inactif.

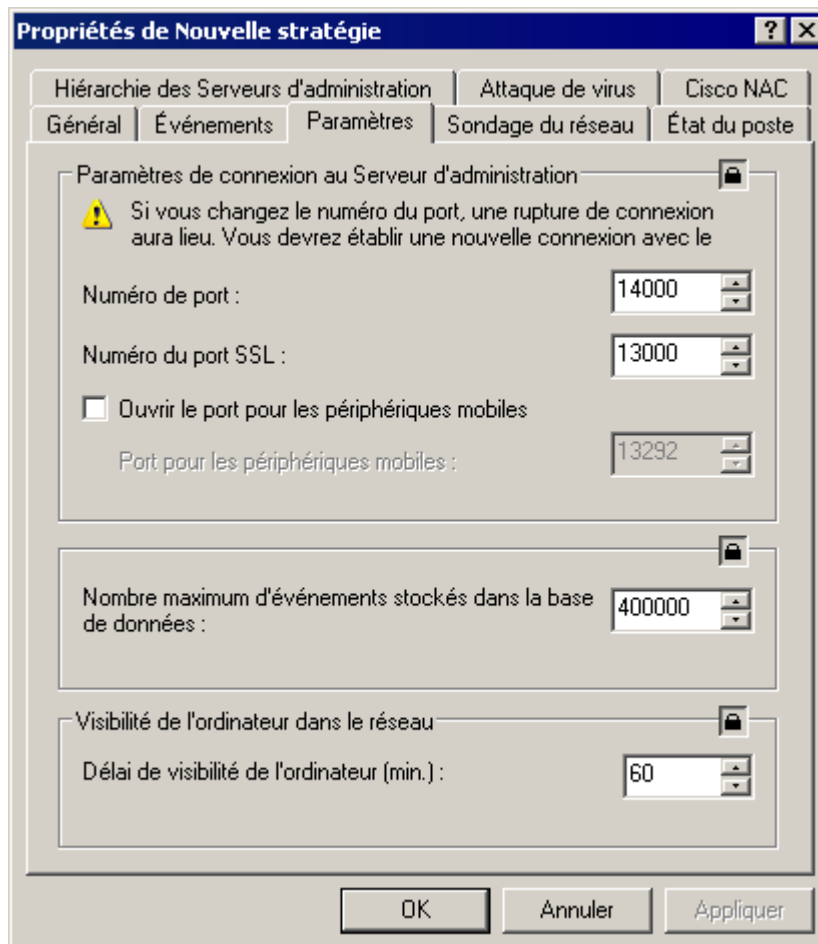


Illustration 67. Modification d'une stratégie pour le Serveur d'administration. Onglet **Paramètres**

Sur l'onglet **Sondage du réseau** (cf. ill. ci-après), vous pouvez définir :

- La période de sondage du réseau Windows :
- **Durée d'analyse complète (min.)**. Les informations relatives aux hôtes seront complètement actualisées selon cet intervalle. Celle-ci est établie par défaut à 60 minutes.
- **Durée d'analyse rapide (min.)**. La liste des hôtes connectés au réseau sera actualisée selon l'intervalle défini. Celle-ci est établie par défaut à 15 minutes.
- période de sondage des plages IP. Pour ce faire, définissez dans le champ **Période de sondage (min.)** du groupe adéquat la valeur souhaitée. Celle-ci est établie par défaut à 420 minutes.

- La période de sondage conformément à la structure Active Directory. Pour ce faire, définissez dans le champ **Période de sondage (min.)** du groupe adéquat la valeur souhaitée. Celle-ci est établie par défaut à 60 minutes.

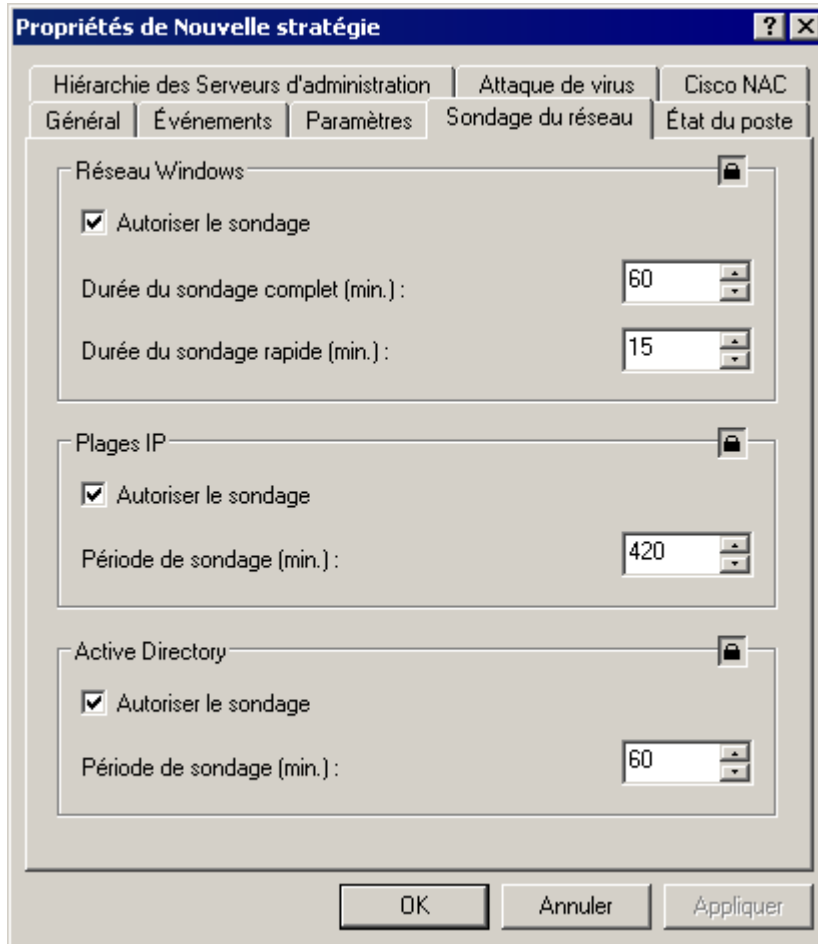


Illustration 68. Modification d'une stratégie pour le Serveur d'administration. Onglet **Sondage du réseau**

Sur l'onglet **Attaque de virus** vous pouvez configurer la génération de l'événement **Attaque de virus** pour tous les types d'application antivirus. Cet onglet est identique à l'onglet des propriétés du Serveur d'administration.

Sur l'onglet **Cisco NAC** vous pouvez établir les correspondances entre les conditions de protection antivirus et les états Cisco NAC. Cet onglet est identique à l'onglet des propriétés du Serveur d'administration.

Sur l'onglet **Hiérarchie des Serveurs d'administration** (cf. ill. ci-après), vous pouvez autoriser ou interdire la modification des paramètres de la hiérarchie des Serveurs. Si la case **Autoriser la modification de la hiérarchie des Serveurs d'administration secondaires** est décochée, les administrateurs des Serveurs d'administration secondaires ne peuvent pas modifier les hiérarchies attribuées par le Serveur principal.

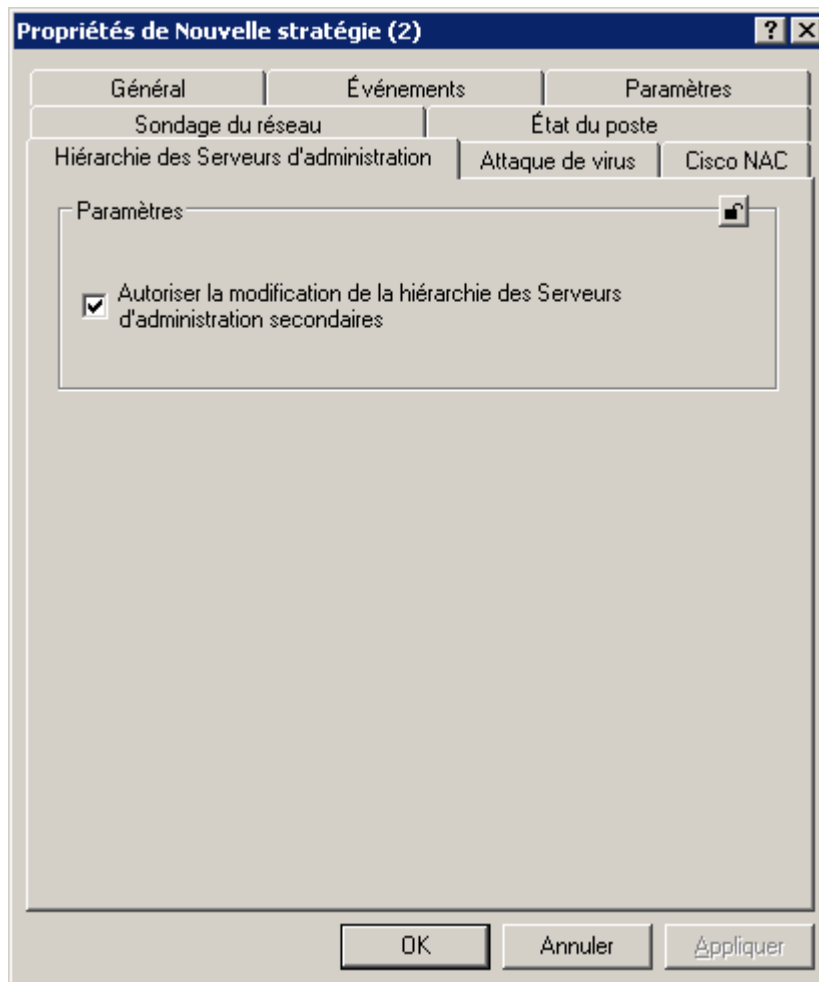


Illustration 69. Modification d'une stratégie pour le Serveur d'administration. Onglet **Hiérarchie des Serveurs d'administration**

EXPORTATION D'UNE STRATEGIE

➔ Pour exporter une stratégie, procédez comme suit :

1. Dans l'arborescence de console, choisissez le groupe requis.
2. Sélectionnez le sous-dossier **Stratégies**.

Dans l'arborescence de la console, vous verrez la liste de toutes les stratégies existantes pour ce groupe.

3. Sélectionnez la stratégie requise.
4. Ouvrez le menu contextuel et sélectionnez la commande **Exporter** ou cliquez sur le lien **Exporter la stratégie dans le fichier** situé dans le panneau des tâches.
5. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier et le chemin d'accès pour l'enregistrement. Cliquez sur **Enregistrer**.

IMPORTATION D'UNE STRATEGIE

➤ *Pour importer une stratégie, procédez comme suit :*

1. Dans l'arborescence de console, choisissez le groupe requis.
2. Sélectionnez le dossier **Stratégies**.
3. Ouvrez le menu contextuel et sélectionnez la commande **Toutes les tâches** → **Importer** ou cliquez sur le lien **Importer la stratégie du fichier** situé dans le panneau des tâches du dossier **Stratégies**.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la stratégie. Cliquez sur **Ouvrir**.

La stratégie ajoutée apparaît dans l'arborescence de la console.

CONVERSION DES STRATEGIES

A l'aide de Kaspersky Administration Kit vous pouvez déplacer les stratégies de version précédente des applications de Kaspersky Lab vers la version actuelle. Ceci peut être utile, par exemple, lors de l'installation du Serveur d'administration 8.0 sur l'ordinateur avec le Serveur d'administration 6.0 installé. Cette procédure s'exécute à l'aide de l'Assistant de conversion des stratégies et des tâches.

➤ *Afin de convertir les stratégies et/ou les tâches de l'application, procédez comme suit :*

1. Dans l'arborescence de la console sélectionnez le Serveur d'administration nécessaire, pour lequel vous voulez convertir les stratégies et/ou les tâches.
2. Dans le menu contextuel sélectionnez le point **Toutes les tâches** → **Assistant de conversion des stratégies et des tâches**. Finalement l'Assistant se lancera. Suivez les instructions de l'Assistant.

3. Dans le champ **Nom de l'application** (cf. ill. ci-après) spécifiez la version de l'application. A la fin de l'Assistant les stratégies et les tâches seront converties pour le fonctionnement avec cette version de l'application.

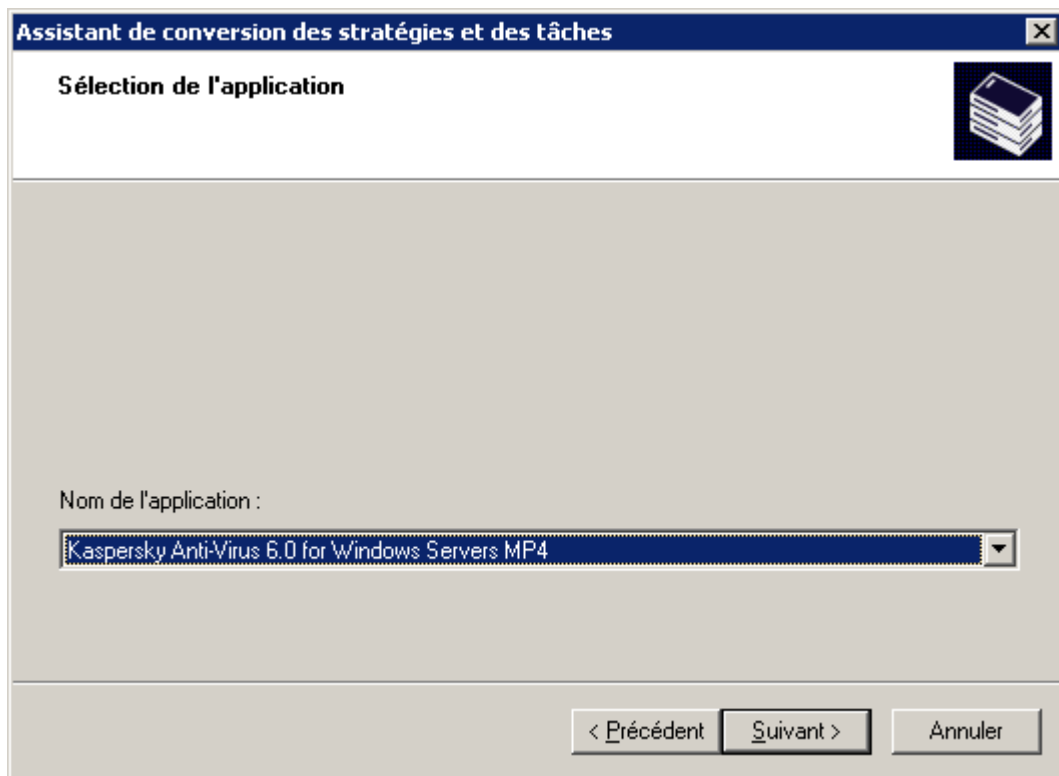


Illustration 70. Sélection de l'application à convertir

4. Dans la fenêtre suivante de l'Assistant (cf. ill. ci-après) cochez les cases en regard des noms des stratégies pour lesquelles la conversion est requise. Après avoir cliqué sur le bouton **Suivant** la conversion des stratégies aura lieu.

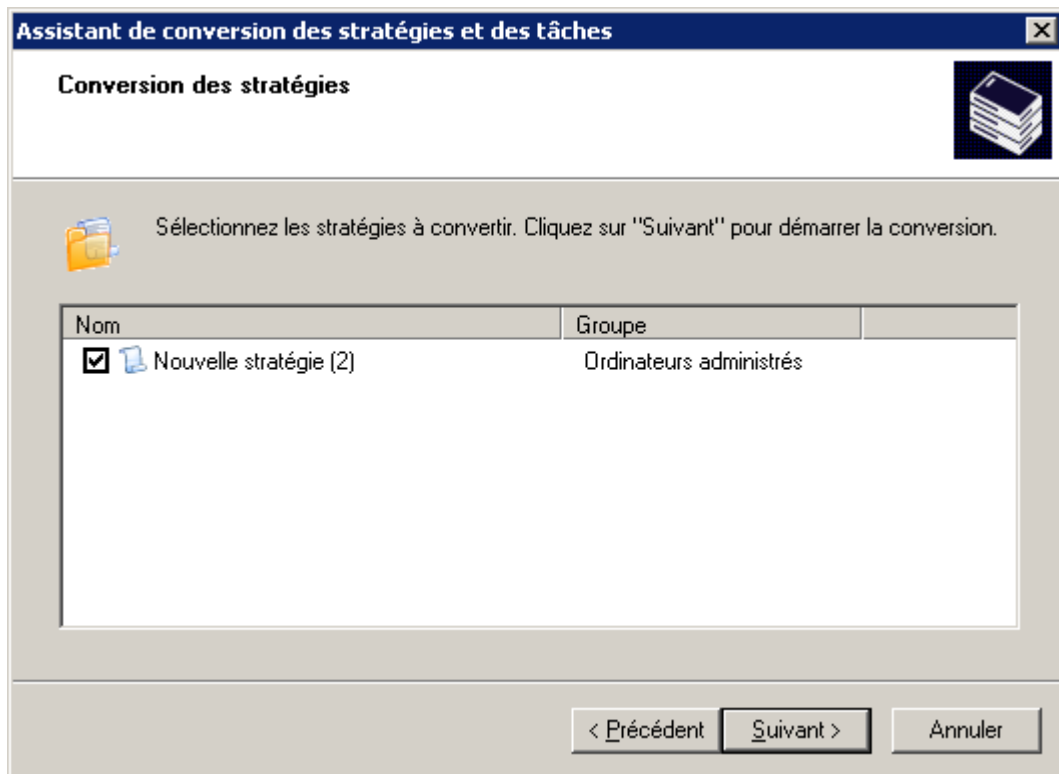


Illustration 71. Sélection des stratégies à convertir

5. Dans la fenêtre suivante de l'Assistant (cf. ill. ci-après) cochez les cases en regard des noms des tâches pour lesquelles la conversion est requise. Après avoir cliqué sur le bouton **Suivant** la conversion des tâches aura lieu.

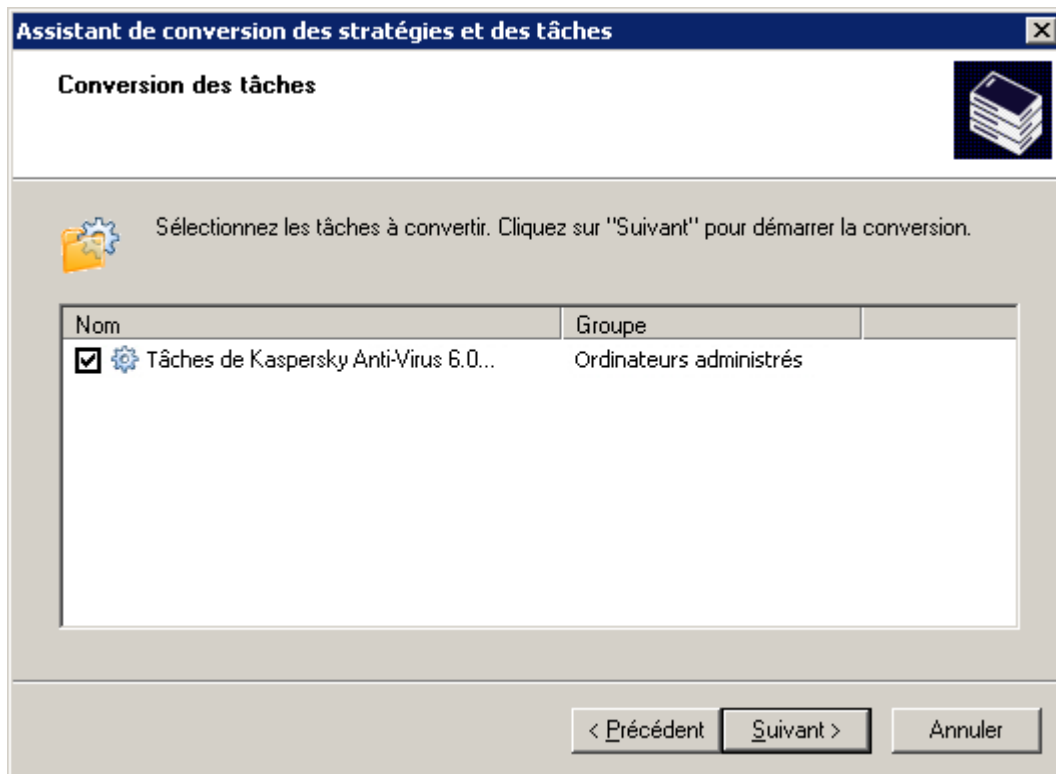


Illustration 72. Sélection des tâches à convertir

Finalement l'Assistant formera des nouvelles stratégies et tâches qui utilisent les paramètres des stratégies et des tâches de version précédente.

GERER LES TACHES

Kaspersky Administration Kit gère le fonctionnement des applications installées sur les postes clients par la création et l'exécution des tâches. Les tâches prennent en charge les fonctions principales : installation d'applications, installation de licences, analyse des fichiers, mise à jour des bases et des modules de l'application, etc. Les tâches sont scindées en types suivants :

- *tâches de groupe* (cf. section "Création d'une tâche de groupe" à la page [101](#)) : exécutées sur tous les postes clients du groupe d'administration ;
- *tâches du Serveur d'administration* (cf. section "Création d'une tâche pour le Serveur d'administration" à la page [113](#)) : exécutées sur le Serveur d'administration ;
- *tâches pour les sélections d'ordinateurs* (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)) : exécutées sur un nombre restreint d'ordinateurs qui ne constituent pas un groupe distinct ;
- *tâches locales* (cf. section "Création d'une tâche locale" à la page [115](#)) : créées et exécutées sur un poste client particulier.

Les tâches créées apparaissent dans l'arborescence de la console dans le dossier correspondant. Une icône figure devant le nom de chaque stratégie et caractérise son état (cf. section "Etats des ordinateurs, des tâches et des stratégies" à la page [333](#)).

TACHES DE KASPERSKY ADMINISTRATION KIT

Le Serveur d'administration exécute les tâches suivantes :

- Diffusion automatique des rapports (cf. section "Tâche de diffusion des rapports" à la page [200](#)).
- Téléchargement des mises à jour dans le référentiel (cf. section "Définition du contenu des mises à jour" à la page [254](#)).
- Sauvegarde des données du Serveur d'administration (cf. section "Sauvegarde des données" à la page [311](#)).

TACHES POUR LES SELECTIONS D'ORDINATEURS

Dans Kaspersky Administration Kit vous pouvez former les tâches pour les sélections d'ordinateurs. Par ailleurs, les ordinateurs dans la sélection peuvent faire partie des groupes d'administration différentes. Kaspersky Administration Kit permet d'exécuter les tâches principales suivantes :

- L'installation à distance de l'application (cf. Manuel d'implantation).
- Message pour utilisateur (cf. section "Envoi du message à l'utilisateur du poste client" à la page [164](#)).
- Changement du Serveur d'administration (cf. section "Tâche de modification du Serveur d'administration" à la page [151](#)).
- Administration du poste client (cf. section "Tâche d'administration du poste client" à la page [154](#)).
- Vérification des mises à jour (cf. section "Analyse des mises à jour récupérées" à la page [258](#)).
- Tâche de retraduction des paquets (cf. Manuel d'implantation).
- L'installation de l'application à distance sur les Serveurs d'administration secondaires (cf. Manuel d'implantation).
- La désinstallation à distance de l'application (cf. Manuel d'implantation).

CREATION D'UNE TACHE DE GROUPE

➡ *Pour créer une tâche de groupe, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe pour lequel vous souhaitez créer une tâche.
2. Sélectionnez le dossier **Tâches de groupe** appartenant au groupe.
3. Ouvrez le menu contextuel et choisissez l'option **Générer** → **Tâche** ou cliquez sur le lien **Créer une tâche**, situé dans le panneau des tâches. Ceci permet de lancer l'assistant de création de tâche. Suivez les instructions de l'Assistant.
4. Indiquez le nom de la tâche. Si une tâche de ce nom existe déjà dans le groupe, **un _1** sera automatiquement ajouté au nouveau nom.

5. Sélectionnez ensuite l'application pour laquelle vous voulez créer une tâche et définissez le type de tâche (cf. ill. ci-après).

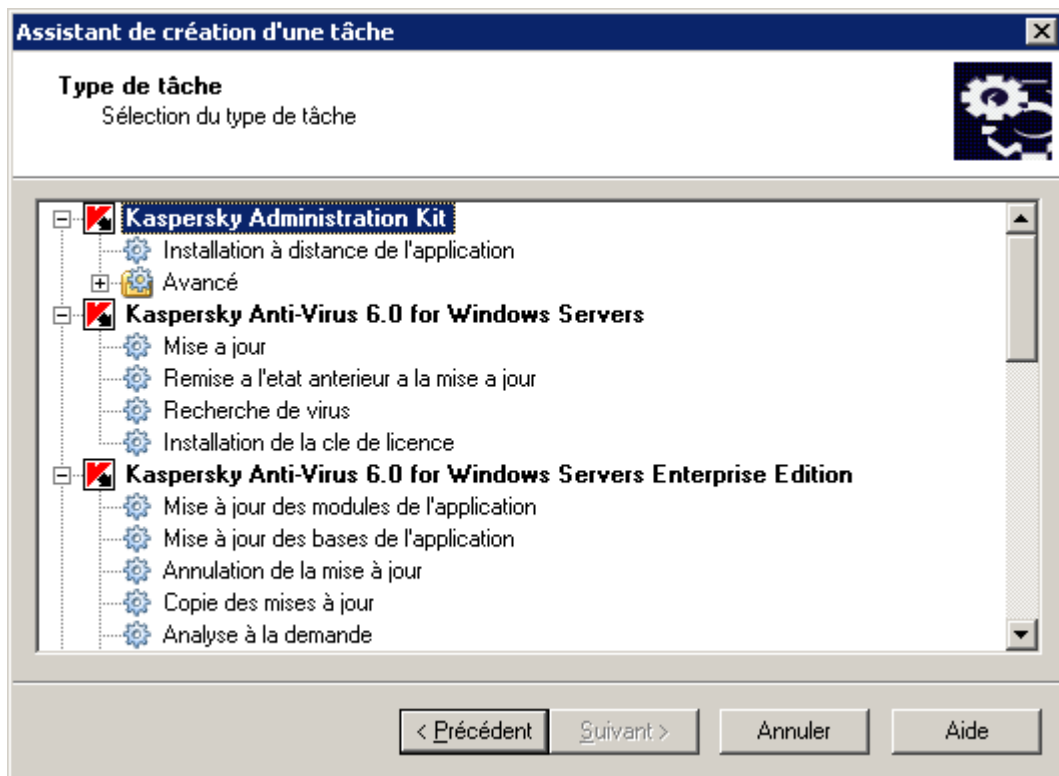


Illustration 73. Création d'une tâche. Choix de l'application et du type de tâche

Pour sélectionner l'application pour laquelle la tâche est créée, sélectionnez l'entrée dans l'arborescence proposée. En guise d'entrées de l'arborescence, vous verrez toutes les applications Kaspersky Lab qui possèdent un plug-in de console installé sur le poste administrateur. Pour déterminer le type de tâche, sélectionnez une des objets imbriqués pour l'application sélectionnée.

6. Ensuite, vous serez invité à configurer les paramètres de la tâche selon l'application choisie (cf. ill. ci-après). Quelques paramètres sont définis par défaut. Pour plus de détails au sujet de la configuration de tâches, reportez-vous à la documentation de l'application en particulier.

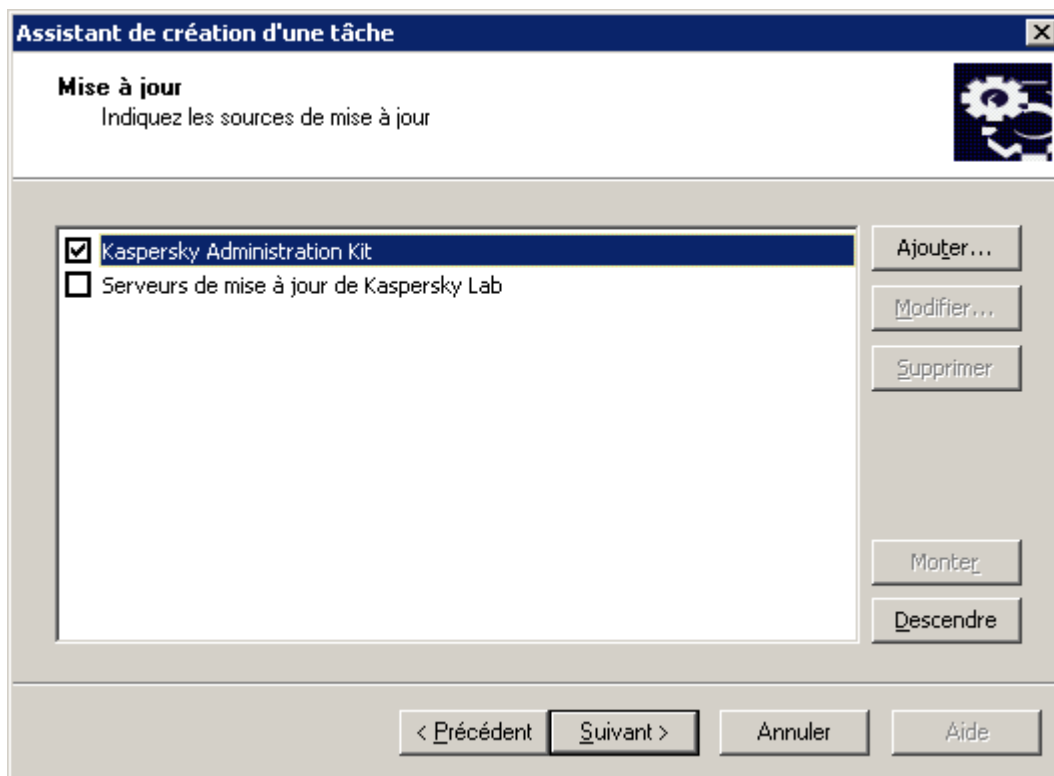


Illustration 74. Configuration d'une tâche

7. Définissez la fréquence et l'heure de démarrage de la tâche. Dans la liste déroulante **Planification pour**, sélectionnez le mode de lancement qui vous convient et configurez la programmation dans le groupe des paramètres qui correspondent au régime sélectionné :
- **Toutes les N heures** ;
 - **Toutes les N minutes** ;
 - **Chaque jour** ;
 - **Chaque semaine** ;
 - **Chaque mois** ;
 - **Une fois** ;
 - **Mode manuel** : lancement manuel depuis la fenêtre principale de Kaspersky Administration Kit à l'aide des commandes **Démarrer** du menu contextuel ou du lien **Lancer la tâche** situé dans le panneau des tâches ;
 - **Après la mise à jour de l'application** : après chaque mise à jour des bases de l'application ;
 - **Au lancement de l'application** ;
 - **Immédiatement** : démarre la tâche immédiatement après avoir terminé l'Assistant ;
 - **Lors du téléchargement des mises à jour dans le référentiel** : automatiquement après le téléchargement des mises à jour par le Serveur d'administration ;
 - **Lors de la détection d'une attaque de virus** ;

- **A la fin d'une autre tâche.**

C'est ici que figurent les modes de lancement des tâches de Kaspersky Administration Kit. Pour les tâches créées pour d'autres applications, la programmation peut varier.

Les tâches créées pour des applications administrables à l'aide de Kaspersky Administration Kit peuvent présenter des modes de démarrage supplémentaires. Pour de plus amples détails, consultez le manuel de l'application concernée.

Si vous avez sélectionné le mode d'exécution de la tâche **Toutes les N heures** (cf. ill. ci-après), définissez :

- La fréquence des démarrages de tâche dans la zone **Toutes les** et la date et heure de départ dans la zone **A partir de**.

Par exemple, si la valeur 2 est affectée à la zone **Toutes les** et la valeur du 3 août 2008 à 15:00:00 se trouve dans la zone **A partir de**, la tâche démarrera toutes les deux heures à partir de 15 heures, le 3 août 2008.

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

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

Cochez la case **Lancer les tâches non exécutées** pour que le système essaie d'exécuter une tâche lors de la prochaine ouverture de l'application sur ce poste client. Si l'option **Mode manuel, Une fois** ou **Immédiatement** a été sélectionnée, la tâche sera exécutée dès l'apparition de l'ordinateur sur le réseau.

Si cette case n'est pas cochée (par défaut), l'exécution de la tâche sur les postes clients aura lieu uniquement selon la programmation et pour les options **Mode manuel, Une fois** et **Immédiatement**, uniquement pour les postes clients visibles dans le réseau.

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

Cochez la case **Répartir le lancement aléatoire de la tâche sur l'intervalle (min.)** et indiquez l'intervalle de temps pendant lequel les postes clients appelleront le Serveur d'administration après le démarrage de la tâche, au lieu de le faire simultanément. Par défaut, cette case n'est pas cochée.

Illustration 75. Lancement d'une tâche Toutes les N heures

Si vous avez sélectionné le mode d'exécution de la tâche **Toutes les N minutes** (cf. ill. ci-après), définissez :

- La fréquence des démarrages de tâche dans la zone **Toutes les** et la date et heure de départ dans la zone **A partir de**.

Par exemple, si la valeur 10 est affectée à la zone **Toutes les** et la valeur du 3 août 2008 à 15:00:00 se trouve dans la zone **A partir de**, la tâche démarrera toutes les 10 minutes à partir de 15 heures, le 3 août 2008.

La fréquence est définie par défaut à 30 et l'heure système de l'ordinateur est utilisée automatiquement pour la date et l'heure de départ.

- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

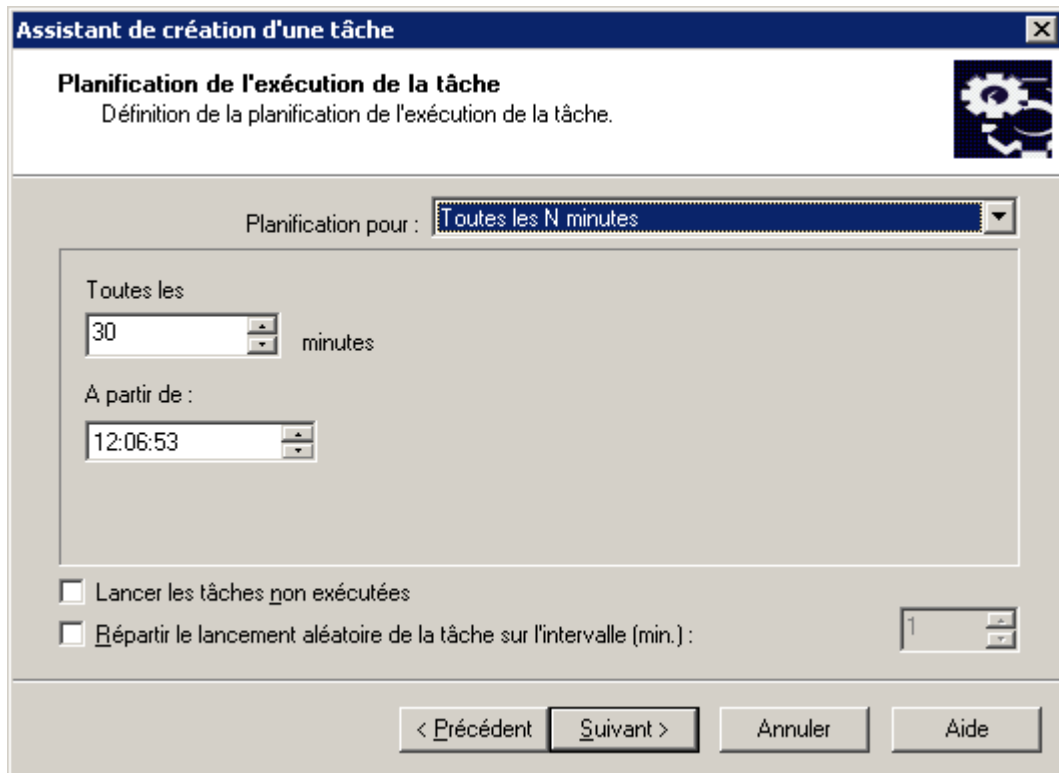


Illustration 76. Lancement d'une tâche Toutes les N minutes

Si vous avez sélectionner le mode **Chaque jour** (cf. ill. ci-après), indiquez :

- La fréquence des démarrages de la tâche dans la zone **Chaque** et **Heure d'exécution**.

Par exemple, si le champ **Chaque** affiche la valeur 2 et le champ **Heure d'exécution** indique 15h00, la tâche commencera une fois tous les deux jours à 3 heures de l'après midi.

La valeur par défaut du champ Chaque N jour est 2 et l'heure système est utilisée par défaut comme heure de départ.

- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

Assistant de création d'une tâche

Planification de l'exécution de la tâche
Définition de la planification de l'exécution de la tâche.

Planification pour : **Chaque jour**

Tous les jours

Heure d'exécution :

Lancer les tâches non exécutées

Répartir le lancement aléatoire de la tâche sur l'intervalle (min) :

< Précédent Suivant > Annuler Aide

Illustration 77. Programmation d'une tâche exécutée chaque jour

Si vous avez sélectionné le mode **Chaque semaine** (cf. ill. ci-après), indiquez :

- La fréquence des démarrages de la tâche dans la zone **Chaque** et **Heure d'exécution**. Par défaut, la tâche démarrera le dimanche à 18h00. Vous pouvez modifier l'heure de départ, si nécessaire. Vous pouvez les modifier si nécessaire.

Par exemple, si la valeur de la zone **Chaque** est dimanche et la valeur du champ **Heure d'exécution** est 15h00, la tâche commencera chaque dimanche à 15h00.

- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

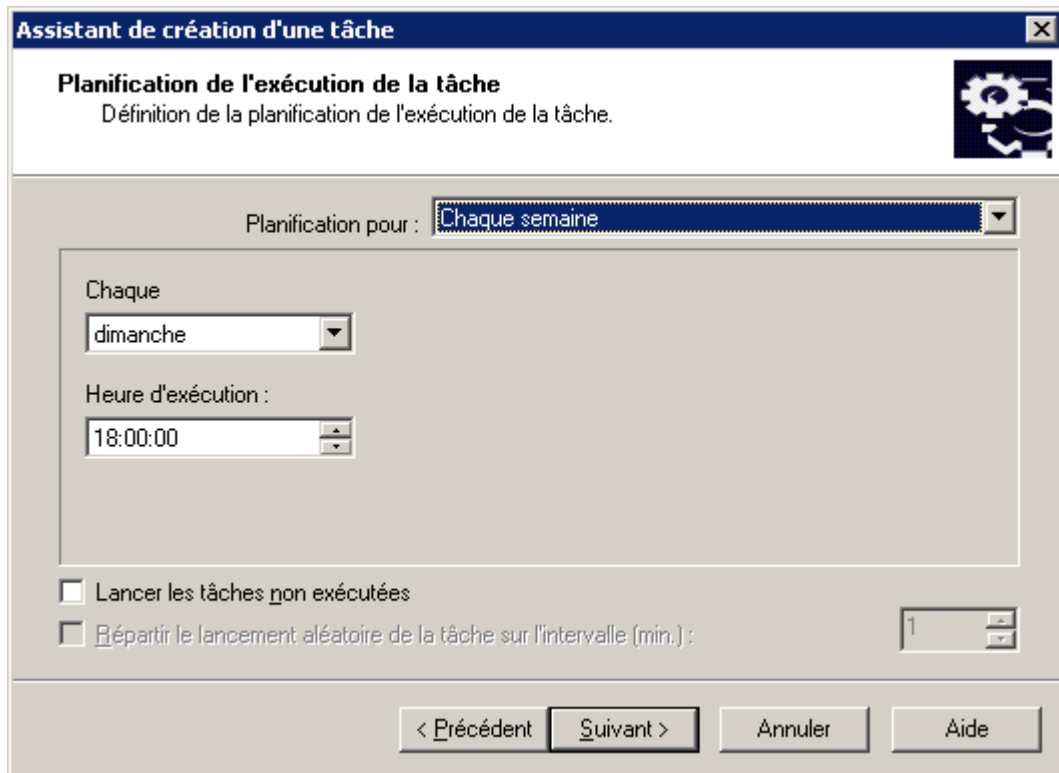


Illustration 78. Exécution chaque semaine de la tâche

Si vous avez sélectionné le mode **Chaque mois** (cf. ill. ci-après), indiquez :

- La fréquence d'exécution de la tâche en définissant le jour et l'heure d'exécution.

Par exemple, si la valeur de la zone **Chaque** contient 20 et la valeur du champ **Heure d'exécution** est 15h00, la tâche commencera le 20 de chaque mois à 15h00.

La valeur par défaut du champ **Chaque** contient 1 et dans le champ **Heure d'exécution** – l'heure système actuelle est utilisée.

- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

Illustration 79. Programmation d'une tâche mensuelle

Si vous définissez le démarrage de la tâche **Une fois** (cf. ill. ci-après), indiquez ce qui suit :

- La date de démarrage de la tâche dans la zone **Date d'exécution**, et l'heure de démarrage dans la zone **Heure d'exécution**. Les valeurs de ces champs sont définies automatiquement et correspondent à la date et à l'heure courante du système. Vous pouvez les modifier si nécessaire.
- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

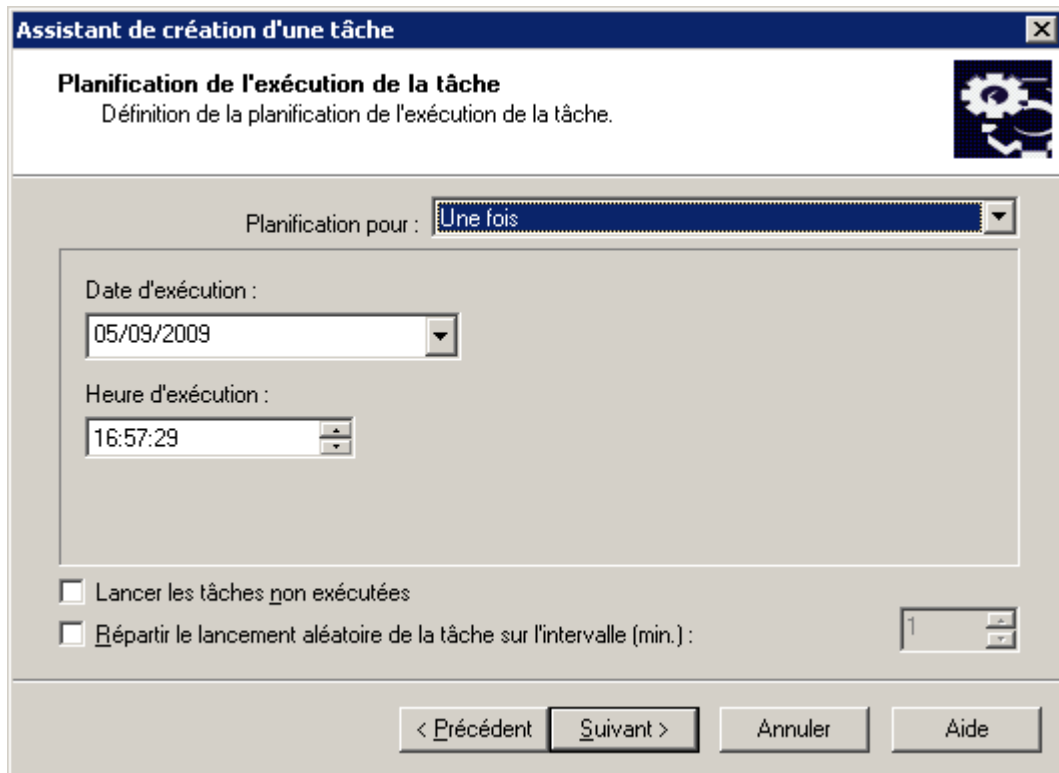


Illustration 80. Lancement ponctuel d'une tâche

Si vous définissez le démarrage de la tâche **Manuellement** (cf. ill. ci-après), au lancement de l'application ou immédiatement après la création de la tâche, définissez :

- La marche à suivre lorsqu'un client est temporairement indisponible.

- Une marge dans l'heure programmée, pendant laquelle la tâche sera exécutée sur les postes clients (voir ci-dessus).

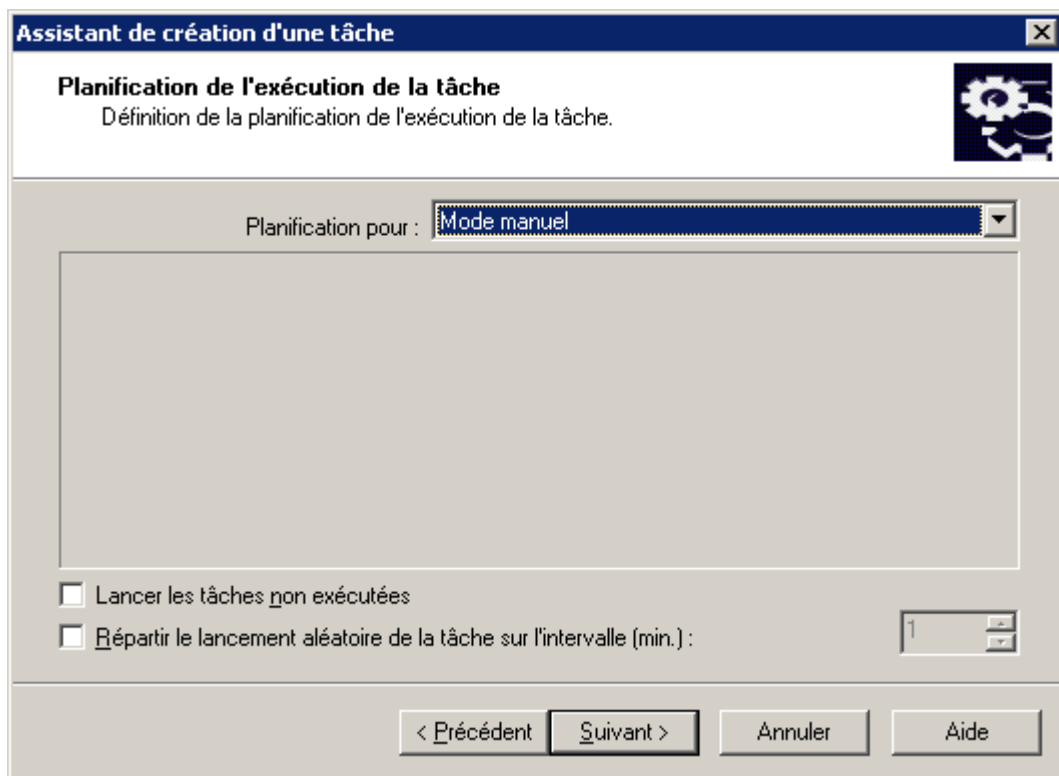


Illustration 81. Lancement manuel d'une tâche

Si vous définissez que la tâche doit être démarrée **A la fin d'une autre tâche** (cf. ill. ci-après), indiquez ce qui suit :

- La tâche après laquelle la tâche courante doit être exécutée. Pour ce faire, sélectionnez la tâche en question dans le champ **Nom de tâche** à l'aide du bouton **Parcourir**. Dans le champ **Résultat de la tâche** indiquez la manière dont la tâche sélectionnée doit se terminer : Accomplie avec succès ou Terminée avec erreur.

- La marche à suivre lorsqu'un client est temporairement indisponible.

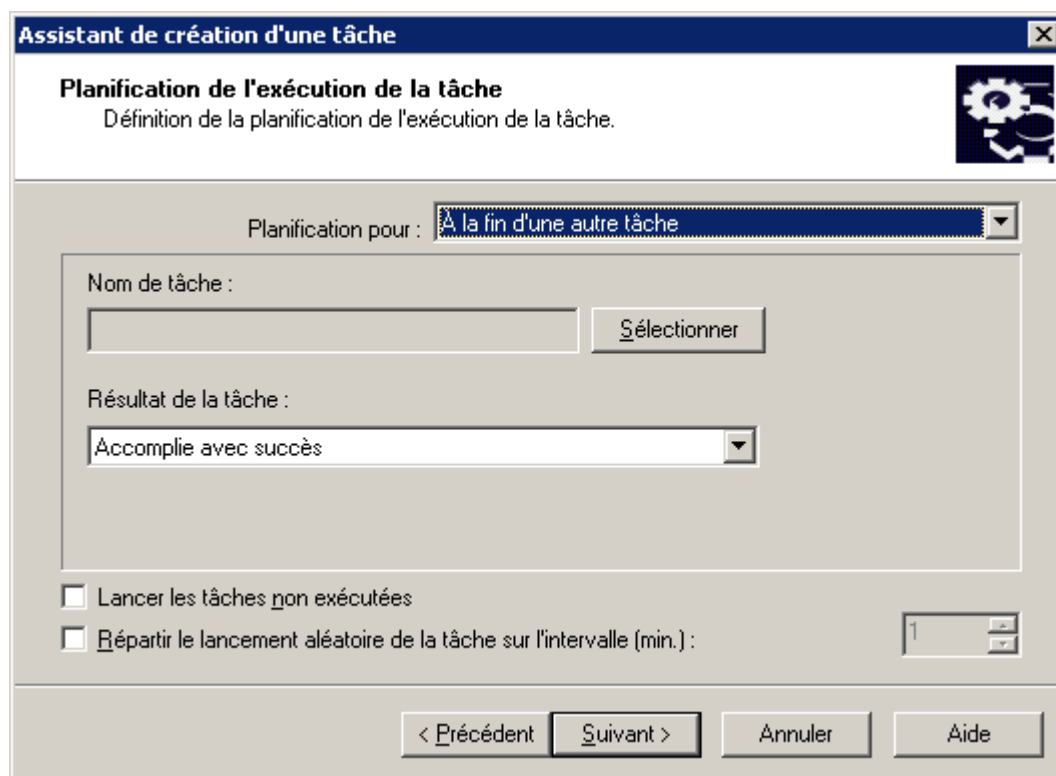


Illustration 82. Exécution à la suite d'une autre tâche

Si vous définissez que la tâche doit être démarrée **A la détection d'une attaque de virus** (cf. ill. ci-après), indiquez ce qui suit :

- Les types d'application susceptibles de démarrer la tâche lorsqu'un événement **Attaque de virus** se produit. Pour ce faire, cochez la case en regard des types d'application en question.

- La marche à suivre lorsqu'un client est temporairement indisponible.

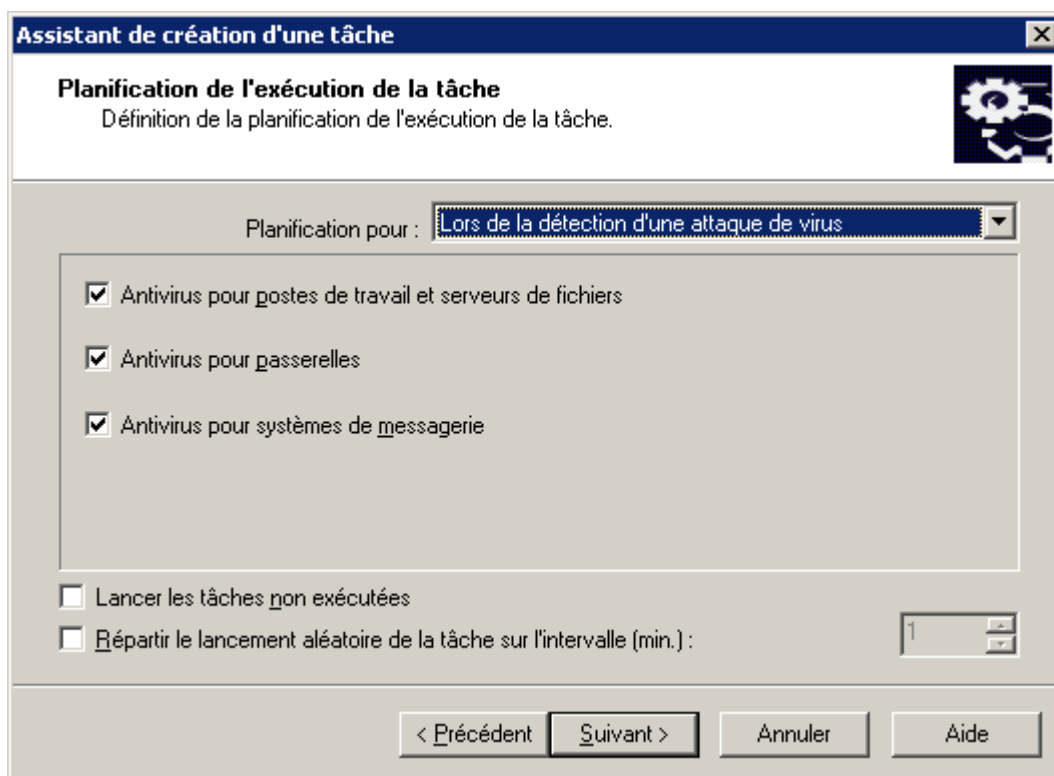


Illustration 83. Exécution lors de la détection d'une attaque de virus

Après la fin de l'Assistant, la tâche que vous venez de créer sera ajoutée aux dossiers **Tâches de groupe** des groupes et sous-groupes correspondants, et affichée dans l'arborescence de la console. Au besoin, vous pouvez configurer des paramètres de la tâche (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)).

CREATION D'UNE TACHE POUR LE SERVEUR D'ADMINISTRATION

➔ Pour créer une tâche pour le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Tâches de Kaspersky Administration Kit**.
2. Ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Tâche**.
3. Indiquez le nom de la tâche. Si une tâche de ce nom existe déjà dans le groupe, un **_1** sera automatiquement ajouté au nouveau nom.
4. Sélectionnez le type de tâche à créer (cf. ill. ci-après).

Trois types de tâches sont prévus pour le Serveur d'administration :

- **Envoi du rapport ;**
- **Sauvegarde des données du Serveur d'administration.**
- **Téléchargement des mises à jour dans le référentiel.**

Si la tâche de copie de sauvegarde ou de mise à jour a déjà été créée pour le Serveur d'administration, alors elle n'apparaîtra pas dans la fenêtre de sélection de type de tâche. L'existence simultanée de deux tâches de ce type n'est pas possible.

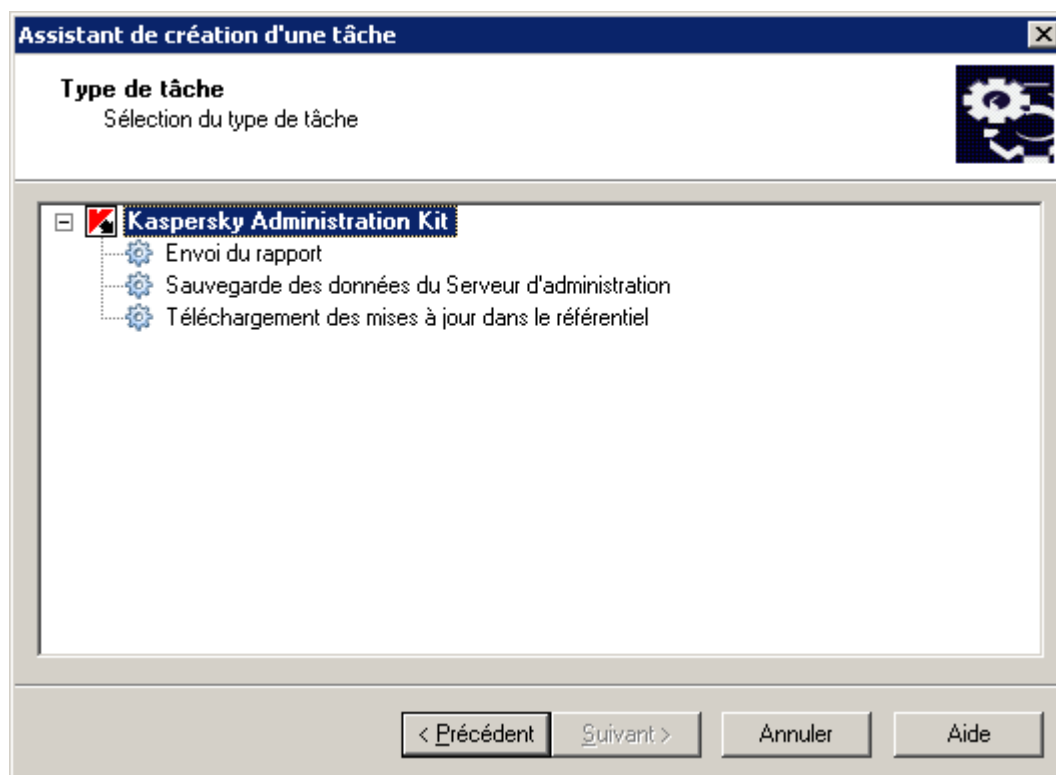


Illustration 84. Création d'une tâche pour le Serveur d'administration. Sélection du type de la tâche

5. Configurez la tâche créée en fonction du type sélectionné. Quelques paramètres sont définis par défaut. Les rubriques correspondantes reprennent les informations sur la création et la configuration des tâches :
 - diffusion des rapports (cf. section "Tâche de diffusion des rapports" à la page [200](#)) ;
 - tâche de sauvegarde (cf. section "Tâche de copie de sauvegarde des données" à la page [311](#)) ;
 - réception des mises à jour (cf. section "Création d'une tâche de téléchargement des mises à jour dans le référentiel" à la page [246](#)).
6. Programmez le lancement de la tâche du Serveur d'administration comme pour selon la programmation d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)).

A la fin de l'Assistant, la tâche sera ajoutée au dossier **Tâches de Kaspersky Administration Kit** et apparaîtra dans l'arborescence de la console.

Pour accéder rapidement à la création de tâches du Serveur d'administration, vous pouvez cliquer sur les liens situés dans le panneau des tâches du dossier **Tâches de Kaspersky Administration Kit**.

CREATION D'UNE TACHE POUR LA SELECTION D'ORDINATEURS

► Pour créer une tâche pour la sélection d'ordinateurs,

dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**, ouvrez le menu contextuel et sélectionnez la commande **Nouveau** → **Tâche**.

L'Assistant de création de tâche lancé est semblable à celui utilisé pour la création de tâches de groupe (cf. section "Création d'une tâche de groupe [101](#)" à la page). L'exception se situe au niveau de la présence d'une étape de définition de la liste des postes clients pour lesquels une tâche est créée pour une sélection d'ordinateurs (cf. ill. ci-après).

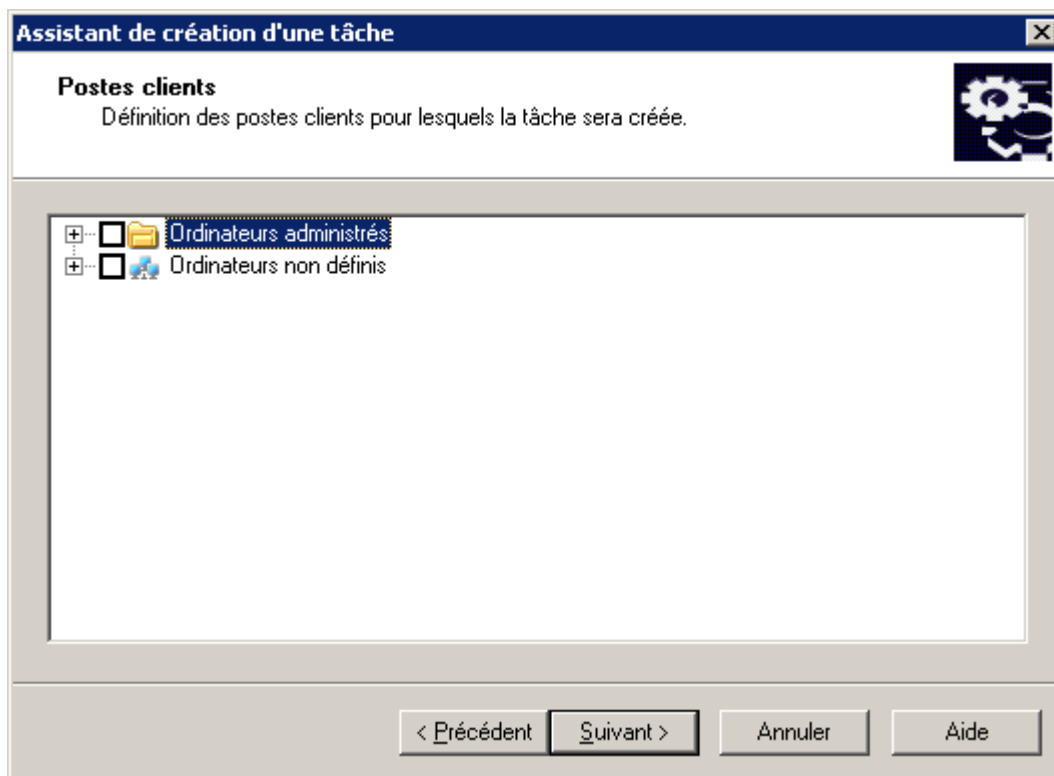


Illustration 85. Création d'une tâche pour la sélection d'ordinateurs. Composition de la liste des ordinateurs pour l'exécution

Sélectionnez les clients du réseau de l'entreprise sur lesquels la tâche sera lancée. Vous pouvez choisir les ordinateurs de différents dossiers, ou tous les ordinateurs du dossier courant. La sélection porte sur les ordinateurs qui figurent ou non dans les groupes d'administration.

Pour passer rapidement à la création d'une tâche pour la sélection d'ordinateurs, cliquez sur le lien **Créer une tâche** situé dans le panneau des tâches du dossier **Tâches pour les sélections d'ordinateurs**.

Les tâches de ce type ne seront exécutées que sur la sélection d'ordinateurs définie. Si de nouveaux postes clients sont ajoutés au groupe que vous avez sélectionné, la tâche ne sera pas exécutée pour ceux-ci. Il faudra créer une nouvelle tâche ou introduire les modifications requises dans les paramètres de la tâche existante.

Après la fin de l'Assistant, la tâche sera ajoutée au dossier **Tâches pour les sélections d'ordinateurs** dans l'arborescence de console et affichée dans le panneau des résultats. Les tâches pour les sélections d'ordinateurs permettent d'effectuer toutes les opérations disponibles pour des tâches de groupe.

CREATION D'UNE TACHE LOCALE

◆ Pour créer une tâche locale pour un poste client, procédez comme suit :

1. Dans le dossier **Ordinateurs administrés** sélectionnez le dossier avec le nom du groupe, contenant le poste client.
2. Dans le panneau des résultats, sélectionnez l'ordinateur pour lequel vous souhaitez créer la tâche et sélectionnez l'option **Propriétés** du menu contextuel.

La fenêtre de consultation des propriétés du poste client **Propriétés de <Nom de poste>** (cf. ill. ci-après) s'affiche ensuite dans la fenêtre principale de l'application.

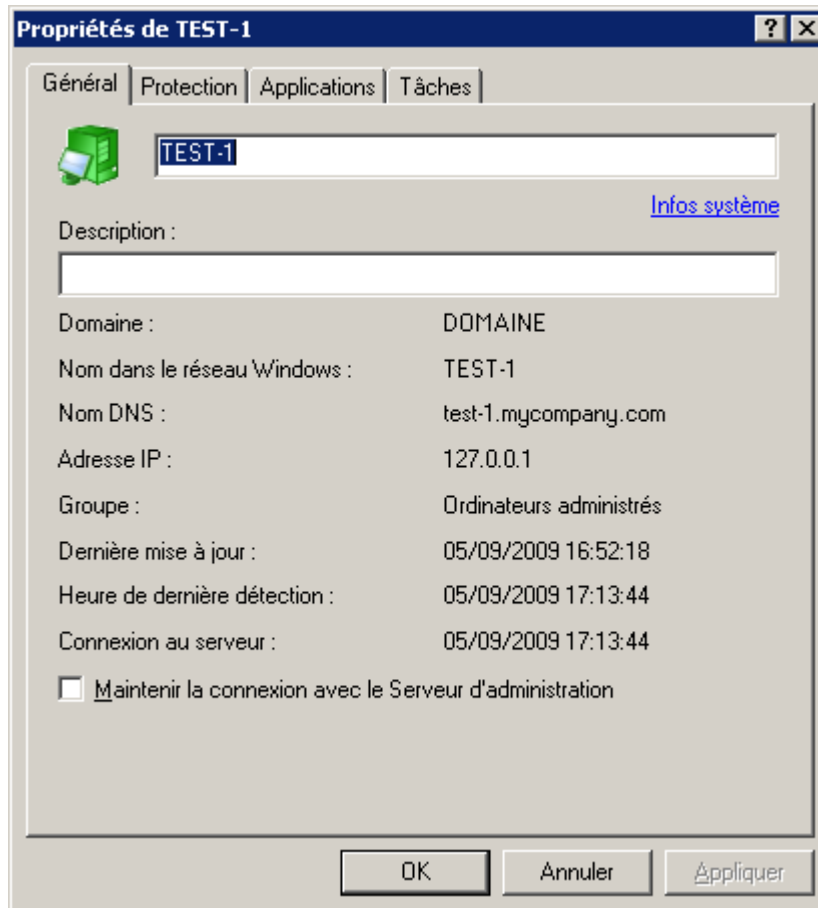


Illustration 86. Affichage des propriétés d'un poste client. Onglet **Général**

3. Ouvrez l'onglet **Tâches** (cf. ill. ci-après). L'onglet affiche toutes les tâches créées pour ce client. Pour créer une nouvelle tâche locale, cliquez sur **Ajouter**. Pour configurer des paramètres de tâche, cliquez sur **Propriétés**.

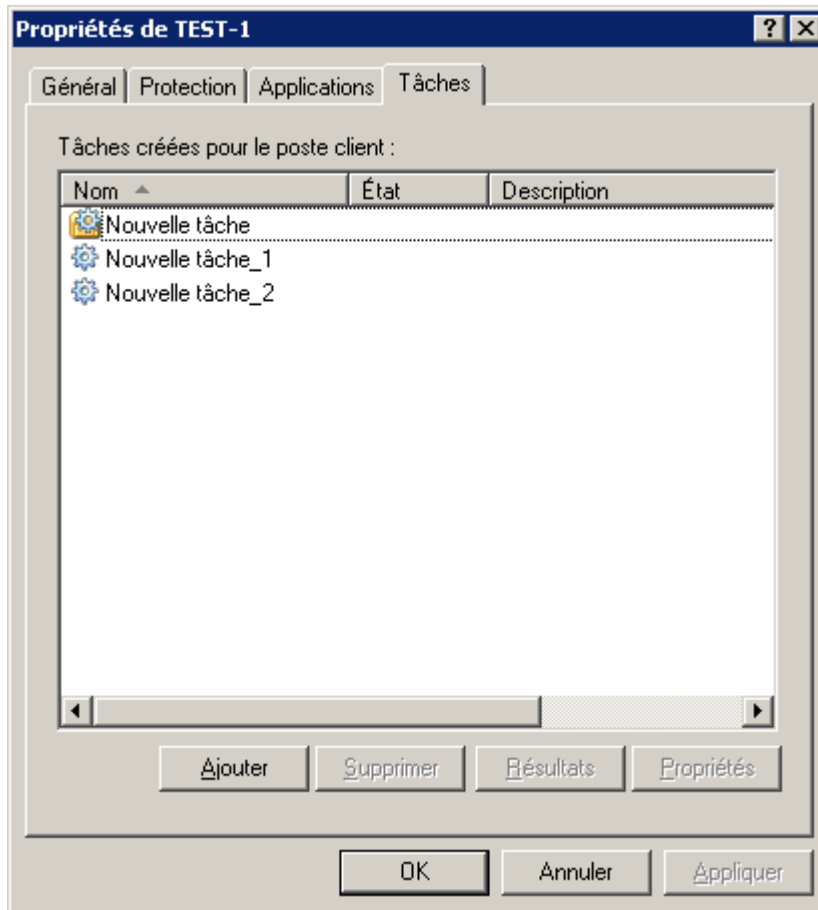


Illustration 87. Affichage des propriétés d'un poste client. Onglet **Tâches**

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

AFFICHAGE ET MODIFICATION DES PARAMETRES DE TACHE

- Pour afficher les paramètres de tâche et les modifier,

ouvrez la fenêtre des propriétés de la tâche.

Pour ce faire, réalisez une des actions suivantes :

- Si vous souhaitez créer ou modifier une tâche de groupe, sélectionnez un groupe requis dans l'arborescence de console puis ouvrez le dossier **Tâches de groupe** et sélectionnez la tâche requise. Ouvrez ensuite le menu contextuel et sélectionnez la commande **Propriétés** ou cliquez sur le lien **Modifier les paramètres de la tâche** situé dans le panneau des tâches.
- Si vous voulez modifier les paramètres de la tâche pour la sélection d'ordinateurs, sélectionnez dans l'arborescence de la console le dossier **Tâches pour les sélections d'ordinateurs**, sélectionnez la tâche requise, ouvrez le menu contextuel et sélectionnez la commande **Propriétés** ou cliquez sur le lien **Modifier les paramètres de la tâche** situé dans le panneau des tâches.
- Si vous devez modifier les paramètres de la tâche pour le Serveur d'administration, sélectionnez dans l'arborescence de la console le dossier **Tâches de Kaspersky Administration Kit**, sélectionnez la tâche requise, ouvrez le menu contextuel et sélectionnez la commande **Propriétés** ou cliquez sur le lien **Modifier les paramètres de la tâche** situé dans le panneau des tâches.

Cela entraînera l'ouverture de la fenêtre **Propriétés: <Nom de la tâche>**, avec les onglets suivants : **Général**, **Paramètres**, **Compte**, **Planification**, **Notification**. La fenêtre des propriétés de la tâche pour la sélection d'ordinateurs contient également l'onglet **Postes clients**.

La boîte de dialogue **Propriétés de <Nom de tâche>** affiche les paramètres par défaut pour ce type, ou la dernière modification des paramètres. Vous pouvez afficher les paramètres réels de cette tâche dans la boîte de dialogue **Propriétés de <Nom de poste>** de l'onglet Tâches.

Sur l'onglet Général (cf. ill. ci-après), vous retrouverez les informations générales sur la tâche : **Général** (cf. ill. ci-après), vous retrouverez les informations générales sur la tâche :

- nom de tâche (vous pouvez le modifier si nécessaire) ;
- l'application pour laquelle la stratégie est créée (par exemple, Kaspersky Anti-Virus for Windows Workstations) ;
- numéro de version de l'application ;
- type de tâche ;
- date et heure de création ;
- la dernière commande exécutée manuellement (**Démarrer**, **Arrêter**, **Suspendre**, **Reprendre**).

Dans la partie inférieure de l'onglet figurent des informations sur la progression de la tâche sur les postes clients, pour lesquels la tâche a été créée. Pour afficher les détails d'exécution de la tâche, cliquez sur **Résultats**.

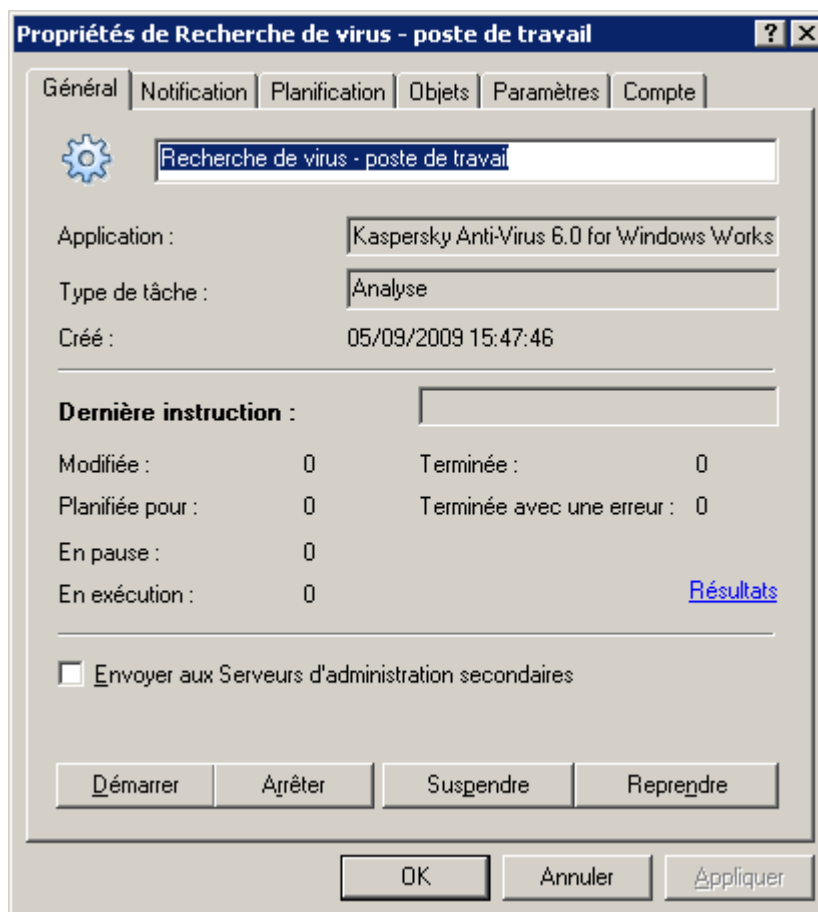


Illustration 88. Modification des propriétés de la tâche. Onglet **Général**

Sur cet onglet, les boutons suivants vous permettent également de contrôler la tâche manuellement : démarrer, arrêter, suspendre, reprendre.

Pour que la tâche soit copiée sur les Serveurs secondaires, cochez la case **Envoyer aux Serveurs d'administration secondaires**.

Sur l'onglet **Paramètres** (cf. ill. ci-après), vous retrouverez les paramètres de la tâche propres à chaque application. Pour plus d'informations sur cet onglet, reportez-vous à la documentation correspondante.

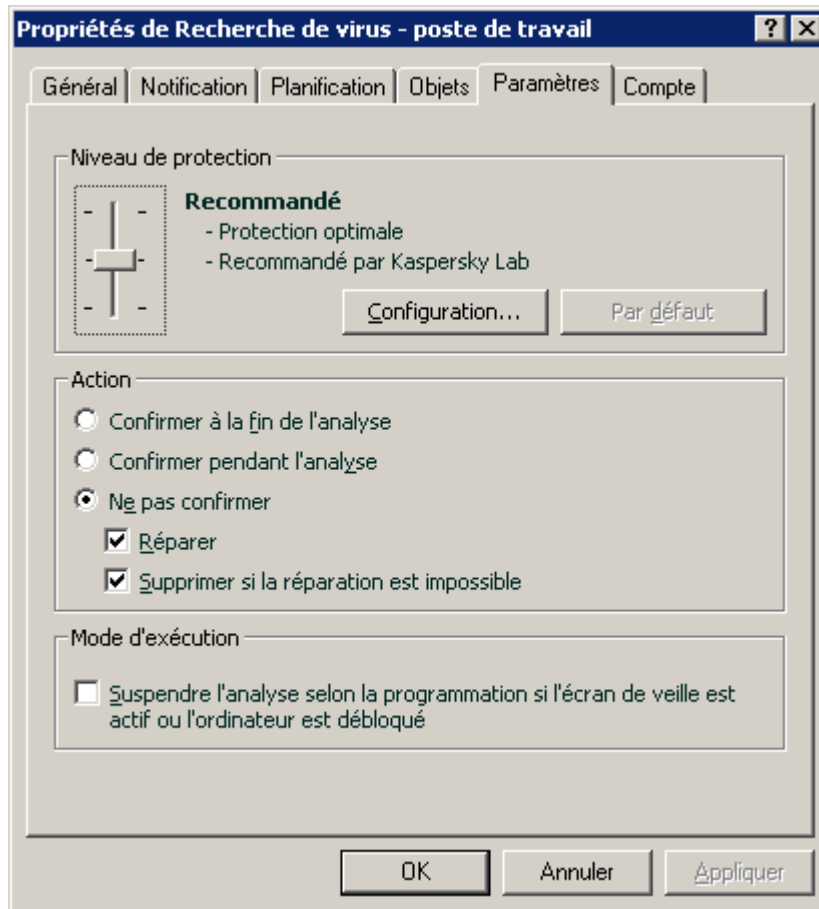


Illustration 89. Modification des propriétés de tâche. Onglet **Paramètres**

Dans l'onglet **Compte** (cf. ill. ci-après), vous pouvez spécifier un compte sous lequel la tâche sera exécutée. Vous avez le choix entre les options suivantes :

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

La sélection d'un compte permet d'éviter des erreurs lors de l'exécution de tâches d'analyse à la demande ou de mise à jour lorsque l'utilisateur lance une tâche sans avoir les privilèges nécessaires.

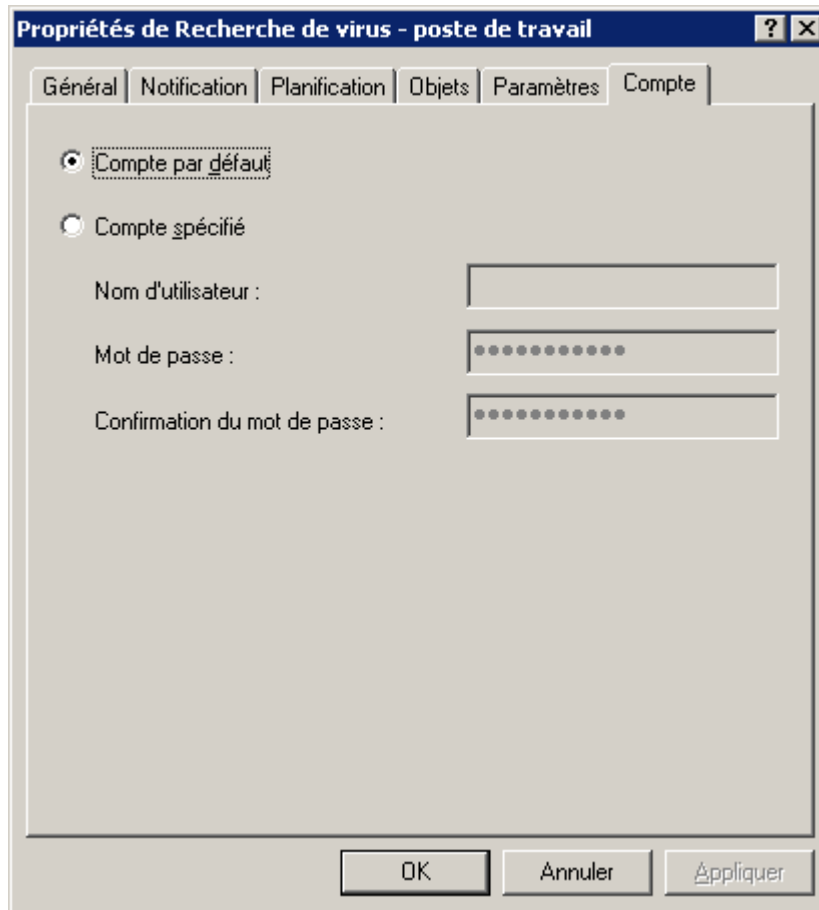


Illustration 90. Modification des propriétés de tâche. Onglet **Compte**

L'onglet **Planification** (cf. ill. ci-après) permet de modifier les paramètres de programmation de la tâche. Le lien **Avancé** permet de réaliser les actions suivantes :

- configurer le démarrage automatique du système d'exploitation (cf. section "Démarrage automatique du système d'exploitation sur les postes clients avant le lancement d'une tâche" à la page [124](#)) sur les ordinateurs éteints avant le lancement de la tâche ;
- activer l'arrêt de l'ordinateur (cf. section "Arrêt de l'ordinateur après l'exécution de la tâche" à la page [124](#)) après l'exécution de la tâche ;
- limiter l'exécution de la tâche dans le temps (cf. section "Limitation de la durée d'exécution de la tâche" à la page [124](#)).

Le contenu de l'onglet **Planification** et sa manipulation sont identiques à ceux de la fenêtre de configuration de la planification lors de la création d'une tâche (cf. section "Création d'une tâche de groupe" à la page [101](#)).

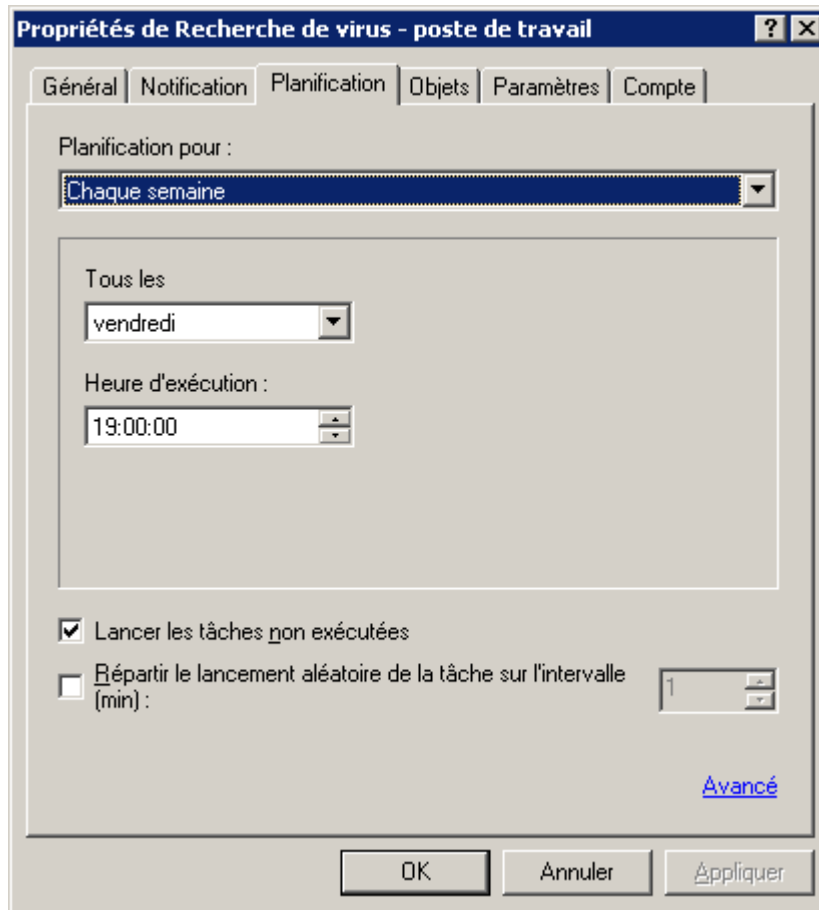


Illustration 91. Modification des propriétés de tâche. Onglet **Planification**

Sur l'onglet **Notification** (cf. ill. ci-après), vous pouvez configurer l'envoi des notifications, avec les comptes-rendus d'activité des tâches :

- Dans la zone **Sauvegarder les informations sur les résultats**, définissez l'emplacement de l'enregistrement des informations sur les résultats. Pour ce faire, cochez les cases suivantes :
 - **Enregistrer en local** pour stocker en local les informations sur chaque client.

Cette option est accessible avec Kaspersky Anti-Virus for Windows File Servers de version 5.0 MP4.

- **Sur le Serveur d'administration pendant (jours)** pour stocker de manière centralisée l'historique des tâches envoyé par les clients au Serveur d'administration. Dans la zone adjacente, indiquez la durée de stockage de l'historique des tâches sur le Serveur. Après la fin de la période indiquée, l'information sera supprimée du serveur.
- **Dans le journal des événements du S.E. du poste client** pour que chaque client enregistre les événements en local, dans leur propre journal d'événement de Windows.
- **Dans le journal des événements du S.E. du Serveur d'administration** pour activer l'enregistrement de tous les événements des applications associés à tous les clients du groupe dans le journal d'événement de Windows, sur un ordinateur équipé du Serveur d'administration.

Dans ce même champ, sélectionnez les événements à enregistrer dans le journal :

- **Sauvegarder tous les événements ;**

- **Sauvegarder les événements relatifs au déroulement des tâches ;**
- **Sauvegarder uniquement le résultat de la tâche.**
- Dans le groupe **Communiquer les résultats** indiquez le mode de notification des résultats de l'exécution de la tâche pour l'administrateur ainsi que d'autres utilisateurs. Le bouton **Paramètres** vous permet de configurer les paramètres de la notification.

Pour ce faire, cochez l'une des cases suivantes :

- **Envoyer par courrier électronique** : envoi de notifications par l'intermédiaire d'un serveur de messagerie.
- **Utiliser NET SEND** : envoi de notifications sur le réseau par l'intermédiaire du service NET SEND. Afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les ordinateurs le Messenger doit être lancé.
- **Lancement du fichier exécutable** : exécuter un programme ou un script dans le cas d'un certain événement.

Les paramètres sont les mêmes que ceux définis dans l'onglet **Notification** des propriétés des événements. Les valeurs utilisées par défaut sont celles définies dans les paramètres du Serveur d'administration (cf. section "Paramètres généraux du Serveur d'administration" à la page 30).

Si vous souhaitez ne recevoir des notifications qu'en cas d'erreurs, cochez la case **Notifier uniquement les erreurs**.

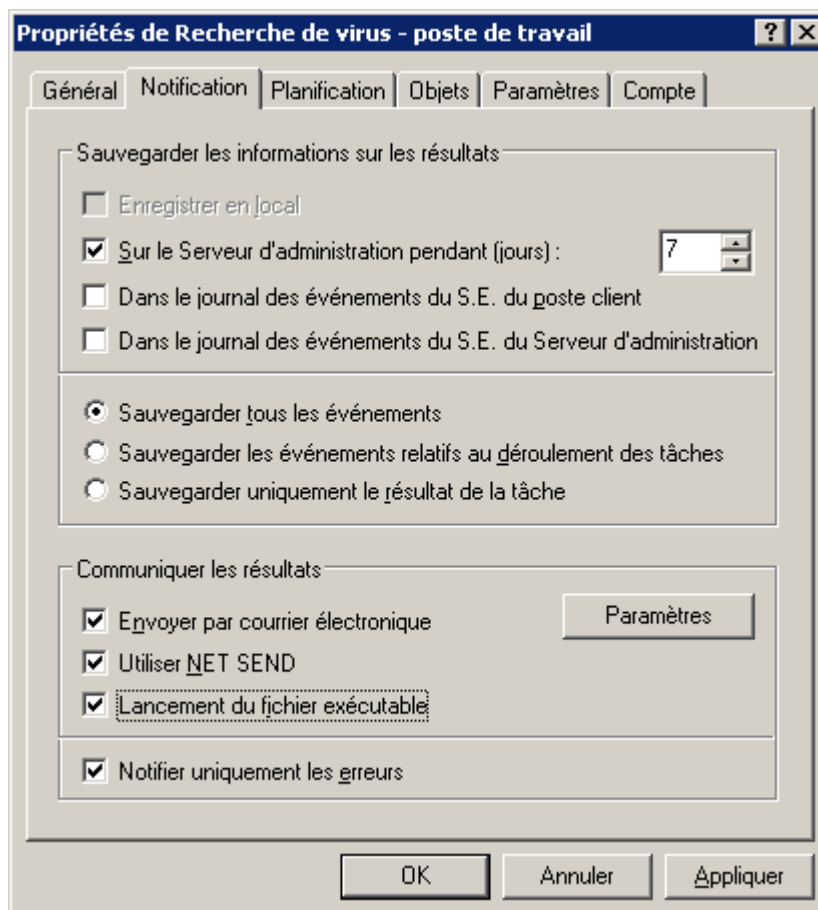


Illustration 92. Modification des propriétés de tâche. Onglet **Notification**

Si la tâche a été créée pour une sélection d'ordinateurs, dans la fenêtre de consultation des paramètres l'onglet **Postes clients** (cf. ill. ci-après) est aussi présent. Il contient la liste des clients sur lesquels la tâche sélectionnée est exécutée. Vous pouvez ajouter et enlever des clients de la liste.

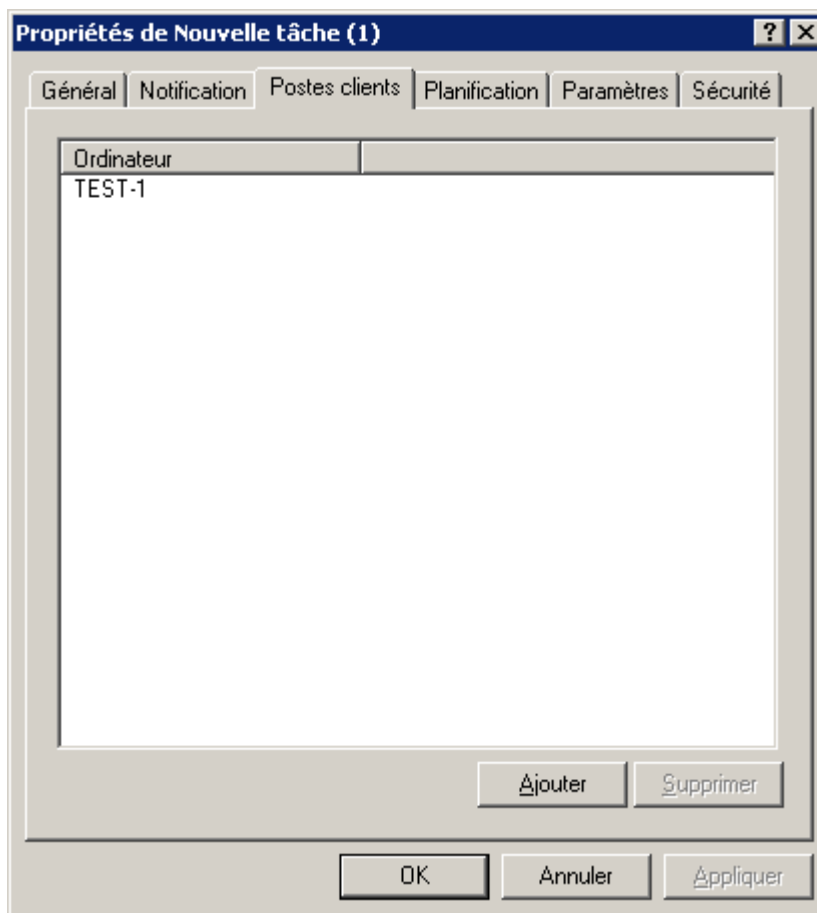



Illustration 93. Modification des propriétés d'une tâche pour la sélection d'ordinateurs. Onglet **Postes clients**

AFFICHAGE D'UNE TACHE DE GROUPE HERITEE DANS LE PANNEAU DES RESULTATS DU GROUPE IMBRIQUE

► Pour que les tâches héritées apparaissent dans le groupe imbriqué dans le dossier **Tâches de groupe**, procédez comme suit :

1. Sélectionnez le dossier **Tâches de groupe** dans le panneau des résultats du groupe imbriqué.
2. Ouvrez le menu contextuel, choisissez **Vue** et cochez la case **Tâches héritées**.

Les tâches de groupe héritées sont alors affichées dans le panneau des résultats en regard de l'icône . Il est possible de visualiser les propriétés des tâches de groupe héritées. La modification des tâches de groupe héritées n'est possible que dans les groupes où elles ont été créées.

DEMARRAGE AUTOMATIQUE DU SYSTEME D'EXPLOITATION SUR LES POSTES CLIENTS AVANT LE LANCEMENT D'UNE TACHE

➤ Pour être sûr que la tâche est bien exécutée sur les postes éteints à l'heure d'exécution programmée, procédez comme suit :

1. Dans l'onglet de la boîte de dialogue de configuration de la tâche **Planification** cliquez sur **Avancé**.
2. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), cochez la case **Activer les ordinateurs avant le lancement de la tâche par la fonction Wake On LAN (min.)**. Ensuite, spécifiez l'heure souhaitée.

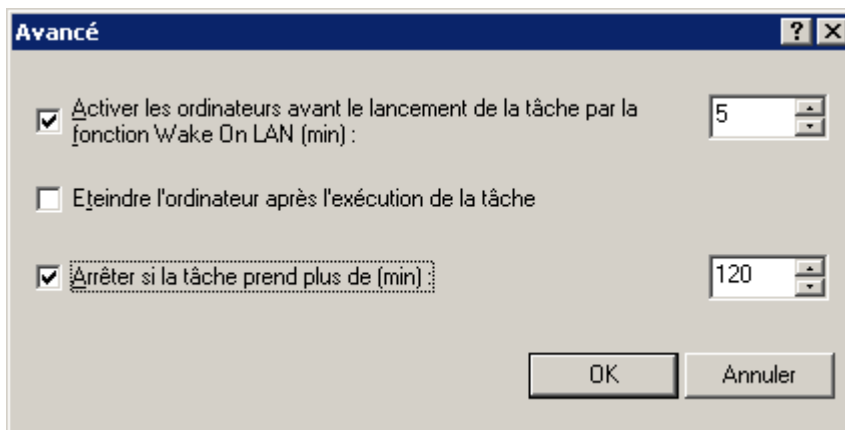


Illustration 94. Activation du démarrage automatique du système d'exploitation

Ceci a pour effet de démarrer le système d'exploitation sur ces postes, avant de lancer la tâche.

Le démarrage automatique du système d'exploitation est accessible uniquement sur les ordinateurs qui supportent la fonction Wake on Lan.

ARRET DE L'ORDINATEUR APRES L'EXECUTION DE LA TACHE

➤ Pour arrêter l'ordinateur après l'exécution de la tâche, procédez comme suit :

1. Dans l'onglet de la boîte de dialogue de configuration de la tâche **Planification**, cliquez sur **Avancé**.
2. Dans la fenêtre qui s'ouvre, cochez la case **Eteindre l'ordinateur après l'exécution de la tâche**.

LIMITATION DE LA DUREE D'EXECUTION DE LA TACHE

➤ Afin de limiter l'exécution de la tâche dans le temps, procédez comme suit :

1. Dans l'onglet de la boîte de dialogue de configuration de la tâche **Planification**, cliquez sur **Avancé**.
2. Dans la fenêtre qui s'ouvre, cochez la case **Arrêter si la tâche prend plus de (min.)** et spécifiez une temporisation avant arrêt de la tâche.

EXPORTATION D'UNE TACHE

Les droits des utilisateurs locaux ne seront pas exportés.

➤ *Pour exporter une tâche de groupe dans un fichier, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Ordinateurs administrés** et sélectionnez le groupe requis.
2. Ouvrez le dossier **Tâches de groupe** appartenant au groupe et sélectionnez la tâche requise.
3. Ouvrez le menu contextuel et sélectionnez la commande **Toutes les tâches** → **Exporter** ou cliquez sur le lien **Exporter la tâche** situé dans le panneau des tâches.
4. Dans la fenêtre ouverte, spécifiez le nom de fichier et l'emplacement sous lequel vous allez enregistrer la tâche. Cliquez sur **Enregistrer**.

➤ *Pour exporter une tâche pour une sélection d'ordinateurs, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Tâches pour une sélection d'ordinateurs** et sélectionnez la tâche requise.
2. Ouvrez le menu contextuel et sélectionnez la commande **Toutes les tâches** → **Exporter** ou cliquez sur le lien **Exporter la tâche** situé dans le panneau des tâches.
3. Dans la fenêtre ouverte, spécifiez le nom de fichier et l'emplacement sous lequel vous allez enregistrer la tâche. Cliquez sur **Enregistrer**.

Les tâches de Kaspersky Administration Kit ne peuvent pas être exportées.

IMPORTATION D'UNE TACHE

➤ *Pour importer une tâche de groupe depuis un fichier, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Ordinateurs administrés** et sélectionnez le groupe requis.
2. Sélectionnez le dossier **Tâches de groupe** appartenant au groupe.
3. Ouvrez le menu contextuel et sélectionnez la commande **Toutes les tâches** → **Importer** ou cliquez sur le lien **Importer la tâche du fichier** situé dans le panneau des tâches du dossier.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la tâche. Cliquez sur **Ouvrir**.

➤ *Pour importer une tâche pour une sélection d'ordinateurs, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches pour les sélections d'ordinateurs**.
2. Ouvrez le menu contextuel et sélectionnez la commande **Toutes les tâches** → **Importer** ou cliquez sur le lien **Importer la tâche du fichier** situé dans le panneau des tâches du dossier.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la tâche. Cliquez sur **Ouvrir**.

Une nouvelle tâche apparaît dans l'arborescence de la console dans le dossier sélectionné.

Si le dossier sélectionné possède déjà une tâche au nom identique à celui de la tâche importée, alors le nom de la tâche recevra un suffixe numérique.

Les tâches de Kaspersky Administration Kit ne peuvent pas être importées.

CONVERSION DES TACHES

A l'aide de Kaspersky Administration Kit vous pouvez déplacer les tâches de version précédente des applications de Kaspersky Lab vers la version actuelle. Pour ce faire, utilisez l'Assistant de conversion des stratégies et des tâches (cf. section "Conversion des stratégies" à la page [97](#)).

DEMARRAGE ET ARRET MANUELS DES TACHES

➤ *Pour lancer ou arrêter manuellement une tâche, procédez comme suit :*

1. Sélectionnez la tâche (de groupe ou pour une sélection d'ordinateurs) requise dans le panneau des résultats.
2. Ouvrez le menu contextuel et sélectionnez la commande **Démarrer** ou **Arrêter**.

Pour accéder rapidement aux opérations, vous pouvez utiliser le lien **Lancer la tâche** ou **Arrêter la tâche**, situé dans le panneau des tâches, ou bien les boutons **Démarrer** ou **Arrêter** situés dans la fenêtre des propriétés des tâches (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)).

SUSPENSION ET REPRISE MANUELLES D'UNE TACHE

➤ *Pour arrêter ou reprendre l'exécution d'une tâche, procédez comme suit :*

Sélectionnez la tâche requise (globale ou pour une sélection de postes) dans le panneau des résultats, ouvrez le menu contextuel et sélectionnez la commande **Suspendre** ou **Reprendre**.

Pour effectuer ces opérations, vous pouvez les exciter de la fenêtre des propriétés (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)) de la tâche sur l'onglet **Général** à l'aide des boutons de commande **Démarrer**, **Arrêter**, **Suspendre** et **Reprendre**.

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.

SUIVI ET AFFICHAGE DES COMPTES-RENDUS D'ACTIVITE DES TACHES

► Pour surveiller l'exécution des tâches,

ouvrez la fenêtre des propriétés (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)) de la tâche souhaitée et sélectionnez l'onglet **Général** (cf. ill. ci-après).

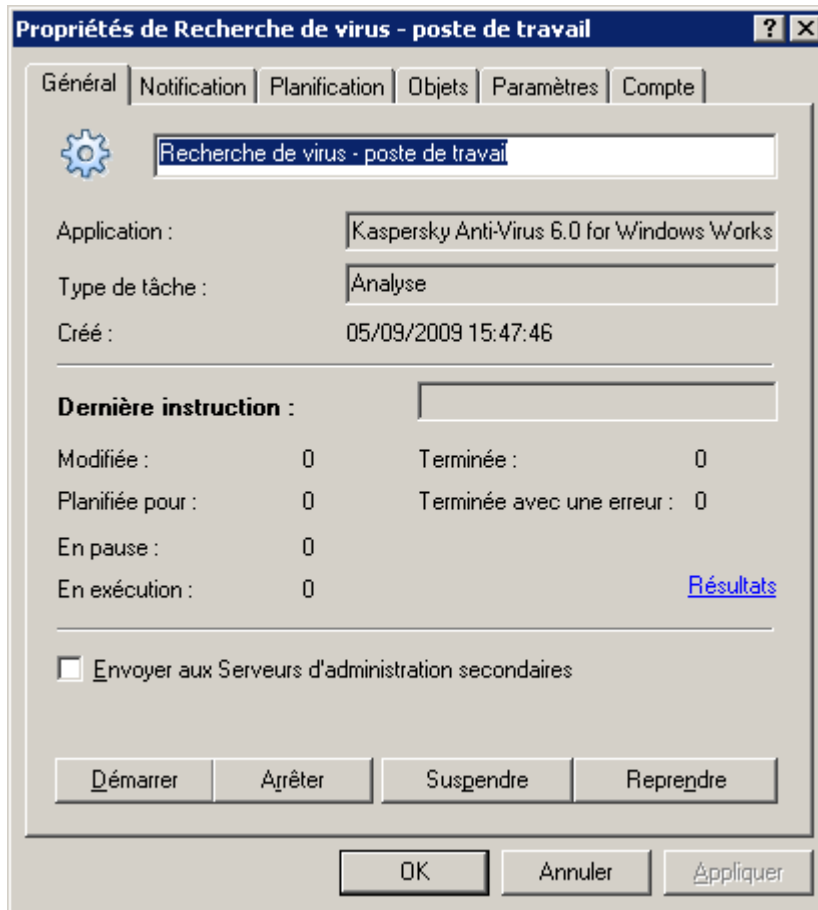


Illustration 95. Modification des propriétés de la tâche. Onglet **Général**

Dans la partie inférieure de l'onglet **Général** les informations suivantes sont affichées :

- **Modifiée** : nombre d'ordinateurs pour lesquels les paramètres de tâche ont été modifiés sur le Serveur d'administration (commande soumise, paramètres modifiés), sans que les modifications ne soient encore synchronisées avec le client.
- **En attente d'exécution** : nombre d'ordinateurs pour lesquels cette tâche est planifiée et dont les paramètres ont été synchronisés avec les données du Serveur d'administration.
- **En pause** : nombre d'ordinateurs sur lesquels cette tâche est suspendue.
- **En cours** : nombre d'ordinateurs sur lesquels cette tâche fonctionne.
- **Terminée** : nombre d'ordinateurs sur lesquels cette tâche s'est terminée avec succès.
- **Terminée avec une erreur** : nombre d'ordinateurs sur lesquels la tâche a échoué.

Des informations similaires sur des tâches en particulier sont affichées dans la fenêtre principale du programme, quand vous affichez les tâches de groupe ou des tâches pour des sélections d'ordinateurs.

AFFICHAGE DE L'HISTORIQUE DES TACHES ENTREPOSE SUR LE SERVEUR D'ADMINISTRATION

➔ Pour afficher l'historique des tâches entreposé sur le Serveur d'administration,

ouvrez la fenêtre des propriétés (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)) de la tâche souhaitée et basculez sur l'onglet **Général** et cliquez sur **Résultats**.

Cette action entraîne l'ouverture de la fenêtre **Résultats de la tâche** (cf. ill. ci-après). La partie supérieure de la boîte de dialogue contient la liste de tous les postes clients pour lesquels la tâche est définie. Les informations proposées sont les suivantes :

- **Poste client** : nom du poste client sur lequel est définie la tâche.
- **Groupe** : nom du groupe auquel appartient ce client.
- **Etat** : état actuel de la tâche.
- **Heure** : date et heure du dernier événement.
- **Description** : description détaillée de l'état actuel de la tâche sur le poste client.

La partie inférieure présente les résultats de l'exécution des tâches sur le poste client sélectionné :

- **Etat** : toutes les modifications de l'état de la tâche.
- **Heure** : date et heure de chaque événement.
- **Description** : description détaillée de chaque événement.

Les informations proposées dans cette fenêtre comprennent les données issues des Serveurs d'administration secondaires.

A l'aide du bouton **Actualiser** vous pouvez actualiser les informations dans le tableau.

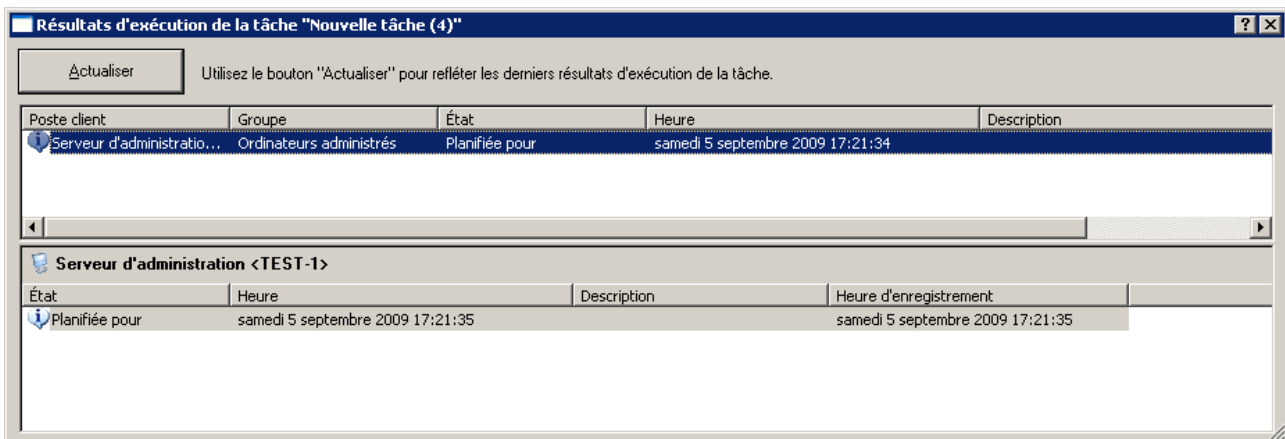


Illustration 96. Affichage de l'historique des tâches entreposé sur le Serveur d'administration

Pour afficher des comptes-rendus d'activité de tâche pour chaque client, ouvrez la boîte de dialogue **Propriétés de <Nom de poste>** sur l'onglet **Tâches** à l'aide du bouton **Résultats**. Ceci affichera l'information entreposée sur le Serveur d'administration.

L'affichage d'informations sur les résultats de l'exécution des tâches enregistrées localement sur le poste client est accessible uniquement avec Kaspersky Anti-Virus for Windows File Servers de version 5.0 MP4 et s'opère via la Console d'administration installée localement sur ce poste.

CONFIGURATION DU FILTRE D'ÉVÉNEMENTS POUR LA TÂCHE DE GROUPE

➔ Pour configurer le filtre des informations qui seront reprises dans la fenêtre **Résultats de la tâche**, procédez comme suit :

1. Utilisez la commande **Filtre** du menu contextuel de la liste des postes client. Cette action entraîne l'ouverture de la fenêtre de configuration du filtre (cf. ill. ci-après). Configurez les paramètres du filtre.
2. Sur l'onglet **Événements**, sélectionnez les caractéristiques des événements et des résultats d'exécution de la tâche qui seront affichés après application du filtre :
 - Sélectionnez dans la liste déroulante le niveau d'importance de l'événement.
 - Afin d'afficher uniquement les résultats des tâches d'un état particulier, sélectionnez l'état de la tâche qui vous intéresse dans le champ **Résultats des tâches**.
 - Cochez la case **Uniquement les derniers résultats des tâches** pour afficher uniquement les résultats de la dernière exécution de la tâche.
 - Si vous souhaitez limiter la quantité d'informations affichées après application du filtre, cochez la case **Limiter le nombre d'événements affichés** et spécifiez le nombre de lignes maximum du tableau.

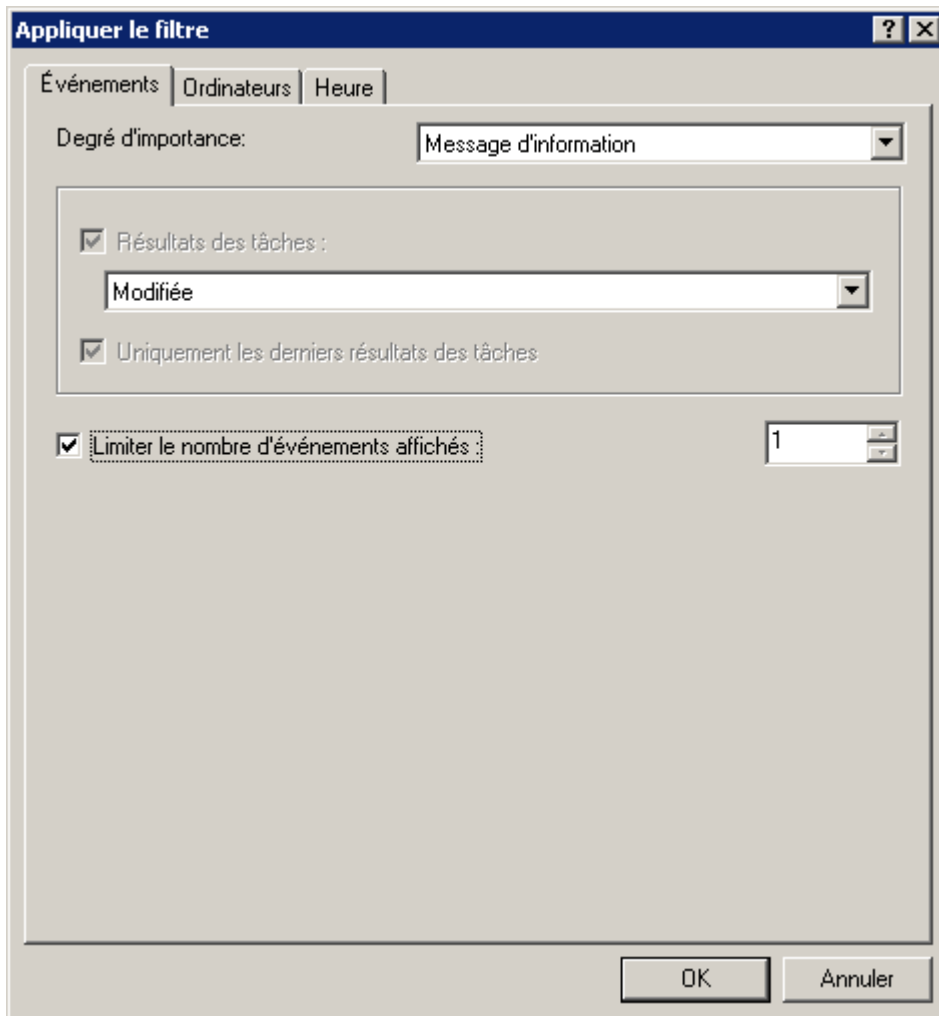


Illustration 97. Configuration du filtre d'événements. Onglet **Événements**

3. L'onglet **Ordinateurs** (cf. ill. ci-après) permet de définir sur quels ordinateurs il faut enregistrer les événements et les résultats de tâche.

Vous pouvez utiliser les paramètres suivants :

- **Nom de l'ordinateur.**
- **Nom de l'ordinateur dans le réseau Windows.**
- **Groupe d'administration.**
- **Domaine DNS.**
- **Domaine Windows.**
- **Intervalle d'adresses IP.** Pour ce faire, cochez les cases correspondantes et saisissez l'adresse IP initiale et finale du poste.

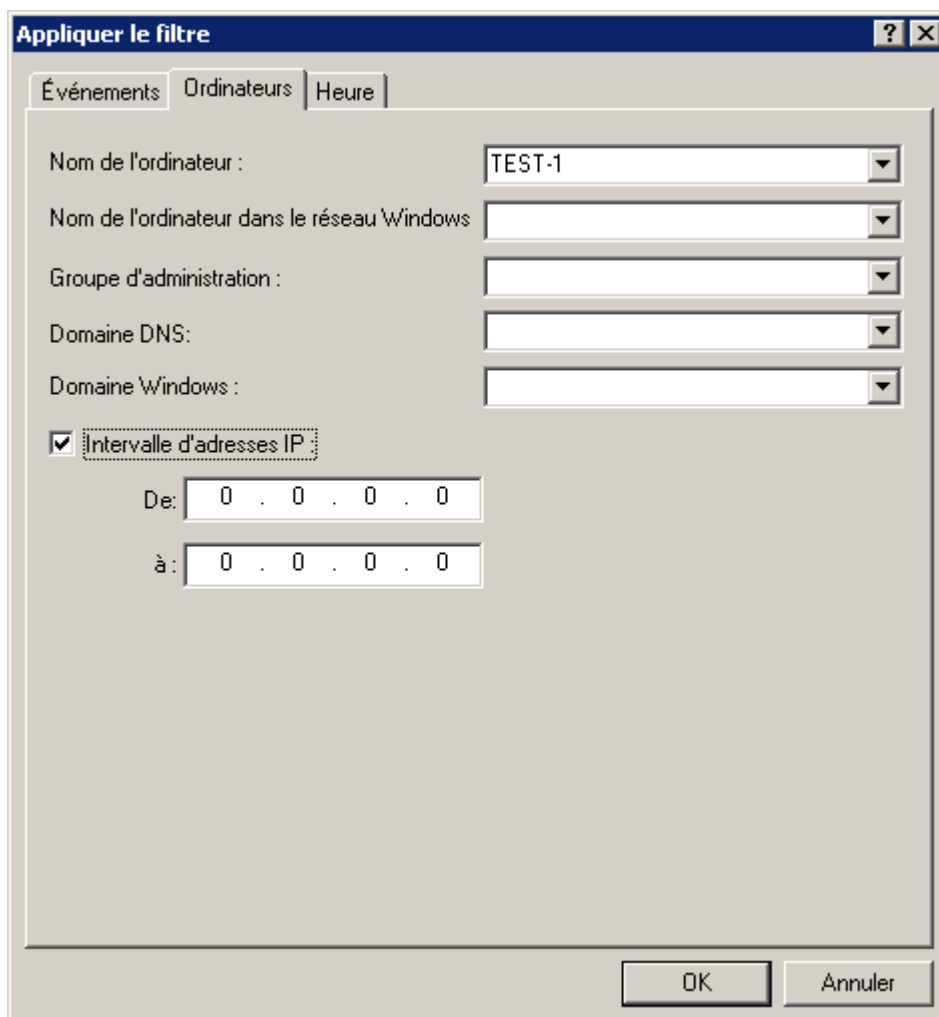


Illustration 98. Configuration du filtre d'événements. Onglet **Ordinateurs**

4. L'onglet **Heure** (cf. ill. ci-après) permet de définir l'heure d'enregistrement des événements et de résultats de tâches.

Vous pouvez sélectionner les options suivantes :

- **Pour la période** : spécifiez le début et la fin de la période couverte. Pour ce faire, dans les champs **de** et **à** sélectionnez **Déclenchement** et indiquez la date et l'heure exactes. Si toutes les informations enregistrées sont nécessaires, sélectionnez **Premier événement** et **Dernier événement**.
- **Au cours des derniers jours** : précisez le nombre de jours. Dans ce cas, le début de l'intervalle correspond au moment de la création de la liste.

Par exemple, si le champ indique 2 jours et que la liste est créée le 24 juin à 15h00. Alors la liste reprendra les données depuis le 22 juin à 15h00.

Illustration 99. Configuration du filtre d'événements. Onglet **Heure**

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

CONFIGURATION DU FILTRE DES EVENEMENTS DU POSTE SELECTIONNE

- *Pour configurer le filtre des informations, du post sélectionné, procédez comme suit :*
 1. Dans le menu contextuel sélectionnez le point **Evénements**.
 2. Dans la fenêtre ouverte **Evénements** cliquez sur le bouton **Filtre**.

3. Dans la fenêtre de dialogue de configuration du filtre indiquez les paramètres de filtre sur les onglets **Événements** (cf. ill. ci-après) et **Heure**.

Sur l'onglet **Événements**, sélectionnez les caractéristiques des événements et des résultats d'exécution de la tâche qui seront affichés après application du filtre :

- Dans le champ **Nom de l'application** sélectionnez le nom de l'application, qui doit produire les événements qui vous intéressent.
- Indiquez le **Numéro de version** de l'application.
- Sélectionnez le **Nom de tâche** qui a déclenché l'événement.
- Dans le champ **Degré d'importance** sélectionnez la gravité de l'événement dans la liste déroulante.

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

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

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

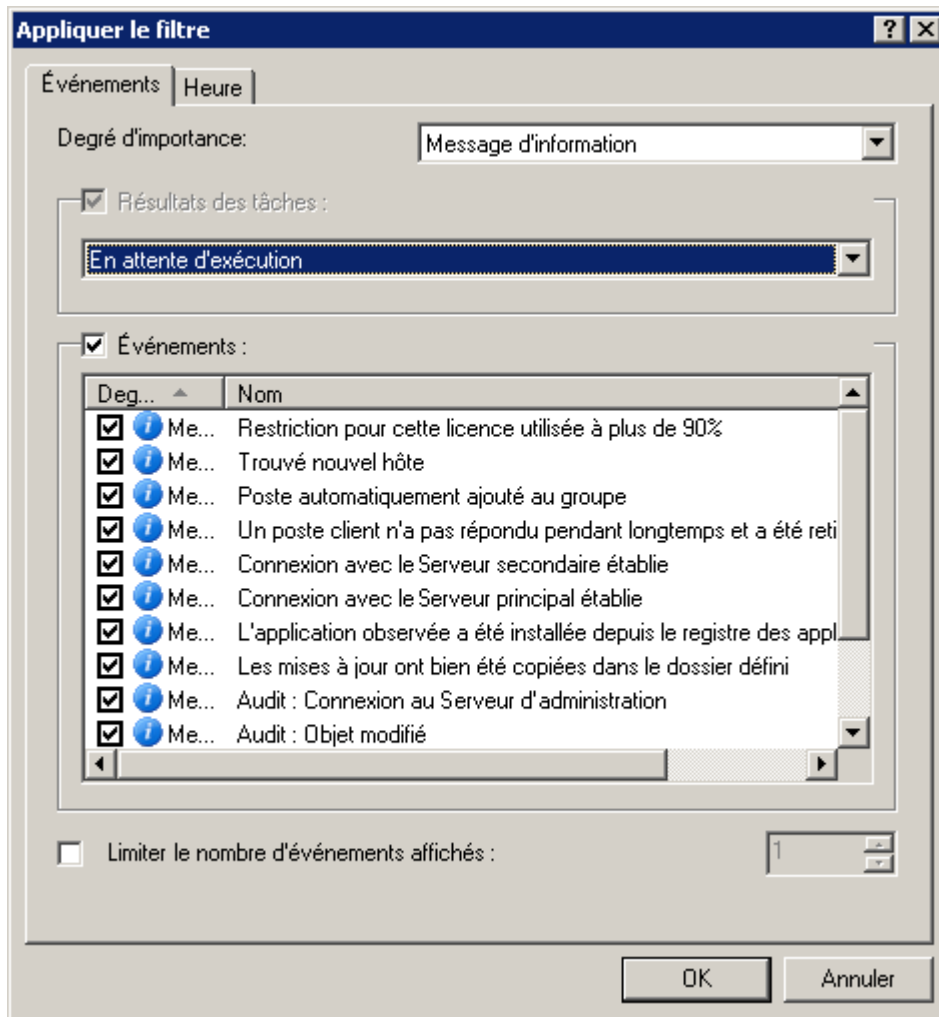


Illustration 100. Configuration du filtre d'événements. Onglet **Événements**

Sur l'onglet **Heure** définissez les paramètres comme pour la tâche de groupe (cf. section "Configuration du filtre d'événements pour la tâche de groupe" à la page 129). L'onglet **Ordinateurs** n'est pas visible car la configuration du filtre s'effectue pour un ordinateur qui a déjà été sélectionné.

4. Quand vous aurez terminé la configuration du filtre, cliquez sur **OK**. Après cela, seules les informations qui vérifient les paramètres indiqués seront affichées dans la fenêtre **Événements**.

ANNULATION DE LA FONCTION DE FILTRE

➤ Pour annuler l'action du filtre, procédez comme suit :

Dans le menu contextuel, sélectionnez la commande **Supprimer le filtre**.

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 via la Console d'administration. Grâce aux paramètres de l'application, il est possible de définir des valeurs individuelles pour les paramètres de fonctionnement de l'application pour chaque poste client du groupe.

AFFICHAGE DES PARAMETRES DE L'APPLICATION

➔ Pour afficher les paramètres de l'application et pour les modifier, procédez comme suit :

1. Dans le dossier **Ordinateurs administrés** sélectionnez le dossier avec le nom du groupe, contenant le poste client.
2. Sélectionnez le dossier **Postes clients**.
3. Dans le panneau des résultats, sélectionnez l'ordinateur pour lequel vous souhaitez modifier les paramètres de l'application et sélectionnez l'option **Propriétés** du menu contextuel.

La boîte de dialogue **Propriétés de <Nom de poste>** s'affiche avec plusieurs onglets.

4. Ouvrez l'onglet **Applications** (cf. ill. ci-après). Il propose un tableau qui reprend la liste complète des applications de Kaspersky Lab installée sur le poste client ainsi que des brèves informations sur chacune d'entre elles.
5. Sélectionnez l'application cible. Vous pouvez :
 - Afficher la liste des événements (cf. section "Sélections d'événements" à la page [214](#)) d'application, qui se sont produits sur le poste client et qui ont été enregistrés par le Serveur d'administration, à l'aide du bouton **Événements**.
 - Afficher les statistiques courantes sur l'exécution de l'application : cliquez sur **Statistiques**. Le Serveur d'administration effectue une requête au client pour obtenir cette information. En cas d'absence de connexion, un message d'erreur approprié est affiché.

- Afficher des informations générales sur une application et configurer les paramètres d'application : cliquez sur **Propriétés** dans la fenêtre **Propriétés de l'application** "<Nom de l'application>".

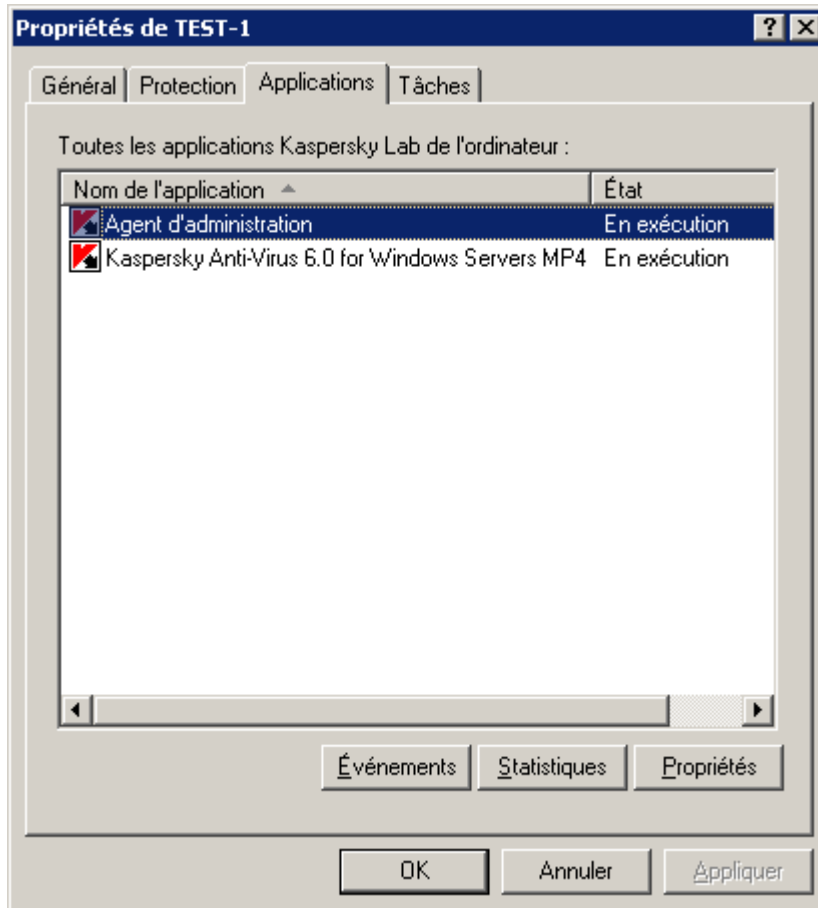


Illustration 101. Affichage des propriétés d'un poste client. Onglet **Applications**

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

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez afficher des informations générales sur l'application, sur les mises à jour installées, la démarrer ou la stopper, afficher les paramètres du plugin correspondant dans le poste administrateur en cliquant sur le lien **Information sur le plug-in**.

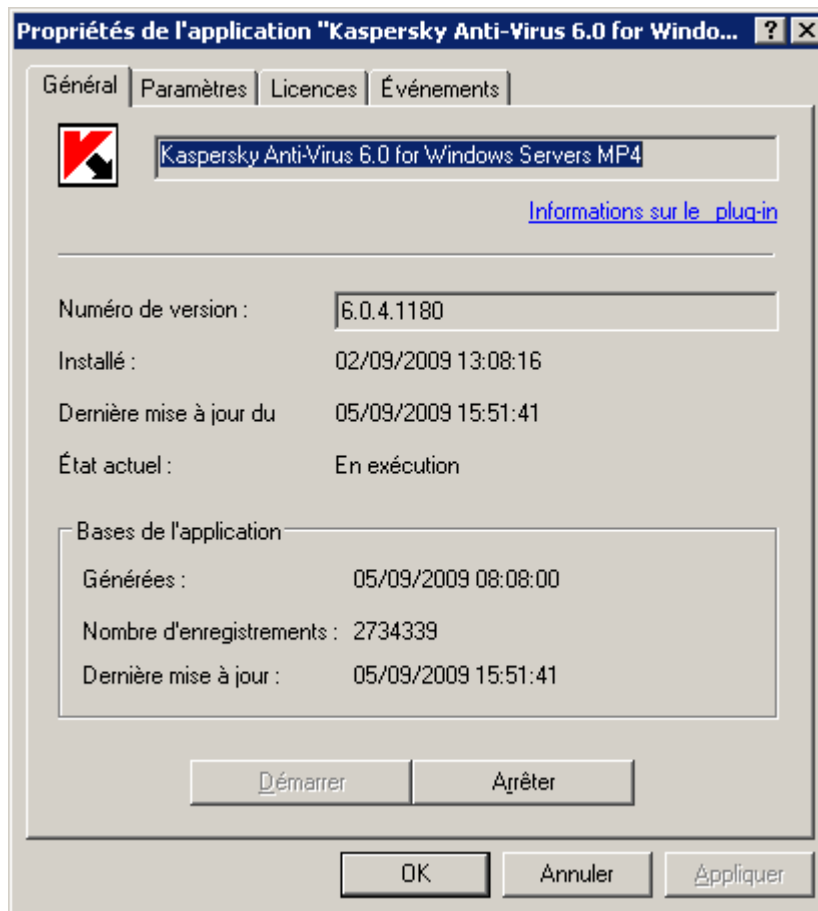


Illustration 102. Affichage des propriétés d'un poste client. Onglet **Général**

L'onglet **Licences** présente des informations détaillées sur les licences active et suivante installées pour l'application (cf. ill. ci-après).

Le groupe **Licence active** reprend les données relatives à la licence actuelle :

- **Numéro** : numéro de la licence ;
- **Type** : type de la licence installée, par exemple, commerciale, démonstration ;
- **Date d'activation** : date d'activation de la licence (lorsque la licence est devenue active) ;
- **Date d'expiration** : date d'expiration de la licence ;
- **Durée de validité** : période de validité de la licence ;
- **Limite compteur d'ordinateurs** : restrictions imposées par la licence.

Le groupe **Licence complémentaire** reprend les données relatives à la licence complémentaire :

- **Numéro** : numéro de la licence ;
- **Type** : type de la licence, par exemple, **commerciale** ;
- **Durée de validité** : période de validité de la licence ;

- **Limite compteur d'ordinateurs** : restrictions imposées par la licence.

L'onglet **Événements** (cf. ill. ci-après) affiche des paramètres qui définissent les règles de traitement des événements dans le fonctionnement de l'application sur le poste client. Vous pouvez les afficher et faire les changements nécessaires. Cet onglet est parfaitement identique à l'onglet du même nom de la fenêtre de configuration de la stratégie pour l'application (cf. section "Affichage et modification des paramètres d'une stratégie" à la page [79](#)).

CONFIGURATION DES PARAMETRES DE L'AGENT D'ADMINISTRATION

- Pour consulter les paramètres de l'Agent d'administration installé sur le poste client, procédez comme suit :
1. Sélectionnez le poste client dans le panneau des résultats, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.
 2. Dans la boîte de dialogue qui s'ouvre, sélectionnez l'onglet **Applications**.
 3. Dans la liste des applications installées sur l'hôte, sélectionnez Agent d'administration puis, cliquez sur **Propriétés**.

Lors de la modification des paramètres de l'Agent d'administration, la fenêtre des paramètres contient, en plus des onglets **Général** (cf. ill. ci-après) et **Événements**, les onglets **Paramètres**, **Stockages**, **Réseau**. Les options affichées sur cet onglet sont identiques à celles des onglets la boîte de dialogue paramètres de stratégie de l'Agent d'administration (cf. section "Configuration des paramètres de stratégie de l'Agent d'administration" à la page [88](#)).

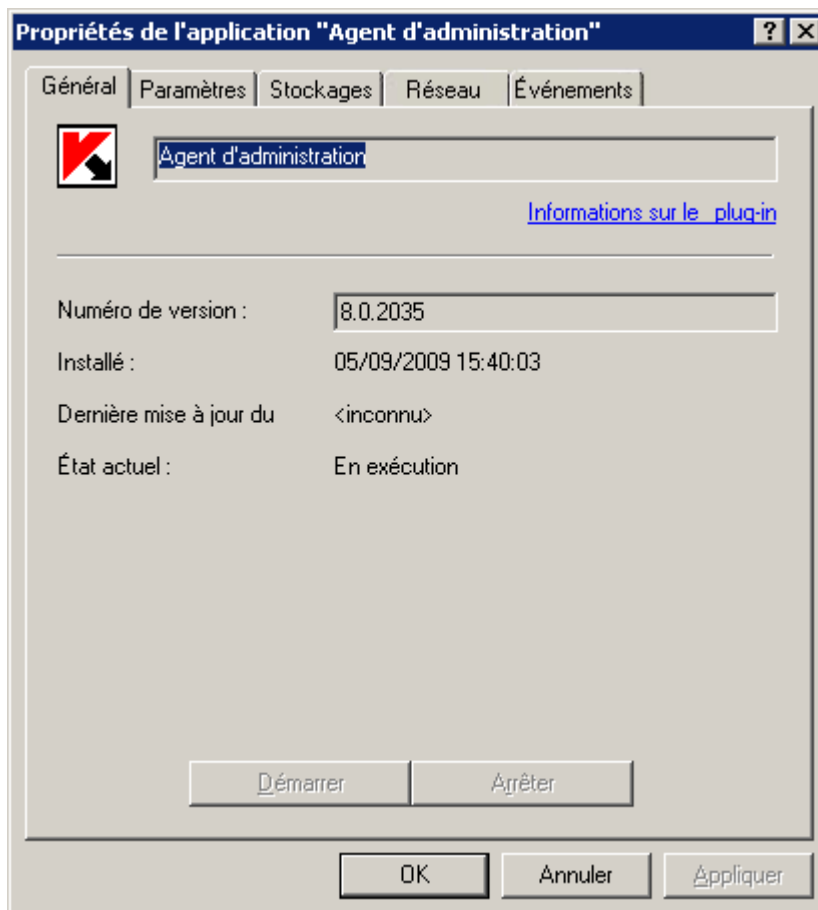


Illustration 103. Fenêtre de configuration de l'Agent d'administration. Onglet **Général**

Pour l'Agent d'administration installé sur l'ordinateur du Serveur, l'onglet **Réseau** n'est pas disponible (cf. ill. ci-après). La configuration des paramètres de connexion au Serveur d'administration n'est pas possible. Elle est réalisée par le programme en tenant compte des composants installés sur un ordinateur.

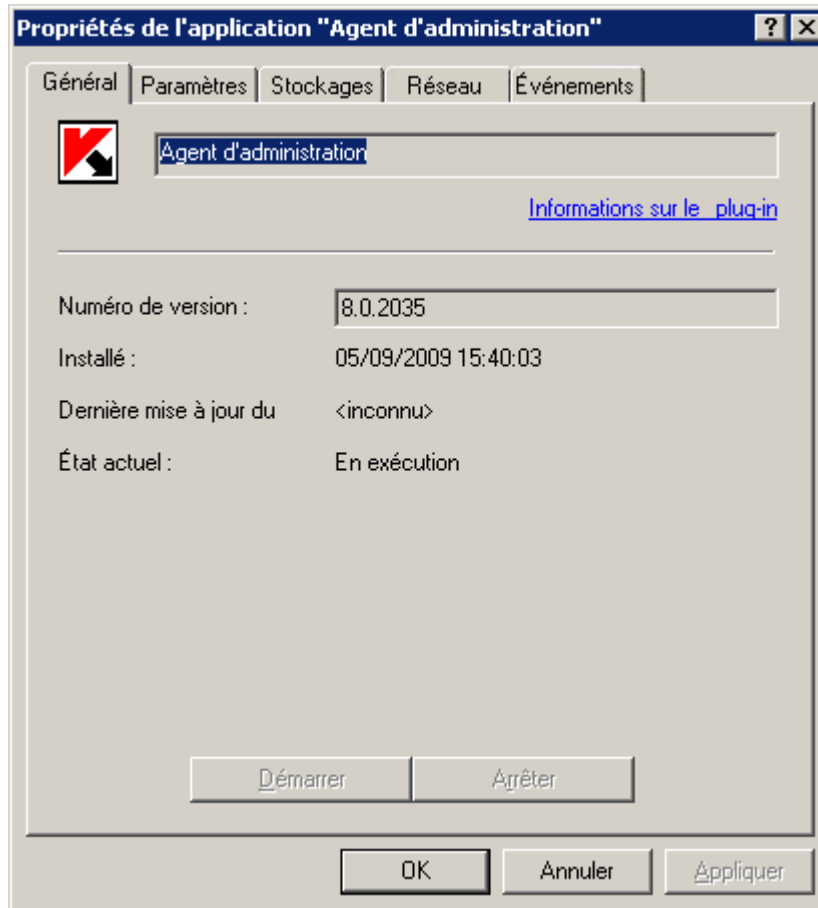


Illustration 104. Fenêtre de configuration des paramètres de l'Agent d'administration installé conjointement avec le Serveur

POSTES CLIENTS

Les postes clients qui figurent dans un groupe d'administration quelconque apparaissent dans le tableau sur le panneau des résultats du sous-dossier **Postes clients**.

DANS CETTE SECTION

Ajout d'ordinateurs à un groupe	139
Affichage d'informations relatives au poste client.....	140
Affichage d'informations sur le système du poste client.....	144
Tâche de modification du Serveur d'administration.....	151
Tâche d'administration du poste client.....	154
Envoi du message à l'utilisateur du poste client.....	164
Connexion manuelle du poste client au Serveur d'administration. Utilitaire klmove.exe	167
Vérification de la connexion du poste client avec le Serveur d'administration.....	168
Utilitaire du diagnostic à distance des postes clients (klactgui).....	169

AJOUT D'ORDINATEURS A UN GROUPE

➤ *Pour inclure un ou plusieurs ordinateurs dans un groupe d'administration défini, procédez comme suit :*

1. Ouvrez le dossier **Ordinateurs administrés**.
2. Sélectionnez le dossier correspondant au groupe dans lequel vous souhaitez ajouter les postes clients.

Si l'ordinateur est ajouté au niveau supérieur de la hiérarchie, sélectionnez le dossier **Ordinateurs administrés**.
3. Sélectionnez le dossier **Postes clients**.
4. Ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Ordinateur**.
5. Cette action lance un Assistant. Suivez ses instructions et définissez le mode d'ajout des postes clients et composez la liste des ordinateurs appartenant au groupe.

Si vous avez choisi le mode d'ajout automatique des ordinateurs (options **Automatiquement, sur la base des données du Serveur d'administration**), alors la liste sera composée sur la base des données obtenues par le Serveur d'administration lors du sondage du réseau Windows de l'entreprise, des plages IP ou des groupes Active Directory. Dans ce cas, la fenêtre de sélection des ordinateurs contient le dossier **Ordinateurs non définis**. Ordinateurs à ajouter à ce groupe. Vous pouvez sélectionner des ordinateurs de dossiers différents ou bien tous les ordinateurs du groupe.

Si vous choisissez d'ajouter manuellement des ordinateurs, vous devrez créer une liste d'ordinateurs dans ce groupe. Vous pouvez créer la liste des adresses dans la fenêtre de l'Assistant à l'aide des boutons **Ajouter** et **Supprimer**, ou l'importer depuis un fichier texte à l'aide du bouton **Importer**. Pour les adresses du poste, utilisez des adresses IP (ou une plage d'adresses IP) ou des noms des postes sur le réseau Windows. Pour importer la liste à partir d'un fichier, parcourez vos dossiers pour retrouver le fichier .txt contenant les adresses d'ordinateurs à ajouter. Chaque adresse doit figurer sur une ligne séparée.

En cas d'ajout manuel d'ordinateurs (sur la base des données saisies par l'administrateur), l'exactitude des informations est vérifiée pour éviter les conflits de nom et garantir leur unicité. Si la base de données du Serveur d'administration dispose d'informations sur l'existence de cet ordinateur dans le réseau Windows, alors l'ordinateur sera intégré au groupe.

Pour accéder rapidement à l'Assistant d'ajout d'ordinateurs dans l'arborescence de la console, ouvrez le dossier **Ordinateurs administrés**, sélectionnez le groupe auquel vous souhaitez ajouter le poste client et utilisez le lien **Ajouter les ordinateurs dans le groupe** situé dans le groupe **Administration des groupes** sous l'onglet **Groupes** du panneau des tâches.

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

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

AFFICHAGE D'INFORMATIONS RELATIVES AU POSTE CLIENT

► *Pour afficher les informations relatives au poste client repris dans le groupe d'administration, procédez comme suit :*

1. Dans le dossier **Ordinateurs administrés** sélectionnez un dossier portant le nom du groupe contenant le poste client et ouvrez le dossier **Postes clients**.

La liste des clients appartenant à ce groupe sera affichée dans le panneau des résultats.

2. Sélectionnez l'ordinateur sur lequel vous souhaitez obtenir des informations et utilisez la commande **Propriétés** du menu contextuel.

La boîte de dialogue **Propriétés de <Nom de poste>** s'affiche avec plusieurs onglets (cf. ill. ci-après).

Pour retrouver le poste client recherché, utilisez la fonction de recherche (cf. section "Recherche" à la page [298](#)).

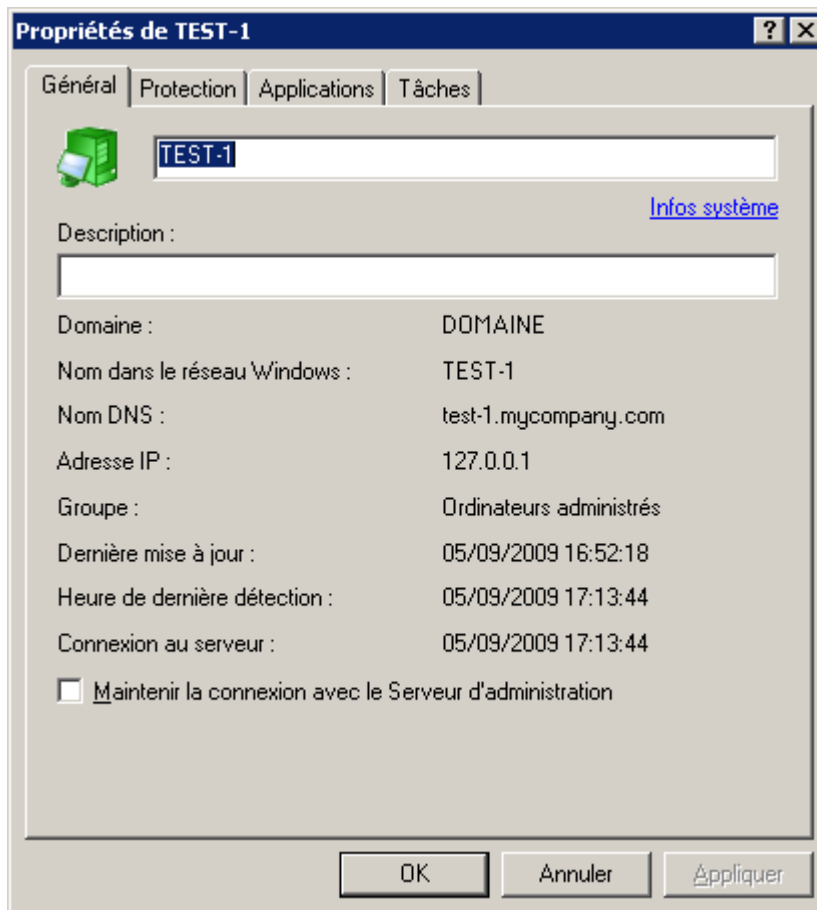


Illustration 105. Affichage des propriétés d'un poste client. Onglet **Général**

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez :

- Afficher les paramètres de réseau de l'ordinateur.
- Modifier le nom du poste client dans le groupe d'administration. Ce nom est généralement attribué par le Serveur d'administration ; il correspond au nom de l'ordinateur sur le réseau Windows.
- Saisir une description du poste.
- Définir la nature de la connexion entre le poste client et le Serveur d'administration en sélectionnant **Maintenir la connexion avec le Serveur d'administration**. Si l'option est sélectionnée, la connexion entre le Serveur d'administration et le poste client ne s'interrompra pas. Si elle n'est pas cochée (par défaut), le poste client ne se connectera au Serveur d'administration que pour synchroniser ou échanger des données.

Il convient de définir une connexion permanente uniquement avec les postes clients les plus importants, car le Serveur d'administration ne soutient pas plus de 1500 connexions en même temps.

- Obtenir des informations sur le système dans la fenêtre **Informations relatives au système** (cf. section "**Affichage d'informations sur le système du poste client**" à la page [144](#)), qui s'ouvre via le lien **Info système**. Cette fenêtre reprend les informations relatives aux éléments matériels et logiciels du poste client des utilisateurs connectés à l'ordinateur.

Toutes les informations sont transmises sur la base des données reçues lors de la dernière synchronisation du poste client avec le Serveur d'administration.

L'onglet **Protection** (cf. ill. ci-après) affiche l'état actuel de la protection antivirus sur un poste client. Il affiche les informations suivantes :

- **Etat du poste** : indicateur d'état du poste client, attribué d'après les critères de diagnostic de la protection antivirus et de l'activité réseau du poste, tels que déterminés par l'administrateur. Le champ situé en dessous de l'état répertorie les conditions définissant les états du poste client.
- **Etat de la protection en temps réel** : situation actuelle de la protection en temps réel du poste client.
- **Dernière analyse à la demande** : date et heure de la dernière analyse antivirus du poste client.
- **Virus trouvés** : nombre de virus détectés sur le poste client (compteur des virus détectés) depuis l'installation de l'application antivirus (première analyse de l'ordinateur) ou depuis la dernière remise à zéro du compteur. Pour remettre à zéro le compteur, cliquez sur **Remettre à zéro**.

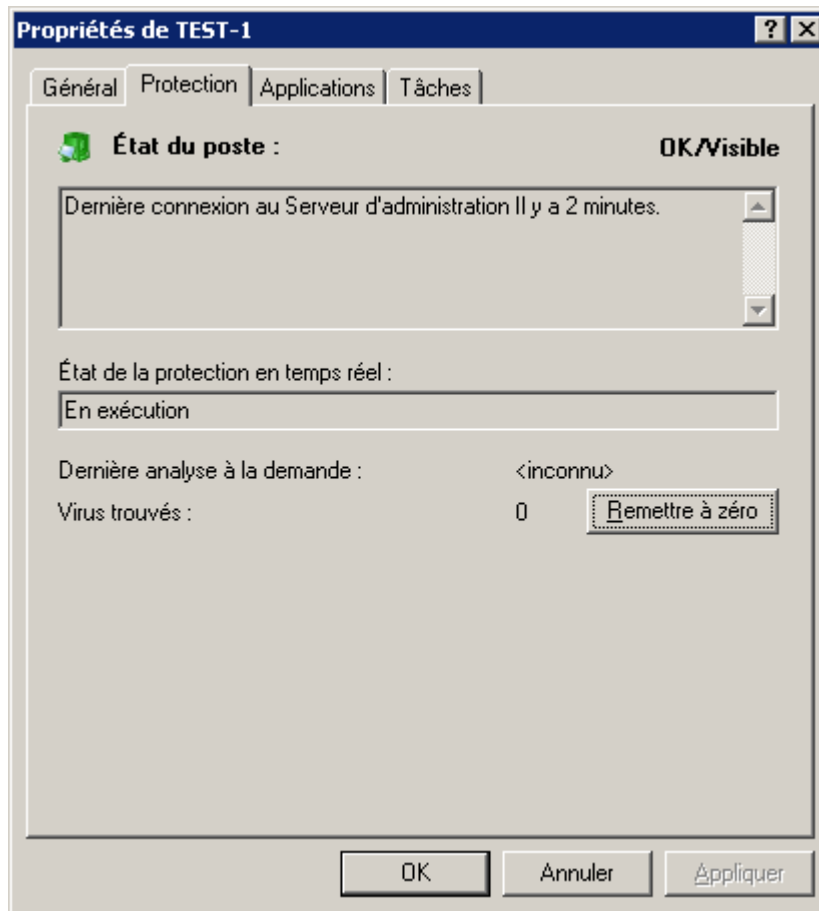


Illustration 106. Affichage des propriétés d'un poste client. Onglet **Protection**

L'onglet **Applications** (cf. ill. ci-après) énumère toutes les applications de Kaspersky Lab installées sur le poste client. Vous pouvez afficher des informations générales sur une application, contrôler son exécution, et configurer ses paramètres (cf. section "Paramètres locaux d'application" à la page [133](#)).

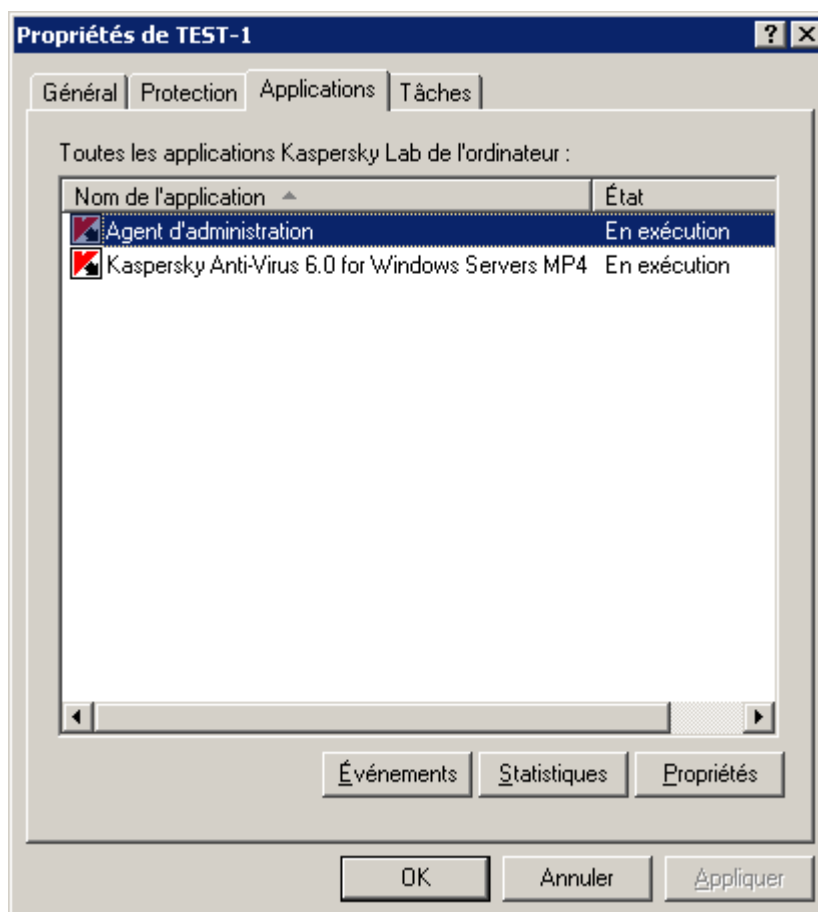


Illustration 107. Affichage des propriétés d'un poste client. Onglet **Applications**

Sur l'onglet **Tâches** (cf. ill. ci-après) vous pouvez contrôler des tâches pour des postes clients (afficher des tâches existantes, les supprimer et en créer de nouvelles, les lancer et les interrompre, modifier leurs paramètres, et afficher les comptes-rendus d'exploitation). La liste des tâches est proposée sur la base des données reçues lors de la dernière synchronisation du client avec le Serveur. Le Serveur d'administration questionne le client au sujet de l'état courant de tâche. Si la connexion échoue, l'état n'est pas affiché.

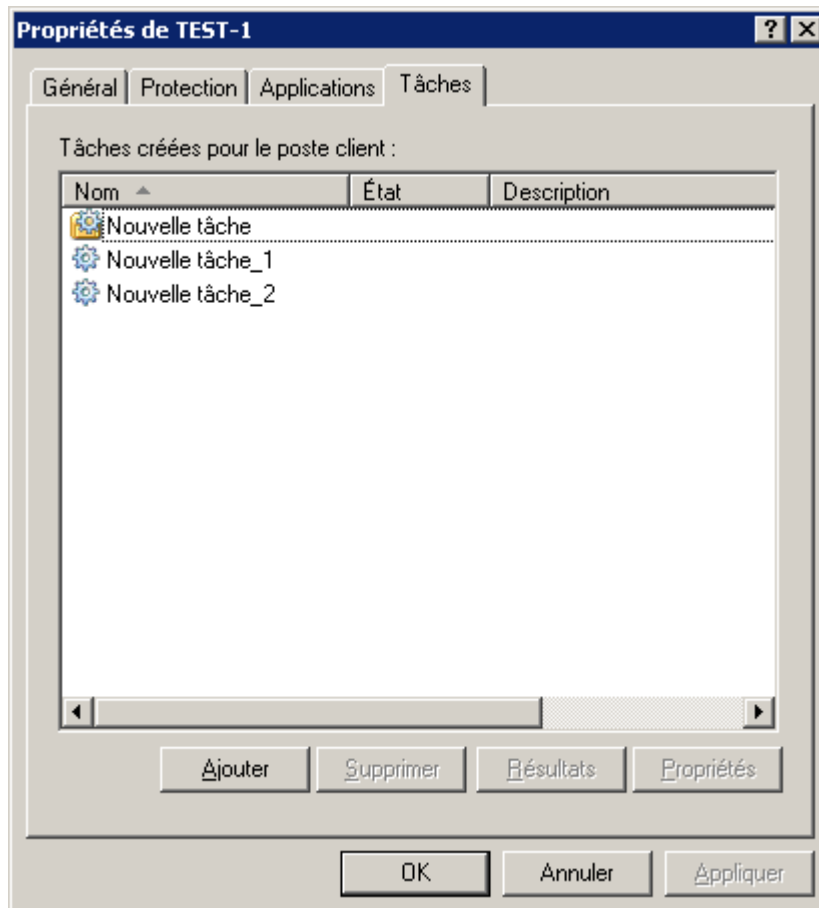


Illustration 108. Affichage des propriétés d'un poste client. Onglet **Tâches**

AFFICHAGE D'INFORMATIONS SUR LE SYSTEME DU POSTE CLIENT

La fenêtre **Informations sur le système** contient des informations détaillées sur le système du poste client et propose les onglets suivants :

- **Général** (cf. ill. ci-après).

Cet onglet propose les informations relatives au système d'exploitation et au matériel du poste client.

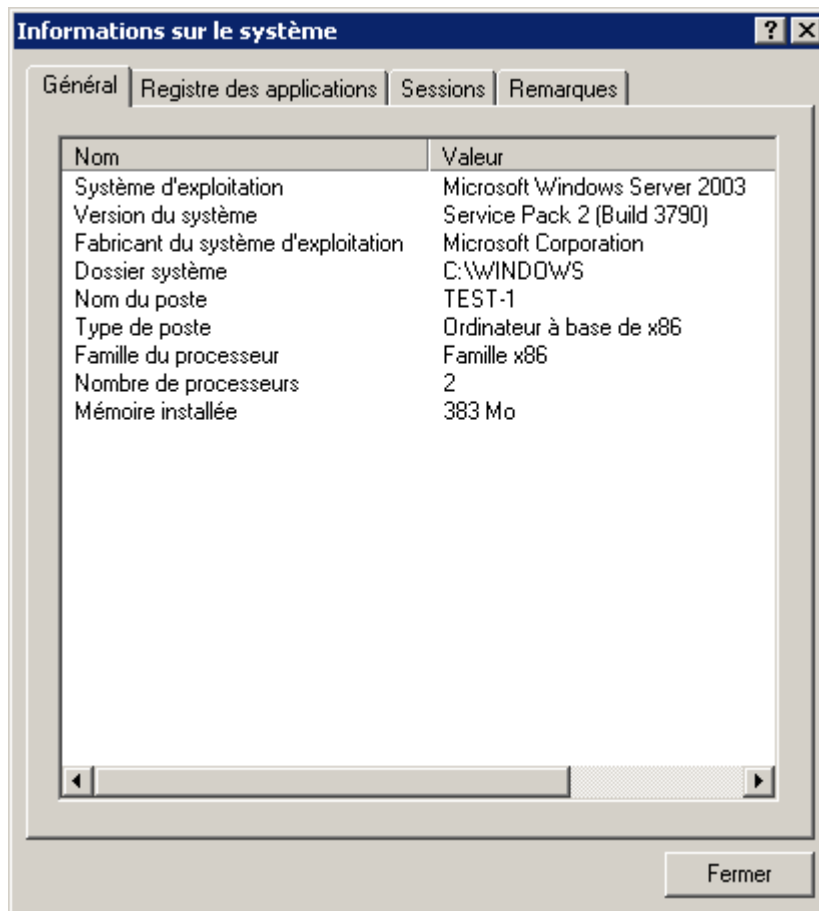


Illustration 109. Fenêtre de consultation des informations sur le système du poste client. Onglet **Général**

- **Registre des applications** (cf. ill. ci-après).

Cet onglet contient une liste des programmes installés sur le poste client.

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

Cochez la case **Afficher uniquement les applications de sécurité incompatibles**, si vous souhaitez que la liste des applications reprenne uniquement les applications de sécurité incompatibles avec les applications de Kaspersky Lab.

Si vous souhaitez que la liste reprenne les paquets de mise à jour installés, cochez la case **Afficher les mises à jour**.

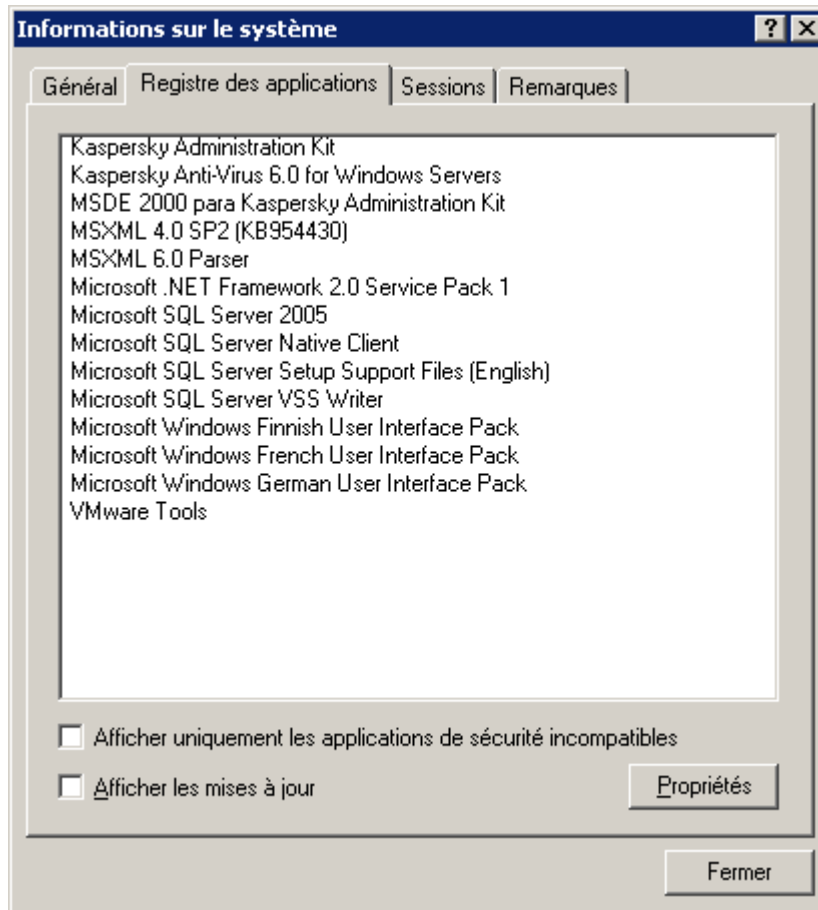


Illustration 110. Fenêtre de consultation des informations sur le système du poste client. Onglet **Registre des applications**

Pour obtenir les informations relatives à une application en particulier, sélectionnez-la dans la liste puis cliquez sur **Propriétés**. La fenêtre qui s'ouvre (cf. ill. ci-après) reprendra les informations relatives à l'application sur la base des données du registre.

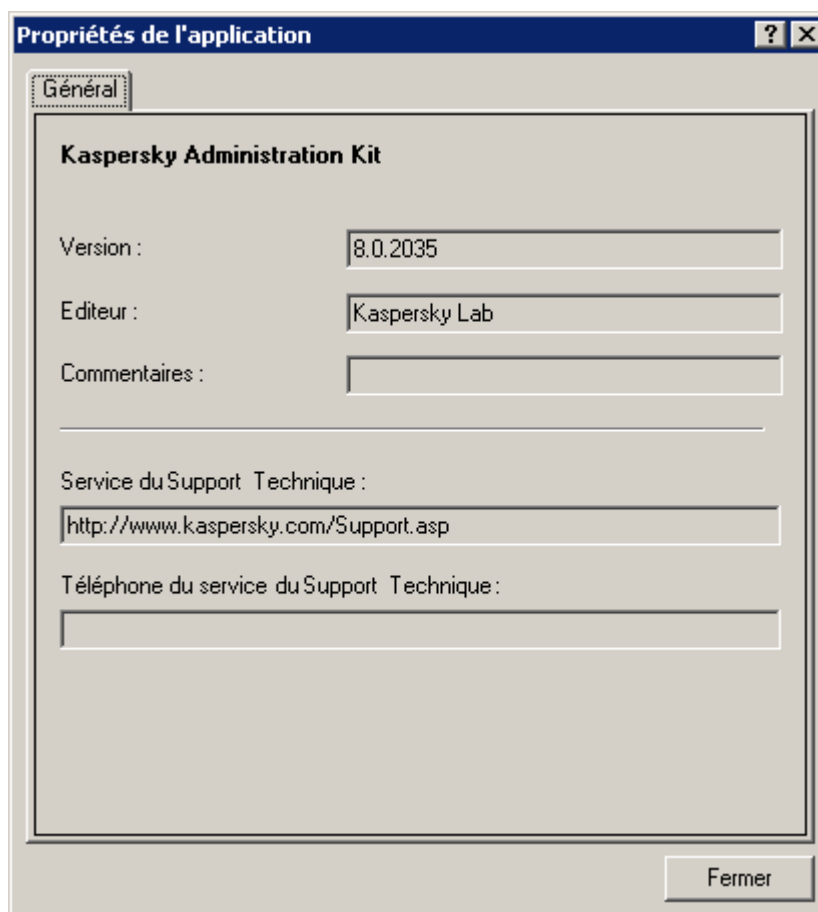


Illustration 111. Fenêtre de consultation des informations sur l'application

- **Sessions** (cf. ill. ci-après).

Cet onglet propose les informations relatives aux sessions actuelles de travail avec le poste client. En fonction des données obtenues du poste client, les informations suivantes sont reprises dans le tableau pour chaque session :

- **Nom** ;
- **Nom du participant** ;
- **Compte** ;

- **Courrier électronique.**

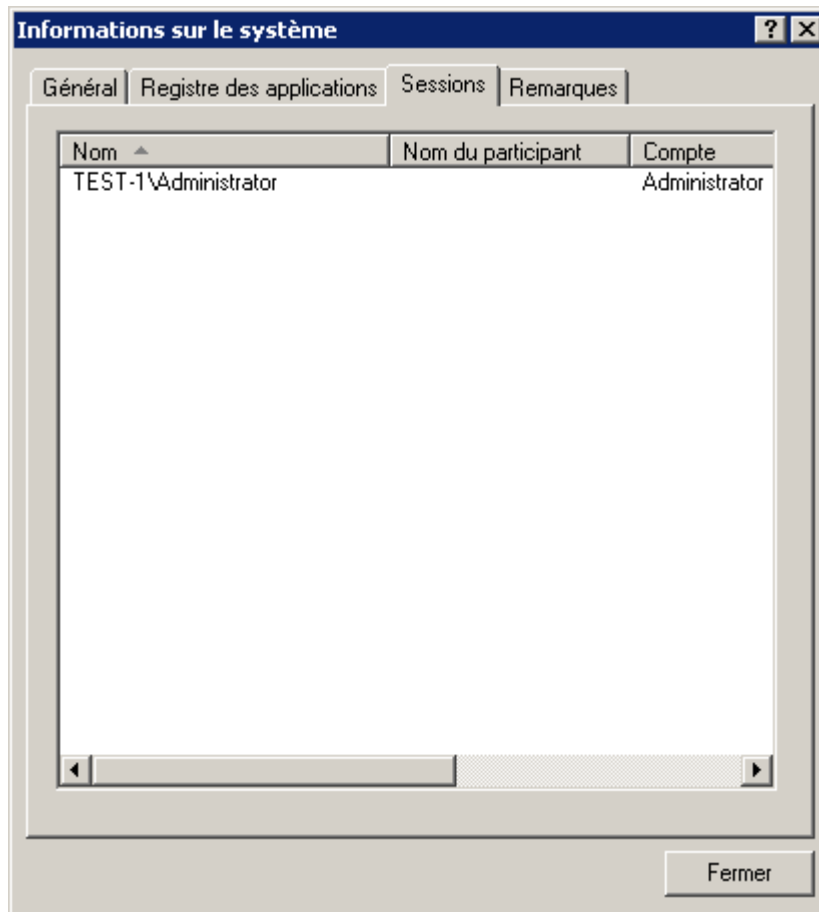


Illustration 112. Fenêtre de consultation des informations sur le système du poste client. Onglet **Sessions**

- **Remarques** (cf. ill. ci-après).

Cet onglet vous permet de rédiger, de lire ou de modifier des remarques. Vous pouvez inclure dans ces remarques toutes les informations dont vous avez besoin sur le poste client. Pour faciliter l'utilisation, il est possible de définir des degrés d'importance.

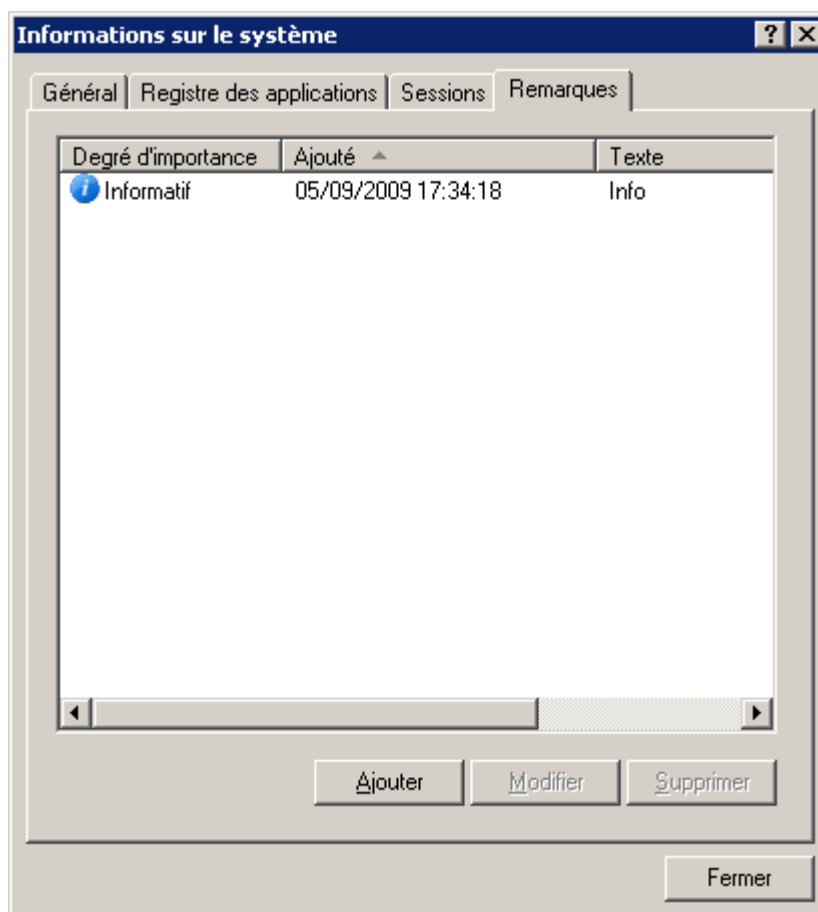


Illustration 113. Fenêtre de consultation des informations sur le système du poste client. Onglet **Remarques**

Pour ajouter une nouvelle remarque, cliquez sur le bouton **Ajouter** et dans la fenêtre qui s'ouvre (cf. ill. ci-après) :

- Sélectionnez le degré d'importance dans la liste déroulante : **Informatif**, **Critique**, **Avertissement**.

- Dans le champ **Texte de la remarque** saisissez le texte. La colonne Texte de la liste des remarques (cf. ill. ci-dessus) reprendra les premiers mots du texte saisi.

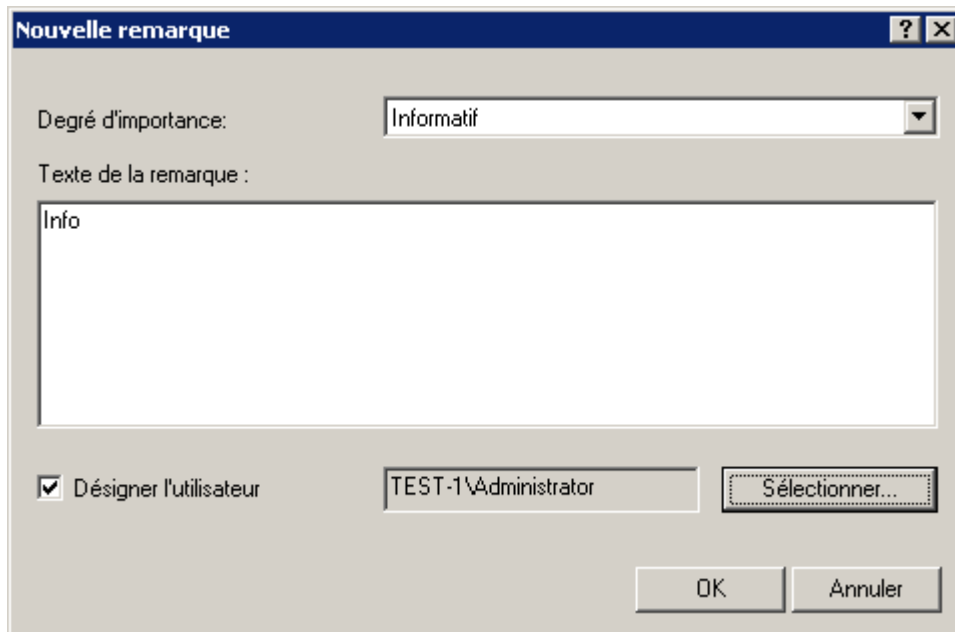


Illustration 114. Création d'une nouvelle remarque

- Si la remarque concerne un utilisateur particulier de l'ordinateur, cochez la case **Désigner l'utilisateur** et à l'aide du bouton **Sélectionner** sélectionnez l'utilisateur requis dans la fenêtre qui s'ouvre (cf. ill. ci-après).

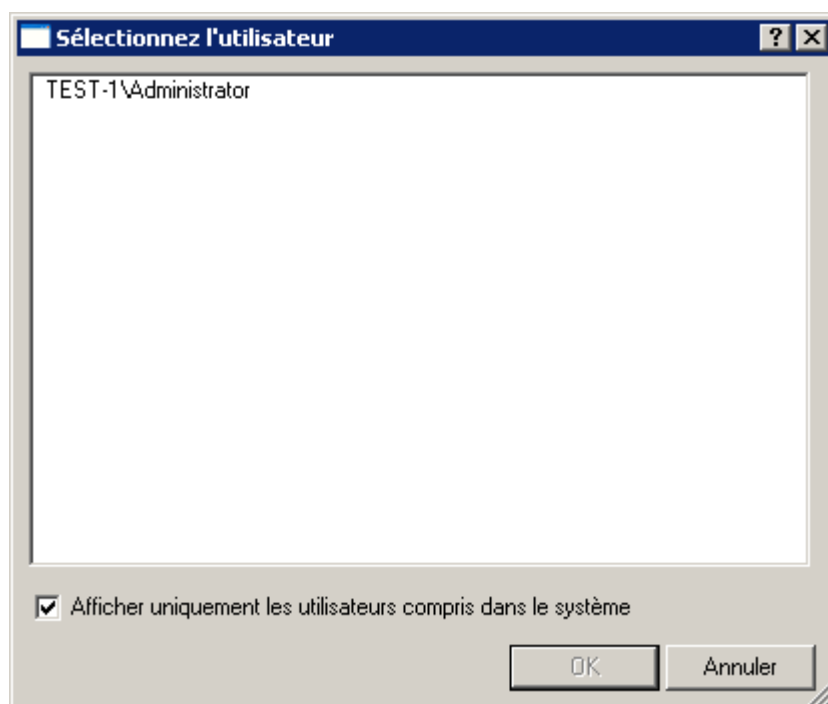


Illustration 115. Modification d'une remarque. Sélection de l'utilisateur

Afin que les utilisateurs qui se sont connectés au système sur cet ordinateur s'affichent dans la liste, cochez la case **Afficher uniquement les utilisateurs compris dans le système**. Si la case n'est pas cochée, la liste reprendra tous les utilisateurs enregistrés sur les ordinateurs du groupe d'administration.

TACHE DE MODIFICATION DU SERVEUR D'ADMINISTRATION

➔ Pour créer une tâche de modification pour le Serveur d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page 22), qui gère les ordinateurs déplacés.
2. Lancer l'Assistant de création d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page 101) ou d'une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page 114).
3. Au moment de sélectionner l'application et de définir le type de tâche (cf. ill. ci-après), sélectionnez : **Kaspersky Administration Kit**, déployez le dossier **Avancé** et sélectionnez la tâche **Modification du Serveur d'administration**.

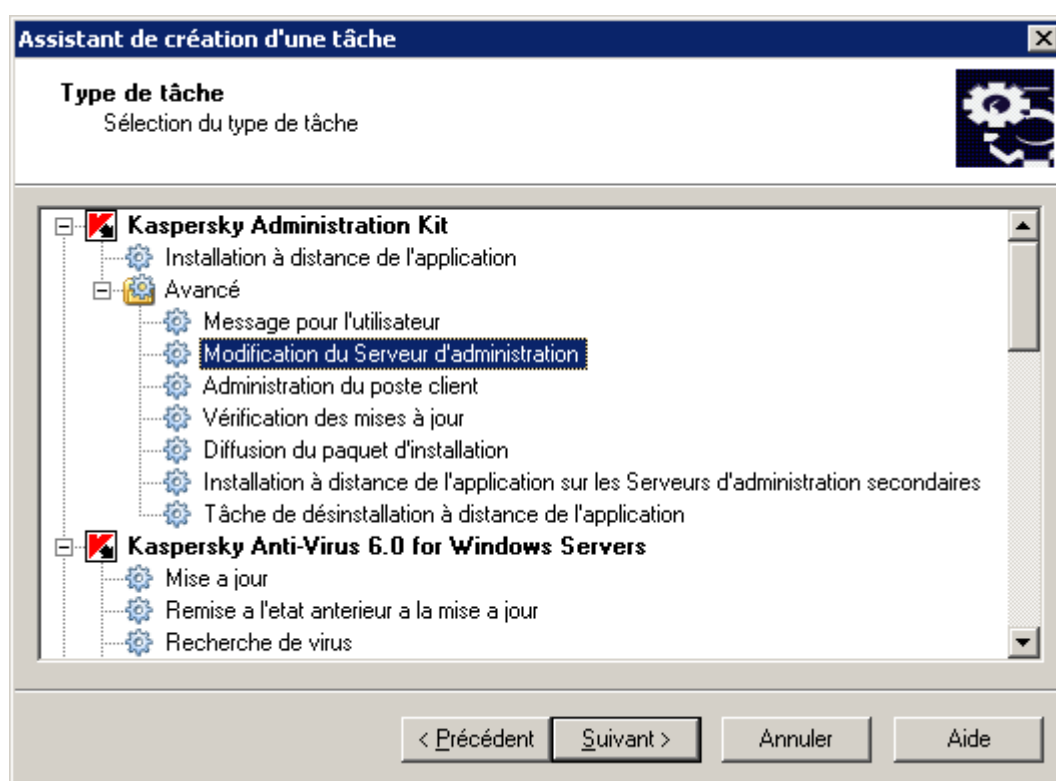


Illustration 116. Sélection de l'application à installer

4. A l'étape suivante (cf. ill. ci-après), définissez les paramètres employés par le composant Agent d'administration installé sur les postes clients, afin de se connecter au nouveau Serveur.

Illustration 117. Définition du Serveur et sélection du certificat.

Dans le groupe **Paramètres de connexion au Serveur d'administration** :

- Indiquez l'adresse du Serveur d'administration dans le groupe d'administration duquel les postes clients doivent être déplacés. En guise d'adresse, vous pouvez utiliser l'adresse IP ou le nom de l'ordinateur dans le réseau Windows.
- Définissez le numéro de port utilisé pour se connecter au nouveau Serveur d'administration. Le numéro de port par défaut est 14000.
- Définissez le numéro de port utilisé pour se connecter au nouveau Serveur d'administration par protocole SSL. Le numéro de port par défaut est 13000.
- Cochez la case **Utiliser le serveur proxy** si la connexion au Serveur d'administration s'opère via un serveur proxy. Dans le champ **Adresse du serveur proxy**, saisissez son adresse. Remplissez les champs **Nom d'utilisateur** et **Mot de passe** si l'authentification est requise pour accéder au serveur proxy.

Par la suite, vous pouvez changer les paramètres de tâche dans l'onglet **Paramètres** (cf. ill. ci-après) de la fenêtre des propriétés des tâches (cf. section "Affichage et modification des paramètres de tâche" à la page [117](#)).

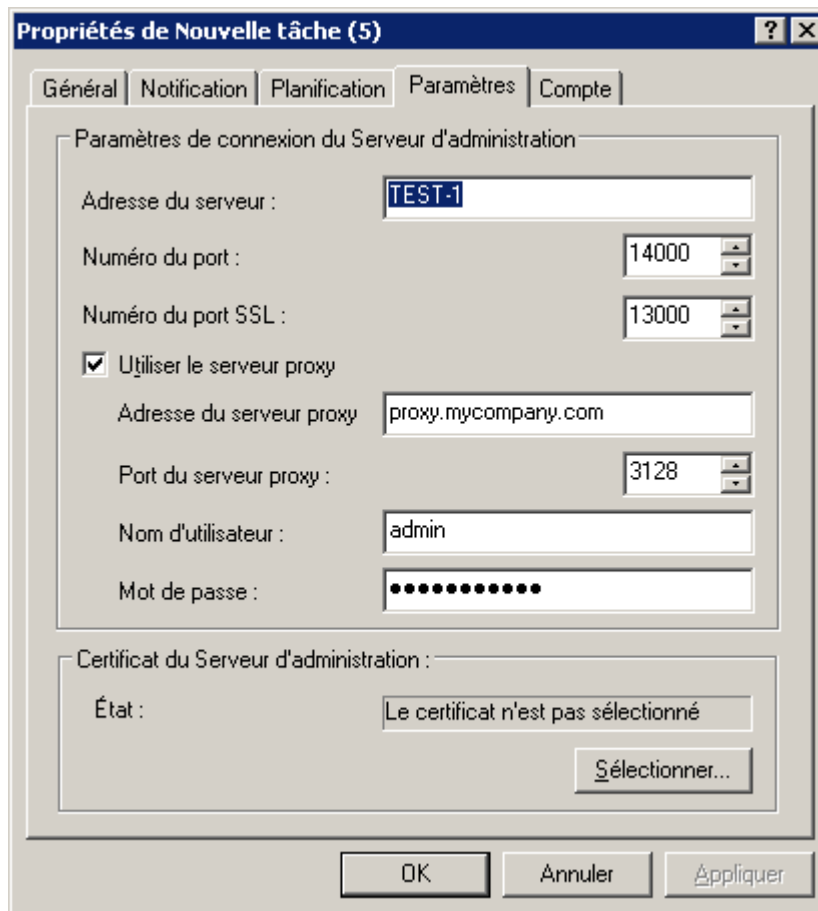


Illustration 118. Affichage des paramètres de la tâche de modification du Serveur d'administration.

Aussi dans cette fenêtre dans le groupe **Certificat du Serveur d'administration** à l'aide du bouton **Sélectionner**, il est possible de spécifier le fichier du certificat pour authentifier l'accès au nouveau Serveur d'administration.

Le fichier du certificat possède l'extension **.cer** et se trouve sur le Serveur d'administration sur lequel les ordinateurs sont déplacés dans le dossier Cert du dossier de destination indiqué lors de l'installation de Kaspersky Administration Kit. Vous pouvez copier le fichier de certification dans un dossier partagé ou un périphérique externe de sauvegarde. Cette copie peut être utilisée pour configurer des paramètres d'accès au Serveur de la copie du fichier.

- Si vous créez une tâche pour une sélection d'ordinateurs, vous devrez absolument composer une liste (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)) des postes clients sur lesquels la tâche sera exécutée. En cas de réussite de l'exécution de la tâche, ces ordinateurs seront déplacés dans le groupe d'administration défini dans les paramètres de la tâche du Serveur d'administration et placés dans le groupe **Ordinateurs non définis**.

Si vous créez une tâche de groupe, tous les clients du groupe sélectionné seront affectés à un nouveau Serveur d'administration. Pour le client où le Serveur d'administration est installé, la tâche de remplacement du Serveur ne pourra pas être exécutée.

- Pour compléter la création de la tâche, programmez celle-ci pour la lancer (cf. section "Création d'une tâche de groupe" à la page [101](#)) à une certaine heure.

TACHE D'ADMINISTRATION DU POSTE CLIENT

Kaspersky Administration Kit permet de gérer à distance les postes clients à l'aide des tâches suivantes :

- Allumer l'ordinateur (cf. section "Allumer le poste client" à la page [154](#)).
- Eteindre l'ordinateur (cf. section "Eteindre le poste client" à la page [157](#)).
- Redémarrer l'ordinateur (cf. section "Redémarrage du poste client" à la page [160](#)).

ALLUMER LE POSTE CLIENT

► Pour **Allumer l'ordinateur**, procédez comme suit :

1. Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page [22](#)), qui gère les ordinateurs déplacés.
2. Lancer l'Assistant de création d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)) ou d'une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)).
3. Sélectionnez le type de tâche (cf. ill. ci-après).

Pour ce faire, dans la fenêtre **Type de tâche** de l'Assistant des tâches dans l'entrée **Kaspersky Administration Kit** ouvrez le dossier **Avancé** et sélectionnez **Administration du poste client**.

4. Cliquez sur le bouton **Suivant**, pour continuer la création de la tâche de l'administration du poste client.

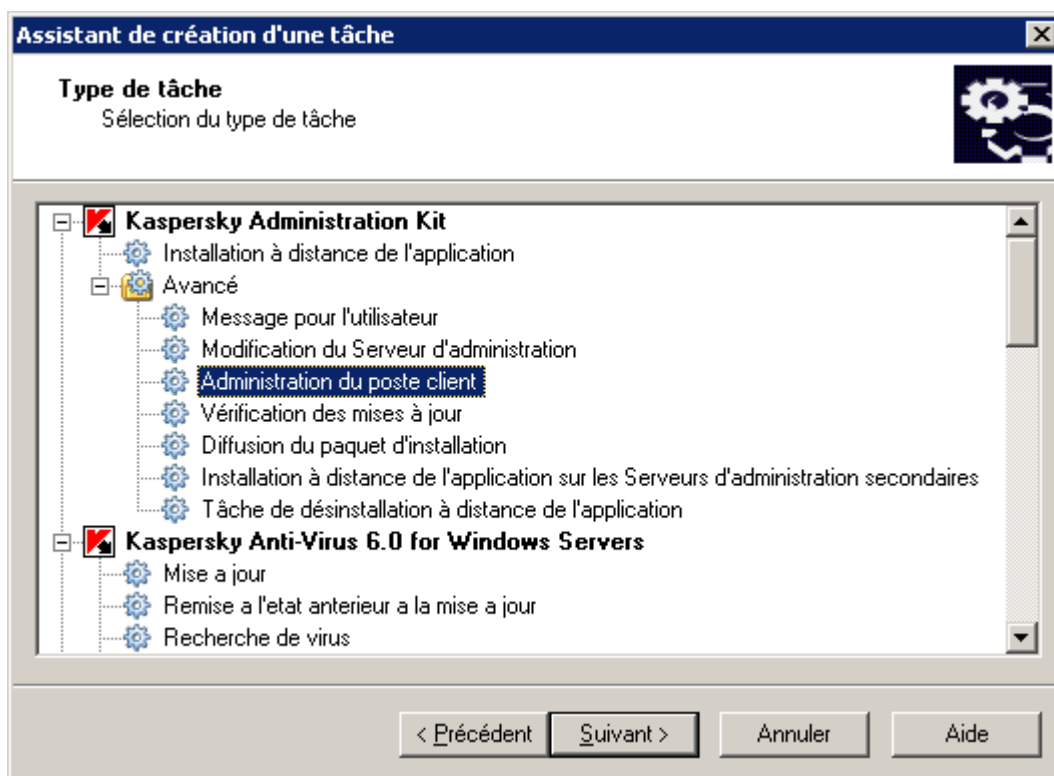


Illustration 119. Sélection du type de la tâche

5. Sélectionnez le point **Allumer l'ordinateur** dans la fenêtre **Paramètres** (cf. ill. ci-après).

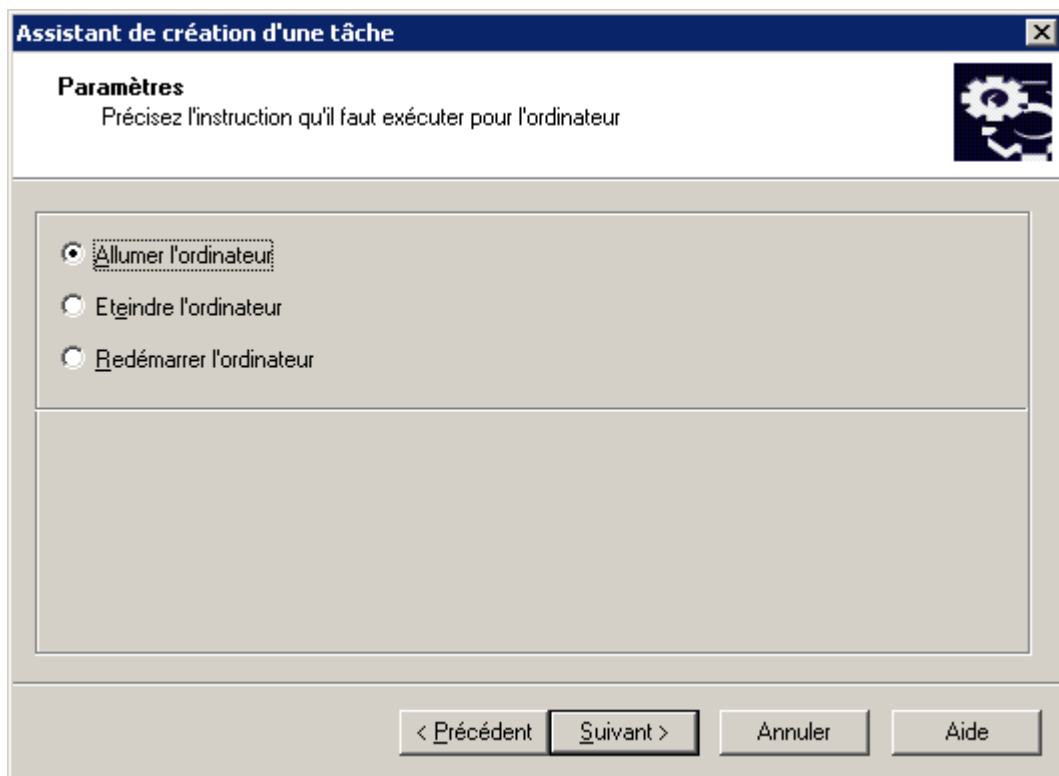


Illustration 120. Paramètres de la tâche

6. Sélectionnez les ordinateurs dans les groupes d'administration (cf. ill. ci-après), sur lesquels la tâche sera lancée. Cliquez sur **Suivant**.

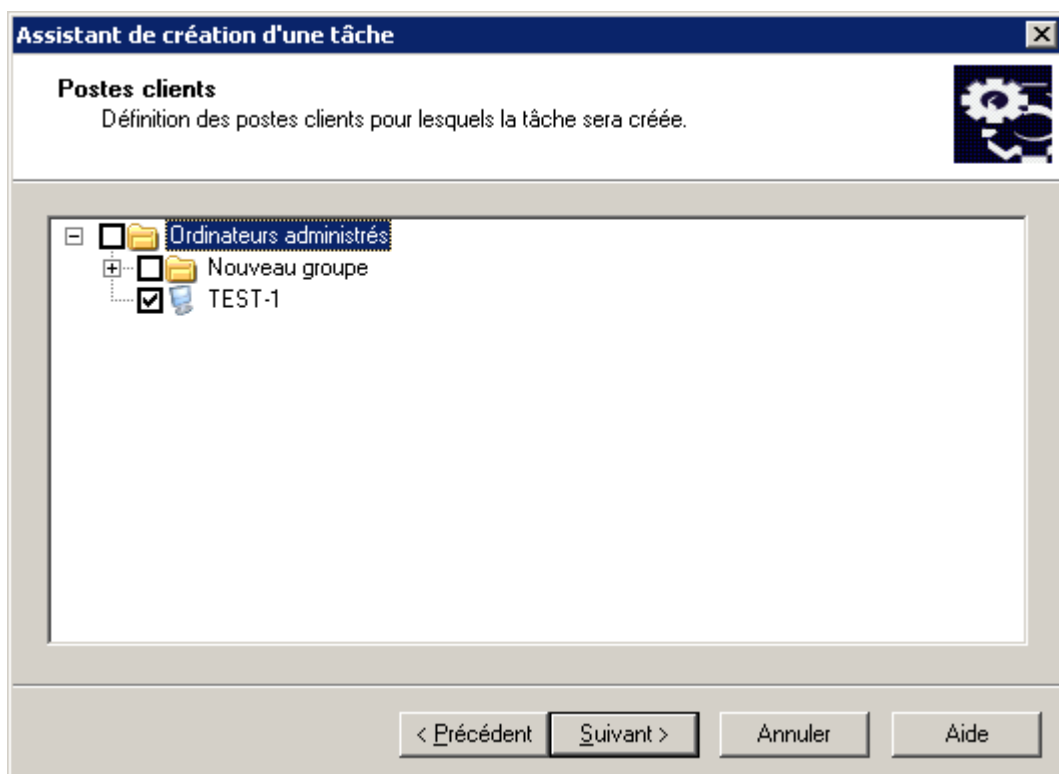


Illustration 121. Sélection de l'ordinateur

- Planifiez la tâche (cf. section "Création d'une tâche de groupe" à la page 101) (cf. ill. ci-après). Cliquez sur **Suivant**.

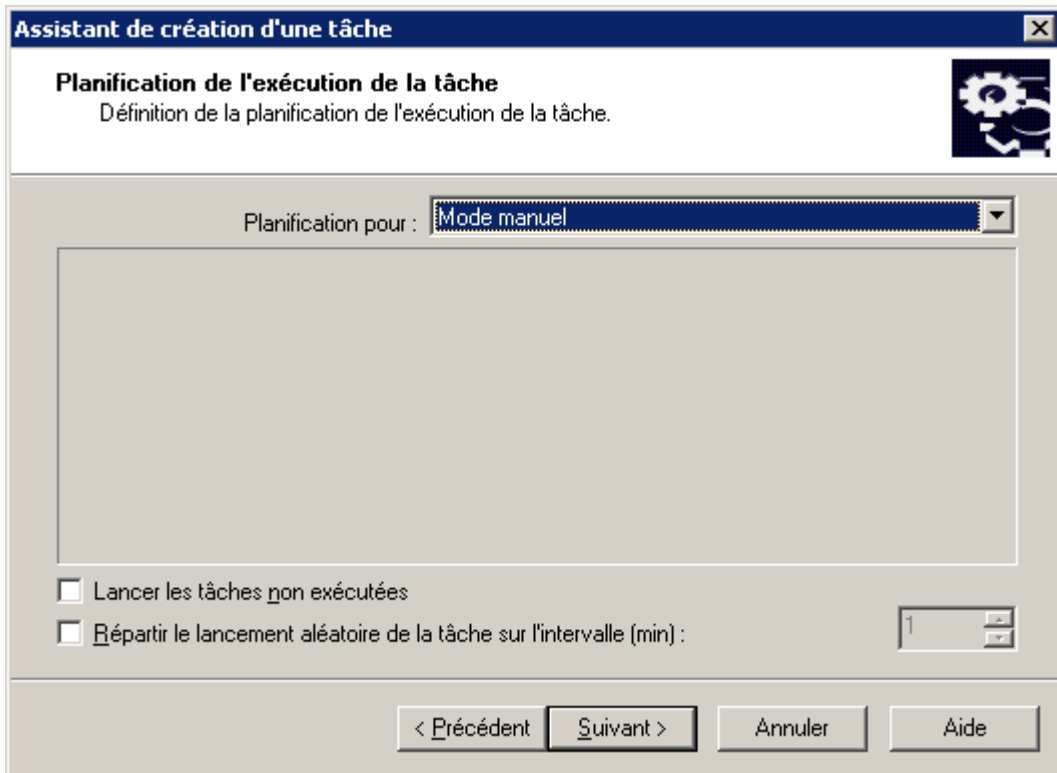


Illustration 122. Programmation de la tâche

- Appuyez sur le bouton **Terminer** (cf. ill. ci-après) pour terminer la création de la tâche.

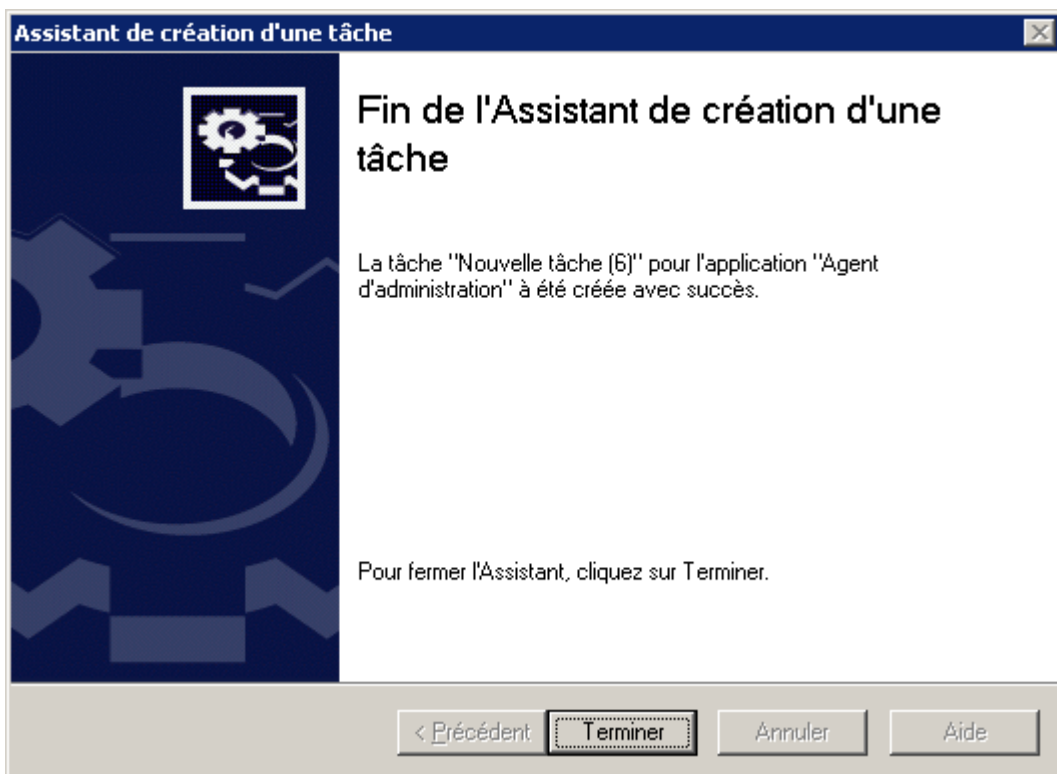


Illustration 123. Fin de la création d'une tâche

ETEINDRE LE POSTE CLIENT

➔ Pour **Eteindre l'ordinateur**, procédez comme suit :

1. Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page [22](#)), qui gère les ordinateurs déplacés.
2. Lancer l'Assistant de création d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)) ou d'une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)).
3. Sélectionnez le type de tâche (cf. ill. ci-après).

Pour ce faire, dans la fenêtre **Type de tâche** de l'Assistant des tâches dans l'entrée **Kaspersky Administration Kit** ouvrez le dossier **Avancé** et sélectionnez **Administration du poste client**.

4. Cliquez sur le bouton **Suivant**, pour continuer la création de la tâche de l'administration du poste client.

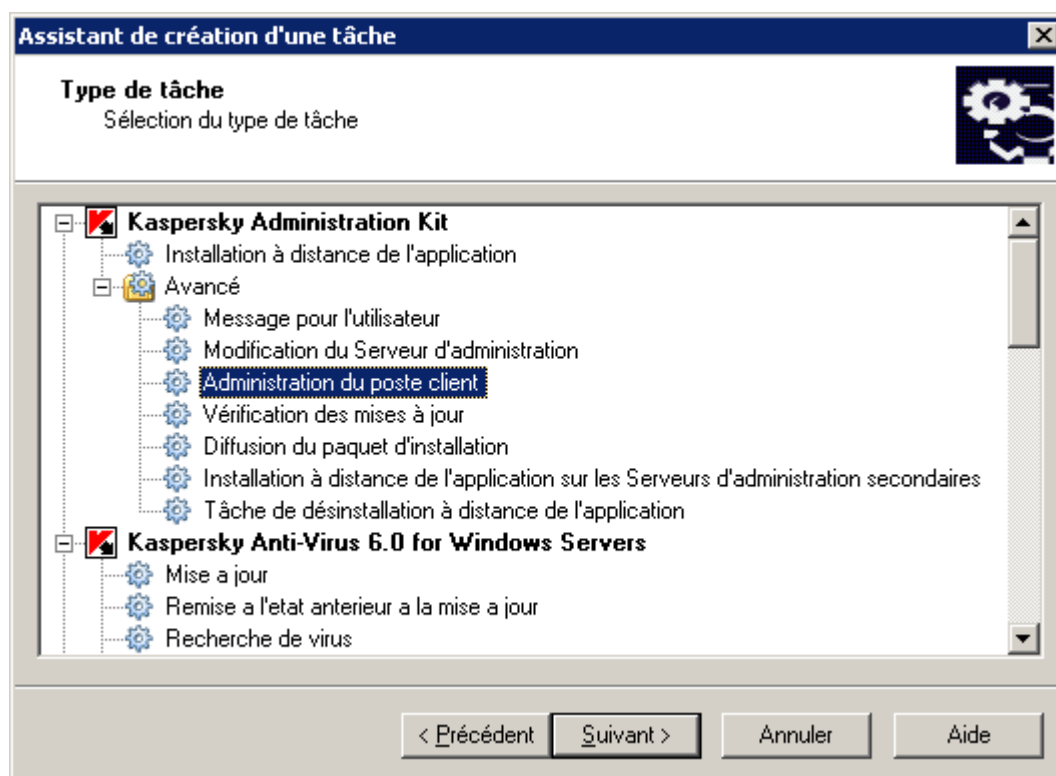


Illustration 124. Sélection du type de la tâche

5. Sélectionnez le point **Eteindre l'ordinateur** dans la fenêtre **Paramètres** (cf. ill. ci-après).

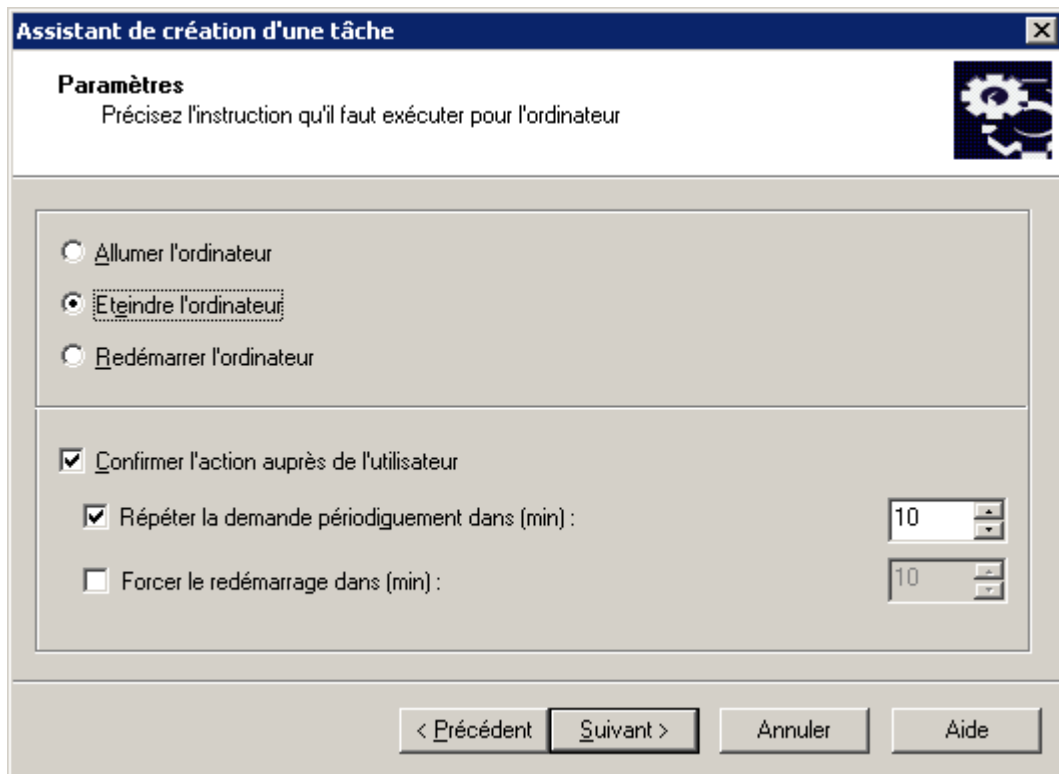


Illustration 125. Paramètres de la tâche

Si vous ne voulez pas que le Serveur demande la confirmation de l'exécution de la tâche au poste client, désélectionnez la case **Confirmer l'action auprès de l'utilisateur** dans la partie inférieure de la fenêtre (la case est cochée par défaut).

Dans le champ **Répéter la demande périodiquement dans (min.)** indiquez, dans combien de minutes Kaspersky Administration Kit demandera l'utilisateur confirmer l'arrêt (par défaut la période est de 10 minutes).

Dans le champ **Forcer l'arrêt après (min.)**, définissez l'intervalle de temps à l'issue duquel le Serveur d'administration réalisera le redémarrage (cf. ill. ci-dessus).

Cliquez sur **Suivant**.

6. Sélectionnez les ordinateurs dans les groupes d'administration (cf. ill. ci-après), sur lesquels la tâche sera lancée. Cliquez sur **Suivant**.

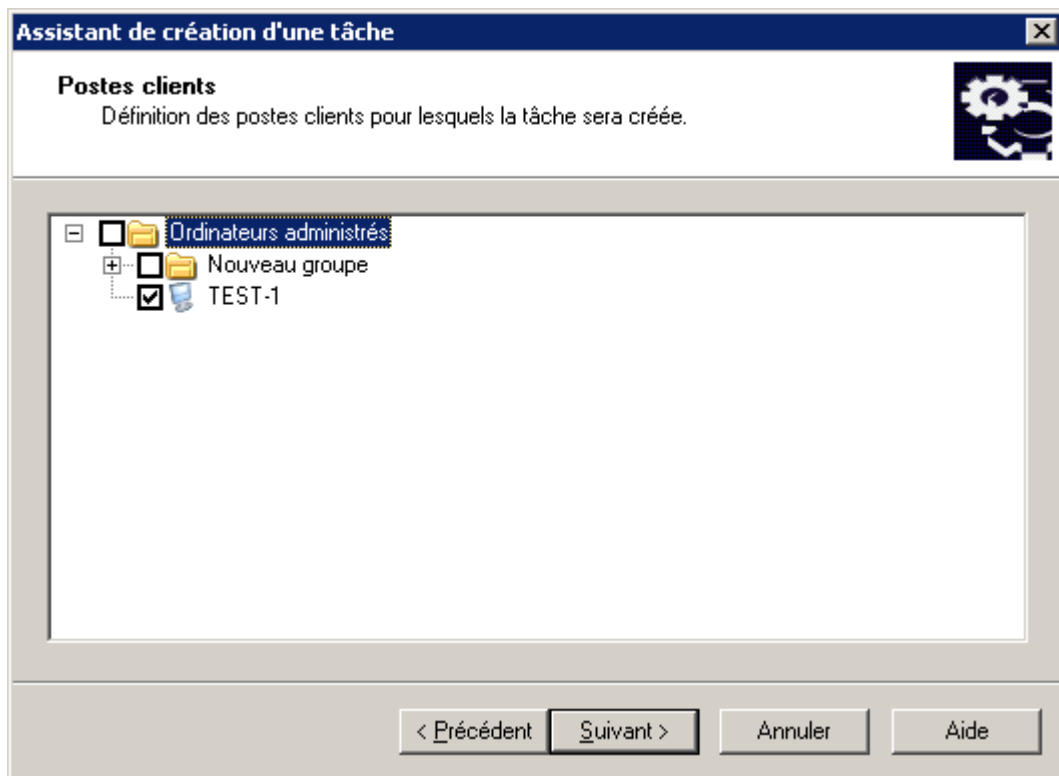


Illustration 126. Sélection de l'ordinateur

7. Planifiez la tâche (cf. section "Création d'une tâche de groupe" à la page [101](#)) (cf. ill. ci-après). Cliquez sur **Suivant**.

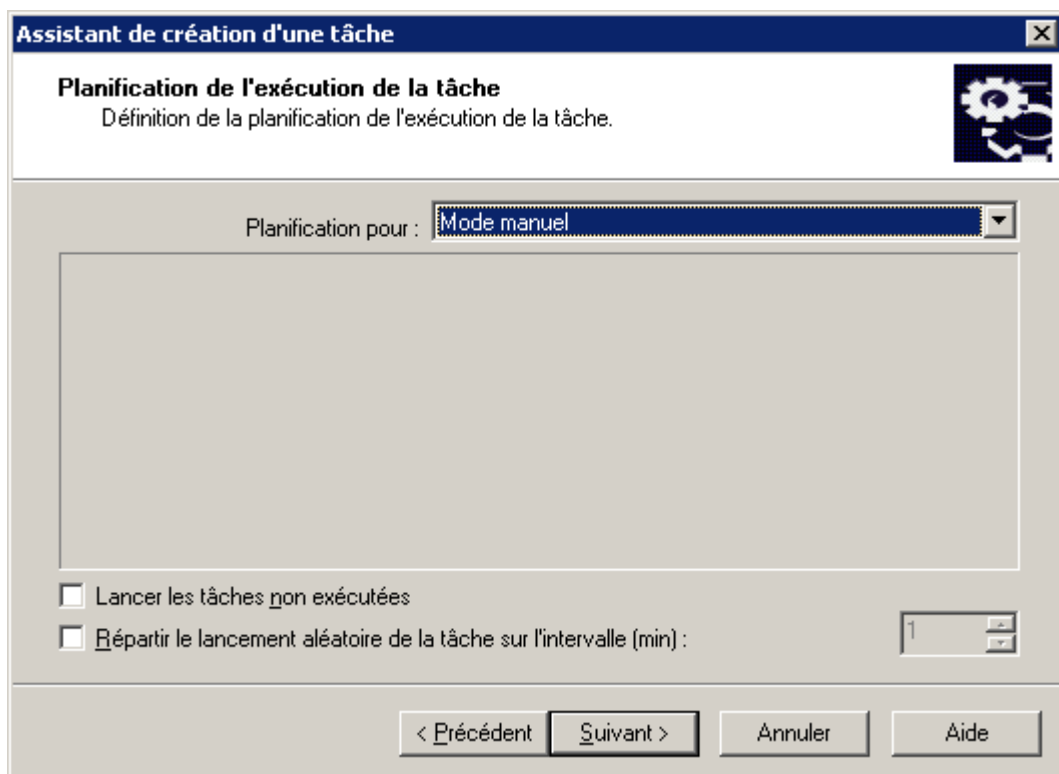


Illustration 127. Programmation de la tâche

- Appuyez sur le bouton **Terminer** (cf. ill. ci-après) pour terminer la création de la tâche.

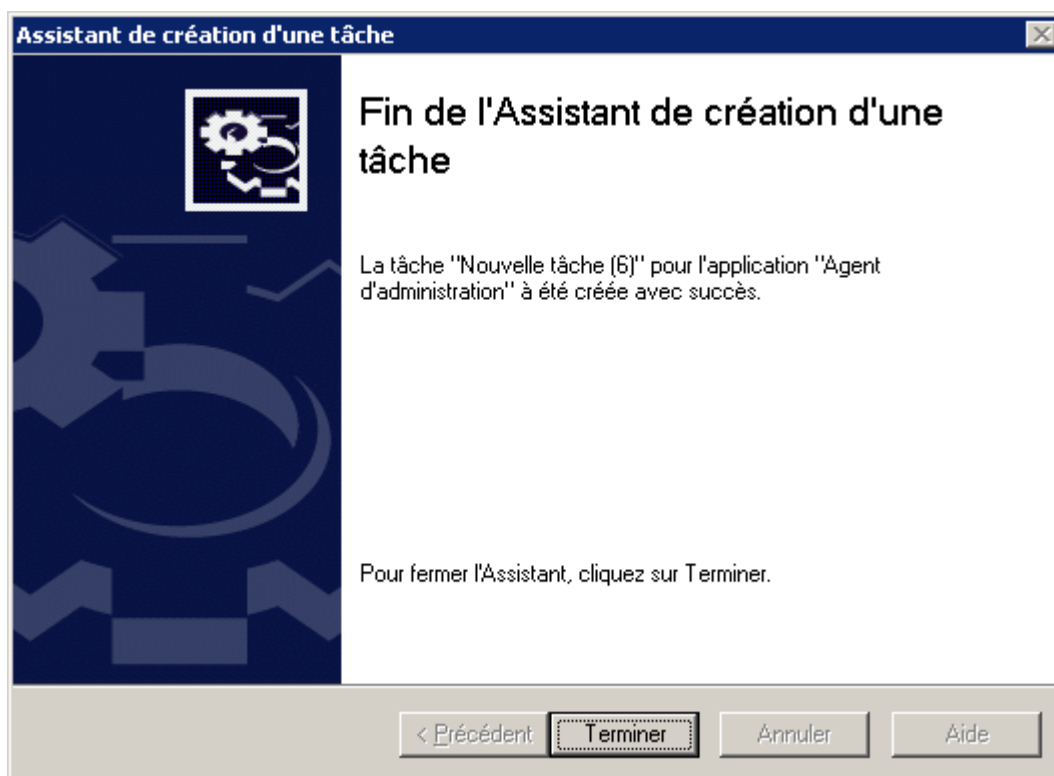


Illustration 128. Fin de la création d'une tâche

REDEMARRAGE DU POSTE CLIENT

➔ Pour **Redémarrer l'ordinateur**, procédez comme suit :

- Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page [22](#)), qui gère les ordinateurs déplacés.
- Lancer l'Assistant de création d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)) ou d'une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)).
- Sélectionnez le type de tâche (cf. ill. ci-après).

Pour ce faire, dans la fenêtre **Type de tâche** de l'Assistant des tâches dans l'entrée **Kaspersky Administration Kit** ouvrez le dossier **Avancé** et sélectionnez **Administration du poste client**.

4. Cliquez sur le bouton **Suivant**, pour continuer la création de la tâche de l'administration du poste client.

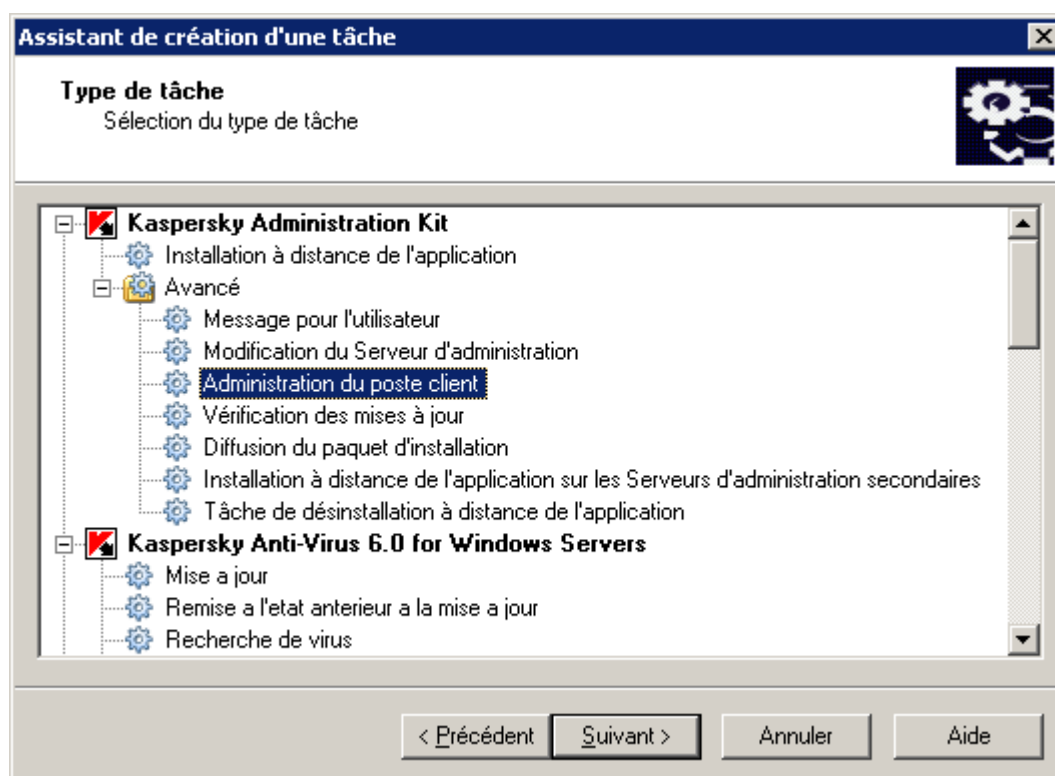


Illustration 129. Sélection du type de la tâche

5. Sélectionnez le point **Redémarrer l'ordinateur** dans la fenêtre **Paramètres** (cf. ill. ci-après).

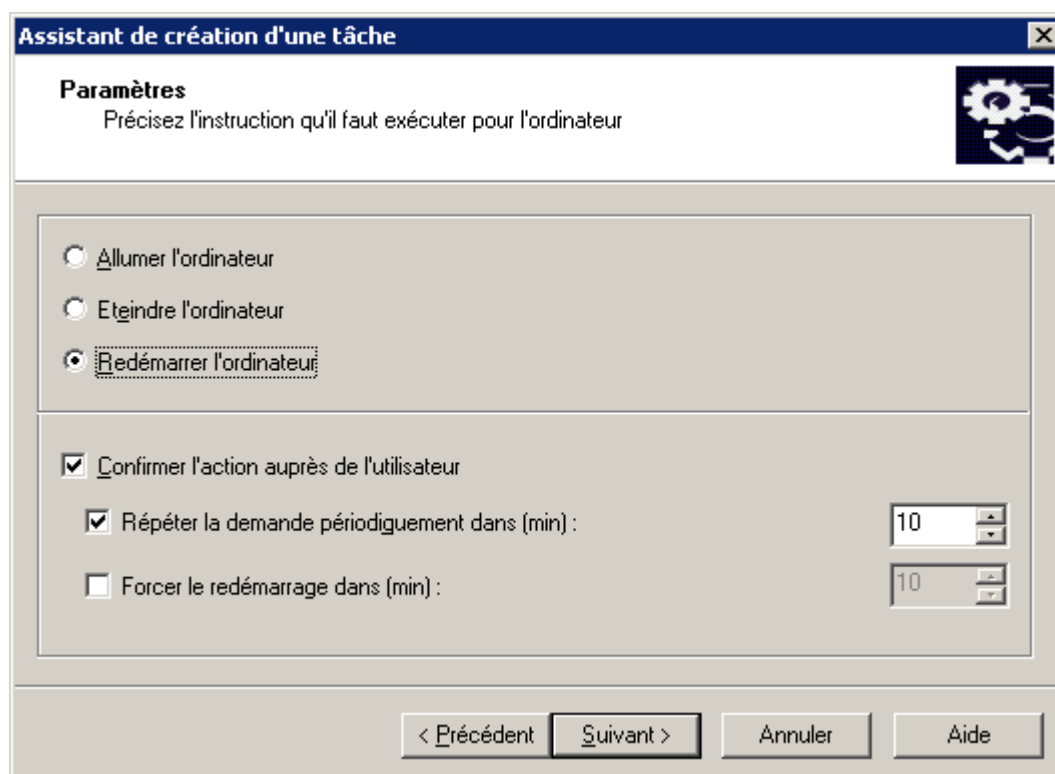


Illustration 130. Paramètres de la tâche

Si vous ne voulez pas que le Serveur demande la confirmation de l'exécution de la tâche au poste client, désélectionnez la case **Confirmer l'action auprès de l'utilisateur** dans la partie inférieure de la fenêtre (la case est cochée par défaut).

Dans le champ **Répéter la demande périodiquement dans (min.)** indiquez, dans combien de minutes Kaspersky Administration Kit demandera l'utilisateur confirmer l'exécution de la commande (par défaut la période est de 10 minutes).

Dans le champ **Forcer le redémarrage dans (min.)**, définissez l'intervalle de temps à l'issue duquel le Serveur d'administration réalisera le redémarrage (cf. ill. ci-après).

Cliquez sur **Suivant**.

6. Sélectionnez les ordinateurs dans les groupes d'administration (cf. ill. ci-après), sur lesquels la tâche sera lancée. Cliquez sur **Suivant**.

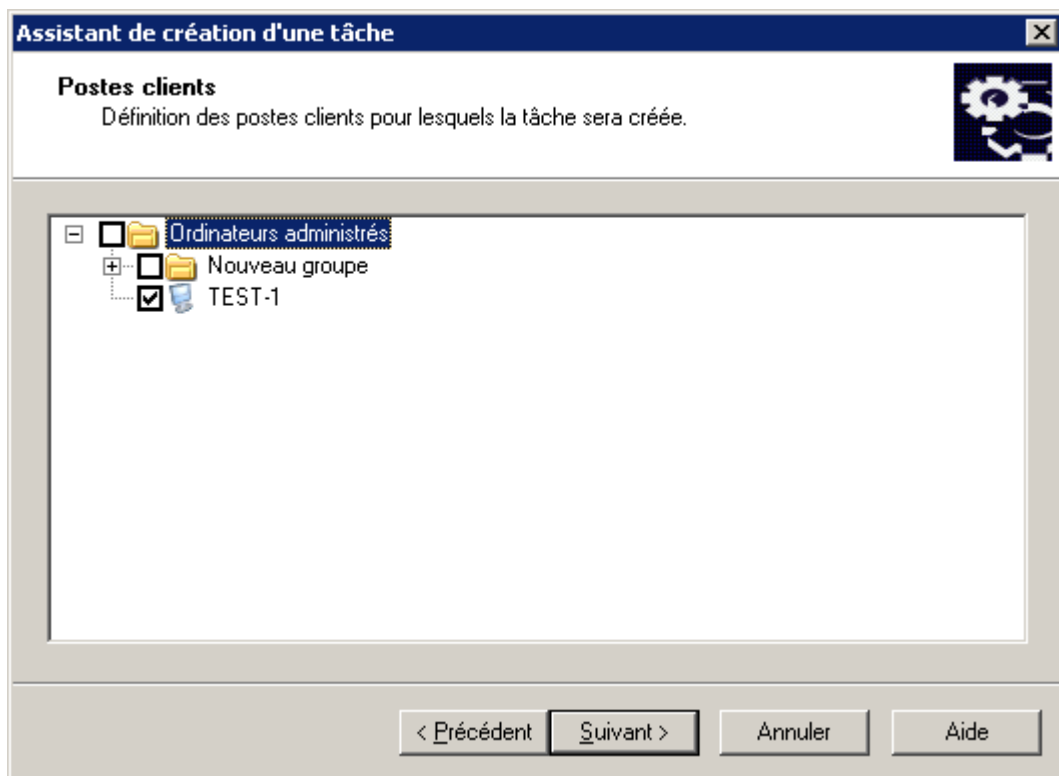


Illustration 131. Sélection de l'ordinateur

7. Planifiez la tâche (cf. section "Création d'une tâche de groupe" à la page 101) (cf. ill. ci-après). Cliquez sur **Suivant**.

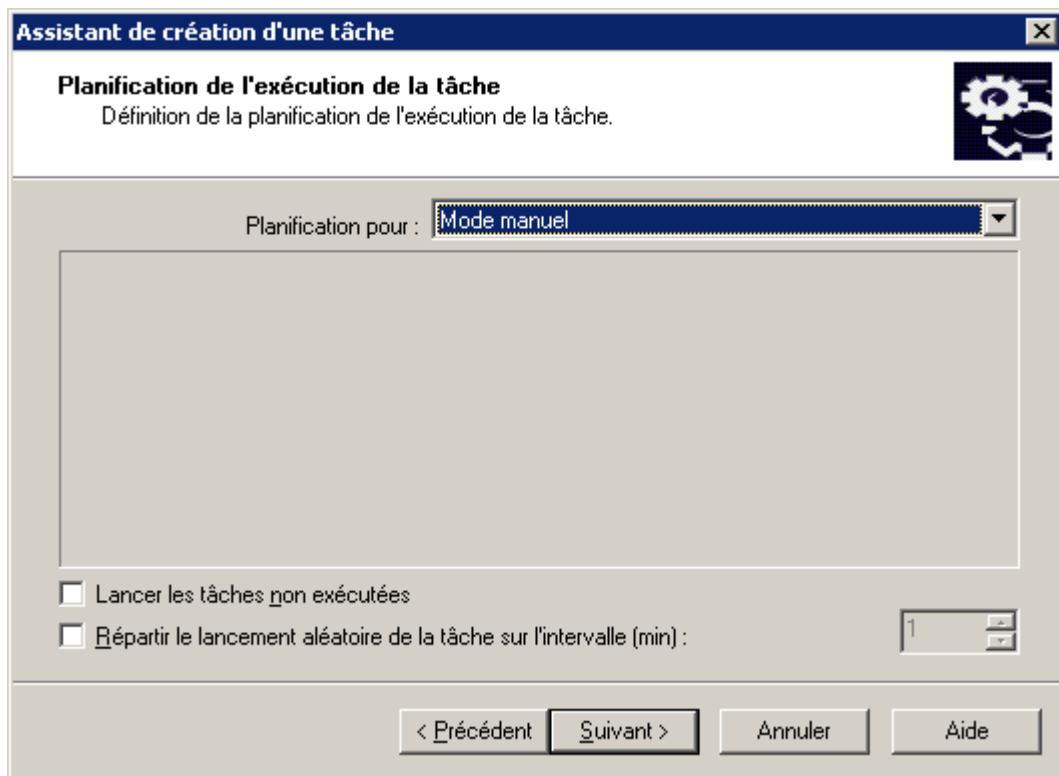


Illustration 132. Programmation de la tâche

8. Appuyez sur le bouton **Terminer** (cf. ill. ci-après) pour terminer la création de la tâche.

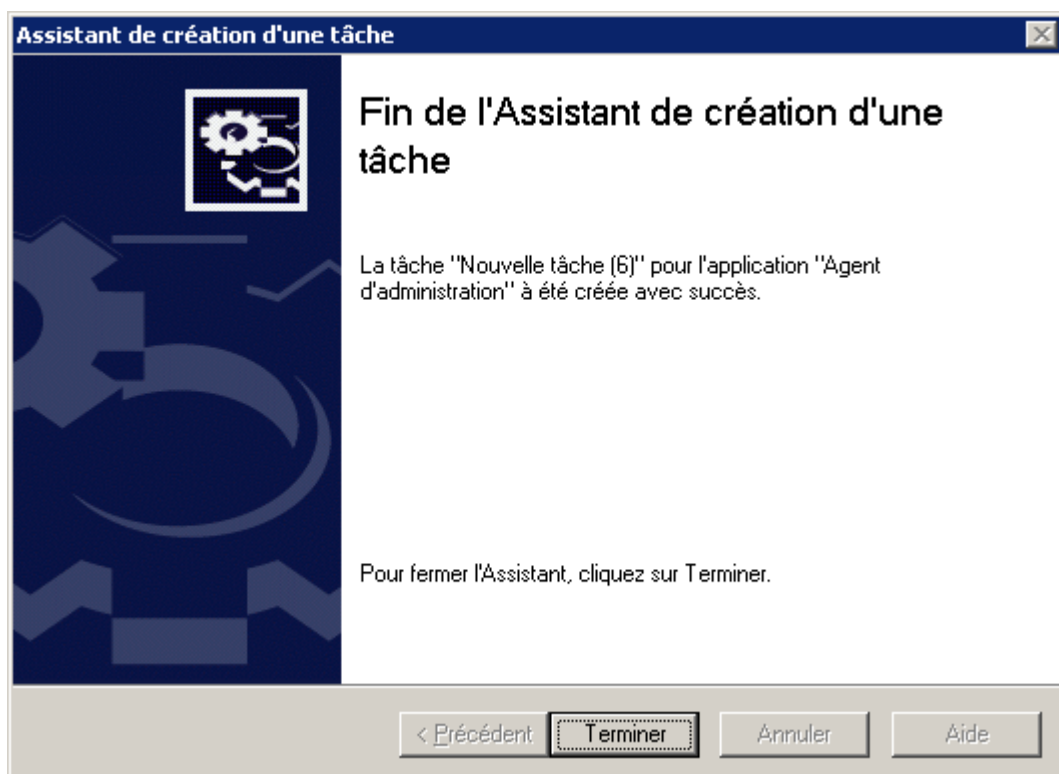


Illustration 133. Fin de la création d'une tâche

ENVOI DU MESSAGE A L'UTILISATEUR DU POSTE CLIENT

➤ Pour envoyer un message à l'utilisateur, procédez comme suit :

1. Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page [22](#)), qui gère le poste client.
2. Lancer l'Assistant de création d'une tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)) ou d'une tâche pour l'ensemble d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)).
3. Dans la fenêtre de l'Assistant **Type de tâche** déployez l'entrée **Kaspersky Administration Kit**, et ensuite le dossier joint **Avancé**.
4. Dans la liste des tâches sélectionnez **Message pour l'utilisateur** (cf. ill. ci-après) puis cliquez sur le bouton **Suivant**.

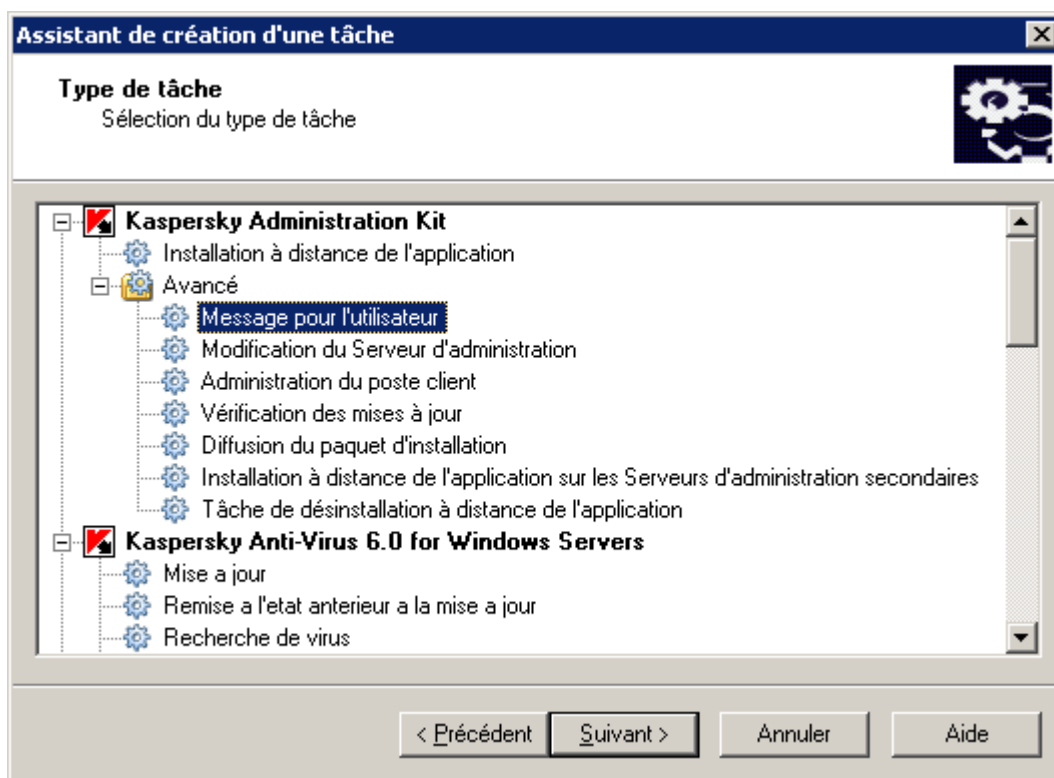


Illustration 134. Message pour l'utilisateur

- Saisissez le texte de message qui s'affichera sur l'écran de l'utilisateur. Le texte peut contenir les liens, que l'utilisateur utilisera pour passer à la ressource correspondante (cf. ill. ci-après). Cliquez sur **Suivant**.

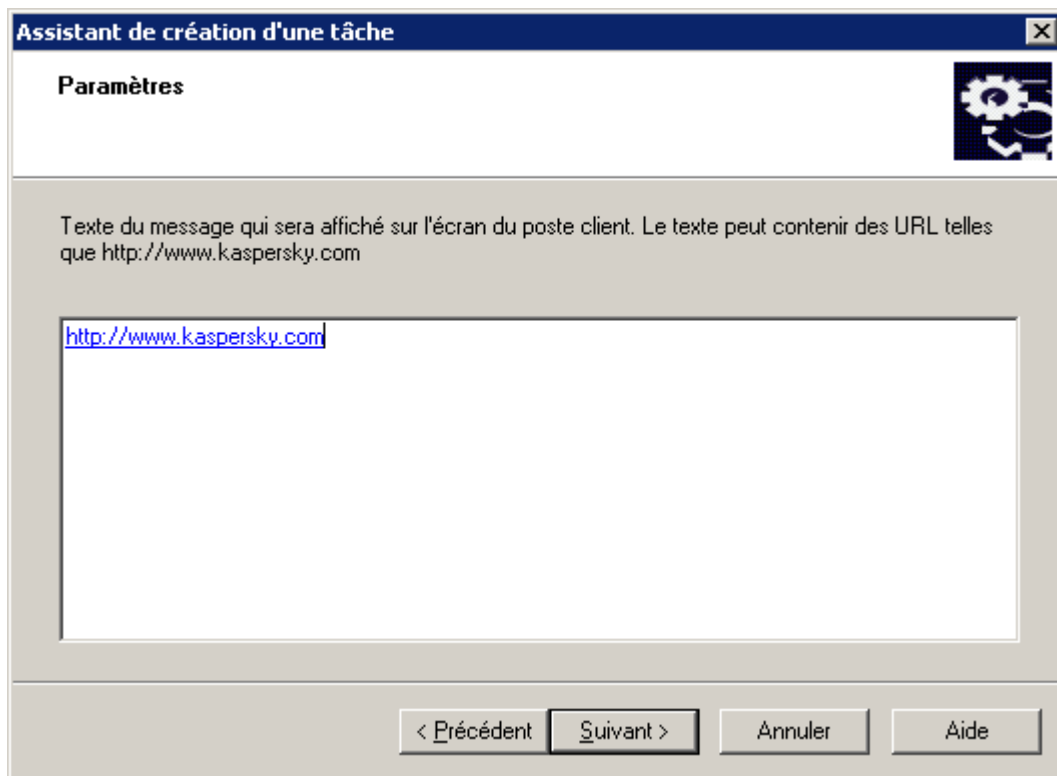


Illustration 135. Texte du message pour l'utilisateur

- Sélectionnez les ordinateurs dans les groupes d'administration, sur lesquels la tâche sera lancée (cf. ill. ci-après). Cliquez sur **Suivant**.

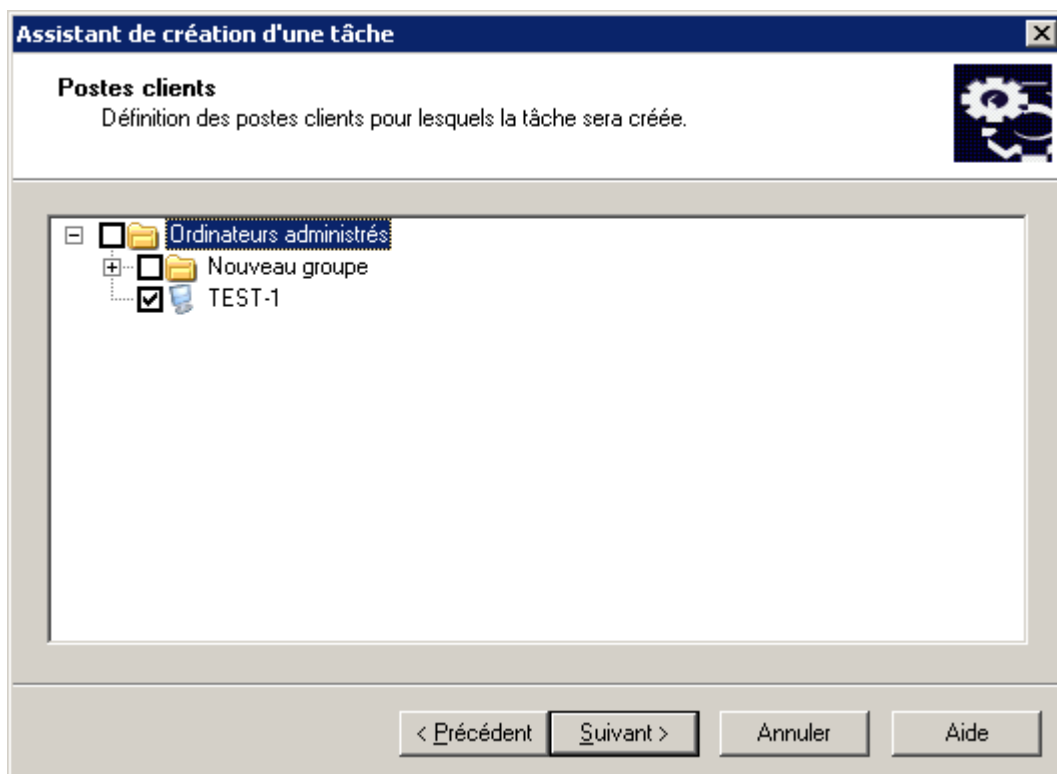


Illustration 136. Sélection de l'ordinateur

- Planifiez la tâche (cf. section "Création d'une tâche de groupe" à la page 101) (cf. ill. ci-après). Cliquez sur **Suivant**.

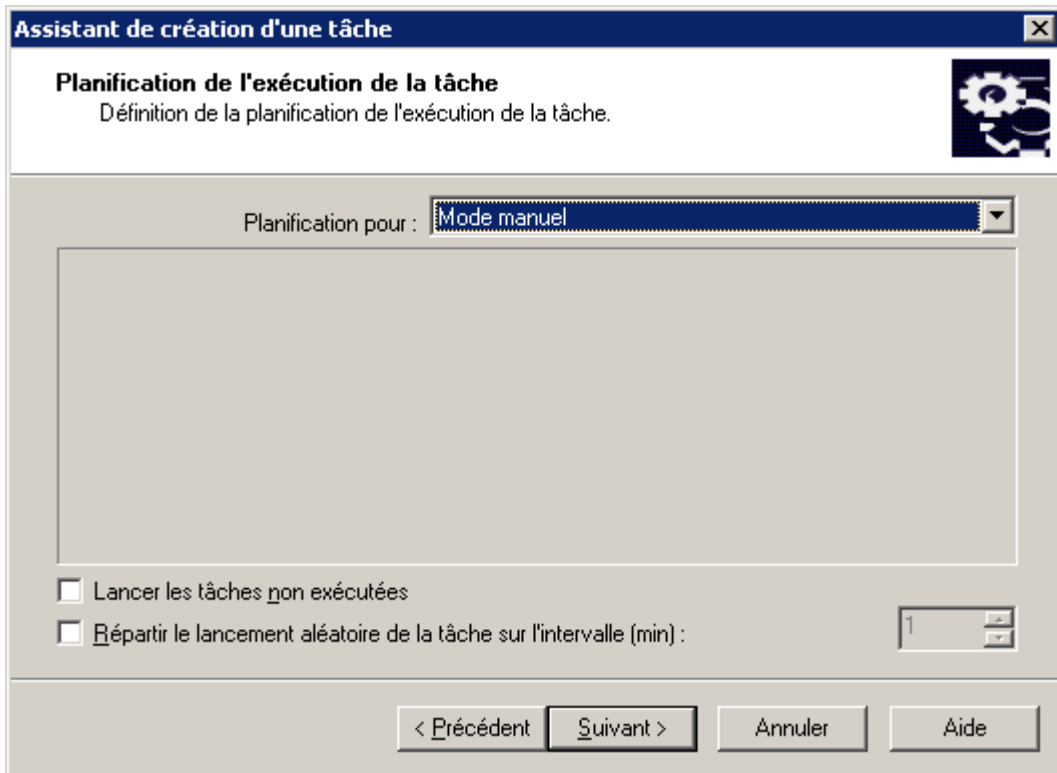


Illustration 137. Programmation de la tâche

- Appuyez sur le bouton **Terminer** (cf. ill. ci-après) pour terminer la création de la tâche.

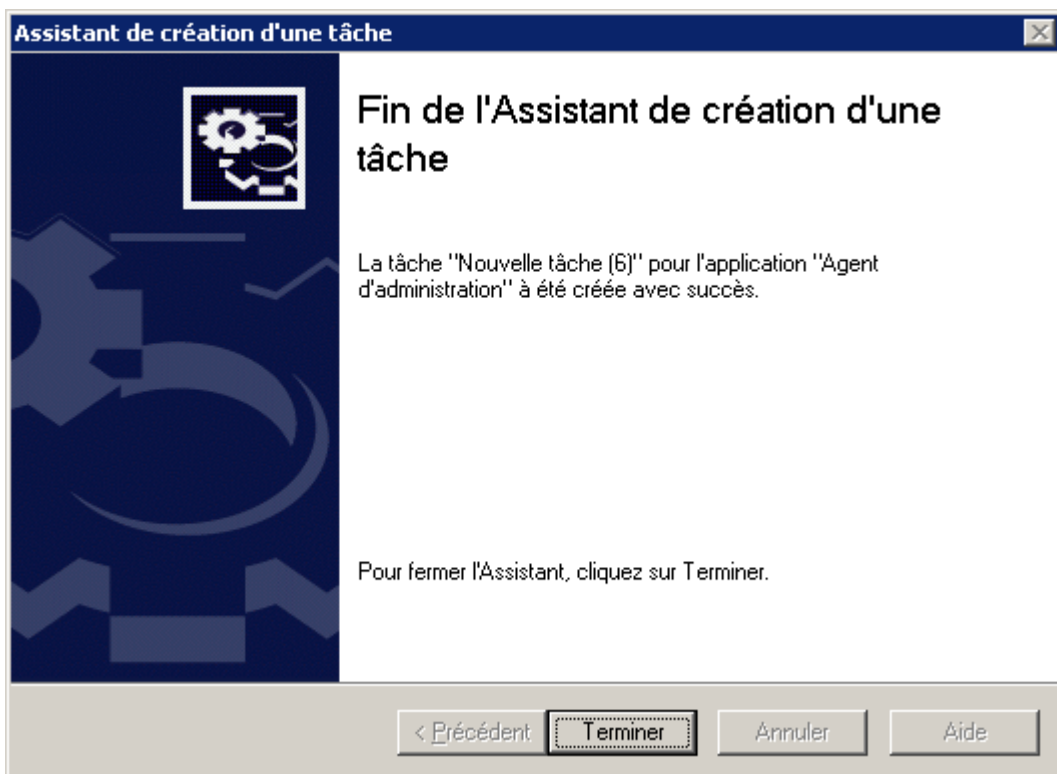


Illustration 138. Fin de la création d'une tâche

CONNEXION MANUELLE DU POSTE CLIENT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLMOVER.EXE

➔ Pour connecter un poste client au Serveur d'administration,

depuis la ligne de commande du poste client, lancez l'utilitaire `klmover.exe` compris dans le paquet d'installation de l'Agent d'administration.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve placé à la racine du dossier d'installation défini lors de l'installation du composant et son exécution, en fonction des paramètres de ligne de commande, effectue les actions suivantes :

- connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués ;
- enregistre les résultats de l'opération dans le fichier journal des événements, ou les affiche à l'écran.

Syntaxe de l'utilitaire :

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

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les résultats de l'exécution dans le fichier journal, par défaut les informations sont conservées dans le fichier `stdout.tx` ; si le paramètre n'est pas utilisé, les résultats et les messages d'erreur sont affichés à l'écran.
- `-address <adresse serveur>` : adresse du Serveur d'administration pour la connexion ; l'adresse peut être une adresse IP, un nom NetBIOS ou DNS de l'ordinateur.
- `-pn <numéro du port>` : numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration, par défaut le port 14000 est utilisé.
- `-ps <numéro du port SSL>` : numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Par défaut, il s'agit du port 13000.
- `-nossl` : utilise une connexion non sécurisée au Serveur d'administration ; si aucun modificateur n'est utilisé, la connexion à l'Agent d'administration est établie à l'aide du protocole sécurisé SSL.
- `-cert <chemin complet du fichier certificat>` : utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au nouveau Serveur d'administration. Si aucun modificateur n'est utilisé, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.
- `-silent` : exécute l'utilitaire en mode non interactif ; ce paramètre est utile, par exemple, pour exécuter l'outil à partir du script d'ouverture de session de l'utilisateur.
- `-dupfix` : paramètre utilisé en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le kit de distribution), par exemple, par restauration depuis une image disque.

VERIFICATION DE LA CONNEXION DU POSTE CLIENT AVEC LE SERVEUR D'ADMINISTRATION

Kaspersky Administration Kit offre la possibilité de vérification de la connexion du poste client avec le Serveur d'administration grâce à :

- utilitaires klnagchk.exe ;
- actions **Analyser la connexion**.

L'utilitaire klnagchk.exe donne l'information détaillée sur les paramètres de connexion des postes clients. L'action **Analyser la connexion** reflète l'accès à l'ordinateur du côté du Serveur d'administration.

VERIFICATION MANUELLE DE LA CONNEXION DU POSTE CLIENT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLNAGCHK.EXE

➔ Afin de vérifier la connexion entre le poste client et le Serveur d'administration à l'aide de klnagchk.exe

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

Après l'installation de l'Agent d'administration, cet utilitaire se trouve placé à la racine du dossier d'installation défini lors de l'installation du composant et son exécution, en fonction des paramètres de ligne de commande, effectue les actions suivantes :

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

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nomFichier>] 1 [-sp] [-savecert <chemin du fichier certificat>] [-restart]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur, ainsi que les résultats de l'exécution ; par défaut les informations sont conservées dans le fichier stdout.tx ; si le paramètre n'est pas utilisé, les résultats et les messages d'erreur sont affichés à l'écran.
- `-sp` : affiche le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy ; ce paramètre est utilisé si la connexion au Serveur d'administration est effectuée via un serveur proxy.
- `-savecert <nom du fichier>` : enregistre le certificat utilisé pour accéder au serveur d'administration dans le fichier spécifié.
- `-restart` : redémarre l'Agent d'administration après exécution de l'utilitaire.

VERIFIER LA CONNEXION ENTRE LE POSTE CLIENT ET LE SERVEUR D'ADMINISTRATION A L'AIDE DE L'ACTION ANALYSER LA CONNEXION.

➤ Afin de vérifier la connexion entre le poste client et le Serveur d'administration à l'aide de l'action **Analyser la connexion**, procédez comme suit :

1. Sélectionnez le poste client ou le Serveur d'administration secondaire.
2. Dans son menu contextuel sélectionnez le point **Analyser la connexion**.

Finalement la fenêtre, qui contient l'information sur l'accessibilité ou l'inaccessibilité de l'ordinateur, s'ouvre.

La capacité de fonctionnement de l'Agent d'administration est définie à la base de l'information, que le Serveur d'administration possède sur le poste client.

UTILITAIRE DU DIAGNOSTIC A DISTANCE DES POSTES CLIENTS (KLACTGUI)

L'utilitaire *klactgui* est prévu pour l'exécution des opérations suivantes sur l'ordinateur à distance :

- Activation et désactivation du traçage, modification du niveau de traçage, téléchargement du fichier de traçage (cf. section "Activation et désactivation du traçage, téléchargement du fichier de traçage" à la page [170](#)).
- Téléchargement des paramètres des applications (à la page [172](#)).
- Téléchargement des journaux des événements (à la page [174](#)).
- Lancement du diagnostic et téléchargement des résultats de son fonctionnement (cf. section "Lancement du diagnostic et téléchargement de ses résultats" à la page [175](#)).
- Lancement et arrêt des applications (cf. section "Lancement, relancement et arrêt des applications" à la page [177](#)).

➤ Pour fonctionner avec l'utilitaire, procédez comme suit :

1. Installez l'utilitaire sur n'importe quel ordinateur.

Pour ce faire, dépaquetez les archives téléchargées et lancez le fichier *klactgui_ru.msi* (ou *klactgui_en.msi*). Les fichiers de l'utilitaire sont enregistrés dans le dossier *C:\Program Files\Kaspersky Lab\klactgui*. La désinstallation de l'utilitaire s'effectue par les moyens standards du système d'exploitation.

Lancez l'utilitaire du menu **Démarrer** → **Applications** → **klactgui** ou dans le panneau des résultats de la Console d'administration ouvrez le menu contextuel du poste client et sélectionnez le point **Outils externes** (à la page [323](#)) → **Diagnostic à distance**.

2. Pour se connecter à l'ordinateur, dans la fenêtre de l'utilitaire procédez comme suit (cf. ill. ci-après) :
 - Sélectionnez l'option de fonctionnement **Accès à l'aide des outils du réseau Microsoft Windows**.
 - Saisissez dans le champ **Ordinateur** le nom d'ordinateur, duquel l'information doit être recueillie.
 - Indiquez un compte pour se connecter à l'ordinateur :
 - **Se connecter au nom de l'utilisateur en cours** : la connexion aura lieu sous un compte utilisateur actuel.

- **Utiliser, lors de la connexion, le nom d'utilisateur et le mot de passe fournis** : se connecter sous un compte indiqué. Lors de la sélection de cette option indiquez **Nom d'utilisateur** et **Mot de passe** du compte requis.

La connexion doit avoir lieu sous un compte de l'administrateur local de l'ordinateur.

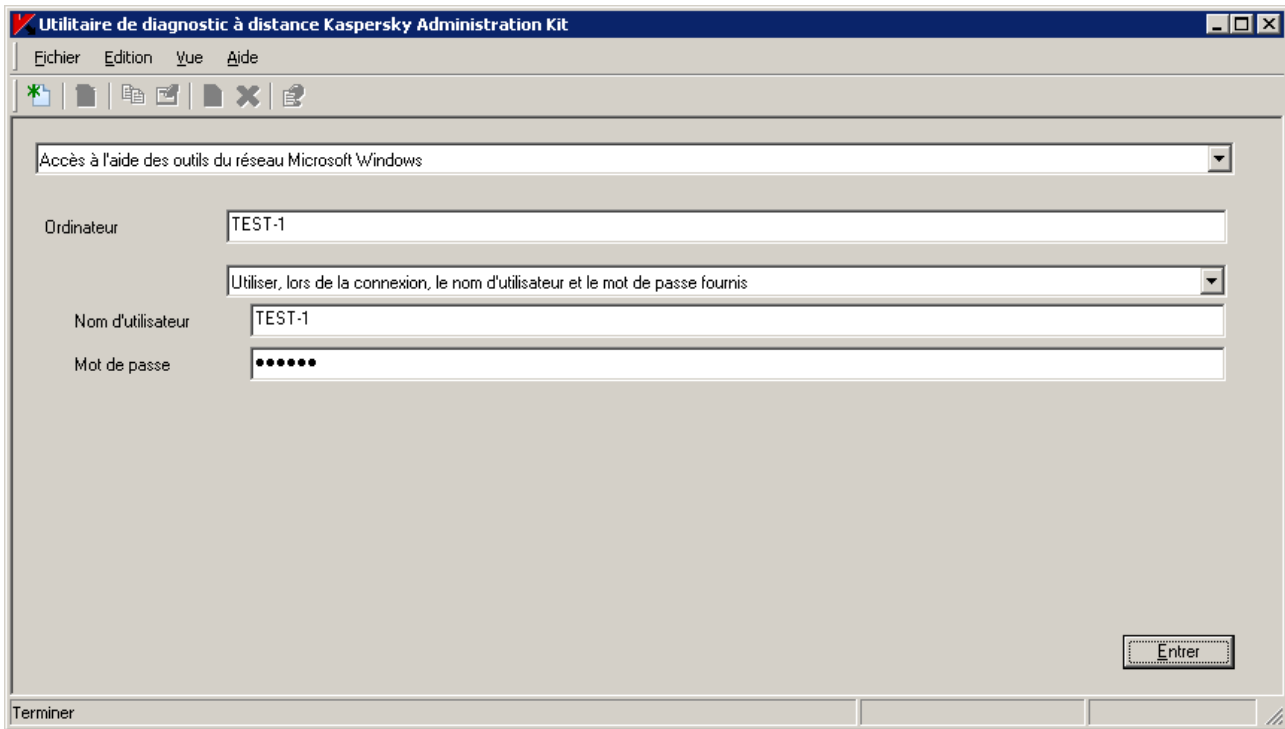


Illustration 139. Connexion à l'ordinateur

3. Après avoir indiqué les données requises pour la connexion, cliquez sur **Entrer**.
4. Dans la fenêtre ouverte exécutez les opérations nécessaires et téléchargez les fichiers requis.

L'utilitaire sauvegarde les fichiers téléchargés des postes clients sur le bureau de l'ordinateur, depuis lequel il était lancé.

ACTIVATION ET DESACTIVATION DU TRAÇAGE, TELECHARGEMENT DU FICHIER DE TRAÇAGE

➤ Pour activer et désactiver le traçage, procédez comme suit :

1. Connectez-vous à l'ordinateur requis.

2. Dans l'arborescence sélectionnez l'application, pour laquelle il est nécessaire de froncer le traçage, et en haut à gauche passez au lien **Activer le traçage** (cf. ill. ci-après).

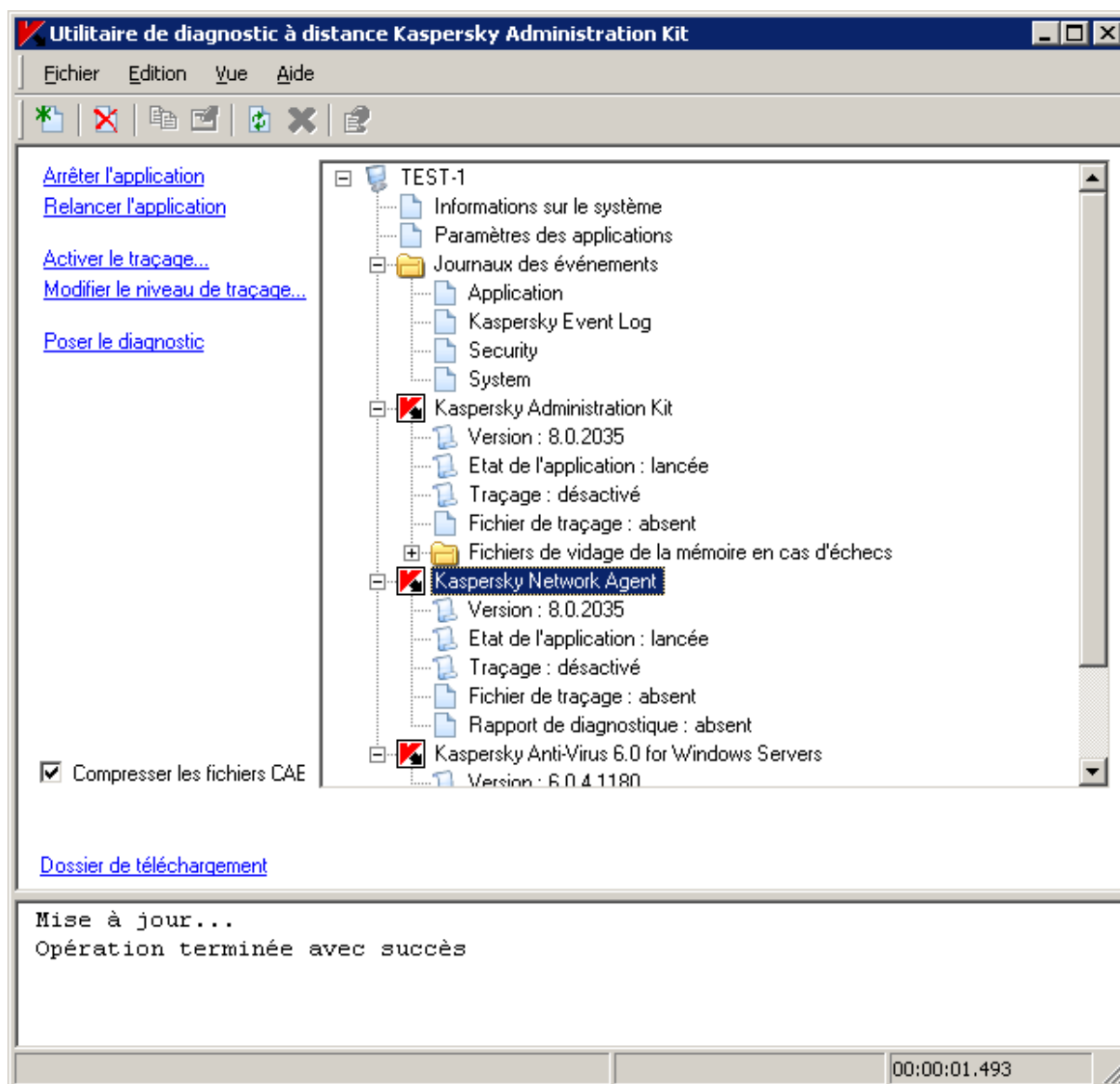


Illustration 140. Activation du traçage

Activation et désactivation du traçage des applications avec l'autodéfense sont possibles uniquement avec la présence via le Serveur d'administration.

Dans quelques cas pour activer le traçage de Kaspersky Anti-Virus il est conseillé de relancer le produit et la tâche correspondante. Vous pouvez arrêter l'Anti-Virus par Kaspersky Administration Kit (propriétés du poste client → onglet **Applications**), et le lancement de Kaspersky Anti-Virus est possible par cet utilitaire (quand Kaspersky Anti-Virus est désactivé, en haut à gauche de la fenêtre le lien **Exécuter l'application** apparaît).

- Après l'activation du traçage, les fichiers de traçage apparaissent en tant que les sous-points du traçage. Pour télécharger sélectionnez le fichier nécessaire et à gauche de la fenêtre passez au lien **Télécharger le fichier** pour télécharger le fichier en entier (cf. ill. ci-après). Pour les fichiers de grande taille la possibilité de télécharger uniquement les dernières parties de traçage est offerte.

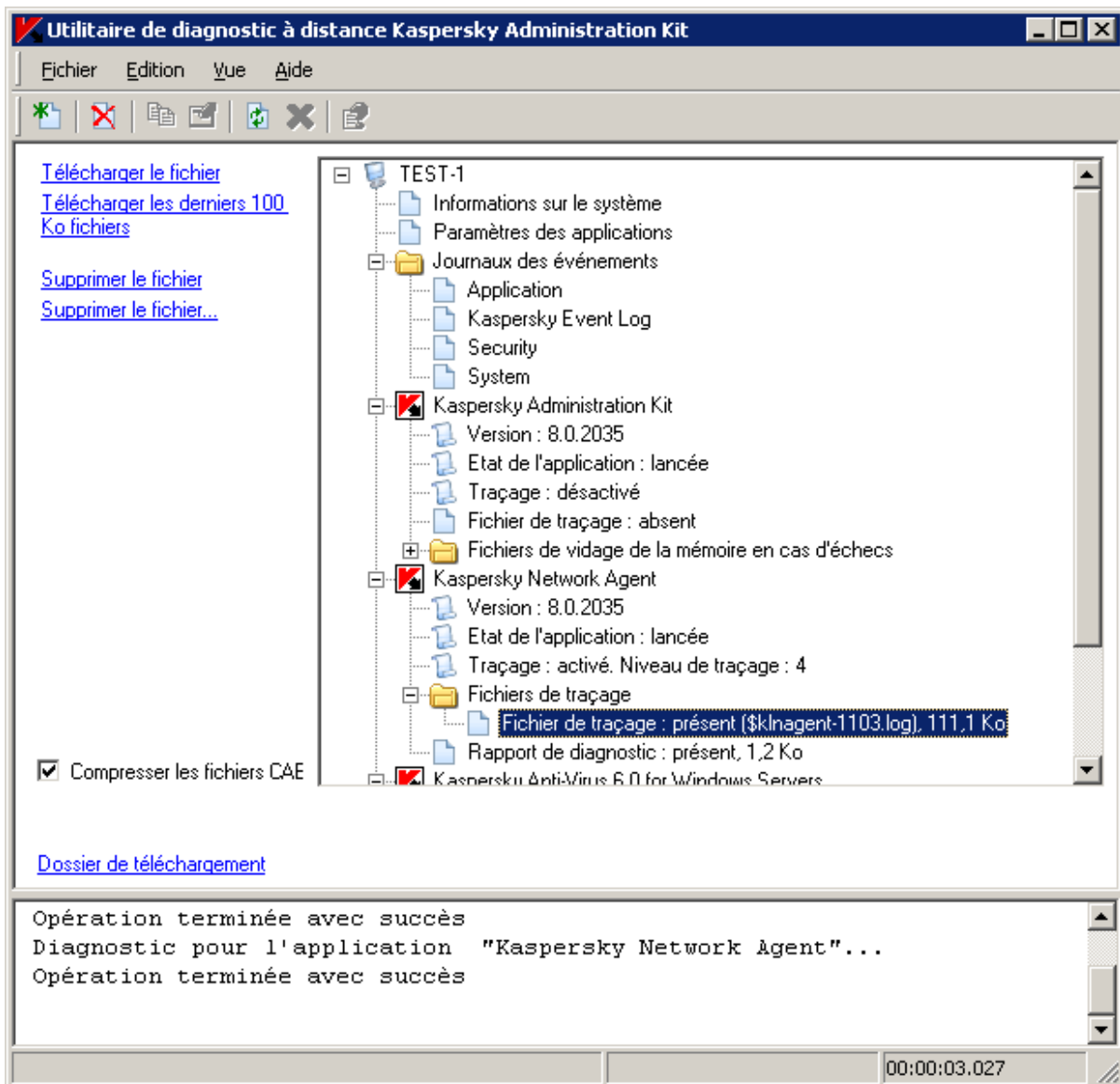


Illustration 141. Téléchargement du fichier de traçage

Vous pouvez aussi supprimer le fichier défini. Cependant, la suppression des fichiers est possible uniquement après l'arrêt de traçage.

- Pour désactiver le traçage, sélectionnez l'application et à gauche de la fenêtre passez au lien **Désactiver le traçage**.

TELECHARGEMENT DES PARAMETRES DES APPLICATIONS

➤ Pour télécharger les paramètres des applications, procédez comme suit :

- Connectez-vous à l'ordinateur requis.
- Sélectionnez le nom d'ordinateur dans l'arborescence et à gauche de la fenêtre passez au lien :

- **Charger les informations relatives au système** : pour obtenir la totalité de l'information sur le système du poste client.
- **Charger les paramètres des applications** : pour charger les paramètres des applications de Kaspersky Lab installées sur cet ordinateur.
- **Composer le fichier de vidage de la mémoire pour le processus** : pour générer et télécharger le vidage de l'application indiquée (cf. ill. ci-après).

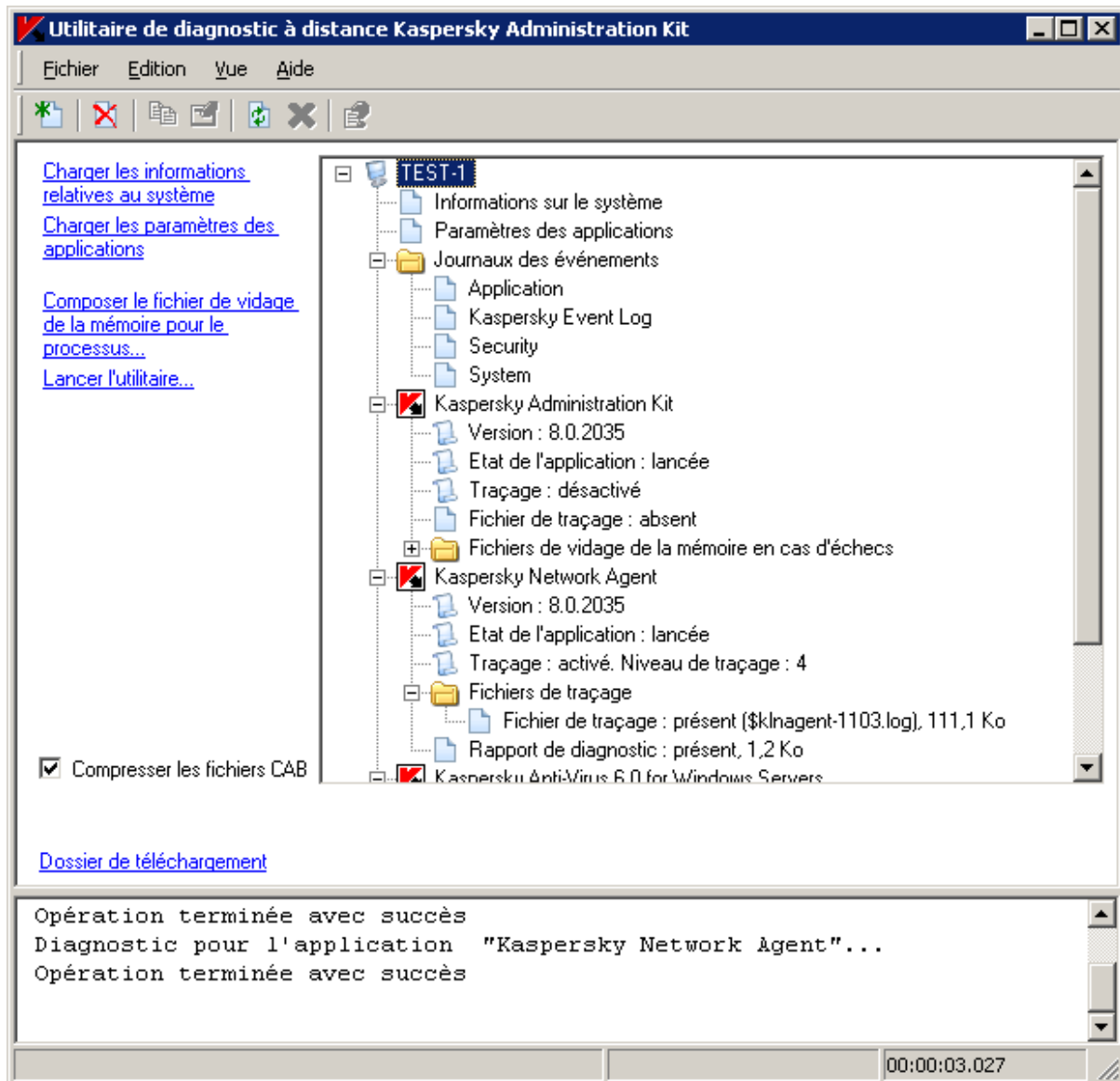


Illustration 142. Formation d'un fichier de vidage de la mémoire du processus

Dans la fenêtre ouverte indiquez le fichier exécutable, pour lequel il est nécessaire de former le fichier de vidage de la mémoire (cf. ill. ci-après).

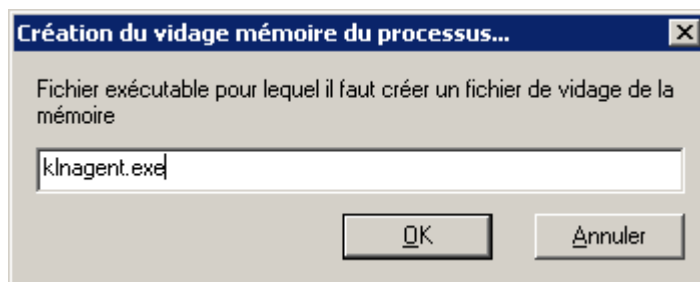


Illustration 143. Formation d'un fichier de vidage de la mémoire

- **Lancer l'utilitaire** : pour télécharger sur l'ordinateur à distance, exécuter l'utilitaire indiqué et télécharger les résultats de son fonctionnement.

TELECHARGEMENT DES JOURNAUX DES EVENEMENTS

► Pour télécharger les journaux des événements, procédez comme suit :

1. Connectez-vous à l'ordinateur requis.

2. Dans le dossier **Journaux des événements** sélectionnez le journal et à gauche de la fenêtre, passez au lien **Charger le journal des événements Kaspersky Event Log** (cf. ill. ci-après).

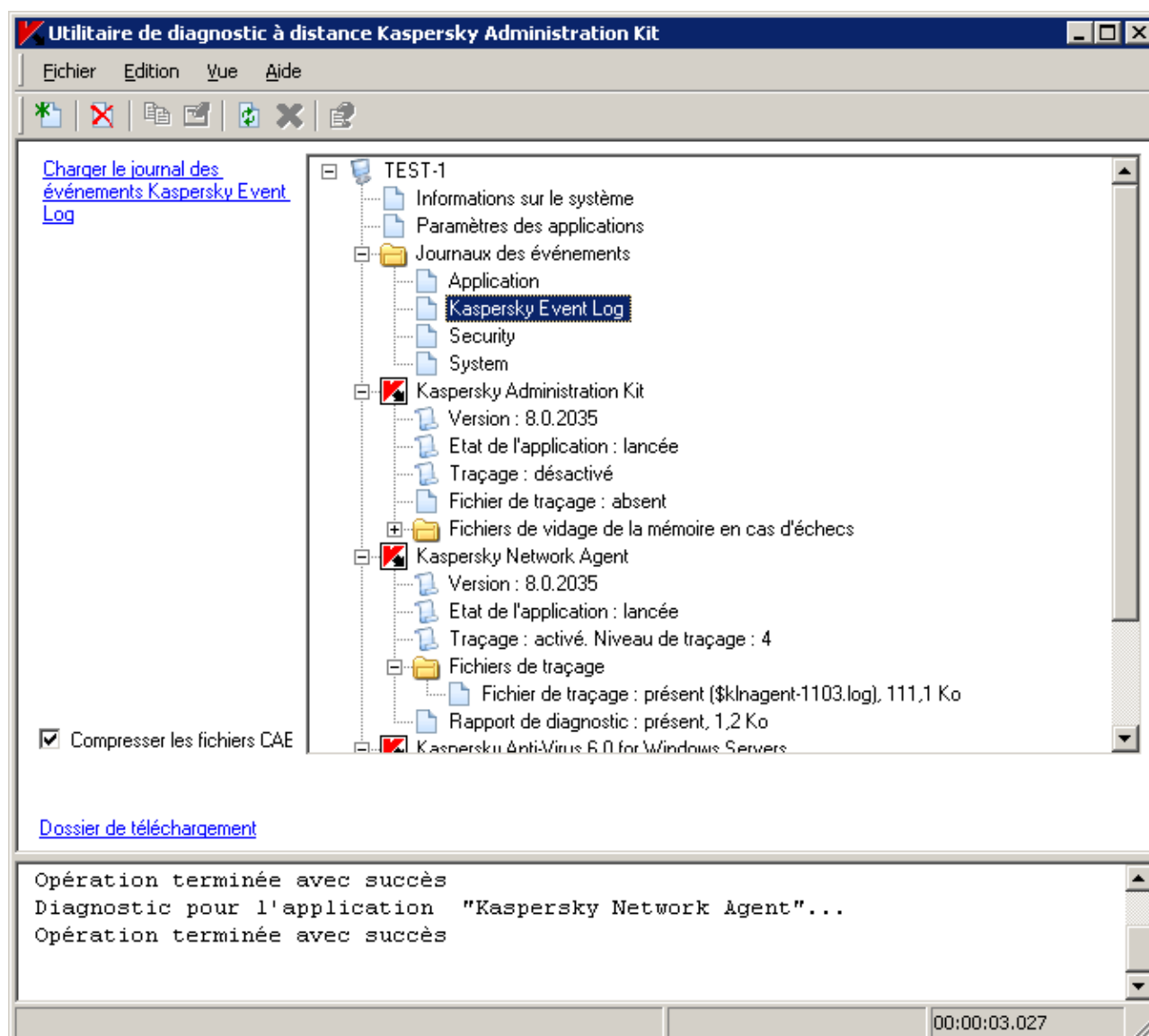


Illustration 144. Charger le journal des événements

LANCEMENT DU DIAGNOSTIC ET TELECHARGEMENT DE SES RESULTATS

- Pour lancer le diagnostic pour l'application, procédez comme suit :

1. Connectez-vous à l'ordinateur requis.

- Sélectionnez l'application nécessaire dans l'arborescence et à gauche de la fenêtre passez au lien **Poser le diagnostic** (cf. ill. ci-après).

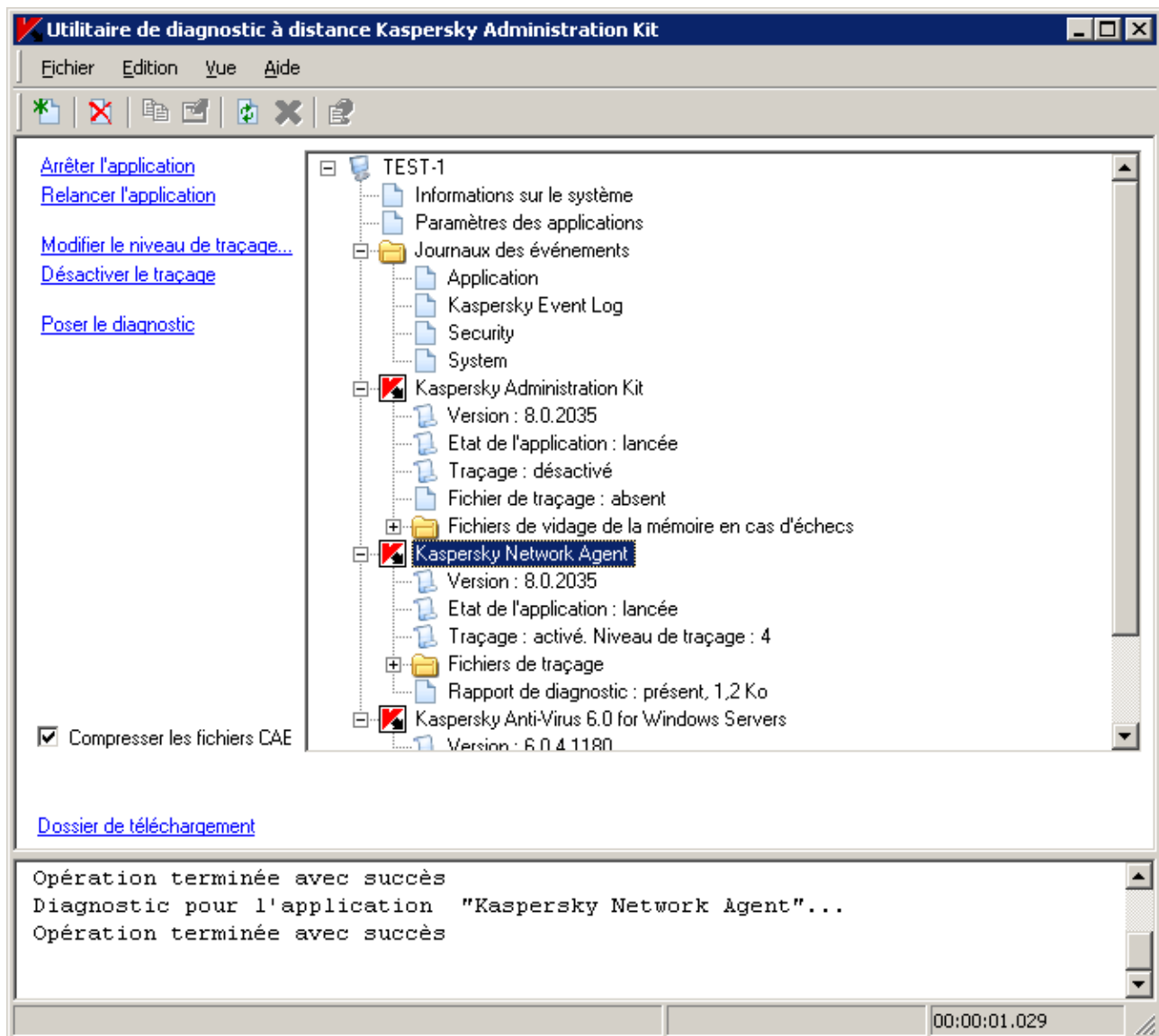


Illustration 145. Exécution du diagnostic

3. Après avoir créé le rapport de diagnostic vous pouvez le télécharger, en passant au lien **Télécharger le fichier** (cf. ill. ci-après).

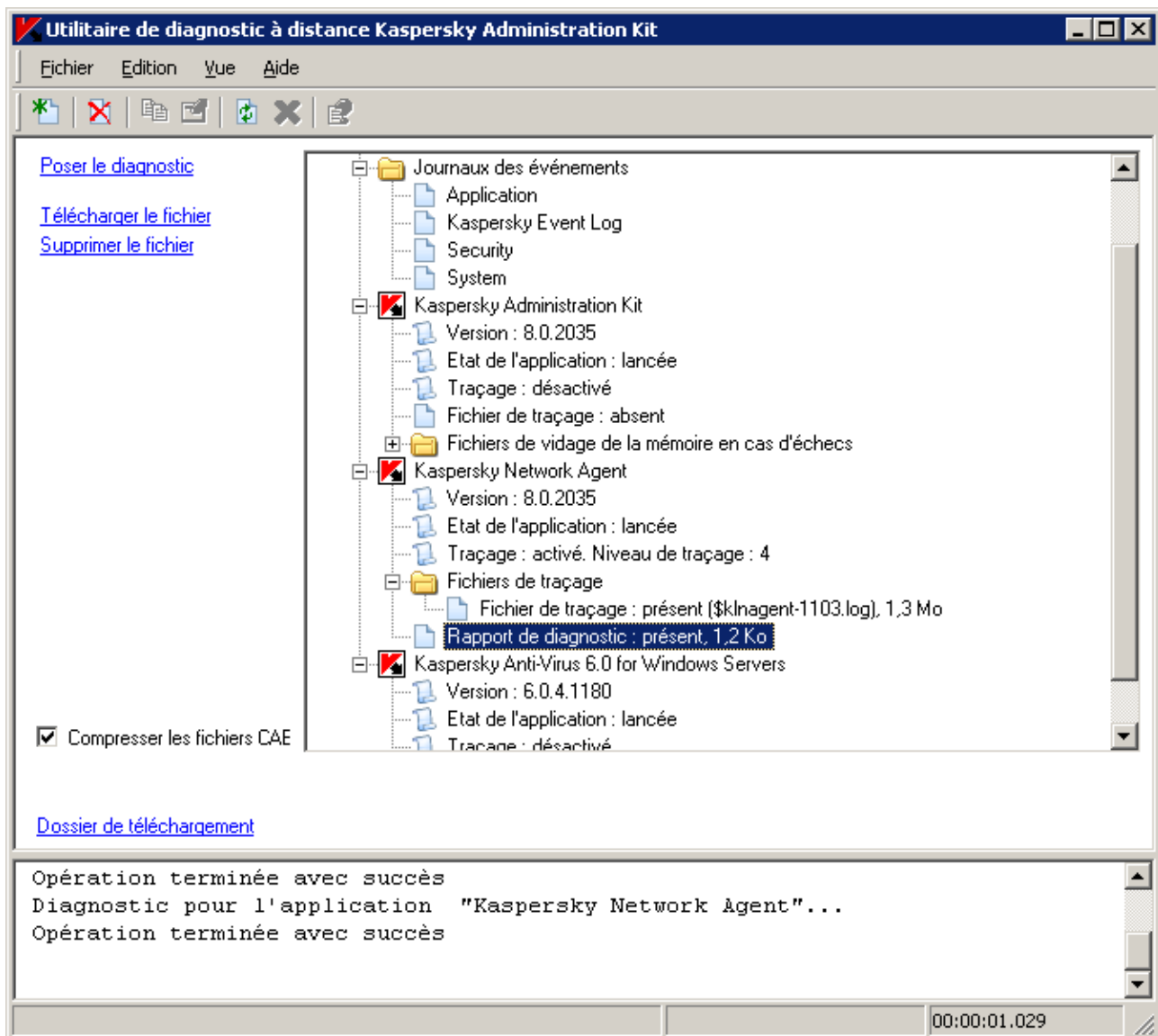


Illustration 146. Téléchargement du rapport de diagnostic

LANCEMENT, RELANCEMENT ET ARRÊT DES APPLICATIONS

Lancement, arrêt et relancement des applications sont possibles uniquement avec la présence via le Serveur d'administration.

➔ Pour lancer, arrêter ou relancer l'application, procédez comme suit :

1. Connectez-vous à l'ordinateur requis.
2. Sélectionnez l'application nécessaire dans l'arborescence et à gauche de la fenêtre passez au lien (cf. ill. ci-après) :
 - **Arrêter l'application.**
 - **Relancer l'application.**

- Exécuter l'application.

Selon l'action sélectionnée, l'application sera lancée, arrêtée ou relancée.

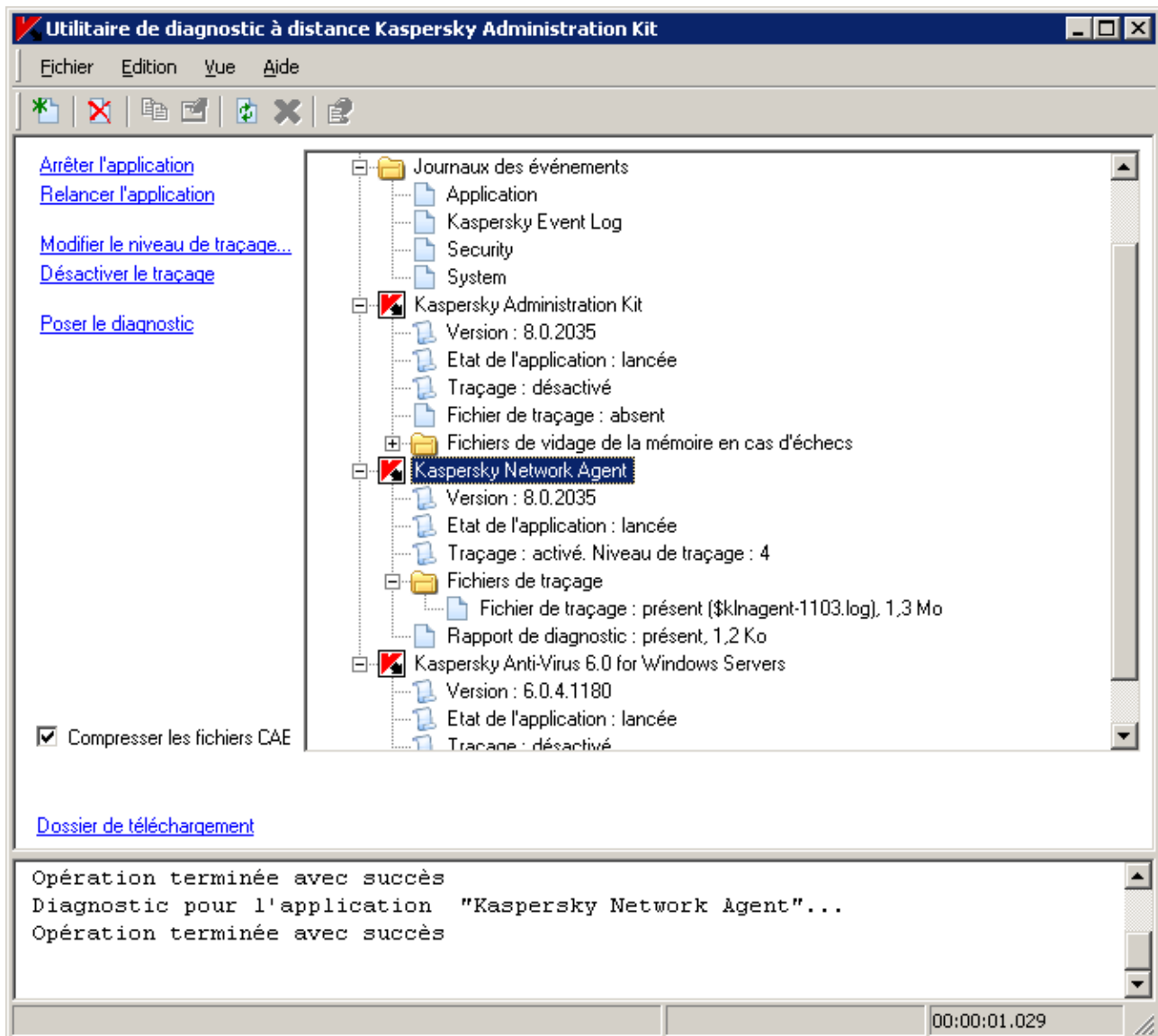


Illustration 147. Lancement, arrêt ou relancement de l'application

RAPPORTS ET NOTIFICATIONS

Les informations relatives à l'état du système de protection antivirus peuvent être présentées sous la forme de rapports. Les rapports sont composés sur la base des informations contenues sur le Serveur d'administration et peuvent être créés pour :

- pour la sélection de postes clients ;
- les ordinateurs appartenant à un groupe d'administration déterminé ;
- une sélection de postes clients issus de divers groupes d'administration ;
- tous les ordinateurs dans le réseau (accessible pour le rapport de déploiement).

L'application propose une sélection de modèles de rapport standard. Il est possible également de composer des modèles personnalisés. Les rapports sont accessibles sous le dossier **Rapports et notifications** de l'arborescence de la console.

Outre la manipulation des rapports, le dossier **Rapports et notifications** permet de passer à la configuration des paramètres généraux des notifications du Serveur d'administration.

DANS CETTE SECTION

Créer le nouveau rapport	179
Affichage des statistiques.....	182
Affichage et modification des modèles de rapport.....	191
Génération et affichage de rapports	197
Tâche de diffusion des rapports	200
Rapports d'hierarchie des Serveurs d'administration	204
Limitation du nombre d'entrées dans le rapport	205
Limite de notifications.....	207
Notifications.....	207

CREER LE NOUVEAU RAPPORT

► *Pour créer un nouveau modèle de rapport, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications** et utilisez la commande **Générer** → **Rapport**. Cette action lance un Assistant.
2. Indiquez le nom de modèle. Si un modèle de ce nom existe déjà, un **(1)** sera automatiquement ajouté au nouveau nom.
3. Sélectionnez le type de rapport. Les étapes suivantes dépendent de votre choix.
4. Indiquez la période couverte par le rapport (cf. ill. ci-après). Vous pouvez choisir des dates fixes de rapport ou laisser la date de fin sans définir. Dans ce second cas, le programme utilisera la date courante du système pour

la date de fin du rapport. Vous pouvez également choisir l'option **Des derniers jours** et préciser le nombre de jours dans le champ associé. Dans ce cas, le début de l'intervalle correspond au moment de la création du rapport. Par exemple, si le champ indique 2 jours et que le rapport est créé le 24 juin à 15h00, alors le rapport reprendra les données depuis le 22 juin à 15h00.

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

Illustration 148. Créer le nouveau rapport. Définir la période de rapport

5. Spécifiez les objets pour lesquels vous voulez créer le rapport (cf. ill. ci-après) :
 - **Rapport sur un groupe** : crée un rapport sur les ordinateurs appartenant à un groupe.
 - **Rapport sur une liste d'ordinateurs** : crée un rapport pour des ordinateurs des groupes d'administration.

- **Rapport pour la requête de postes clients** : pour n'importe quelle requête de postes clients.

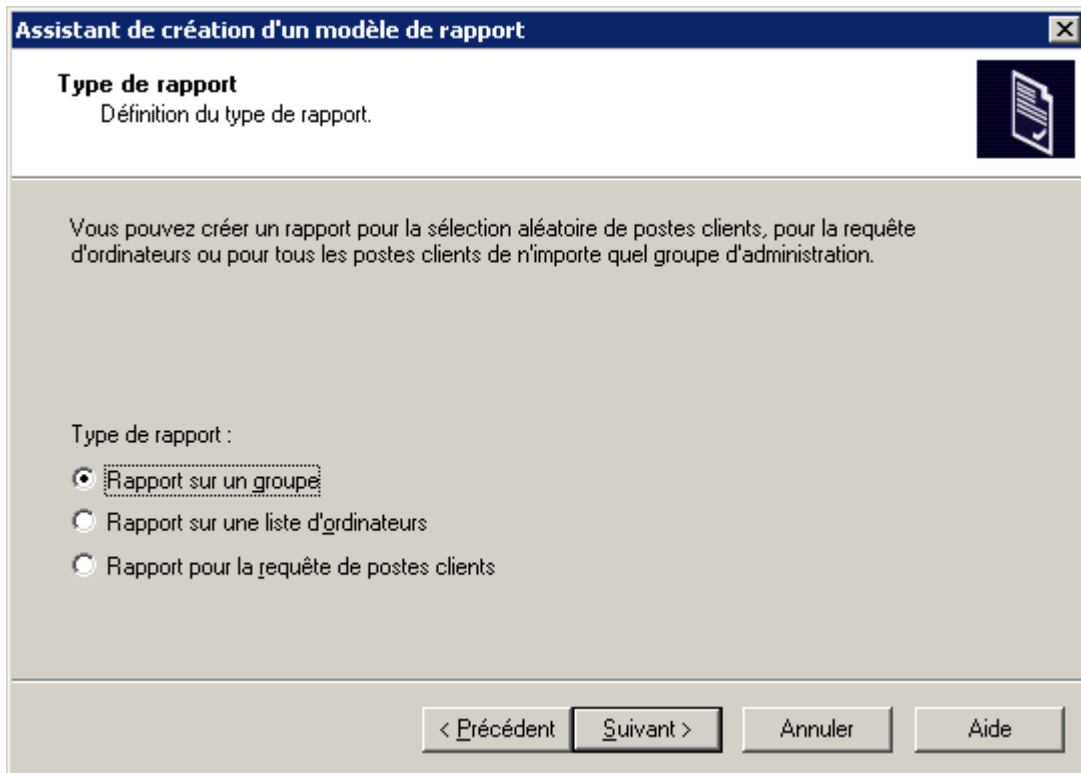


Illustration 149. Créer le nouveau rapport. Sélection des objets du rapport

6. Ensuite, en fonction du type de rapport sélectionné à l'étape suivante, indiquez le groupe, la sélection de postes clients ou la requête de postes clients dont les informations doivent figurer dans le rapport (cf. ill. ci-après). Terminez l'Assistant.

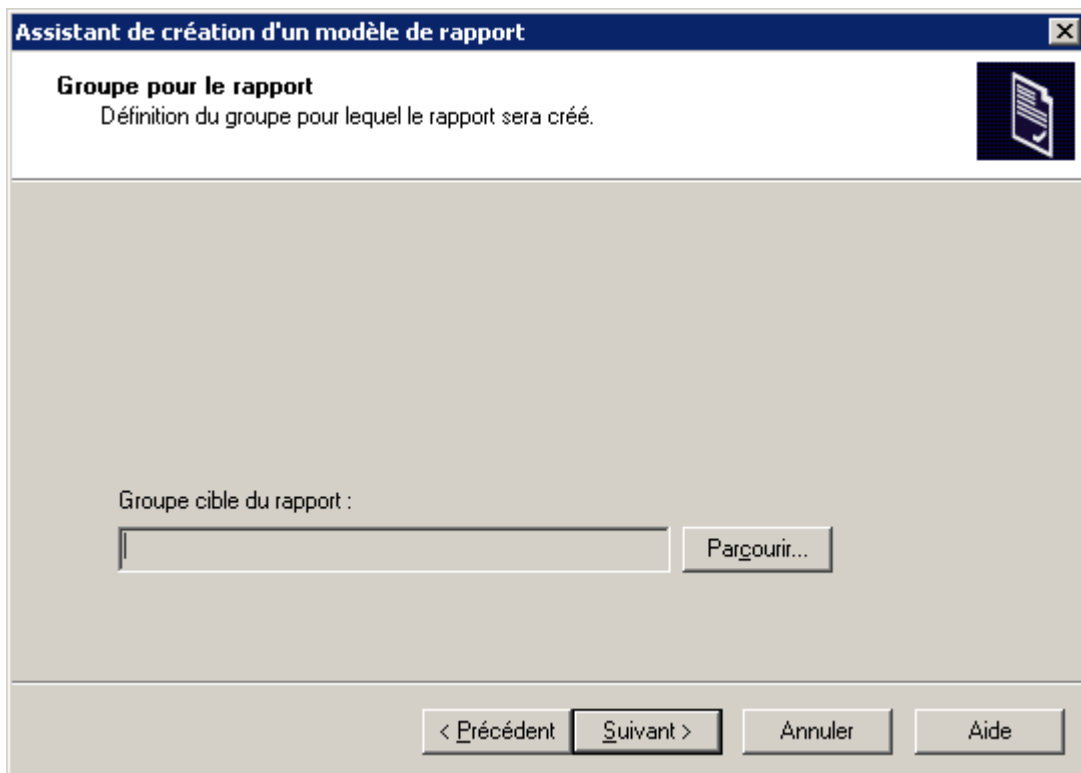


Illustration 150. Création d'un modèle pour des rapports, sélection des postes clients

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

AFFICHAGE DES STATISTIQUES

Dans Kaspersky Administration Kit la représentation graphique des informations sur l'état de la protection antivirus sont reprises dans le dossier **Rapports et notifications** sous l'onglet **Statistiques**. L'onglet peut contenir plus pages, chacune contenant des volets d'informations qui représentent clairement les données statistiques. Les volets d'informations se présentent sous la forme de tableau ou de diagrammes (camemberts ou colonnes) qui facilitent la comparaison des données et qui présentent clairement les interactions. Les données des volets d'informations sont actualisées en permanence et représentent l'état actuel du système de protection antivirus.

L'onglet **Statistiques** permet à l'administrateur de parcourir les données statistiques sur l'état actuel de la protection, des mises à jour, des statistiques antivirus, des statistiques générales, etc.

L'onglet **Statistiques** propose un panneau de résultats élargi (cf. ill. ci-après).

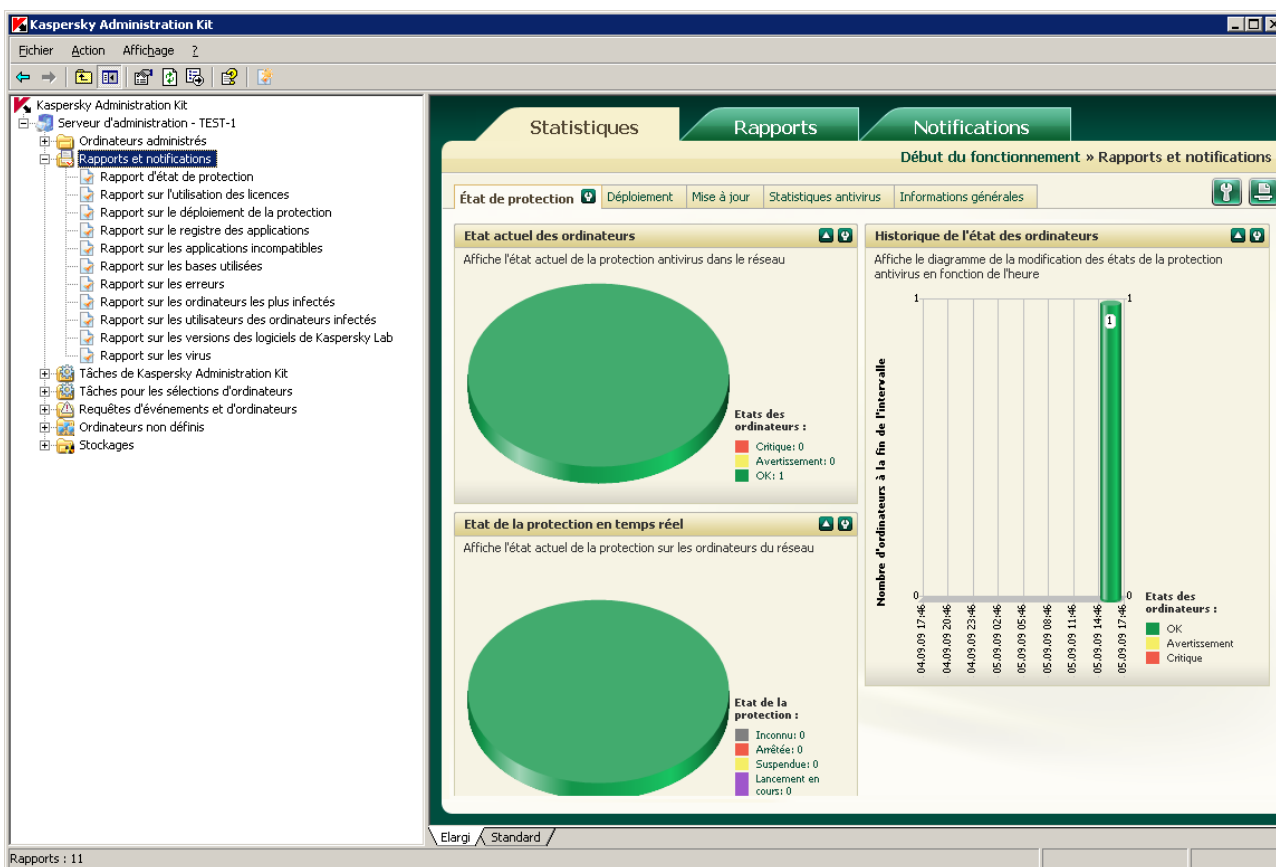





Illustration 151. Panneau des résultats de l'onglet **Statistiques**

La composition des pages, le nombre de volets d'informations et les modes de représentation des données peuvent être modifiés par l'administrateur.

Afin de modifier les paramètres d'affichage des statistiques, utilisez les boutons suivants :


- – configurer le contenu des pages ;
- – configurer la page de statistiques (le bouton se trouve à côté du nom de la page) ;
- – configurer les paramètres d'affichage de la barre quelconque (le bouton se trouve à côté du nom de la barre) ;

-  et  – rouler et dérouler le volet d'informations ;
-  – imprimer la page des statistiques.

CREATION DE LA PAGE DE STATISTIQUES

Dans Kaspersky Administration Kit vous pouvez créer les pages propres de statistiques, qui contiennent les volets d'informations nécessaires.

► Pour ajouter un volet d'informations à la page, procédez comme suit :

1. Cliquez sur le bouton , situé en haut à droite de l'onglet **Statistiques**. De ce fait la fenêtre de configuration des paramètres de l'onglet s'ouvrira (cf. ill. ci-après).

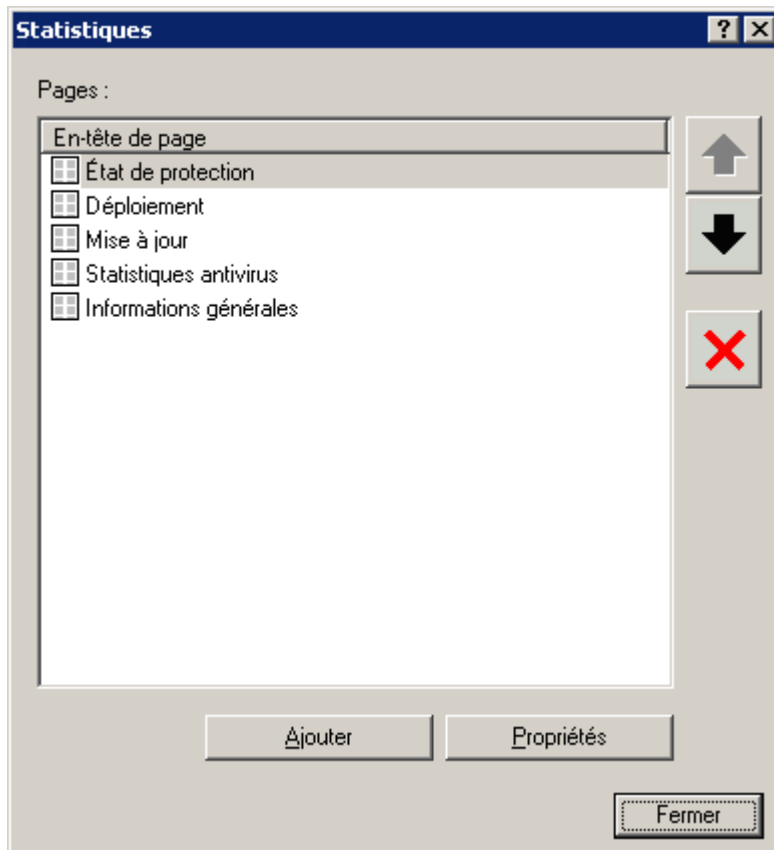


Illustration 152. Configuration des paramètres de l'onglet

2. Cliquez sur le bouton **Ajouter**, situé dans la fenêtre **Statistiques**. Cela entraîne l'ouverture de la fenêtre des propriétés de la nouvelle page (cf. ill. ci-après).

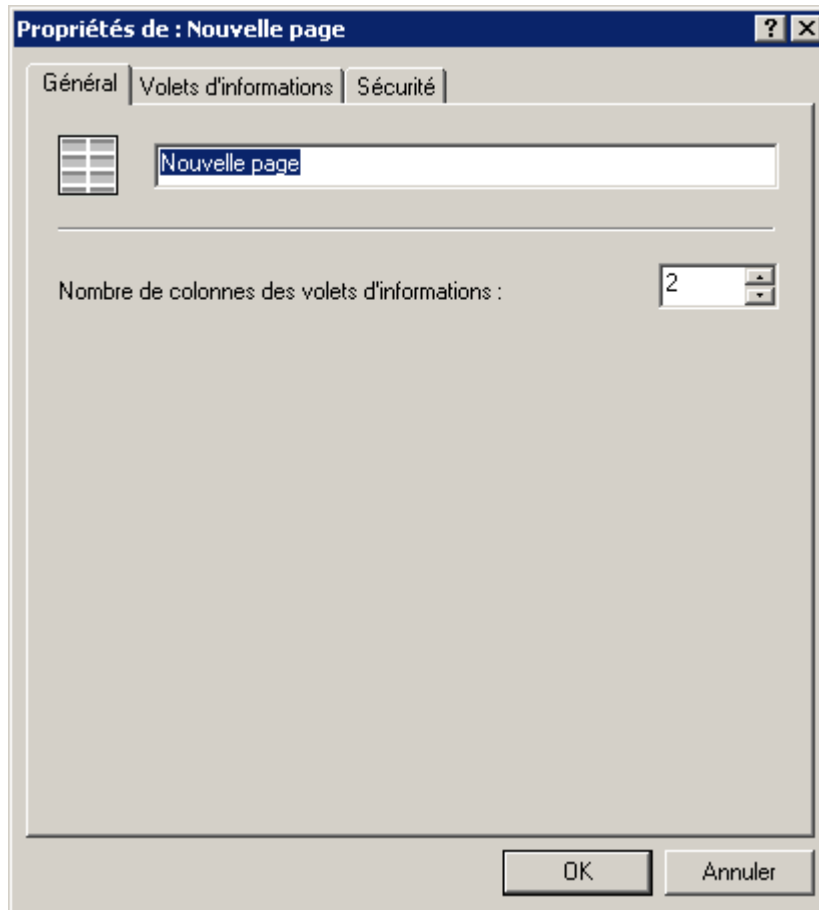



Illustration 153. Fenêtre de configuration de la nouvelle page

3. Indiquez les paramètres de la page :
 - Dans l'onglet **Général** indiquez les valeurs des paramètres suivants :
 - le nom de page ;
 - le nombre de colonnes dans les volets d'informations.
 - Dans l'onglet **Volets d'informations** formez l'ensemble des volets d'informations (cf. section "Création du volet d'information" à la page [186](#)).
4. Cliquez sur le bouton **OK** pour terminer la création de la page.

MODIFICATION DE L'ENSEMBLE DES PAGES DE STATISTIQUES

➤ Pour modifier l'ensemble des pages de statistiques, procédez comme suit :

1. Cliquez sur le bouton , situé en haut à droite de l'onglet **Statistiques**. De ce fait la fenêtre de configuration des paramètres de l'onglet s'ouvrira (cf. ill. ci-après).

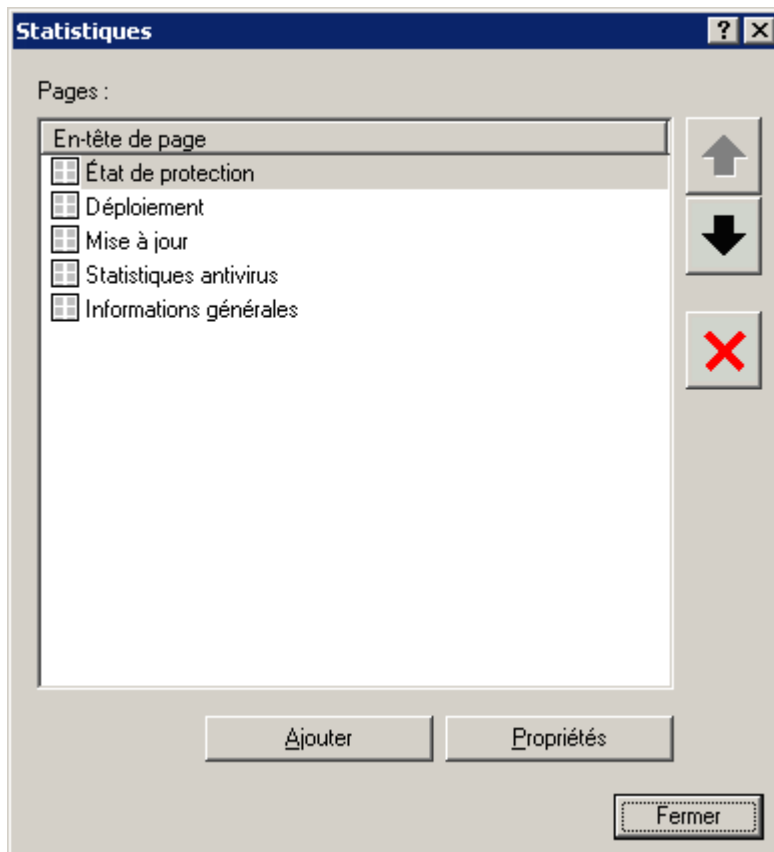






Illustration 154. Configuration des paramètres de l'onglet

2. Sélectionnez l'en-tête de page. Vous pouvez modifier l'ensemble des pages à l'aide des boutons suivants :
 - **Ajouter** : ajouter les pages dans l'onglet ;
 - **Propriétés** : modifier les paramètres de la page ;
 -  – supprimer la page ;
 -  et  – modifier l'ordre des pages sous l'onglet.

CREATION DU VOLET D'INFORMATION

➤ Pour ajouter un volet d'informations à la page, procédez comme suit :

1. Cliquez sur le bouton  situé à côté du nom de la page. Ceci permet d'ouvrir la boîte de dialogue de configuration de la page (cf. ill. ci-après).

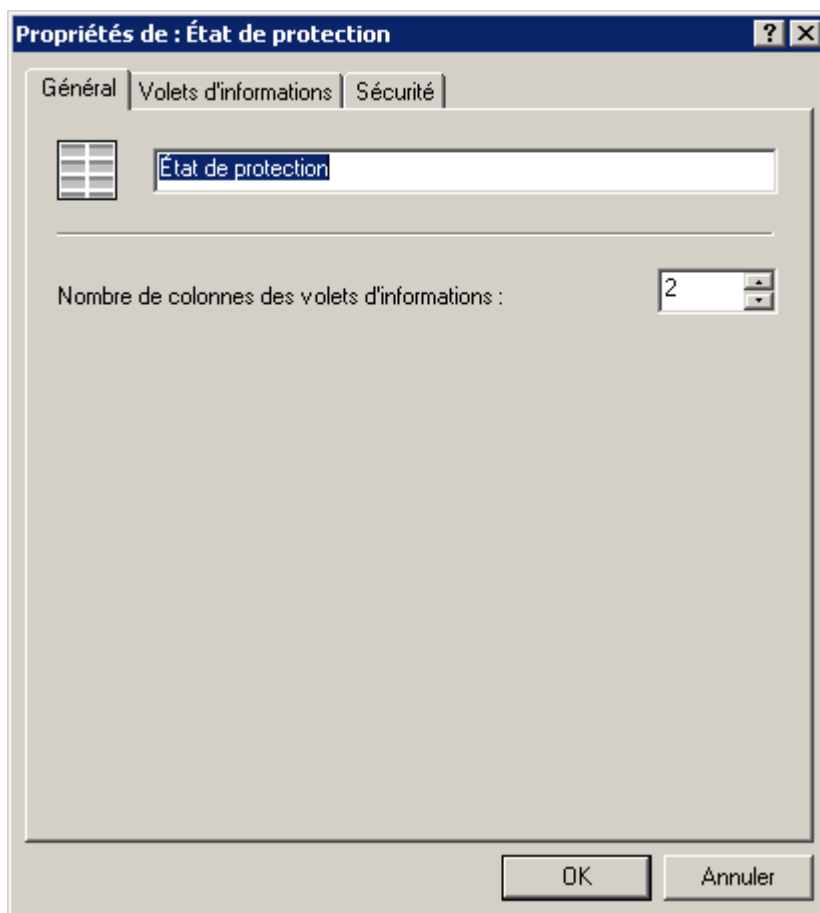


Illustration 155. Fenêtre de configuration des paramètres de la page

2. Cliquez sur le bouton **Ajouter**, situé sur l'onglet **Volets d'informations** de la fenêtre de configuration de la page. Finalement la fenêtre **Nouveau tableau de bord** (cf. ill. ci-après), qui contient la liste des volets d'informations.

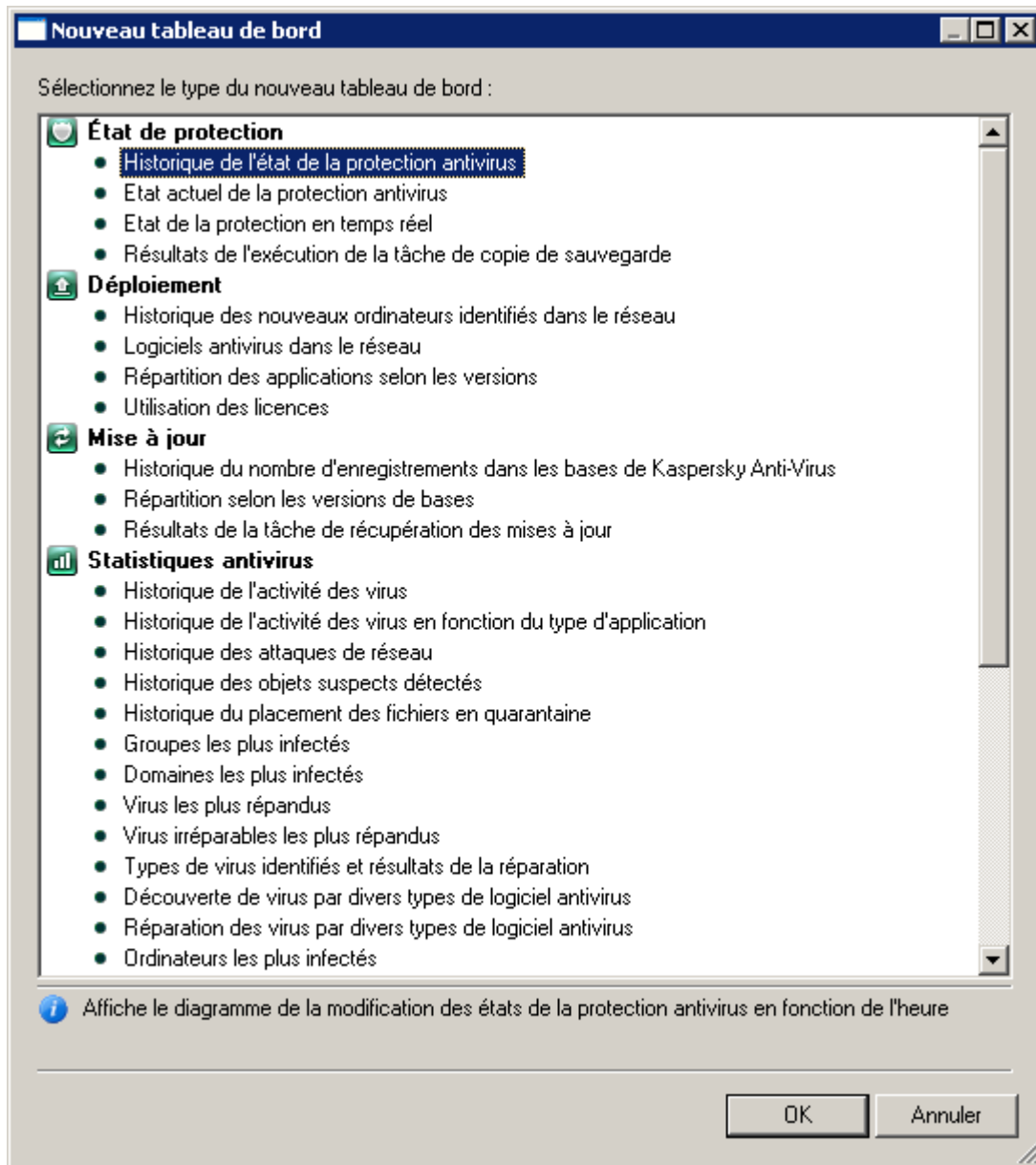


Illustration 156. Fenêtre **Nouveau tableau de bord**

- Sélectionnez de la liste le type de volet d'informations créé (cf. ill. ci-dessus). La liste des types est prédéfinie et ne peut être modifiée. Cliquez sur le bouton **OK**. Cette action entraîne l'ouverture de la fenêtre de configuration du volet d'informations (cf. ill. ci-après).

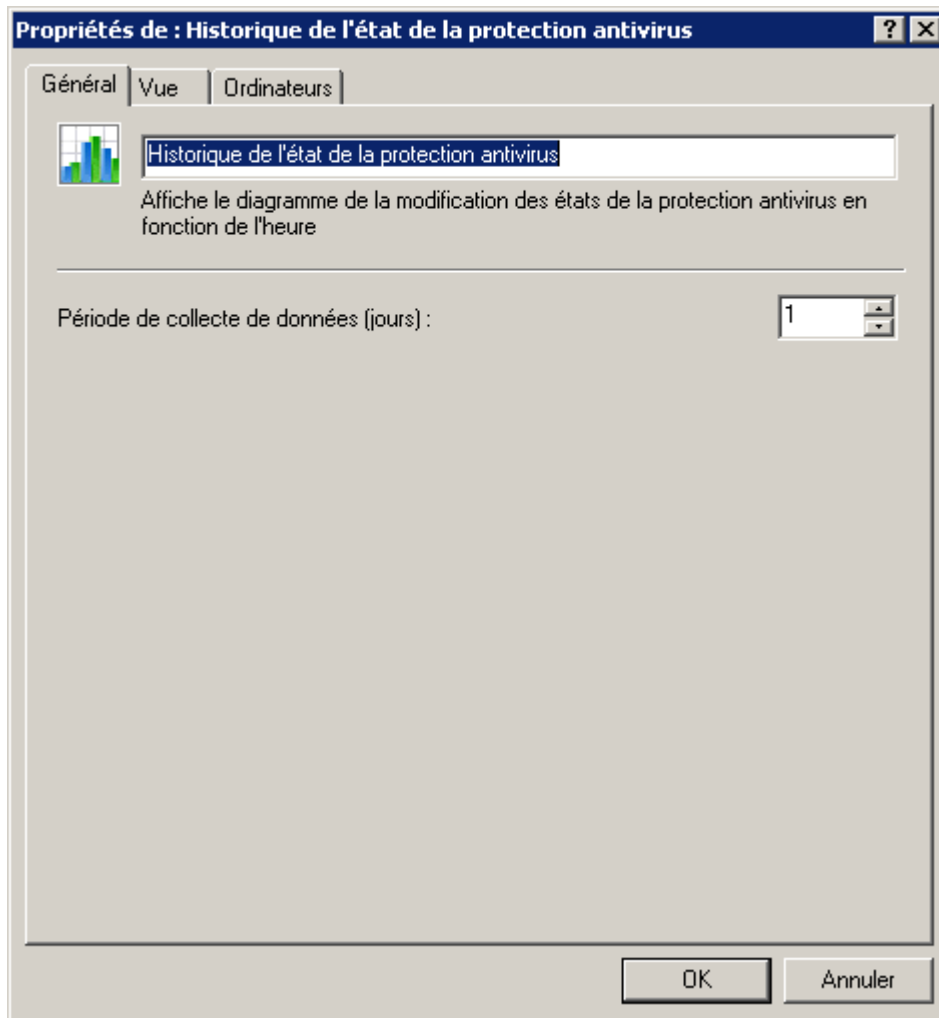


Illustration 157. Onglet **Général**

- Définissez les paramètres du volet d'informations :
 - Sur l'onglet **Général** (cf. ill. ci-dessus) précisez les valeurs des paramètres suivants :
 - nom du volet d'informations ;
 - période de collecte des données (jours). La période commence au moment de création du volet.

- Sur l'onglet **Vue** (cf. ill. ci-après) sélectionnez le type de représentation des informations (tableaux ou diagrammes), en sélectionnant la valeur nécessaire de la liste déroulante et définissez les paramètres qui correspondent à ce type.

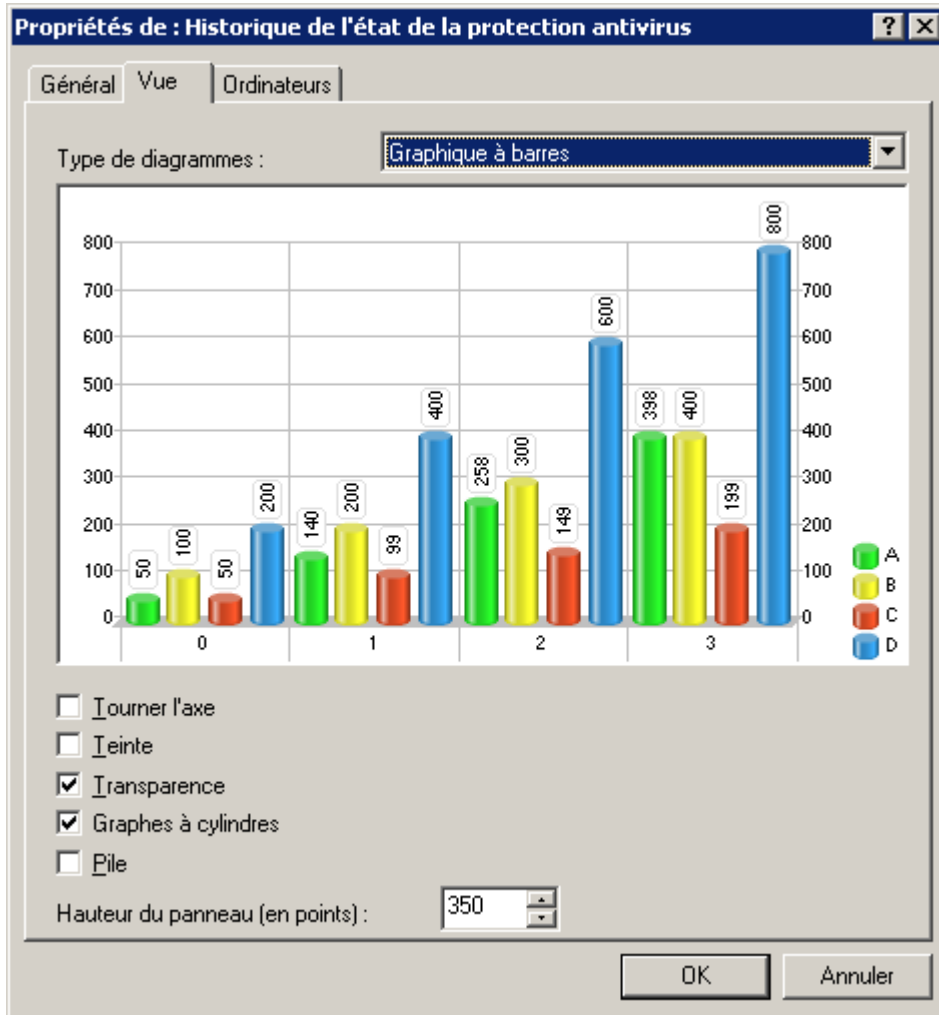


Illustration 158. Onglet **Vue**


- Désignez, sous l'onglet **Ordinateurs**, les ordinateurs au sujet desquels les données doivent être affichées dans le volet d'informations. La modification de l'onglet **Ordinateurs** n'est pas accessible pour tous les volets d'informations.

Cliquez sur le bouton **OK** pour terminer la configuration des paramètres du volet d'informations.

5. Cliquez sur le bouton **OK** pour terminer l'ajout du volet d'informations.

MODIFICATION DE L'ENSEMBLE DES PANNEAUX D'INFORMATIONS

► Pour modifier l'ensemble des panneaux d'informations, procédez comme suit :

1. Cliquez sur le bouton  situé à côté du nom de la page. Ceci permet d'ouvrir la boîte de dialogue de configuration de la page (cf. ill. ci-après).

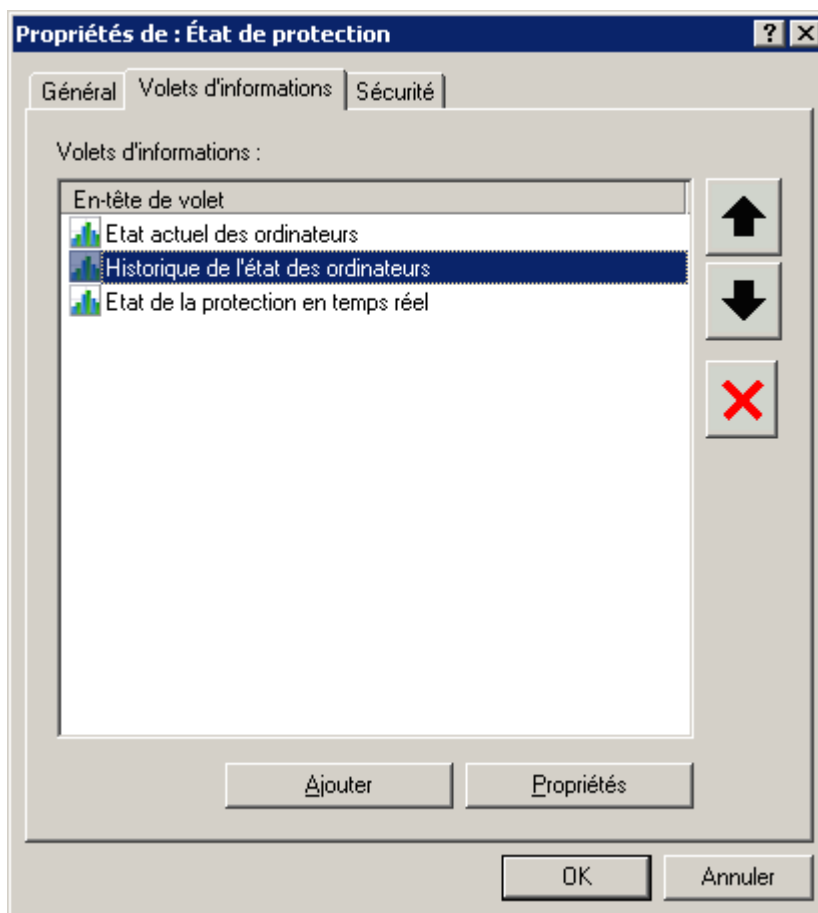





Illustration 159. Configuration de la page

2. Sélectionnez l'onglet **Volets d'informations**.
3. Sélectionnez l'en-tête de volet d'informations. Vous pouvez modifier l'ensemble des volets à l'aide des boutons suivants :
 - **Ajouter** : ajouter un volet d'informations à la page ;
 - **Propriétés** : modifier les paramètres du volet d'informations ;
 -  – supprimer un volet d'informations ;
 -  et  – modifier l'ordre des volets sur la page.

AFFICHAGE ET MODIFICATION DES MODELES DE RAPPORT

➔ Pour afficher et/ou modifier un modèle de rapport,

connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page 22) et ouvrez dans l'arborescence de la console le dossier **Rapports et notifications**. L'arborescence de la console présente une liste de modèles de rapport disponibles. Sélectionnez le modèle requis et utilisez la commande **Propriétés** du menu contextuel.

La boîte de dialogue de configuration du modèle de rapport **Propriétés de <Nom de modèle de rapport>** s'affiche. Les onglets qu'elle présente dépendent du type de rapport.

Sur l'onglet **Général** (cf. ill. ci-après), vous retrouverez les informations générales sur le modèle. Vous pouvez :

- modifier le nom du modèle du rapport ;
- consulter le nom du type de rapport, sa description, la date et l'heure de création et la dernière modification des paramètres ;
- limiter le nombre d'entrées reflétées dans le rapport (cf. section "Limitation du nombre d'entrées dans le rapport" à la page 205) ;
- cocher la case **Version à imprimer** afin que le rapport soit formaté pour l'impression ;
- inclure l'utilisation des données des Serveurs d'administration secondaires (cf. section "Rapports d'hierarchie des Serveurs d'administration" à la page 204) à l'aide du lien **Configurer la hiérarchie des Serveurs d'administration**.

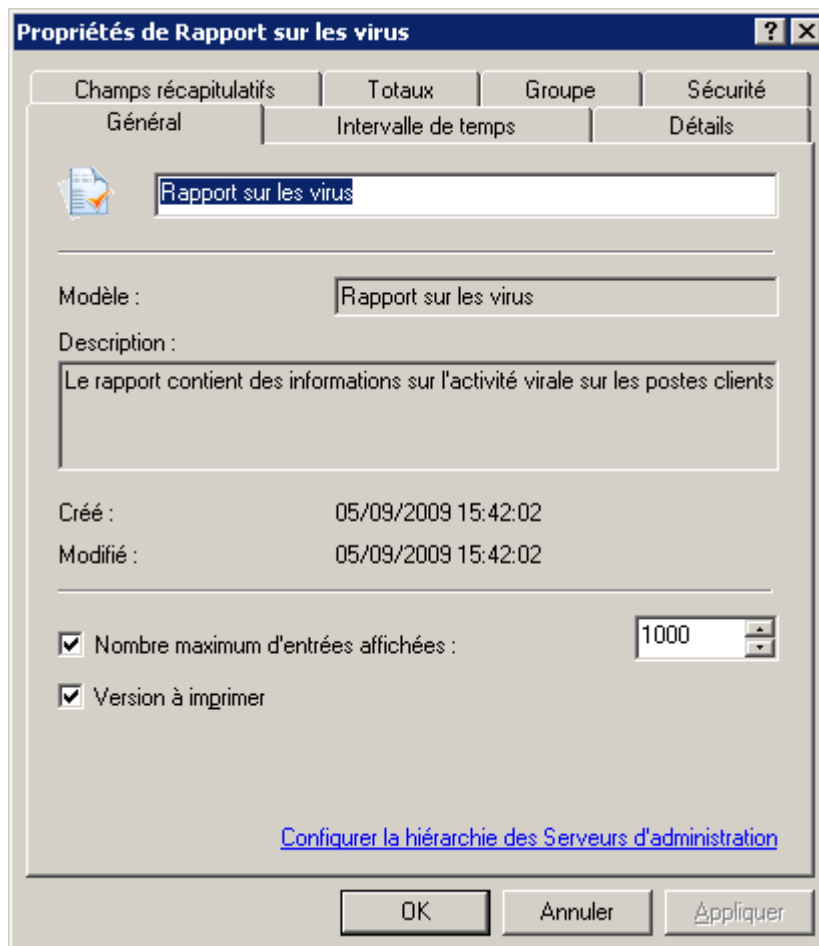


Illustration 160. Fenêtre des paramètres du modèle de rapport. Onglet **Général**

L'onglet **Détails** (cf. ill. ci-après) permet de définir les champs composant le tableau des données reprises dans le rapport, l'ordre de tri des entrées ainsi que les paramètres du filtre.

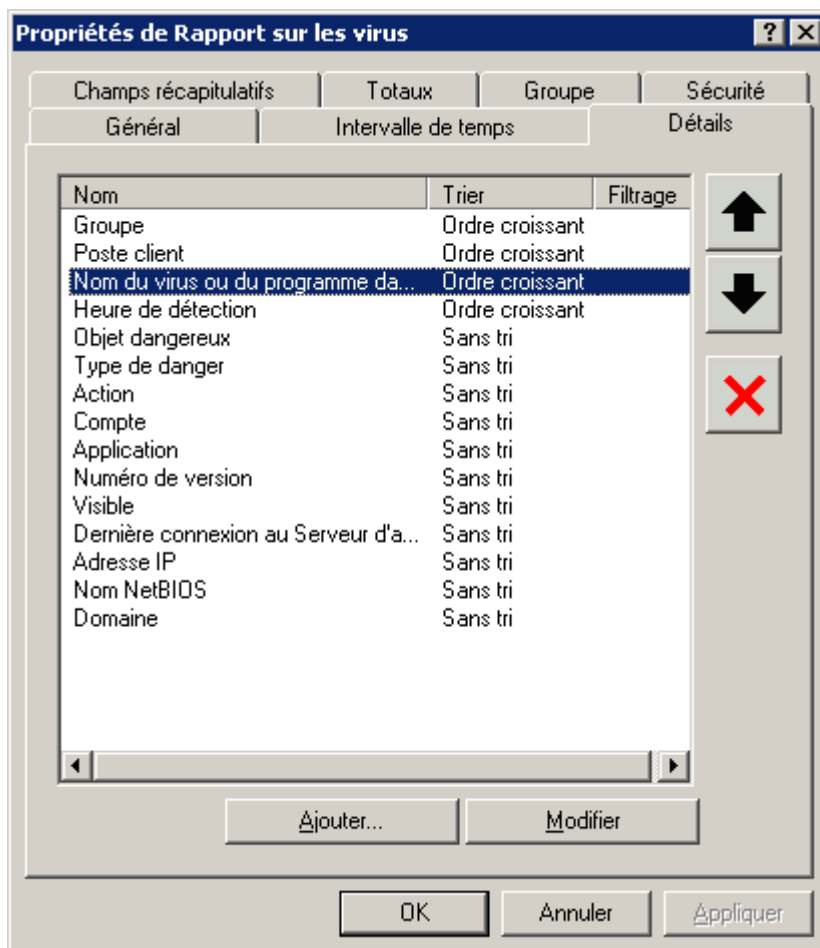


Illustration 161. Fenêtre de configuration du modèle de rapport. Onglet **Détails**

Pour créer une liste de champs, cliquez sur **Ajouter** et **Supprimer**. Vous pouvez modifier l'ordre des champs à l'aide des boutons **Monter** et **Descendre**. Pour modifier le classement dans un champ et configurer le filtre, cliquez sur **Modifier**. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), effectuez les configurations suivantes :

- Pour définir l'ordre de tri des entrées du champ sélectionné, cochez la case **Trier les valeurs du champ** et faites un choix entre **Ordre croissant** et **Ordre décroissant** ;

- Pour filtrer les enregistrements du champ sélectionné, cochez la case **Filtrer les valeurs du champ** et spécifiez les conditions du filtre dans les champs inférieurs. Chaque champ du rapport dispose de ses propres critères de filtrage.

Modifier le champ

Nom du champ :
Nom du virus ou du programme dangereux

Trier les valeurs du champ

Ordre croissant
 Ordre décroissant

Filtrer les valeurs du champ

Inclure dans le rapport les valeurs répondant à la condition suivante :

Condition : est égal à

Valeur :

OK Annuler

Illustration 162. Sélection de l'ordre de classement des champs du rapport

Définissez dans l'onglet **Champs récapitulatifs** (cf. ill. ci-après) les champs qui vont constituer le tableau des données de synthèse reprises dans le rapport et l'ordre du classement des entrées. Les paramètres repris sur cet onglet (à l'exception du filtrage) sont identiques aux paramètres de l'onglet **Détails**.

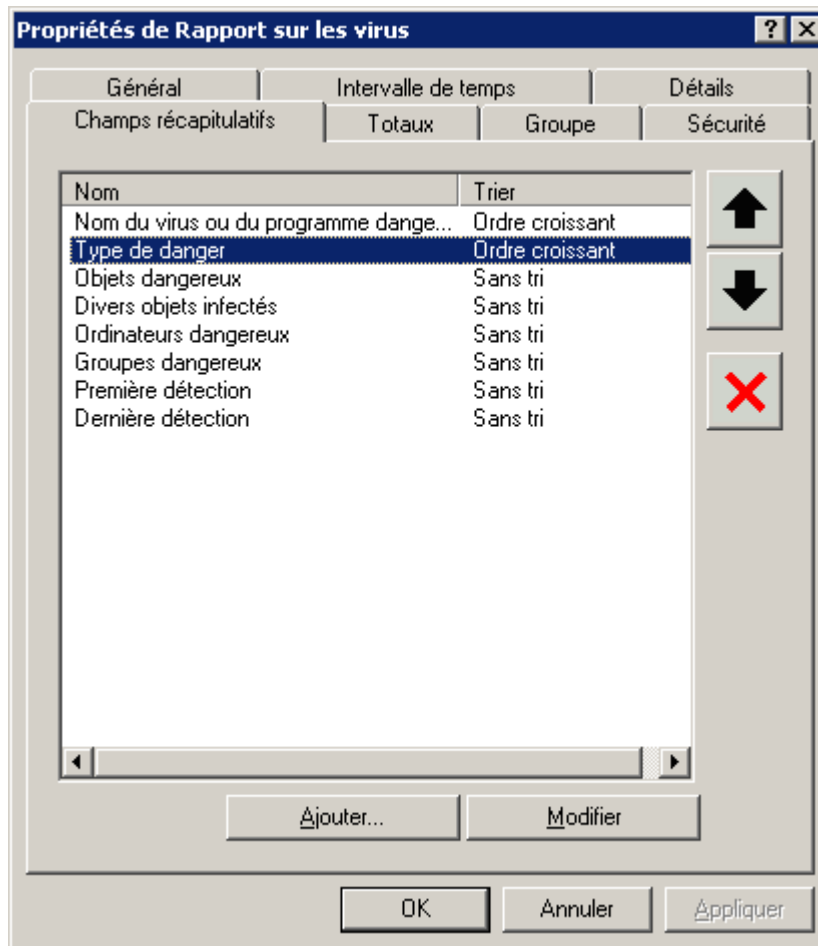


Illustration 163. Fenêtre de configuration du modèle de rapport. Onglet **Champs récapitulatifs**

L'onglet **Totaux** (cf. ill. ci-après) permet de définir les champs de calcul du rapport. Pour supprimer un champ du modèle, sélectionnez-le dans la liste **Champs de rapport** et cliquez sur **Supprimer**. Pour ajouter un champ au modèle de rapport, sélectionnez-le dans la liste **Champs disponibles** et cliquez sur **Ajouter**.

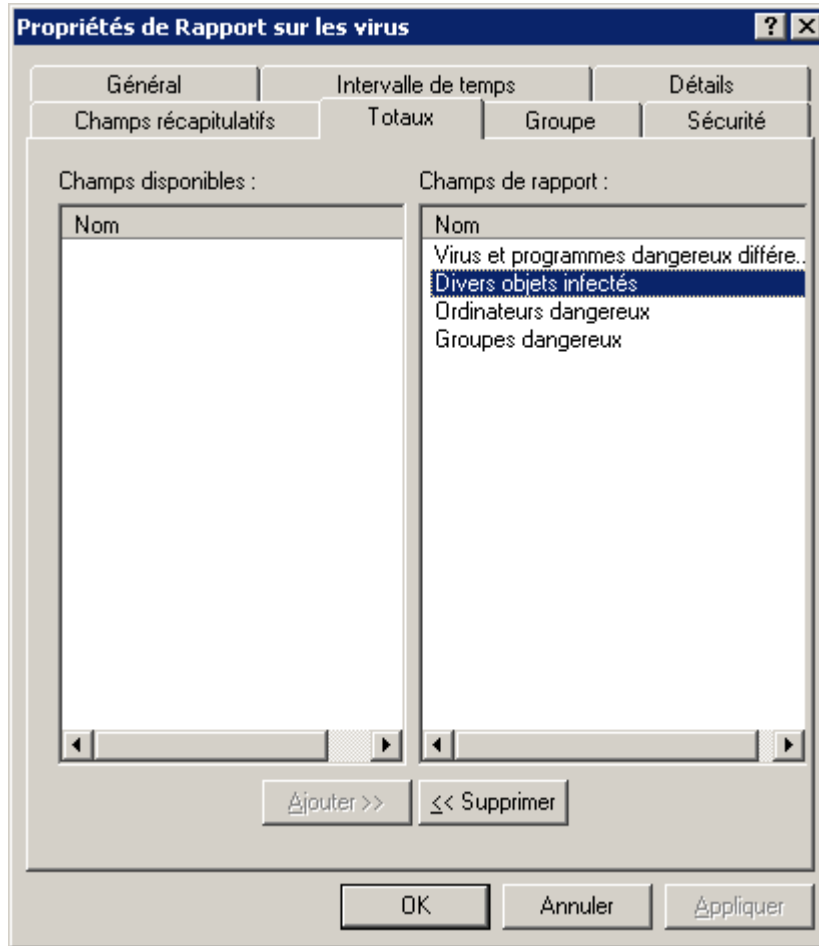


Illustration 164. Fenêtre de configuration du modèle de rapport. Onglet **Totaux**

L'onglet **Groupe** affiche le groupe, dont l'information est incluse dans le rapport. Les paramètres sont similaires aux paramètres de la fenêtre correspondante dans l'Assistant de création de modèle de rapport.

L'onglet **Sécurité** (cf. ill. ci-après) propose les privilèges des utilisateurs et des groupes d'utilisateur pour la manipulation du modèle du rapport.

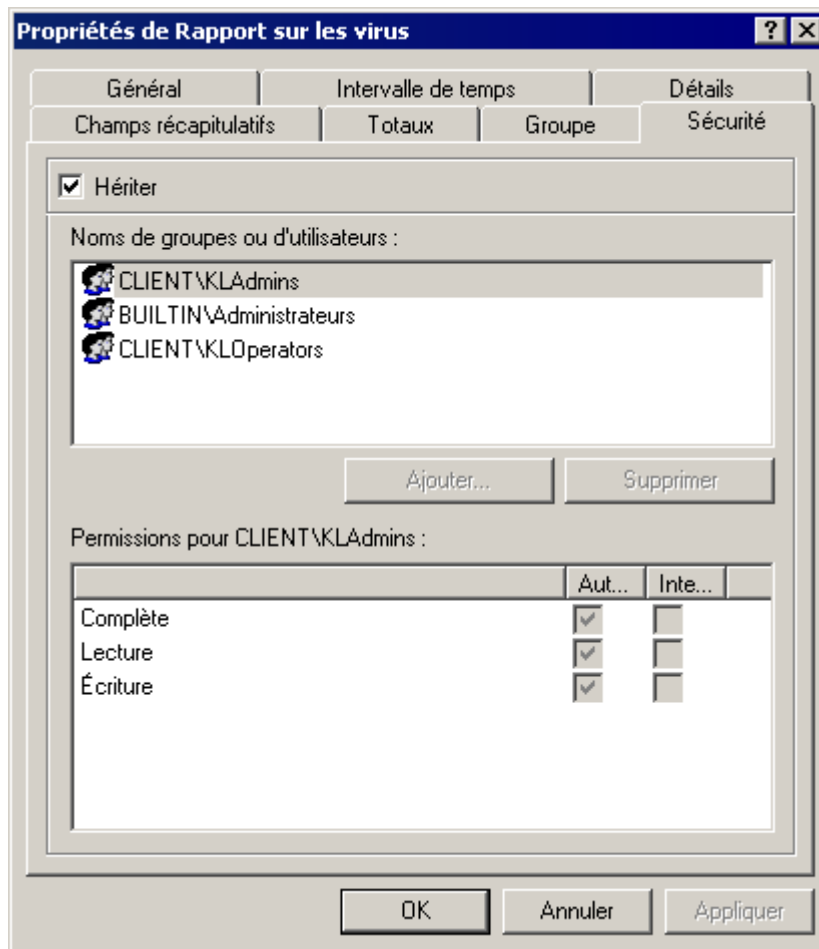


Illustration 165. Fenêtre de configuration du modèle de rapport. Onglet **Sécurité**

La présence ou l'absence de cet onglet est définie par les paramètres d'interface de l'utilisateur. Afin de configurer l'affichage de cet onglet, passez au menu **Vue** → **Configuration de l'interface** et cochez la case dans la ligne **Afficher les onglets avec les paramètres de sécurité**.

Par défaut, les droits d'utilisation d'un modèle de rapport sont hérités des propriétés du Serveur d'administration (cf. section "Affectation des droits pour travailler avec le Serveur" à la page 27), où l'on définit les privilèges de manipulation de tous les objets administrés par le Serveur. Afin de définir des privilèges d'accès à un modèle du rapport différents de ceux définis dans les paramètres du Serveur d'administration, il faut décocher la case **Hériter**.

La partie supérieure de l'onglet reprend la liste des utilisateurs et des groupes des utilisateurs qui possèdent l'accès au Serveur d'administration. La partie inférieure reprend les privilèges possibles :

- **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.

1. Sélectionnez le groupe d'utilisateurs.
2. Dans la colonne **Autoriser** cochez les cases en regard des autorisations octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.

3. Dans la colonne **Interdire** cochez les cases en regard des autorisations qui ne peuvent être octroyées à l'utilisateur. Si vous cochez la case **Complète** toutes les cases sont automatiquement cochées.

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

Pour supprimer le groupe ou l'utilisateur, il faut sélectionner l'objet dans la liste et cliquer sur le bouton **Supprimer**.

Il est impossible de supprimer le groupe d'administrateurs de Kaspersky Administration Kit (KLAdmins).

Pour appliquer les paramètres, il faut cliquer sur le bouton **Appliquer** ou **OK**.

GENERATION ET AFFICHAGE DE RAPPORTS

➤ *Pour produire un rapport et l'afficher dans la fenêtre de la Console d'administration dans le panneau des résultats, procédez comme suit :*

1. Connectez-vous au Serveur d'administration (cf. section "Administration des Serveurs d'administration" à la page [22](#)).
2. Dans l'arborescence de la console, ouvrez le dossier **Rapports et notifications** qui reprend la liste des modèles de rapports.
3. Sélectionnez le modèle qui vous intéresse dans l'arborescence de la console.

Le rapport généré s'affiche dans le panneau des résultats. L'apparence du rapport correspond au modèle sélectionné (cf. ill. ci-après), avec les éléments suivants :

- le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur les objets couverts par le rapport ;
- diagramme illustrant les données générales du rapport ;
- tableau avec les données récapitulatives (champs calculés et récapitulatifs du rapport) ;

- tableau avec les données détaillées.

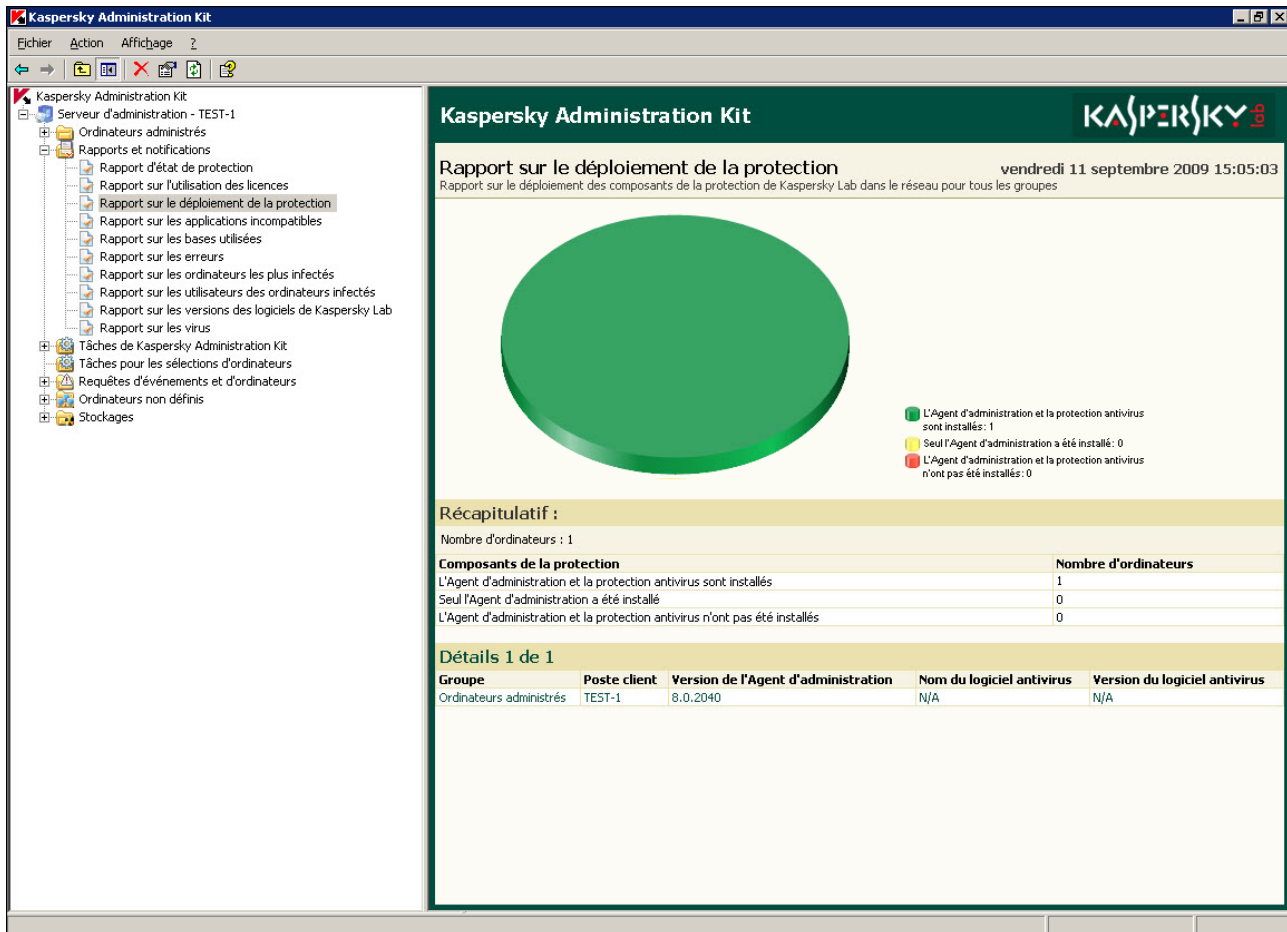


Illustration 166. Affichage du rapport dans le panneau des résultats

➤ Pour enregistrer le rapport composé sur un disque et l'afficher dans la fenêtre du navigateur, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le modèle qui vous intéresse (cf. ci-après).
2. Ouvrez le menu contextuel et utilisez la commande **Enregistrer**.
3. Dans l'Assistant qui s'ouvre cliquez sur le bouton **Suivant**.

- Dans la fenêtre suivante indiquez le chemin d'accès au dossier, dans lequel vous voulez sauvegarder le fichier de rapport, et dans le menu ouvert sélectionnez le format, dans lequel vous voulez enregistrer le rapport (cf. ill. ci-après). Cliquez sur **Suivant**.

Assistant d'enregistrement des rapports

Dossier
Sélectionnez le dossier pour l'enregistrement des fichiers du rapport

Désignez le dossier d'enregistrement des fichiers du rapport :

Sélectionnez le format du rapport :

Illustration 167. Sauvegarde du rapport. Sélection du dossier en vue de l'enregistrement sur le disque

5. Dans la fenêtre finale de l'Assistant cochez la case en regard de **Ouvrir le dossier du rapport** et cliquez sur le bouton **Terminer** (cf. ill. ci-après).

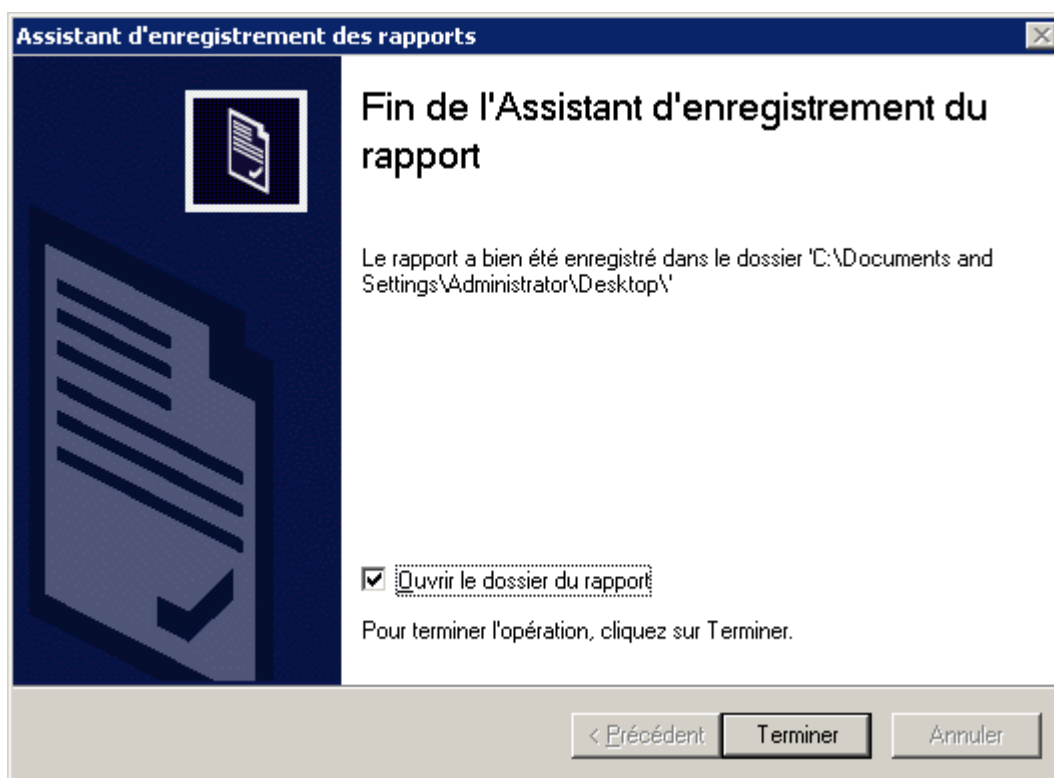


Illustration 168. Sauvegarde du rapport. Fin de l'Assistant

6. Finalement le dossier, où vous avez enregistré le fichier de rapport, s'ouvrira.

TACHE DE DIFFUSION DES RAPPORTS

La tâche de diffusion des rapports est créée automatiquement dans le cas, si les paramètres du courrier électronique ont été spécifiés lors de l'installation de Kaspersky Administration Kit.

➔ Pour créer une tâche de diffusion des rapports, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches de Kaspersky Administration Kit**, ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Tâche**.
2. Créez une tâche du Serveur d'administration (cf. section "Création d'une tâche pour le Serveur d'administration" à la page [113](#)). Lors de la création d'une tâche, spécifiez les valeurs suivantes pour les paramètres :

3. En guise de type de tâche, indiquez **Envoi du rapport** (cf. ill. ci-après).

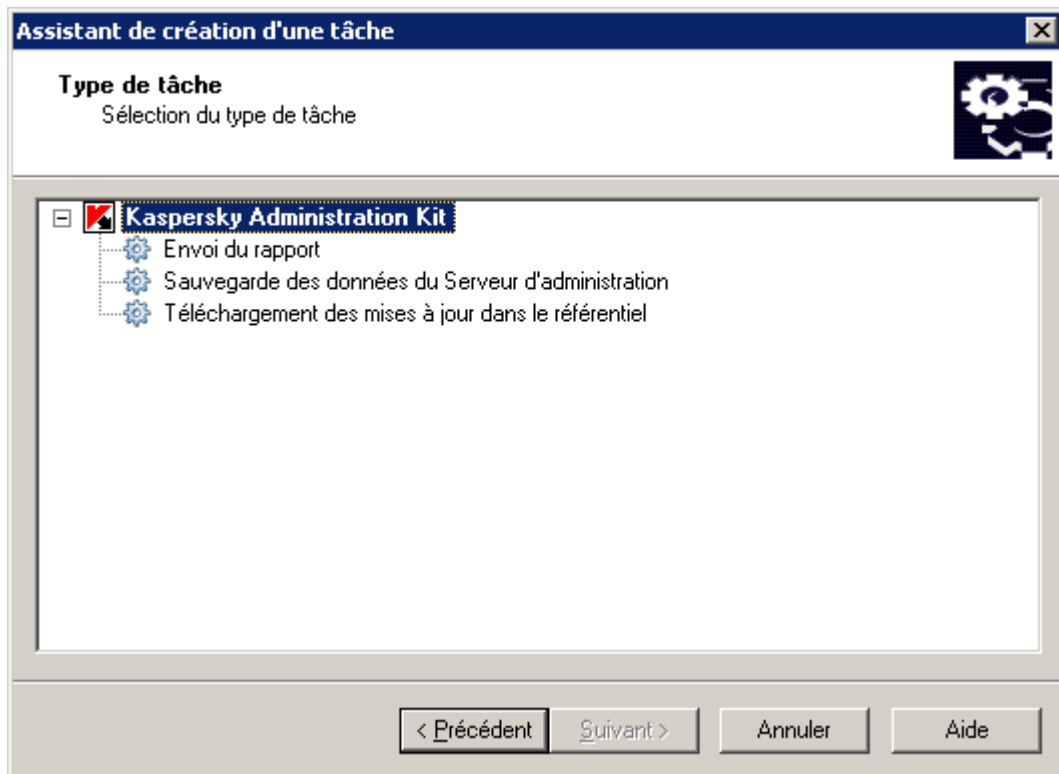


Illustration 169. Création d'une tâche de diffusion du rapport

4. Dans la fenêtre **Paramètres** (cf. ill. ci-après) :

A l'aide des cases à cocher, sélectionnez dans la liste les modèles sur la base desquels les rapports seront rédigés en vue d'une diffusion par courrier électronique.

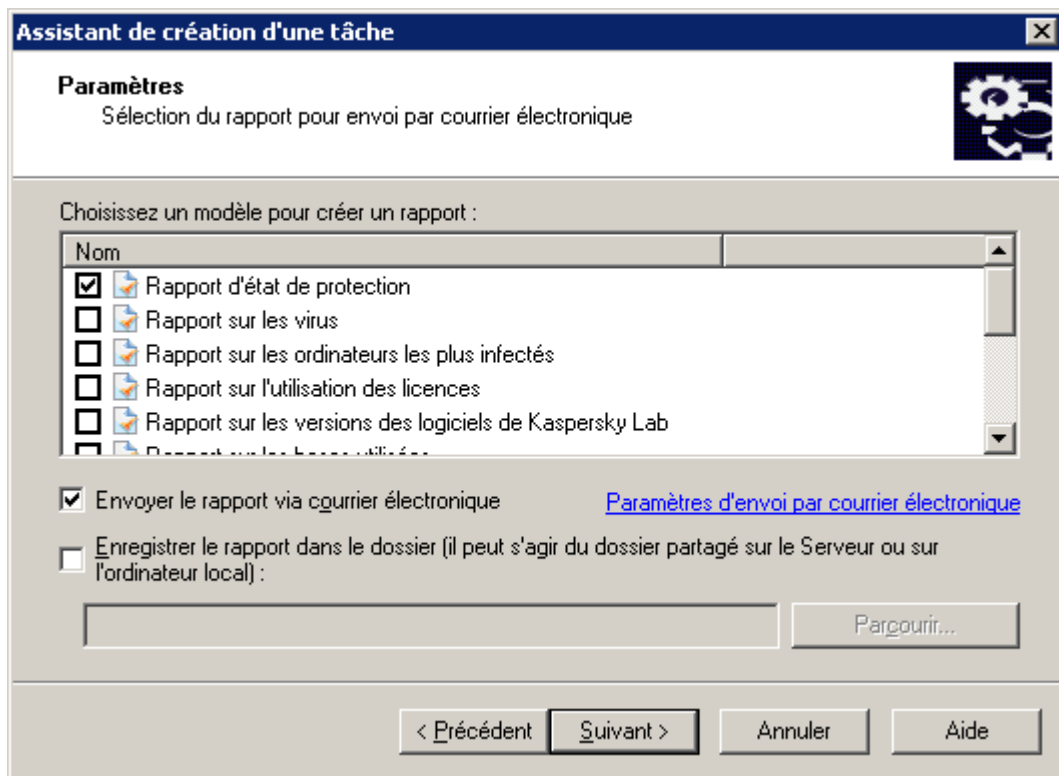


Illustration 170. Création d'une tâche de diffusion de rapports. Configuration des paramètres

Afin que les rapports soient envoyés par courrier électronique au fur et à mesure de leur création, cochez **Envoyer le rapport via courrier électronique** et à l'aide du lien **Paramètres d'envoi par courrier électronique**, désignez les paramètres.

Par défaut, ce sont les paramètres du Serveur d'administration définis lors de la configuration sur l'onglet **Notifications** (cf. section "**Affichage et modification des paramètres d'une stratégie**" à la page 79) dans la fenêtre des propriétés du dossier **Rapports et notifications**.

Dans la fenêtre **Paramètres de notification par courrier électronique** (cf. ill. ci-après), vous devez saisir vos propres paramètres :

- **Adresse du courrier électronique** : adresse du courrier électronique à laquelle les rapports seront envoyés conformément aux modèles sélectionnés et au format d'envoi indiqué ;
- **Objet** : titre du message prêt à être envoyé et contenant les rapports générés ;
- Dans le groupe **Paramètres du courrier électronique** sélectionnez une des options suivantes :
 - **Appliquer les paramètres du Serveur d'administration**, pour que les paramètres repris sous l'onglet **Notifications** dans la fenêtre des propriétés du dossier **Rapports et notifications** soient utilisés lors de l'envoi des messages électroniques.

- **Configurer de manière indépendante** afin de définir de nouveaux paramètres de serveur SMTP.

Illustration 171. Création d'une tâche de diffusion de rapports. Configuration des paramètres d'envoi par courrier électronique

Pour conserver les rapports dans le dossier, cochez la case **Enregistrer le rapport dans le dossier** et à l'aide du bouton **Parcourir**, ouvrez la fenêtre **Sélection des dossiers** et désignez le dossier dans lequel les rapports devront être enregistrés.

Pour créer une tâche de diffusion des rapports, vous pouvez également utiliser la commande **Envoi des rapports** du menu contextuel du dossier de l'arborescence de la console qui correspond au modèle de rapport voulu ou cliquer sur le lien **Créer une tâche de diffusion des rapports**, dans le panneau des tâches du dossier **Tâches de Kaspersky Administration Kit**.

➤ Pour modifier les paramètres de la tâche, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Tâches de Kaspersky Administration Kit**.
2. Sélectionnez la tâche de diffusion des rapports requise.
3. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.
4. Dans la fenêtre qui s'ouvre, ouvrez l'onglet **Paramètres** (cf. ill. ci-après). Cet onglet affiche les mêmes paramètres définis lors de la création de la tâche :
 - ensemble de modèles pour la composition des rapports ;
 - actions avec le rapport ;
 - paramètres de la diffusion par courrier électronique.

5. Spécifiez les valeurs requises des paramètres.
6. Lorsque la configuration est terminée, cliquez sur **Appliquer** ou **OK**.

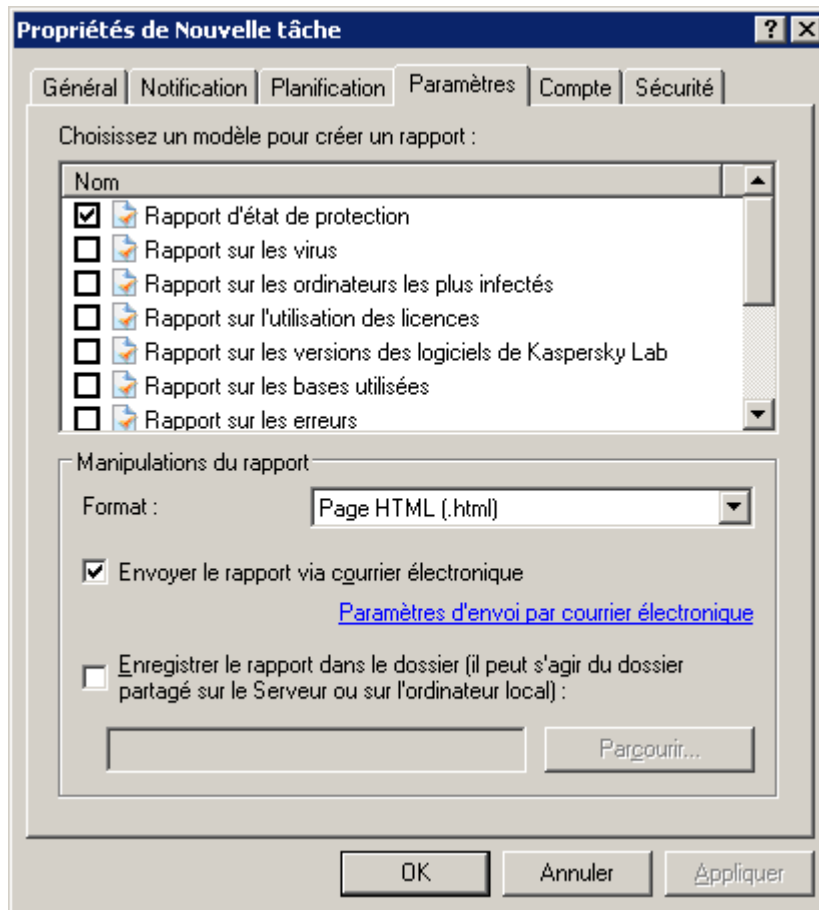


Illustration 172. Configuration des paramètres de la tâche de diffusion des rapports

Pour modifier la sélection de modèles pour la création des rapports, dans le groupe **Choisissez un modèle pour créer un rapport**, cochez les cases en regard des rapports qu'il faut absolument envoyer par courrier électronique et désélectionnez les cases en regard des rapports qui ne doivent pas être envoyés par courrier électronique.

Pour modifier les paramètres de diffusion des rapports par courrier électronique, cliquez sur le lien **Paramètres d'envoi par courrier électronique** et dans la fenêtre qui s'ouvre modifiez les valeurs des paramètres suivants.

Pour passer rapidement à la configuration des paramètres de la tâche de diffusion des rapports, cliquez sur le lien **Modifier les paramètres de la tâche** situé sur le panneau des tâches de la tâche qui vous intéresse.

RAPPORTS D'HIERARCHIE DES SERVEURS D'ADMINISTRATION

► Pour configurer l'utilisation de l'information dans un rapport des Serveurs d'administration secondaires, procédez comme suit :

1. Dans le dossier **Rapports et notifications** sélectionnez le rapport nécessaire et en ouvrant son menu contextuel sélectionnez le point **Propriétés**.

2. Dans la fenêtre qui s'ouvre, à l'onglet **Général** sur le lien **Configurer la hiérarchie des Serveurs d'administration** ouvrez la fenêtre **Hiérarchie des Serveurs d'administration** (cf. ill. ci-après).

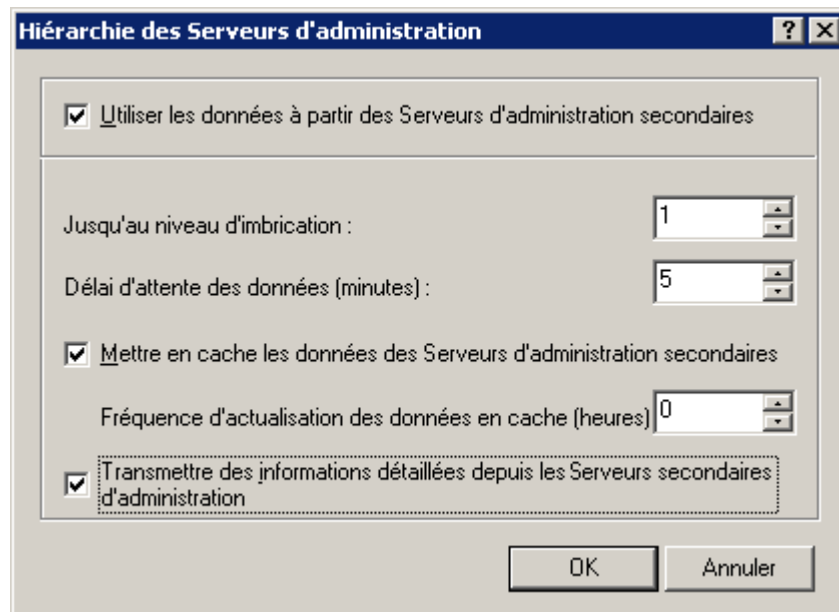


Illustration 173. Fenêtre **Hiérarchie des Serveurs d'administration**

3. Configurez les paramètres pour une hiérarchie des serveurs :

- Dans le champ **Utiliser les données à partir des Serveurs d'administration secondaires** cochez la case, si vous souhaitez utiliser des informations provenant de Serveurs secondaires.
- Dans le champ **Jusqu'au niveau d'imbrication** indiquez le degré d'imbrication des Serveurs d'administration sur lesquels vous voulez collecter des informations, en fonction de la hiérarchie du réseau.
- Spécifiez les valeurs nécessaires dans le champ **Délai d'attente des données (minutes)**. Si, lorsque ce délai est écoulé, les informations provenant du Serveur secondaire n'ont pas été réceptionnées, le Serveur est considéré comme inaccessible (cette information sera incluse dans le rapport).
- S'il est impossible d'obtenir les informations actuelles du Serveur secondaire, alors le rapport général sera produit à l'aide des données obtenues lors de la dernière connexion réussie. Pour que les données des Serveurs d'administration secondaires soient consignées dans la cache, cochez la case **Mettre en cache les données des Serveurs d'administration secondaires** et désignez la fréquence de mise en cache des données dans le champ **Fréquence d'actualisation des données en cache (heures)**.
- Pour que les informations reprises dans la section **Détails** du rapport soient transmises au Serveur d'administration principal, cochez la case **Transmettre des informations détaillées depuis les serveurs secondaires d'administration**, si la case n'est pas cochée sur le Serveur principal, seules les informations pour la section **Récapitulatif** apparaîtront dans le rapport.

4. Après avoir configuré les paramètres, cliquez sur **OK**.

LIMITATION DU NOMBRE D'ENTREES DANS LE RAPPORT

- ➔ Pour limiter le nombre d'entrées reprises dans un rapport, procédez comme suit :

Sélectionnez le modèle nécessaire du rapport dans le dossier **Rapports et notifications**. Dans le menu contextuel, cliquez sur **Propriétés** puis sur l'onglet **Général** (cf. ill. ci-après), cochez la case **Nombre maximum d'entrées affichées**. Définissez la valeur dans le champ à droite.

Pour appliquer le paramètre, cliquez sur **Appliquer** ou **OK**.

The image shows a Windows-style dialog box titled "Propriétés de Rapport sur les virus". It has a standard title bar with a question mark and a close button. The dialog is divided into four tabs: "Champs récapitulatifs", "Totaux", "Groupe", and "Sécurité". The "Général" tab is selected. Inside the "Général" tab, there are three sub-sections: "Intervalle de temps" and "Détails". The "Intervalle de temps" section contains a text box with "Rapport sur les virus" and a "Modèle :" label with another text box containing "Rapport sur les virus". The "Détails" section contains a "Description :" label and a text area with the text "Le rapport contient des informations sur l'activité virale sur les postes clients". Below this, there are two lines of text: "Créé : 05/09/2009 15:42:02" and "Modifié : 05/09/2009 15:42:02". At the bottom of the "Détails" section, there are two checked checkboxes: "Nombre maximum d'entrées affichées :" with a spin box set to "1000", and "Version à imprimer". A blue hyperlink "Configurer la hiérarchie des Serveurs d'administration" is located at the bottom of the dialog. At the very bottom, there are three buttons: "OK", "Annuler", and "Appliquer".

Illustration 174. Fenêtre des paramètres du modèle de rapport. Onglet **Général**

LIMITE DE NOTIFICATIONS

➔ Afin de configurer la restriction du nombre de notifications, procédez comme suit :

1. Passez au lien **Configurer la restriction du nombre de notifications** situé dans les propriétés du dossier **Rapports et notifications**. Cette action entraîne l'ouverture de la fenêtre de configuration de la restriction du nombre de notifications (cf. ill. ci-après).

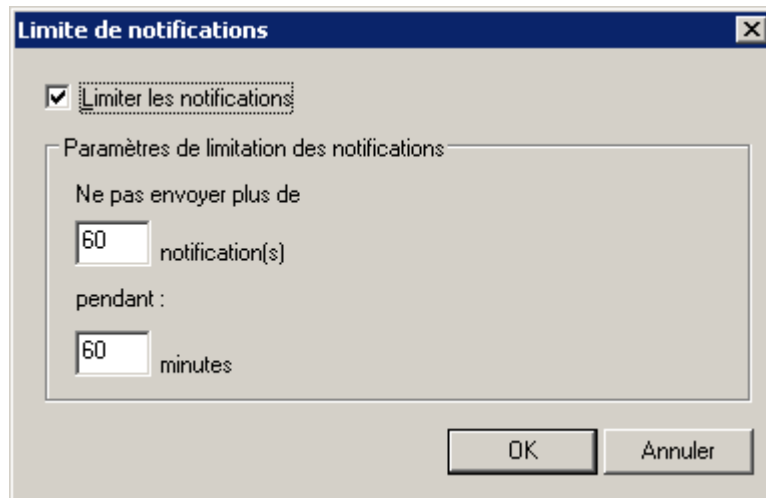


Illustration 175. Limite de notifications

2. Dans la fenêtre ouverte cochez la case **Limiter les notifications** et définissez les valeurs des paramètres suivants :
 - nombre maximum des notifications envoyées par le Serveur d'administration ;
 - période de temps pendant lequel le Serveur d'administration peut générer des notifications.
3. Cliquez sur le bouton **OK** pour terminer la configuration de la restriction du nombre de notifications.

NOTIFICATIONS

Kaspersky Administration Kit offre la possibilité de configurer des paramètres généraux des notifications du Serveur d'administration.

L'administrateur peut aussi configurer les paramètres des notifications sur les événements du Serveur d'administration, de Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers.

Kaspersky Administration Kit permet de sélectionner le mode de notifications qui vous convient le mieux :

- Courrier électronique (cf. section "Notification par courrier électronique" à la page [208](#)).
- NET SEND (cf. section "Notifications via NET SEND" à la page [210](#)).
- Fichier exécutable à lancer (cf. section "Notification à l'aide du fichier exécutable" à la page [211](#)).

NOTIFICATION PAR COURRIER ELECTRONIQUE

➤ Afin de configurer les paramètres généraux des notifications par courrier électronique, procédez comme suit :

1. Ouvrez l'onglet **Notifications** dans les propriétés du dossier **Rapports et notifications**. Ceci permet d'ouvrir la boîte de dialogue de configuration de notification.
2. Définissez les valeurs des paramètres (cf. ill. ci-après).

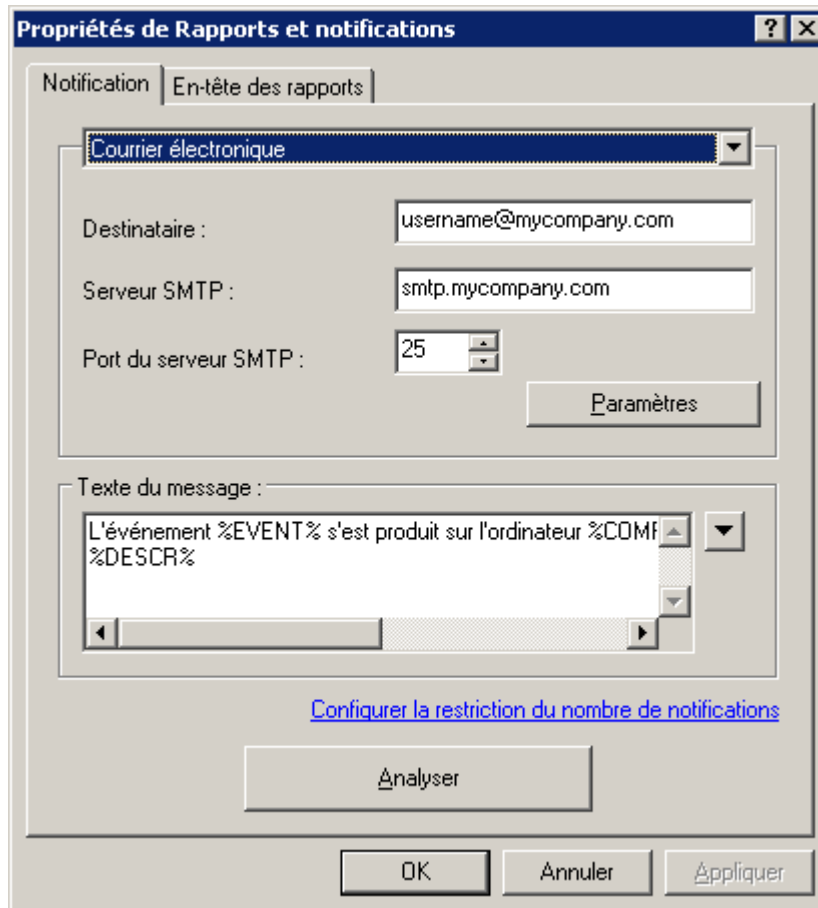


Illustration 176. Modification des paramètres de notification par courrier électronique

3. De la liste déroulante sélectionnez le mode de notification **Courrier électronique** (cf. ill. ci-dessus). Dans ce cas :
 - dans la zone **Destinataire** indiquez l'adresse de messagerie du destinataire. Vous pouvez indiquer plusieurs adresses séparées par une virgule ou un point-virgule ;
 - saisissez l'adresse du serveur de messagerie dans la zone **Serveur SMTP** (vous pouvez utiliser une adresse IP ou le nom dans le réseau Windows) ;
 - dans la zone **Port du serveur SMTP** spécifiez le numéro de port du serveur SMTP (le numéro de port par défaut est 25) ;

- définissez le sujet du message de notification. Cliquez sur **Paramètres** et dans la boîte de dialogue affichée (cf. ill. ci-après), remplissez le champ **Objet**. Le texte de la notification peut donner des informations sur l'événement enregistré. Pour apporter ces explications, sélectionnez les paramètres suivants dans les listes déroulantes disponibles à travers le bouton ▾. Si le serveur SMTP nécessite une authentification, précisez le **Nom d'utilisateur** et le **Mot de passe** dans les zones correspondantes.

Paramètres [?] [X]

Objet :
 ▾

Autorisation ESMTTP requise

Nom d'utilisateur :

Mot de passe :

Confirmation du mot de passe :

L'adresse du courrier électronique de l'expéditeur. Si le paramètre n'est pas défini, l'adresse du destinataire sera utilisée.
 Attention : il est déconseillé d'indiquer une adresse de courrier électronique qui n'existe pas dans ce champ.

OK Annuler

Illustration 177. Définition des paramètres d'envoi des notifications. Expéditeur et objet des notifications

- Indiquez les paramètres de restriction des notifications.

- Pour vérifier les valeurs spécifiées dans l'onglet Paramètres, envoyez manuellement des messages de test. Pour ce faire, cliquez sur **Analyser**. Cette action entraîne l'ouverture de la fenêtre d'envoi d'une notification d'essai (cf. ill. ci-après). En cas d'erreur, des informations détaillées seront fournies.

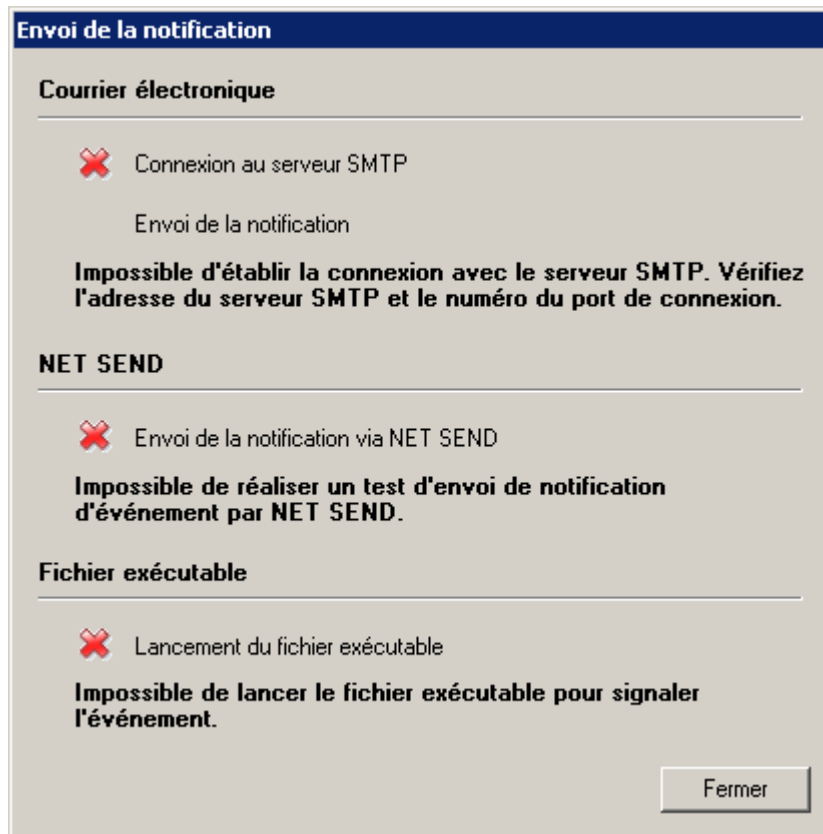


Illustration 178. Définition des paramètres d'envoi des notifications. Envoi d'une notification d'essai

- Cliquez sur le bouton **OK** pour terminer l'opération.

NOTIFICATIONS VIA NET SEND

- Afin de configurer les paramètres généraux des notifications à l'aide de NET SEND, procédez comme suit :
 - Sélectionnez l'onglet **Notifications** dans les propriétés du dossier **Rapports et notifications**. Ceci permet d'ouvrir la boîte de dialogue de configuration de notification.
 - Dans la liste déroulante sélectionnez le mode de notification **NET SEND** (cf. ill. ci-après).

Dans ce cas, indiquez l'adresse des ordinateurs qui recevront les notifications par le réseau. Vous pouvez également utiliser une adresse IP ou le nom de l'ordinateur dans le réseau Windows. Vous pouvez écrire plus d'une adresse séparée par une virgule ou un point-virgule. Afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les ordinateurs le Messenger doit être lancé.

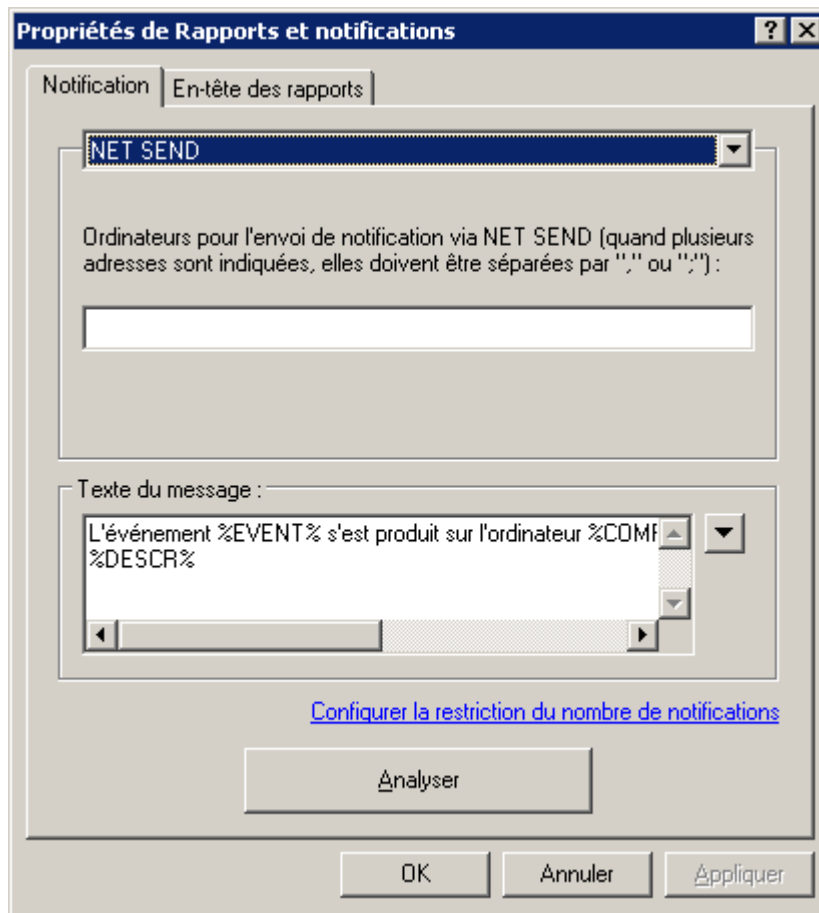


Illustration 179. Configuration de l'envoi des notifications. Envoi de notifications à l'aide de NET SEND

3. Indiquez les paramètres de restriction des notifications.
4. Pour vérifier les valeurs spécifiées dans l'onglet Paramètres, envoyez manuellement des messages de test. Pour ce faire, cliquez sur **Analyser**. Cette action entraîne l'ouverture de la fenêtre d'envoi d'une notification d'essai (cf. ill. ci-après). En cas d'erreur, des informations détaillées seront fournies.
5. Cliquez sur le bouton **OK** pour terminer l'opération.

NOTIFICATION A L'AIDE DU FICHIER EXECUTABLE

➤ Afin de configurer les paramètres généraux des notifications à l'aide du lancement du fichier exécutable, procédez comme suit :

1. Sélectionnez l'onglet **Notifications** dans les propriétés du dossier **Rapports et notifications**. Ceci permet d'ouvrir la boîte de dialogue de configuration de notification.
2. Dans la liste déroulante sélectionnez le mode de notification **Fichier exécutable à lancer** (cf. ill. ci-après).

Dans ce cas, appuyez sur le bouton **Sélectionner** pour indiquer le module exécutable à lancer lorsqu'un événement se produit.

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

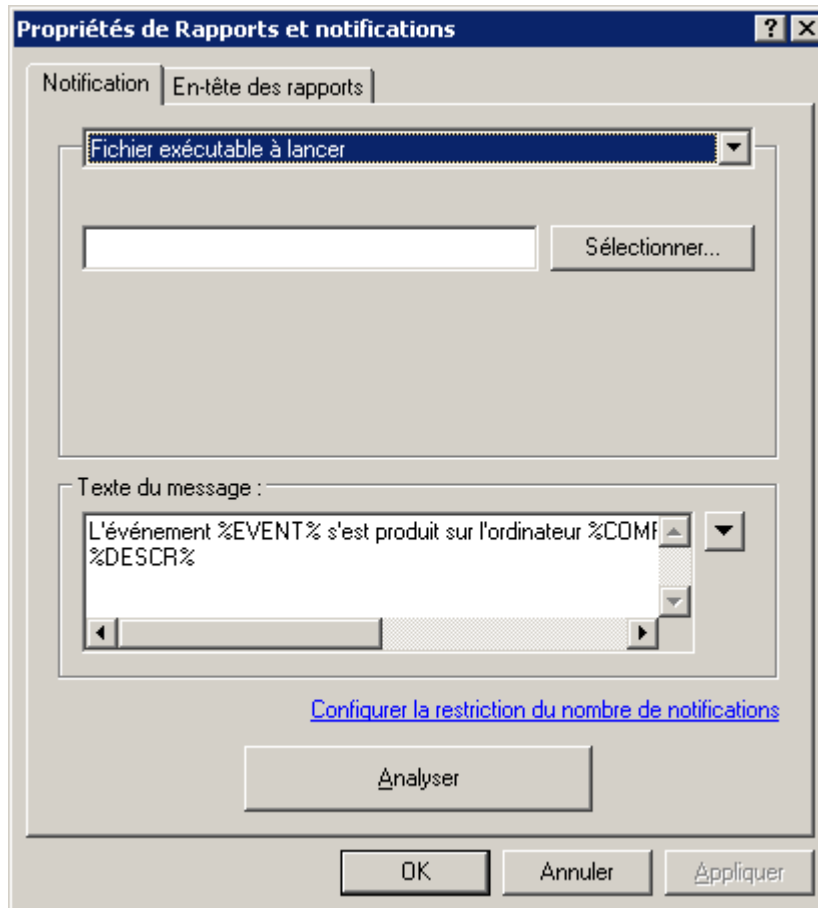


Illustration 180. Configuration de l'envoi des notifications. Envoi de notifications à l'aide d'un exécutable.

Dans la partie inférieure du bloc **Texte du message** (cf. ill. ci-après), écrivez le texte de la notification à envoyer.

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

- **Degré d'importance de l'événement ;**
- **A partir de l'ordinateur ;**
- **Domaine ;**
- **Événement ;**
- **Description d'événement ;**
- **Heure ;**
- **Nom de tâche ;**
- **Application ;**
- **Numéro de version ;**

- Adresse IP ;
 - Adresse IP de la connexion.
3. Indiquez les paramètres de restriction des notifications.
 4. Pour vérifier les valeurs spécifiées dans l'onglet Paramètres, envoyez manuellement des messages de test. Pour ce faire, cliquez sur **Analyser**. Cette action entraîne l'ouverture de la fenêtre d'envoi d'une notification d'essai (cf. ill. ci-après). En cas d'erreur, des informations détaillées seront fournies.
 5. Cliquez sur le bouton **OK** pour terminer l'opération.

EXTRACTION DES EVENEMENTS ET DES ORDINATEURS

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 et de créer des requêtes d'événements et d'ordinateurs. Les données peuvent être enregistrées dans le journal système de Microsoft Windows, ainsi que dans le journal des événements de Kaspersky Administration Kit. Les informations relatives à l'état du système de la protection antivirus et des postes clients sont accumulées dans le dossier **Requêtes d'événements et d'ordinateurs**.

DANS CETTE SECTION

Requêtes d'événements.....	214
Requêtes d'ordinateurs	222

REQUETES D'EVENEMENTS

Les informations relatives aux événements enregistrés durant le fonctionnement du système de protection antivirus sont présentées sous la forme de requêtes et elles sont contenues dans le dossier **Evénements**.

Une fois que l'application a été installée, le dossier contient diverses requêtes standards. Il est possible de créer des requêtes complémentaires et d'exporter des informations relatives aux événements dans un fichier.

AFFICHAGE DU JOURNAL DES EVENEMENTS DE KASPERSKY ADMINISTRATION KIT

► *Pour afficher le journal d'événements de Kaspersky Administration Kit entreposé sur le Serveur d'administration,*

Connectez-vous au Serveur d'administration nécessaire (cf. section "Administration des Serveurs d'administration" à la page [22](#)), déployez le dossier **Requêtes d'événements et d'ordinateurs** → **Evénements** de l'arborescence de la console et sélectionnez le dossier correspondant à la requête qui vous intéresse.

L'offre de requêtes suivantes est proposée par défaut : **Derniers événements, Evénements d'information, Evénements critiques, Erreurs, Avertissements, Evénements d'audit**. Il est impossible de modifier les paramètres de ces requêtes, à l'exception de **Derniers événements**.

Pour ouvrir la requête d'événements souhaitée, vous pouvez aussi cliquer sur le lien correspondant dans la barre des tâches du dossier **Evénements**.

Le panneau de détails présente alors un tableau (cf. ill. ci-après) énumérant tous les événements du type sélectionné entreposés sur ce Serveur d'administration (pour tous les groupes et applications installées). Le tableau possède les colonnes suivantes :

- **Degré d'importance** : degré d'importance de l'événement.
- **Poste client** : nom du client ou du Serveur d'administration sur lequel l'événement s'est produit.
- **Groupe** : nom du groupe auquel appartient ce client.
- **Application** : nom de l'application qui a produit cet événement.

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

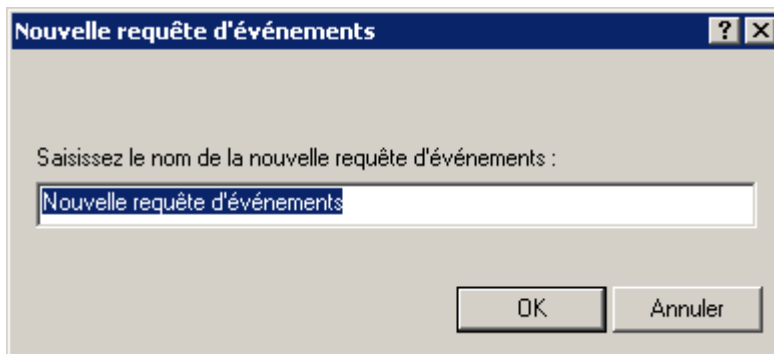


Illustration 182. Création d'une requête d'événements

Vous pouvez modifier l'ordre des colonnes, en ajouter ou en supprimer, pour une requête créée manuellement.

► Pour modifier la sélection des colonnes proposées pour n'importe quelle requête d'événements, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Requêtes d'événements et d'ordinateurs** → **Evénements** et sélectionnez la requête qui vous intéresse.
2. Ouvrez le menu contextuel et sélectionnez la commande **Vue** → **Ajouter/supprimer des colonnes**.
3. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), composez la liste des colonnes à afficher à l'aide des boutons **Ajouter** et **Supprimer**. L'ordre d'affichage des colonnes est défini par les boutons **Monter** et **Descendre**.

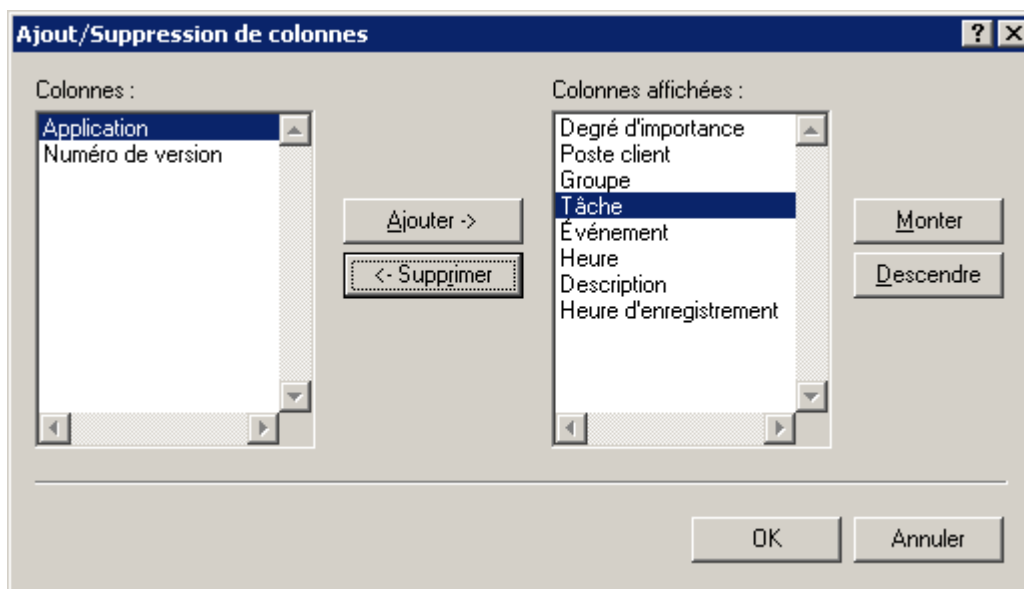


Illustration 183. Fenêtre **Ajout/Suppression de colonnes**

La liste des événements dans le panneau des résultats est actualisée automatiquement selon les paramètres indiqués.

CONFIGURATION D'UNE REQUETE D'EVENEMENTS

► Pour configurer une requête, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Requêtes d'événements et d'ordinateurs**.

2. Ouvrez le dossier **Événements** et sélectionnez la requête d'événements souhaitée.
3. Ouvrez le menu contextuel et utilisez la commande **Propriétés**.

Ceci permet d'ouvrir la boîte de dialogue de configuration des requêtes, qui contient les onglets suivants : **Général**, **Événements**, **Ordinateurs** et **Heure**.

Pour les requêtes d'événements prédéfinies, la fenêtre contient uniquement l'onglet **Général**. La fenêtre des paramètres de la requête **Derniers événements** contient également l'onglet **Heure** où vous pouvez définir l'intervalle de la requête.

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez :

- Modifier le nom de la requête.
- Limiter la quantité d'informations, affichées dans la requête. Pour ce faire, cochez la case **Limiter le nombre d'événements affichés** et spécifiez le nombre de lignes maximum du tableau.
- Limiter le nombre d'événements, où se déroule la recherche des événements de la requête. Pour ce faire, cochez la case **Restreindre la recherche par les derniers événements en quantité** et spécifiez le nombre d'événements de recherche maximum.

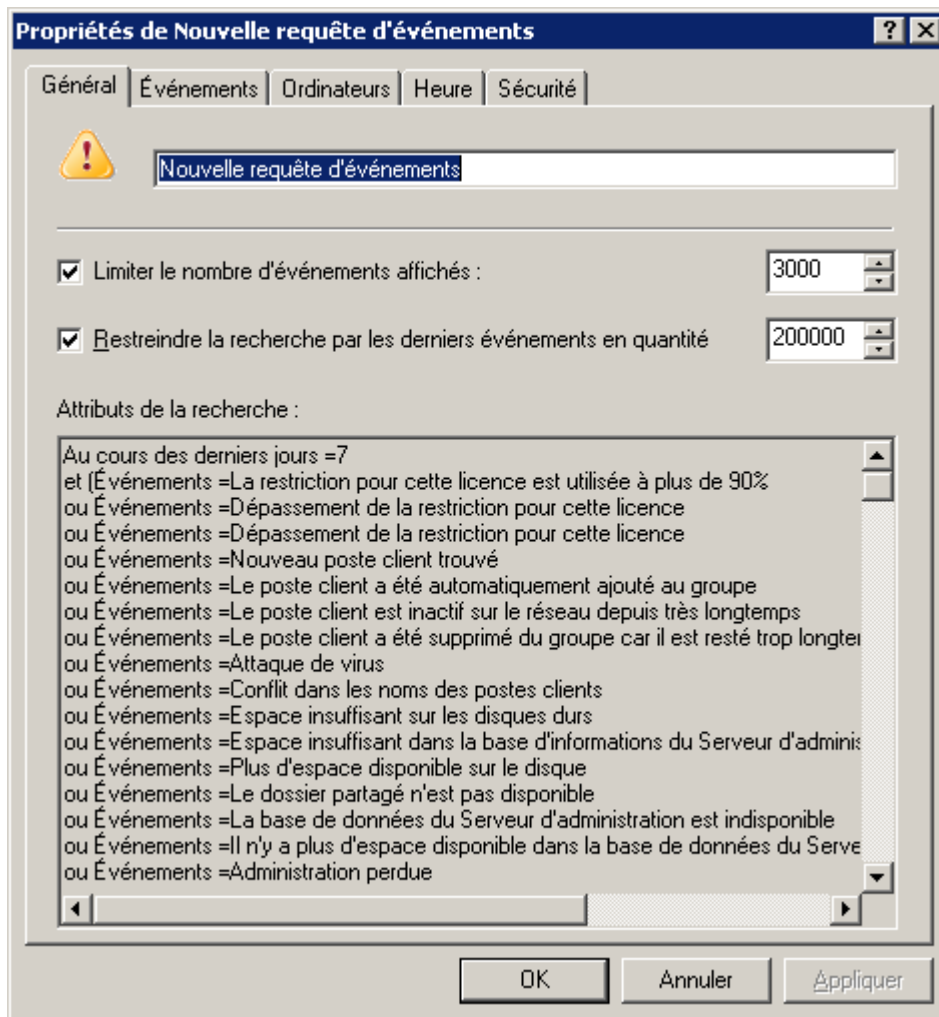


Illustration 184. Configuration d'une requête d'événements. Onglet **Général**

L'onglet **Evénements** (cf. ill. ci-après) permet de définir quels types d'événements et de résultats de tâche devront être compris dans la requête :

- Nom de l'application dont les opérations vous intéressent.
- Numéro de version de l'application.
- Nom de tâche dont vous souhaitez afficher les résultats.
- Sélectionnez dans la liste déroulante le niveau d'importance de l'événement.

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

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

- Cochez la case **Uniquement les derniers résultats des tâches**, afin d'afficher uniquement des informations sur les résultats de la dernière exécution de la tâche.

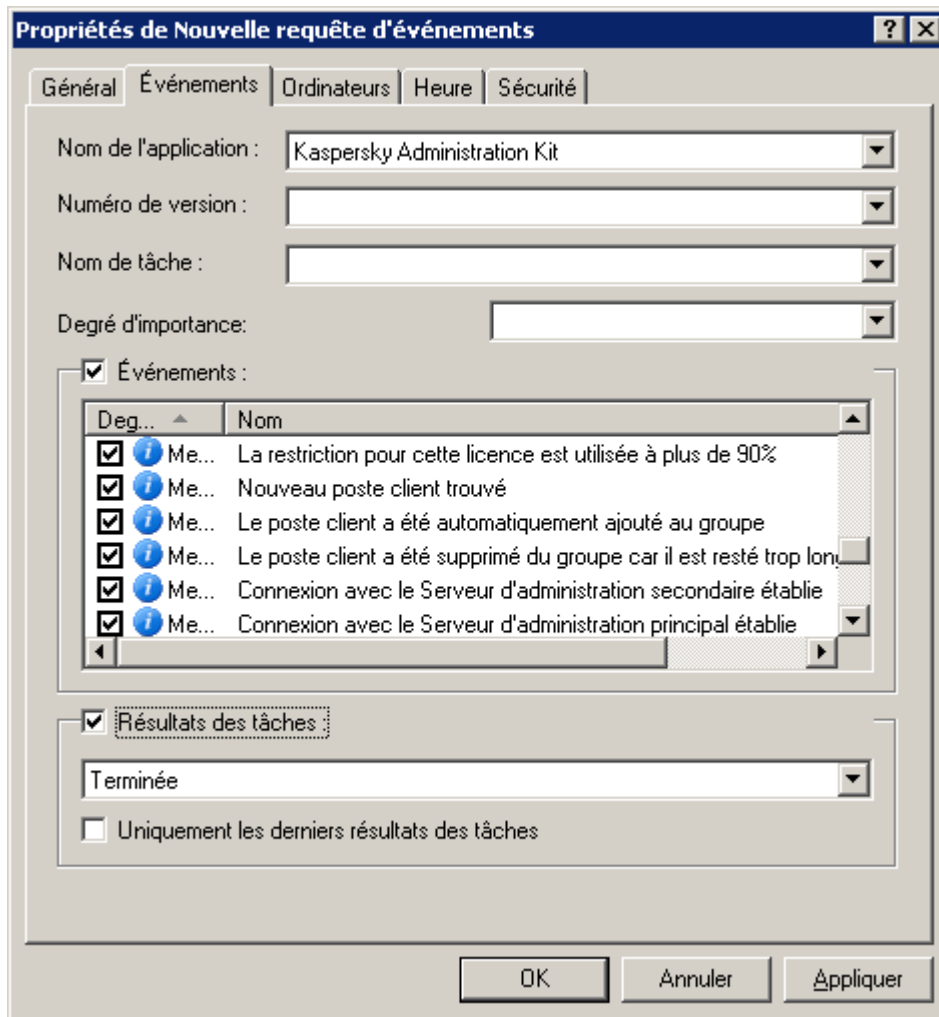


Illustration 185. Configuration d'une requête d'événements. Onglet **Événements**

L'onglet **Ordinateurs** (cf. ill. ci-après) permet de définir quels types d'événements et de résultats de tâche devront être compris dans la requête. Vous pouvez utiliser les paramètres suivants :

- Nom de l'ordinateur ;
- Nom de l'ordinateur dans le réseau Windows ;
- Groupe d'administration ;
- Domaine ;

- Pour spécifier la plage des adresses IP des ordinateurs, cochez la case **Plage d'adresses IP** et renseignez les **adresses IP** de début et de fin.

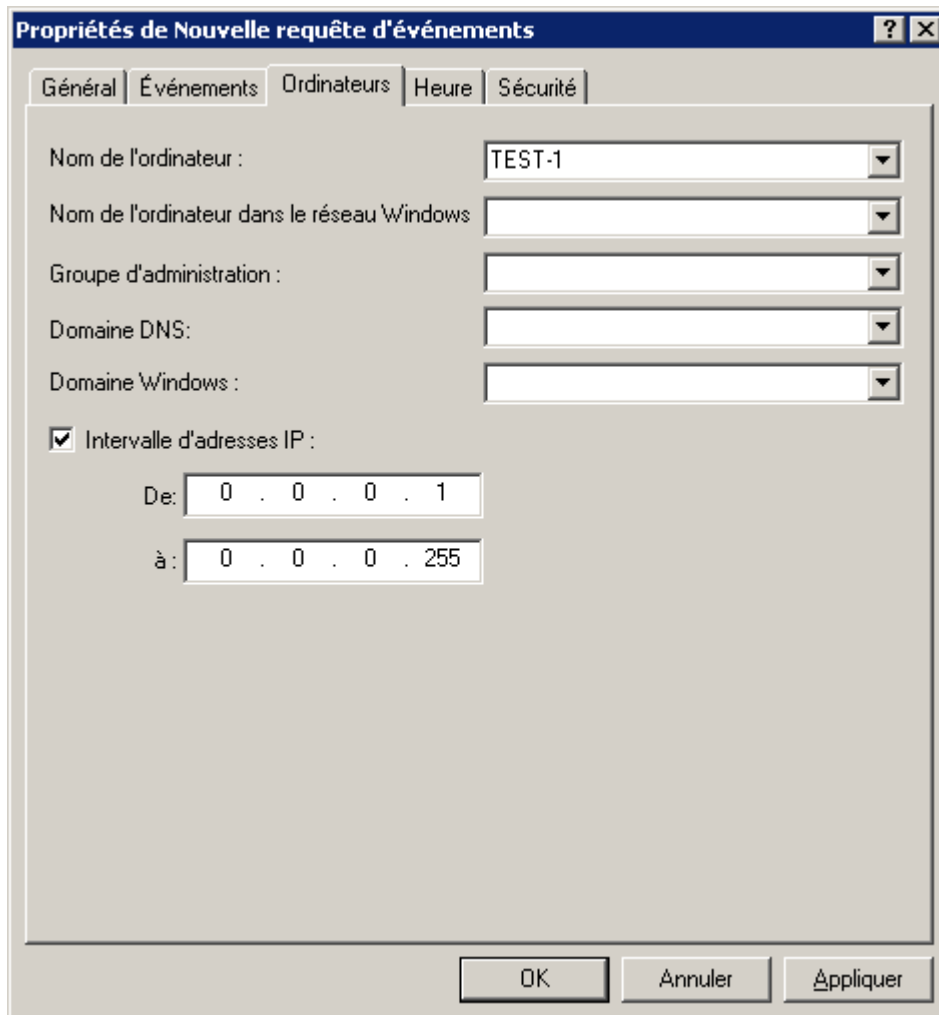


Illustration 186. Configuration d'une requête d'événements. Onglet **Ordinateurs**

L'onglet **Heure** (cf. ill. ci-après) permet de définir l'heure des événements et de résultats de tâches compris dans la requête.

Vous pouvez sélectionner les options suivantes :

- **Pour la période** : spécifiez le début et la fin de la période couverte. Pour ce faire, dans les champs **de** et **à** sélectionnez **Déclenchement** et indiquez la date et l'heure exactes. Si toutes les informations enregistrées sont nécessaires, sélectionnez **Premier événement** et **Dernier événement**.
- **Au cours des derniers jours** : précisez le nombre de jours. Dans ce cas, le début de l'intervalle correspond au moment de la création de la sélection.

Par exemple, si le champ indique 2 jours et que la sélection commence le 24 juin à 15h00, alors la sélection utilisera les données depuis le 22 juin à 15h00.

Illustration 187. Configuration d'une requête d'événements. Onglet **Heure**

Quand vous aurez terminé la configuration, cliquez sur **Appliquer** ou sur **OK**. Le tableau d'événements n'affichera que les informations qui vérifient les paramètres requis.

ENREGISTREMENT D'INFORMATIONS SUR LES EVENEMENTS D'UN FICHIER

➔ Pour enregistrer les informations sur les événements dans un fichier, procédez comme suit

1. Dans l'arborescence de la console, sélectionnez la requête d'événements contenant les événements qui vous intéressent et utilisez la commande **Toutes les tâches** → **Exporter** du menu contextuel. Cette action lance un Assistant.
2. Au cours de cette première étape de l'assistant, spécifiez le chemin et le nom du fichier dans lequel les informations sont enregistrées. Si vous souhaitez n'enregistrer que les événements sélectionnés dans le panneau de résultats, cochez la case **Exporter uniquement les événements sélectionnés**.
3. Au cours de la seconde étape, choisissez le format d'exportation des événements :
 - **Exporter au format de texte séparé par des tabulations** : fichier texte.

- **Exporter au format UNICODE séparé par des tabulations** : fichier texte au format UNICODE.

4. Pour compléter l'assistant, cliquez sur **Terminer**.

SUPPRESSION D'ÉVÉNEMENTS

➤ *Pour supprimer un événement,*

sélectionnez cet événement dans le panneau des résultats et cliquez sur l'option **Supprimer** du menu contextuel.

➤ *Pour supprimer des événements satisfaisant certains critères, procédez comme suit :*

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

L'application ne supprimera que les événements qui satisfont les paramètres de la requête sous le dossier **Événements**.

REQUÊTES D'ORDINATEURS

Les informations relatives à l'état des postes clients sont reprises dans un dossier distinct de l'arborescence de la console : **Requêtes d'événements et d'ordinateurs** → **Requêtes d'ordinateurs**. Les informations sont présentées sous la forme d'une sélection de requêtes et chacune d'entre elle affiche les informations relatives aux ordinateurs qui répondent à des conditions définies. Une fois l'application installée, le dossier contient quelques requêtes standard (cf. ill. ci-après).

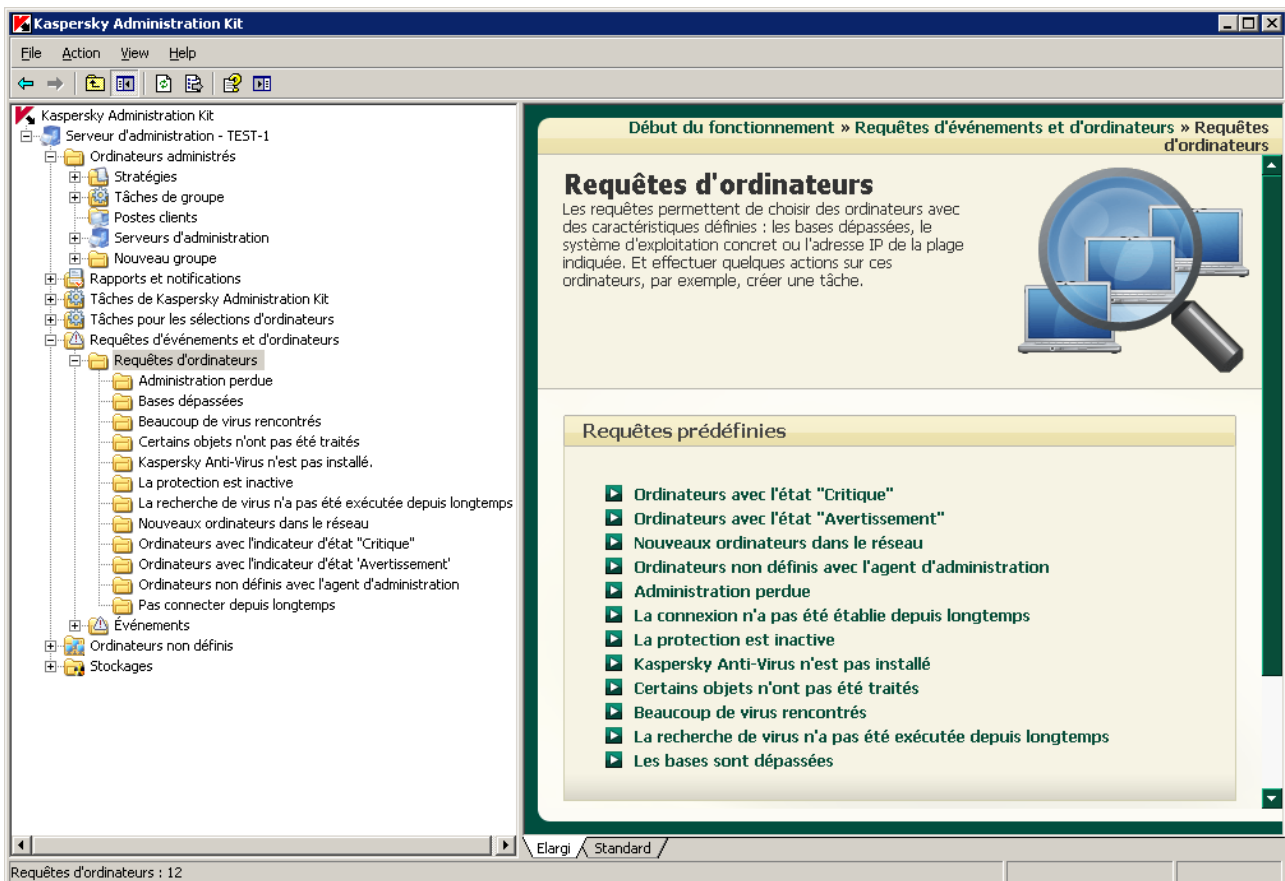


Illustration 188. Dossier **Requêtes d'ordinateurs**

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 de diagnostic s'effectue pour chaque groupe d'administration séparément sur l'onglet **Etat de l'ordinateur**.

AFFICHAGE D'UNE REQUETE D'ORDINATEURS

➔ Pour consulter une requête d'ordinateurs, procédez comme suit :

1. Connectez-vous au Serveur d'administration nécessaire (cf. section "Administration des Serveurs d'administration" à la page [22](#)).
2. Dans l'arborescence de la console, déployez le dossier **Requêtes d'événements et d'ordinateurs** → **Requête d'ordinateurs**.
3. Sélectionnez le dossier correspondant à la requête qui vous intéresse : **Ordinateurs non analysés depuis longtemps**, **Ordinateurs sans logiciel antivirus**, **Ordinateurs sans protection**, **Ordinateurs avec l'indicateur d'état "Critique"**, etc.

Pour accéder rapidement à la requête souhaitée, vous pouvez aussi cliquer sur le lien correspondant dans la barre d'état du dossier **Requêtes d'ordinateurs**.

Le panneau des résultats (cf. ill. ci-après) affichera un tableau contenant la liste complète des ordinateurs validant les paramètres de la requête. Le tableau possède les colonnes suivantes :

- **Nom** : nom du poste client ;
- **Type de S.E.** ;
- **Domaine** : domaine Windows ou groupe de travail auquel appartient l'ordinateur ;
- **Agent/Antivirus** : état des applications installées sur l'ordinateur ;
- **Heure de dernière détection** : date et heure auxquelles l'ordinateur a été détecté pour la dernière fois par le Serveur d'administration dans le réseau ;
- **Dernière mise à jour** : date de la dernière mise à jour des bases ou des applications sur l'ordinateur ;
- **Etat** : état actuel de l'ordinateur (*OK/Avertissement/Critique*) sur la base des critères définis par l'administrateur ;
- **Actualisation des informations** : date de la dernière mise à jour des informations relatives à l'ordinateur sur le Serveur d'administration ;
- **Nom DNS** : nom DNS de l'ordinateur ;
- **Adresse IP** : adresse IP de l'ordinateur ;
- **Connexion au Serveur** : date et l'heure de la dernière connexion de l'Agent d'administration installé sur le poste client, avec le Serveur d'administration ;
- **Adresse IP de la connexion** : adresse IP de la connexion du poste client avec le Serveur d'administration ;

L'adresse IP de la connexion est conservée jusqu'à la tentative de connexion suivante et elle est utilisée s'il est impossible d'établir une connexion avec le poste client à l'aide du nom principal.

- **Virus trouvés** : nombre de virus trouvés sur le poste client ;
- **Analyse à la demande** : date et heure de la dernière analyse antivirus du poste client ;
- **Groupe parent** : nom du groupe d'administration auquel appartient ce client ;

- **Serveur** : serveur d'administration auquel se rapporte l'ordinateur ;
- **Etat de la protection en temps réel** : état de la protection en temps réel de l'ordinateur.

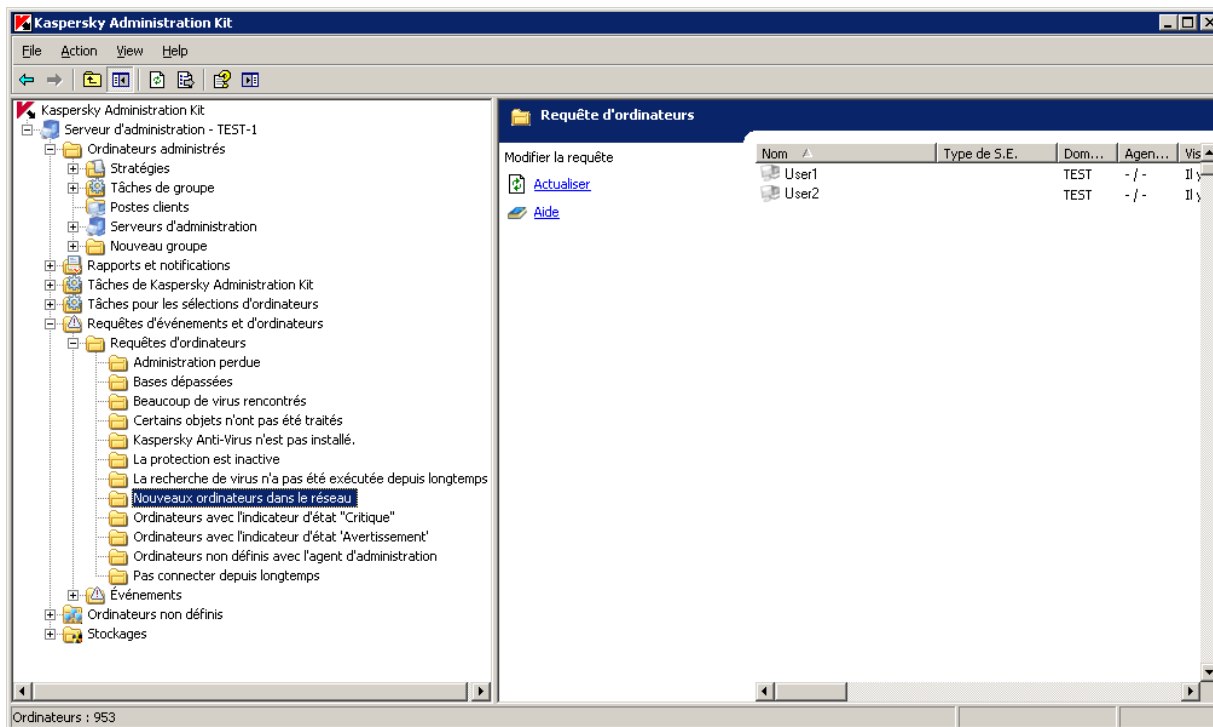


Illustration 189. Affichage d'une requête d'ordinateurs

Vous pouvez trier les données dans n'importe quelle colonne, en ordre croissant ou décroissant, modifier l'ordre des colonnes, en ajouter ou en supprimer. Il n'est pas possible de modifier la sélection de colonnes pour les groupes préconfigurés.

➤ Pour modifier la sélection des colonnes proposées pour n'importe quelle requête d'événements, procédez comme suit :

1. Dans l'arborescence de la console, déployez le dossier **Requêtes d'événements et d'ordinateurs**.
2. Dans le dossier **Requêtes d'ordinateurs**, sélectionnez la requête qui vous intéresse.
3. Ouvrez le menu contextuel et sélectionnez la commande **Vue** → **Ajouter/supprimer des colonnes**.
4. Dans la fenêtre qui s'ouvre (cf. ill. ci-après), composez la liste des colonnes à afficher à l'aide des boutons **Ajouter** et **Supprimer**. L'ordre d'affichage des colonnes est défini par les boutons **Monter** et **Descendre**.

5. Cliquez sur le bouton **OK** terminer.

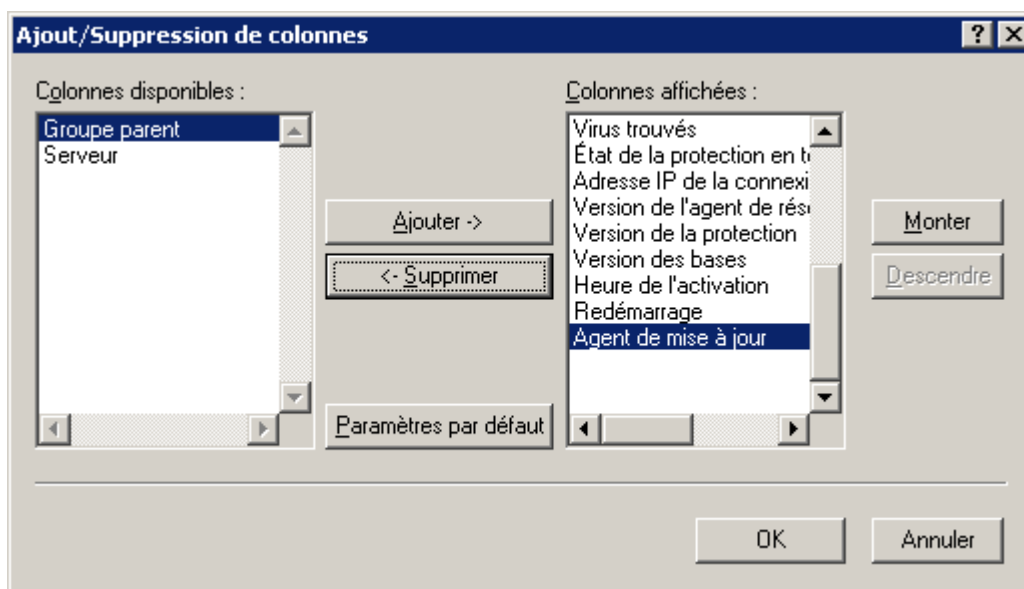


Illustration 190. Fenêtre *Ajout/Suppression de colonnes*

La liste des ordinateurs dans le panneau des résultats est actualisée automatiquement selon les paramètres indiqués.

Pour simplifier l'affichage et la recherche des informations nécessaires, il est prévu de pouvoir créer et configurer des requêtes définies par l'utilisateur.

CREATION D'UNE REQUETE D'ORDINATEURS

► Pour créer une requête d'ordinateurs, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Requêtes d'événements et d'ordinateurs** → **Sélections d'ordinateurs**.
2. Ouvrez le menu contextuel et utilisez la commande **Générer** → **Nouvelle requête**.
3. Dans la fenêtre qui s'ouvre, saisissez le nom de la requête (cf. ill. ci-après) puis cliquez sur le bouton **OK**.

Un nouveau dossier avec le nom spécifié pour la requête apparaîtra alors dans le dossier **Requêtes d'ordinateurs** dans l'arborescence de console. Pour ajouter des ordinateurs à la requête, configurez les paramètres de la requête (cf. section "Configuration de la requête d'ordinateurs" à la page [226](#)).

Pour passer rapidement à la création d'une requête d'ordinateurs, cliquez sur le lien **Créer une requête** situé dans la barre d'état du dossier **Requêtes d'ordinateurs**.

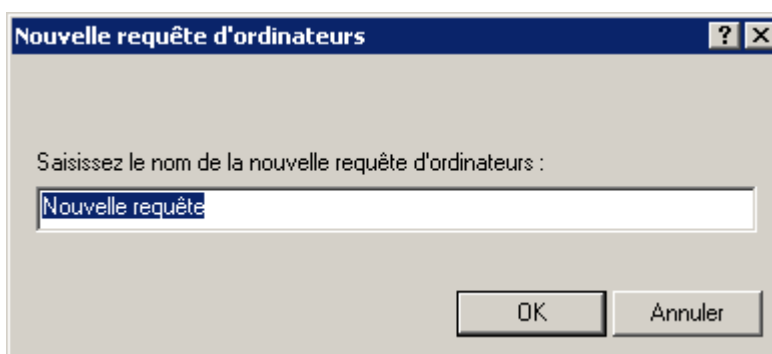


Illustration 191. Création d'une requête d'ordinateurs

CONFIGURATION DE LA REQUETE D'ORDINATEURS.

Kaspersky Administration Kit permet de configurer les sélections d'ordinateurs créées par l'utilisateur.

► Pour configurer une requête d'ordinateurs, procédez comme suit :

1. Sélectionnez la requête d'ordinateurs souhaitée dans l'arborescence de la console et cliquez sur l'option **Propriétés** du menu contextuel.
2. Ceci permet d'ouvrir la boîte de dialogue de configuration des requêtes contenant les onglets suivants : **Général** et **Conditions**.

L'onglet **Sécurité** peut être aussi présent dans la fenêtre.

La présence ou l'absence de cet onglet est définie par les paramètres d'interface de l'utilisateur. Afin de configurer l'affichage de cet onglet, passez au menu **Vue** → **Configuration de l'interface** et cochez la case dans la ligne **Afficher les onglets avec les paramètres de sécurité**.

Sous l'onglet **Général** (cf. ill. ci-après) vous pouvez modifier le nom de la requête et définir la zone de recherche des ordinateurs à l'aide de l'une des options suivantes :

- **Rechercher n'importe quels ordinateurs** : tous les ordinateurs du réseau seront inclus dans la recherche, tant les ordinateurs qui font partie du groupe d'administration, que les ordinateurs non inclus.
- **Rechercher les ordinateurs administrés** : chercher seulement parmi les groupes les ordinateurs client d'administration.
- **Rechercher des ordinateurs non définis** : chercher sur ordinateurs, qui ne consistent pas dans le groupe d'administration.

Pour inclure des données des Serveurs d'administration secondaires dans la requête, cochez la case **Y compris les données des Serveurs secondaires jusqu'au niveau**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

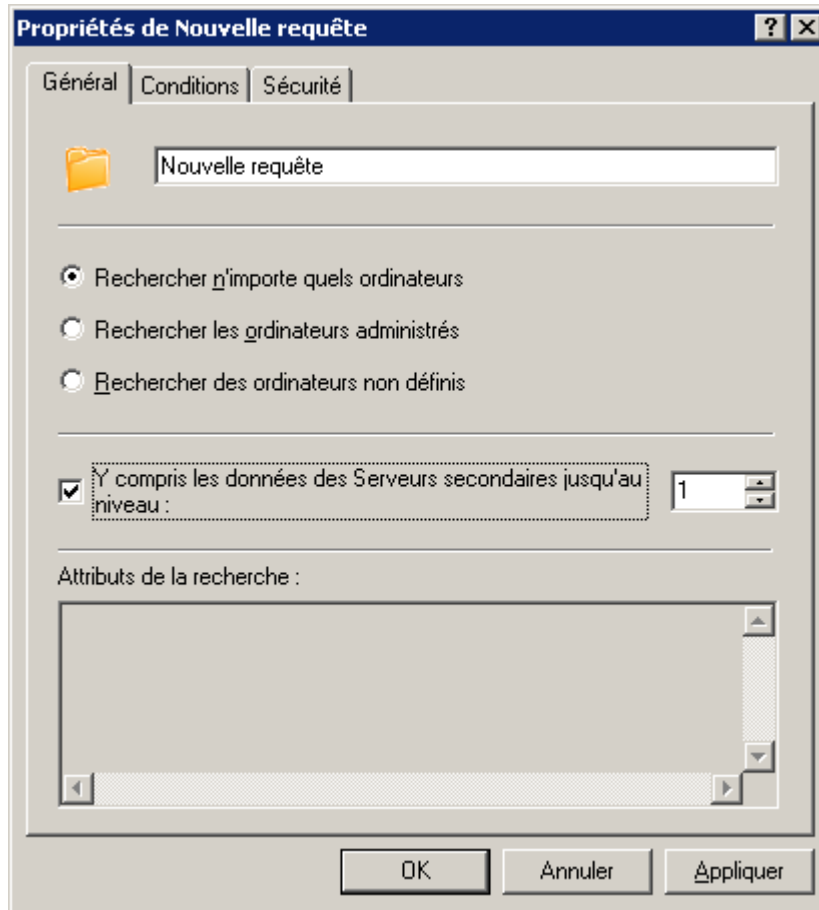


Illustration 192. Configuration de la requête d'ordinateurs.

Sur l'onglet **Conditions** sélectionnez la sélection d'ordinateurs correspondante et cliquez sur le bouton **Propriétés**. Ceci permet d'ouvrir la boîte de dialogue de configuration des requêtes contenant les onglets suivants : **Général**, **Réseau**, **Activité réseau**, **Application**, **Etat du poste**, **Protection antivirus** et **Registre des applications**.

- Sur l'onglet **Réseau** (cf. ill. ci-après) spécifiez les attributs des ordinateurs à inclure dans la requête. Vous pouvez utiliser les paramètres suivants :
 - **Nom de l'ordinateur** dans le groupe d'administration.
 - **Domaine** où sont inclus les ordinateurs.
 - **Intervalle d'adresses IP des ordinateurs** des ordinateurs : pour ce faire, cochez la case **Plage d'adresses IP** et renseignez les adresses de début et de fin.
 - **Le poste se trouve dans la division Active Directory**. Cochez la case et à l'aide du bouton **Sélectionner** indiquez la division Active Directory où sont inclus les ordinateurs.

- **Divisions filles comprises.** Cochez cette case, pour tenir compte des ordinateurs inclus dans les divisions filles de l'unité d'organisation indiquée d'Active Directory, lors de la recherche.

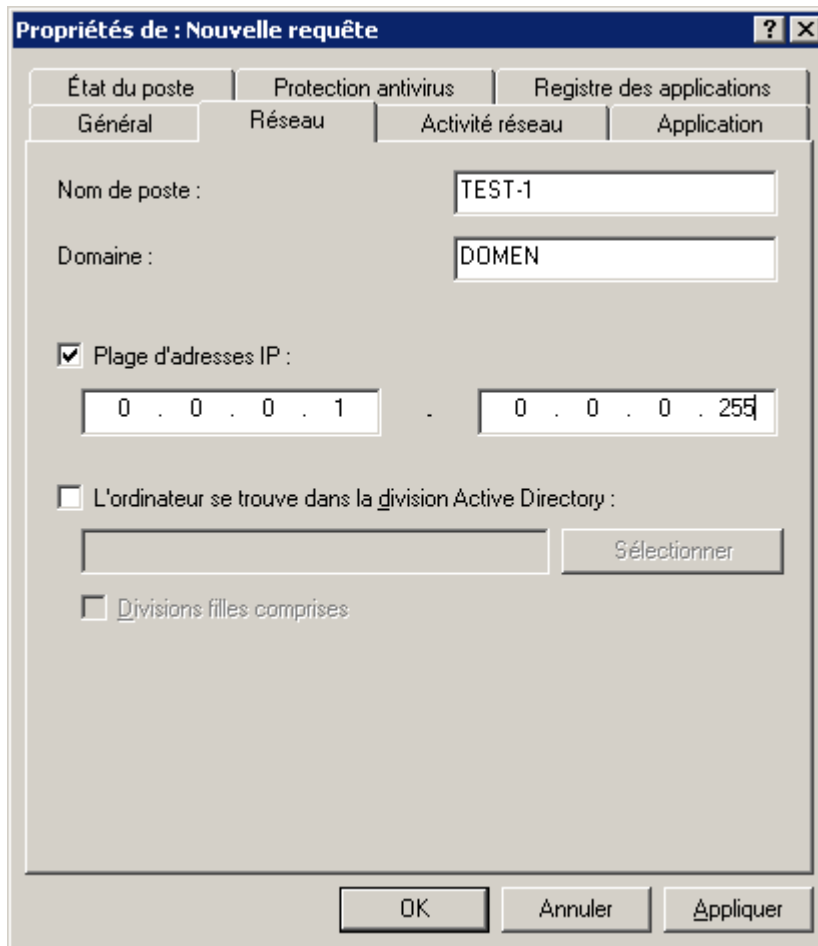


Illustration 193. Configuration de la requête d'ordinateurs. Onglet **Réseau**

- Sur l'onglet **Activité réseau** (cf. ill. ci-après), vous pouvez définir les critères de tri des ordinateurs de la requête :
 - L'ordinateur qui doit être repris dans la requête est-il un agent de mise à jour. Pour ce faire, de la liste déroulante **Est l'agent de mise à jour** vous pouvez sélectionner une des valeurs suivantes :
 - **Oui** pour que la requête soit composée d'ordinateurs qui sont des agents de mise à jour.
 - **Non** pour que la requête soit composée d'ordinateurs qui ne sont pas des agents de mise à jour.
 - Si le paramètre **Maintenir la connexion avec le Serveur d'administration** est activé dans les propriétés du poste client. Pour ce faire, dans la liste déroulante **Paramètre "Maintenir la connexion avec le Serveur d'administration"** sélectionnez la valeur :
 - **Activé**, pour que la requête soit composée d'ordinateurs avec le paramètre activé.
 - **Désactivé**, pour que la requête soit composée d'ordinateurs avec le paramètre désactivé.
 - L'ordinateur, est-il connecté au Serveur d'administration par suite du changement du profil de connexion. Pour ce faire, dans le champ **Changement du profil de connexion** sélectionnez :
 - **Oui**, pour que la requête soit composée d'ordinateurs qui se connectent par suite d'action du profil de connexion.

- **Non**, pour que la requête soit composée d'ordinateurs qui se connectent non par suite d'action du profil de connexion.
- L'ordinateur, se connectait-il au Serveur d'administration dans un intervalle de temps défini. Pour ce faire, cochez la case **Heure de la dernière connexion au Serveur d'administration** et dans les champs ci-dessous indiquez l'intervalle de temps.
- L'ordinateur, est-il détecté en qualité du nouveau lors du sondage du réseau. Pour ce faire, cochez la case **Nouveaux ordinateurs trouvés pendant le sondage du réseau** et indiquez le nombre de jours dans le champ **Période de détection (jours)**.

Propriétés de : Nouvelle requête

État du poste Protection antivirus Registre des applications

Général Réseau **Activité réseau** Application

Est l'agent de mise à jour :

Oui

Paramètre "Maintenir la connexion avec le Serveur d'administration" :

Activé

L'ordinateur est connecté au Serveur d'administration par suite du changement du profil de connexion :

Non

Heure de la dernière connexion au Serveur d'administration :

05/09/2009 18:20:40 - 05/09/2009 18:20:40

Nouveaux ordinateurs trouvés pendant le sondage du réseau

Période de détection (jours) : 1

OK Annuler Appliquer

Illustration 194. Configuration de la requête d'ordinateurs. Onglet **Activité réseau**

- Sur l'onglet **Application** (cf. ill. ci-après) indiquez quelle application de Kaspersky Lab doit être installée sur les ordinateurs. Vous pouvez utiliser les paramètres suivants :
 - Nom de l'application. Sélectionnez la valeur souhaitée dans la liste déroulante. La liste ne fournit que le nom des applications disposant de plug-ins de contrôle installés dans l'espace de travail de l'administrateur.
 - Numéro de version de l'application.
 - Nom de la mise à jour critique de l'application.
 - Dernière mise à jour des modules de l'application. Pour ce faire, cochez la case **Dernière mise à jour des modules de l'application** et spécifiez la date et l'heure de début et de fin de l'intervalle dans les zones de et à.

- Version du système d'exploitation installé sur le poste.

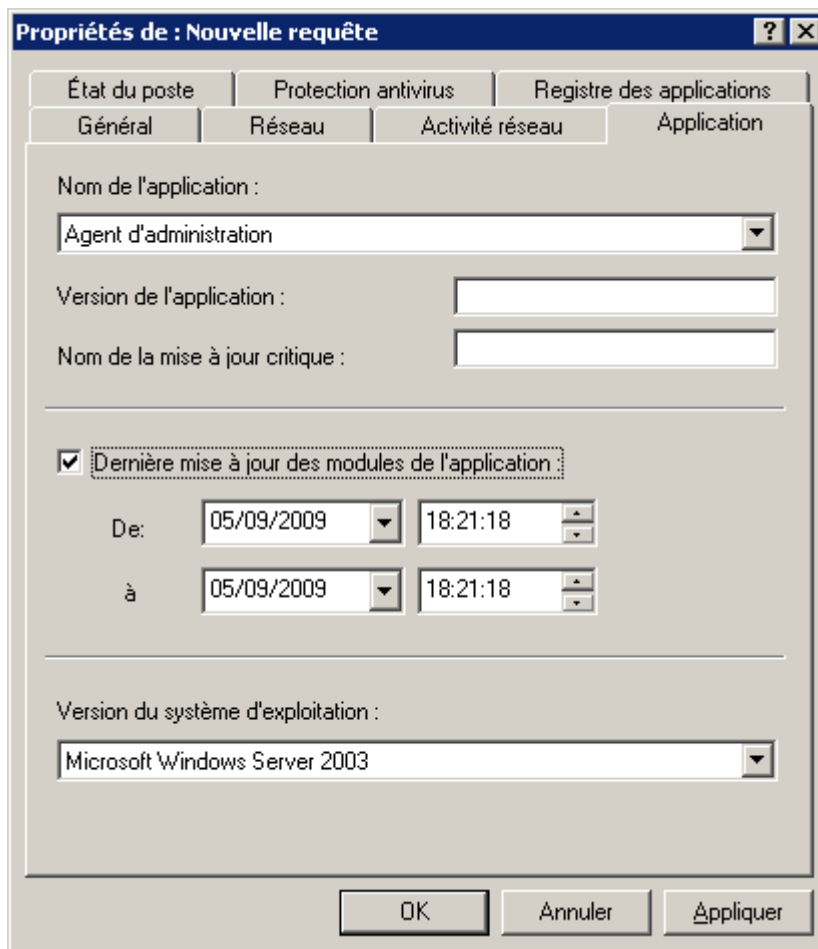


Illustration 195. Configuration de la requête d'ordinateurs. Onglet **Application**

- Spécifiez les critères d'évaluation de la protection antivirus sur les ordinateurs qui vont être inclus dans la requête, depuis l'onglet **Protection antivirus** (cf. ill. ci-après). Vous pouvez spécifier :
 - la date de création des bases antivirus utilisée par les applications ; pour ce faire, cochez la case **Date de publication des bases** et spécifiez la plage horaire pendant laquelle la base de l'application sera créée ;
 - le nombre d'enregistrements dans la base antivirus utilisée par les applications ; pour cela cochez la case **Enregistrements dans les bases** et spécifiez les valeurs minima et maxima de ce paramètre ;
 - l'heure de dernière analyse complète de l'ordinateur par l'une des applications Kaspersky Lab ; pour ce faire, cochez la case **Dernière recherche de virus** et spécifiez le temps pendant lequel l'analyse doit avoir été faite ;

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

The screenshot shows a dialog box titled "Propriétés de : Nouvelle requête" with a "Protection antivirus" tab selected. The "Virus trouvés" checkbox is checked, and the range is set from 1 to 1,000,000. Other options like "Date de publication des bases", "Enregistrements dans les bases", and "Dernière recherche de virus" are also checked with their respective ranges.

Illustration 196. Configuration de la requête d'ordinateurs. Onglet **Protection antivirus**

- Sur l'onglet **Etat du poste** (cf. ill. ci-après), spécifiez les paramètres qui décrivent l'état des postes et celui de la tâche de protection en temps exécutée sur les ordinateurs. Pour ce faire :
 - dans la liste déroulante **Etat du poste** choisissez la valeur requise : *OK*, *Critique* ou *Avertissement* ;
 - dans la liste **Description de l'état du poste** sélectionnez les conditions en fonction desquelles le poste reçoit l'état correspondant ;

- à partir de la liste **Etat de la protection en temps réel** sélectionnez l'état de la protection en temps réel exécutée sur les postes, inclus dans la requête.

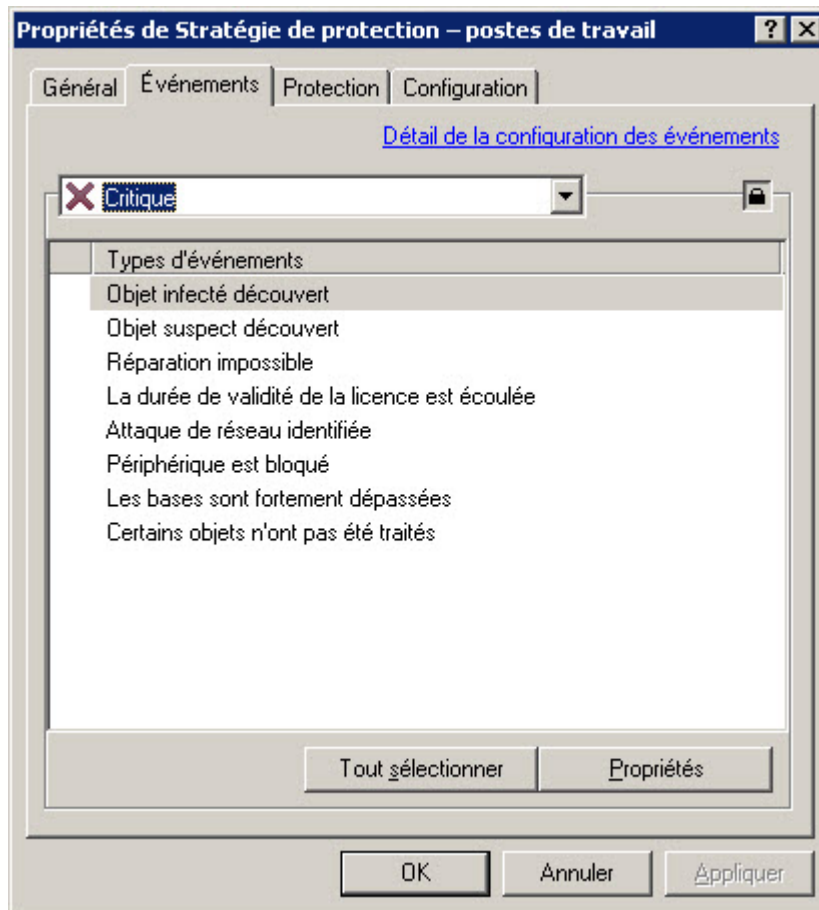


Illustration 197. Configuration de la requête d'ordinateurs. Onglet **Etat du poste**

- Sur l'onglet **Registre des applications** (cf. ill. ci-après), définissez les paramètres de l'application selon lesquels la requête sera réalisée. Pour ce faire, définissez la valeur requise ou laissez les champs suivants vides :
 - Nom de l'application** (à l'aide de la liste déroulante) ;
 - Version de l'application** ;
 - Editeur** (à l'aide de la liste déroulante) ;
 - Nom de l'application de sécurité incompatible**. Dans la liste déroulante, sélectionnez l'application d'autres éditeurs ou l'application de Kaspersky Lab incompatible avec Kaspersky Administration Kit.

Si en guise de critère de recherche vous utilisez un paquet de mises à jour pour une application quelconque, cochez la case **Rechercher selon la mise à jour** et dans les champs correspondants, définissez le nom de la mise à jour, sa version et l'éditeur.

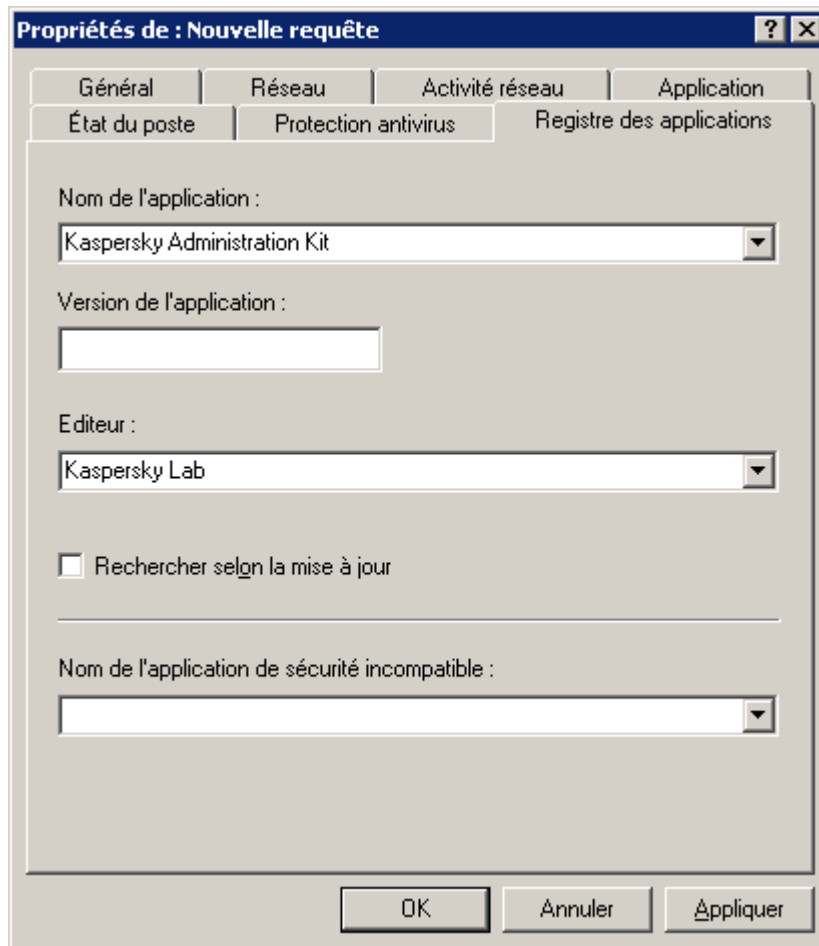


Illustration 198. Configuration de la requête d'ordinateurs. Onglet **Registre des applications**

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

L'onglet **Sécurité** (cf. ill. ci-après) propose les privilèges des utilisateurs et des groupes d'utilisateur pour la manipulation de la requête.

La configuration des paramètres de cet onglet est similaire à la configuration des paramètres de l'onglet **Sécurité** de la fenêtre des propriétés du modèle du rapport (cf. section "Affichage et modification des modèles de rapport" à la page [191](#)).

ORDINATEURS NON DEFINIS

Les informations relatives aux ordinateurs du réseau de l'entreprise qui n'appartiennent pas à un groupe d'administration figurent dans le dossier **Ordinateurs non définis**. Le dossier **Ordinateurs non définis** contient trois sous-dossiers : **Domaines**, **Plages IP** et **Active Directory**.

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 **Ordinateurs non définis** → **Domaines**, dans le sous-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 créée par l'administrateur à l'aide de la création des nouvelles plages IP et de la modification des paramètres existants.

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

1. Sélectionnez le dossier **Ordinateurs non définis** dans l'arborescence de la console.
2. Sélectionnez un des sous-dossiers : **Domaines**, **Active Directory** et **Plages IP**.

Le panneau des résultats reprendra les informations relatives à la structure du réseau informatique dans la représentation correspondante.

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.

DANS CETTE SECTION

Sondage de réseau.....	234
Affichage et modification des paramètres du domaine.....	239
Création de la plage IP.....	241
Affichage et modification des paramètres de plage IP.....	242
Affichage et modification des paramètres du groupe Active Directory.....	245

SONDAGE DE RESEAU

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. Le contenu du dossier **Ordinateurs non définis** est actualisé sur la base du résultat de ces requêtes.

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, seules les informations relatives à la liste des noms NetBIOS des ordinateurs de tous les domaines et des groupes de travail du réseau sont récoltées. Lors du sondage complet, des informations complémentaires sont obtenues : système d'exploitation, adresse IP, nom DNS, etc.
- *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.
- *Sondage des groupes Active Directory.* 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.

Sur la base des informations obtenues et des données sur la structure du réseau de l'entreprise, le Serveur d'administration actualise le contenu du dossier du dossier **Ordinateurs non définis** ainsi que la composition et le contenu du dossier **Ordinateurs administrés**. Notez que les ordinateurs découverts dans le réseau peuvent être automatiquement inclus dans le groupe d'administration défini par l'administrateur.

Le dossier **Ordinateurs non définis** du Serveur d'administration principal reprend entre autres les ordinateurs appartenant au réseau logique des autres Serveurs d'administration (si elles sont situées dans le même sous-réseau). Et vice-versa.

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONDAGE DU RESEAU WINDOWS

➤ Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs non définis** → **Domaines**.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Dans la fenêtre qui s'ouvre, à l'onglet **Général** (cf. ill. ci-après), cochez la case **Autoriser le sondage du réseau Windows**.

Dans les champs inférieurs, indiquez :

- **Durée d'analyse rapide (min.)**. La liste des noms NetBIOS des hôtes connectés aux domaines et groupes de travail du réseau sera actualisée selon l'intervalle défini. Celle-ci est établie par défaut à 15 minutes.
- **Durée d'analyse complète (min.)**. Les informations relatives aux hôtes (système d'exploitation, adresse IP, nom DNS, etc.) seront complètement actualisées selon cet intervalle. Celle-ci est établie par défaut à 60 minutes.

Pour lancer manuellement un sondage complet du réseau informatique, cliquez sur le bouton **Sonder maintenant**.

Pour désactiver l'analyse du réseau Windows, désélectionnez la case **Autoriser le sondage du réseau Windows**.

Pour accéder rapidement à la consultation et à la modification des paramètres de sondage du réseau Windows, cliquez sur le lien **Modifier les paramètres du sondage**, situé dans le panneau des tâches du dossier **Ordinateurs non définis** dans le groupe **Sondage du réseau Microsoft**.

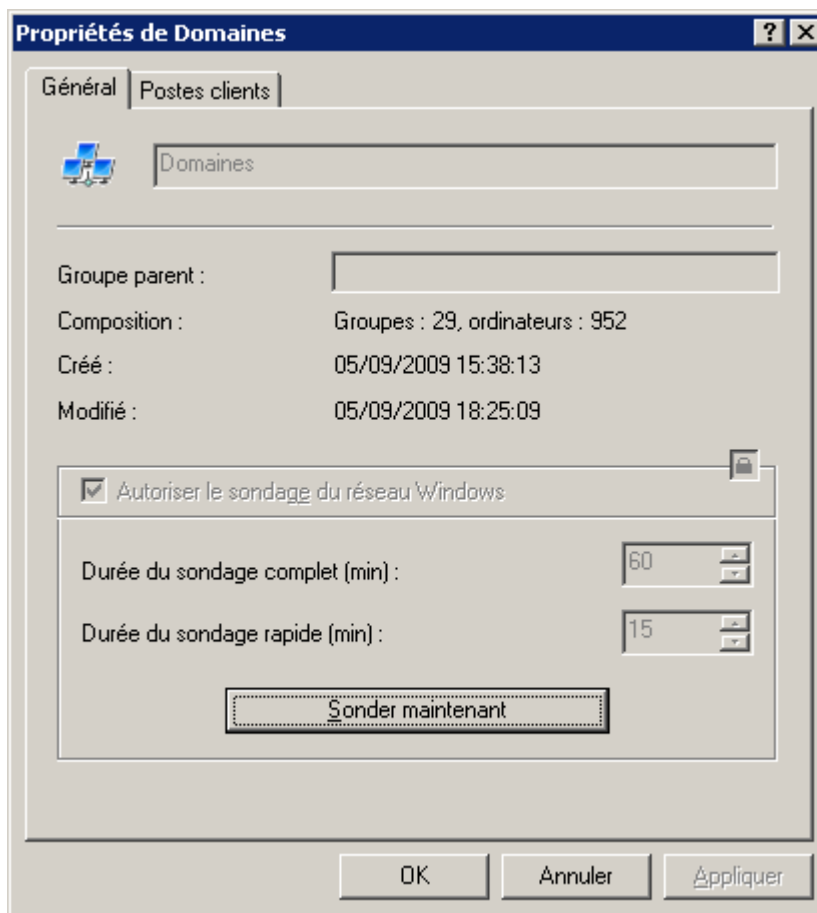


Illustration 199. Affichage des propriétés du groupe **Domaines**

➤ Pour exclure tous les domaines du sondage du réseau, procédez comme suit :

1. Sélectionnez le dossier **Ordinateurs non définis** → **Domaines**.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.

3. Dans la fenêtre qui s'ouvre, à l'onglet **Postes clients** (cf. ill. ci-après), désélectionnez la case **Autoriser le sondage de tous les ordinateurs du groupe**.

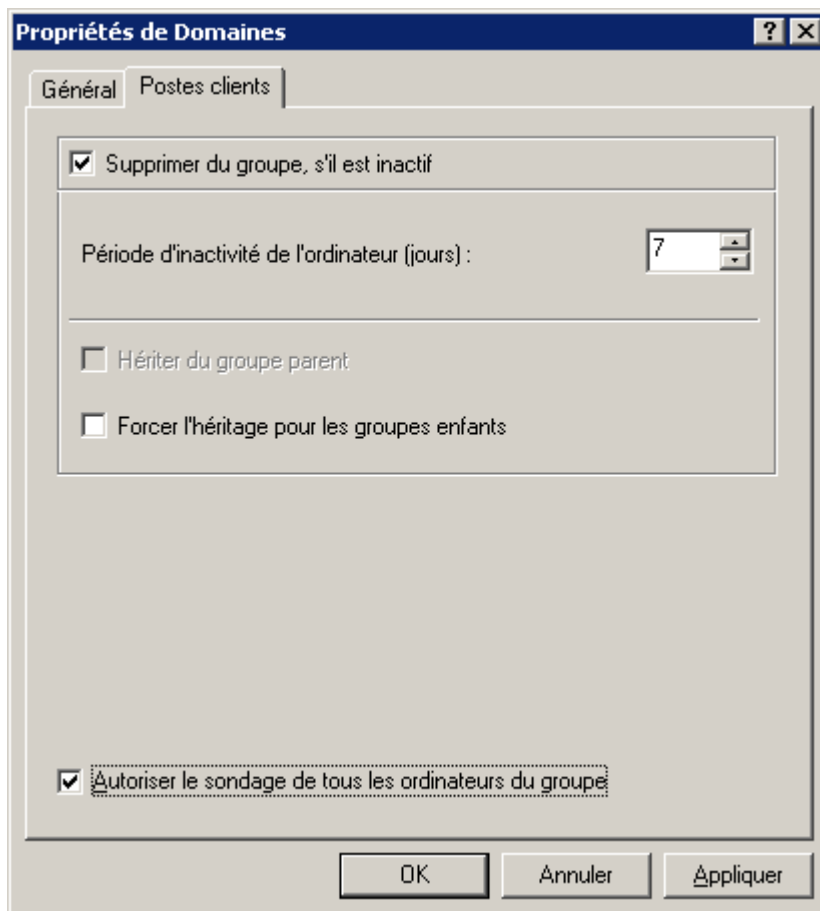


Illustration 200. Affichage des propriétés du groupe **Domaines**. Onglet **Postes clients**

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONDRAGE DES GROUPES ACTIVE DIRECTORY

➔ Pour modifier les paramètres de sondage des groupes Active Directory, procédez comme suit :

1. Sélectionnez **Ordinateurs non définis** → **Active Directory** dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Dans la fenêtre qui s'ouvre, à l'onglet **Général** (cf. ill. ci-après), cochez la case **Autoriser le sondage d'Active Directory**.

Le Serveur d'administration sondera le réseau selon la fréquence définie dans le champ **Période de sondage (min.)**. Celle-ci est établie par défaut à 60 minutes. Vous pouvez modifier cette valeur en saisissant une autre ou annuler le sondage en désélectionnant la case **Autoriser le sondage d'Active Directory**.

Cliquez sur **Sonder maintenant** si vous souhaitez lancer manuellement un sondage complet du réseau informatique.

Pour accéder rapidement à la consultation et à la modification des paramètres de sondage des groupes Active Directory, cliquez sur le lien **Modifier les paramètres du sondage** situé dans le panneau des tâches du dossier **Ordinateurs non définis** dans le groupe **Sondage Active Directory**.

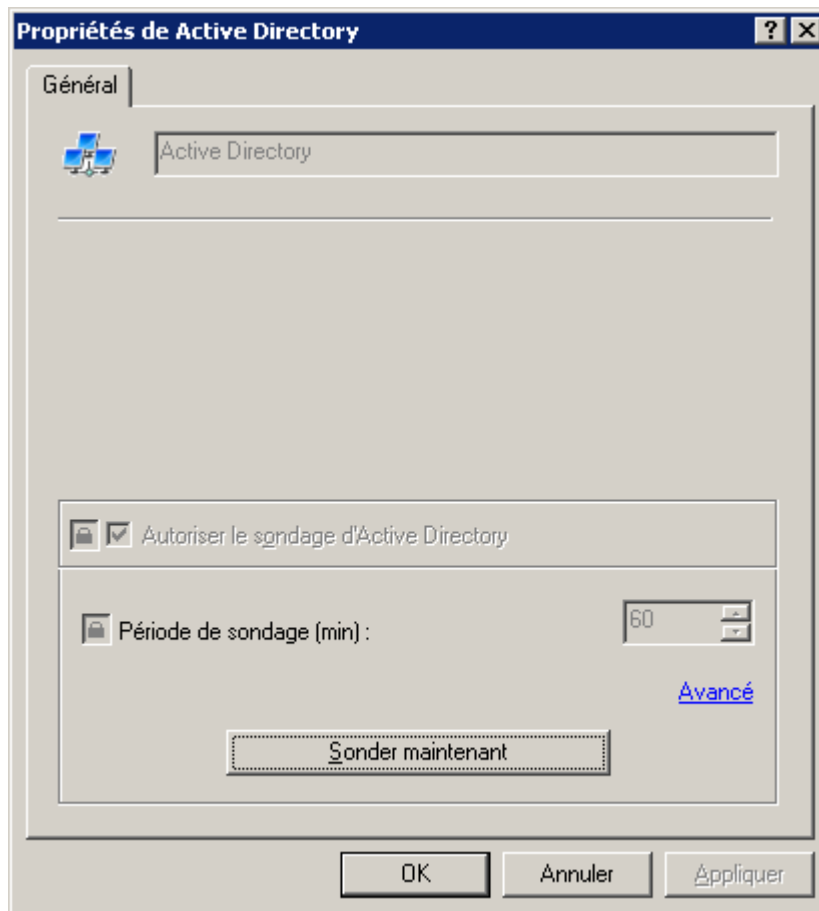


Illustration 201. Affichage des propriétés du groupe **Active Directory**

► Pour exclure un groupe quelconque du sondage complet, procédez comme suit :

1. Sélectionnez le dossier **Ordinateurs non définis** → **Active Directory** et sélectionnez un groupe.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Dans la fenêtre qui s'ouvre, à l'onglet **Général** décochez la case **Autoriser le sondage d'Active Directory**.

AFFICHAGE ET MODIFICATION DES PARAMETRES DE SONNAGE DES PLAGES IP

► Pour modifier les paramètres du sondage des plages IP, procédez comme suit :

1. Sélectionnez **Ordinateurs non définis** → **Plages IP** dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Dans la fenêtre qui s'ouvre, à l'onglet **Général** (cf. ill. ci-après), cochez la case **Autoriser le 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. Il sondera le réseau selon la fréquence définie dans

le champ **Période de sondage des plages IP (min.)**. Celle-ci est établie par défaut à 420 minutes. Vous pouvez modifier cette valeur en saisissant une autre ou annuler le sondage en désélectionnant la case **Autoriser le sondage des plages IP**.

Cliquez sur **Sonder maintenant** si vous souhaitez lancer manuellement un sondage complet du réseau informatique.

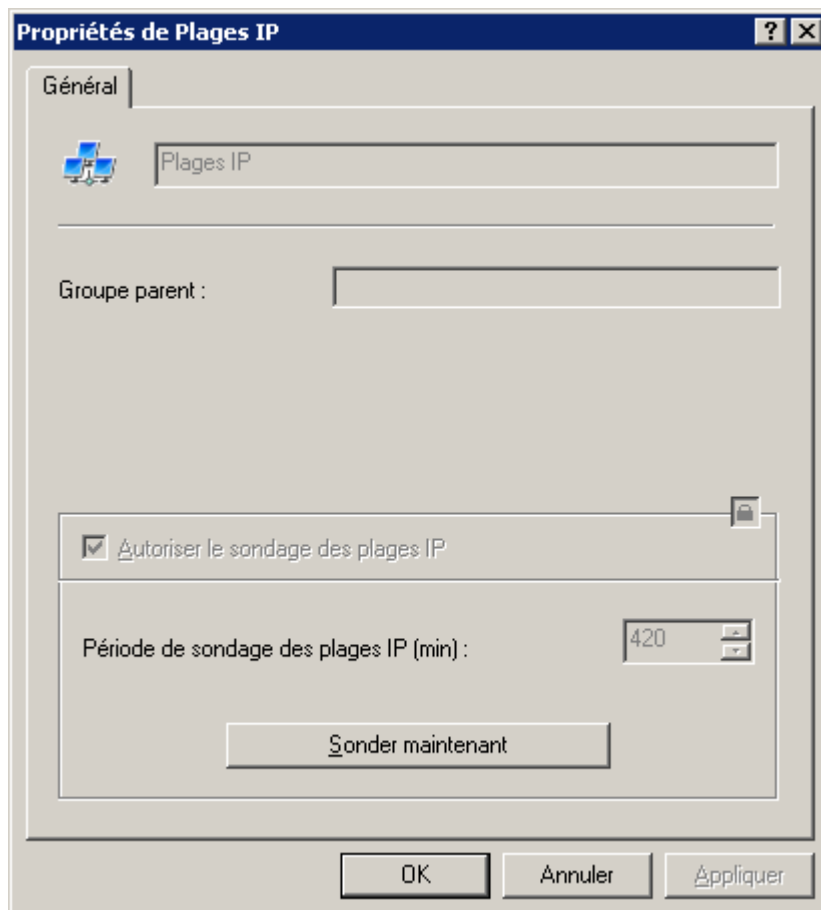


Illustration 202. Affichage des propriétés du groupe *Plages IP*

AFFICHAGE ET MODIFICATION DES PARAMETRES DU DOMAINE

➤ Pour modifier les paramètres du domaine, procédez comme suit :

1. Ouvrez le dossier **Ordinateurs non définis** → **Domaines**.
2. Sélectionnez le dossier correspondant au domaine requis.
3. Ouvrez le menu contextuel et utilisez la commande **Propriétés**.

Cela entraîne l'ouverture de la boîte de dialogue **Propriétés de <Nom du domaine>** contenant les onglets **Général** et **Postes clients**.

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez consulter le nom du domaine et le nom du groupe parent.

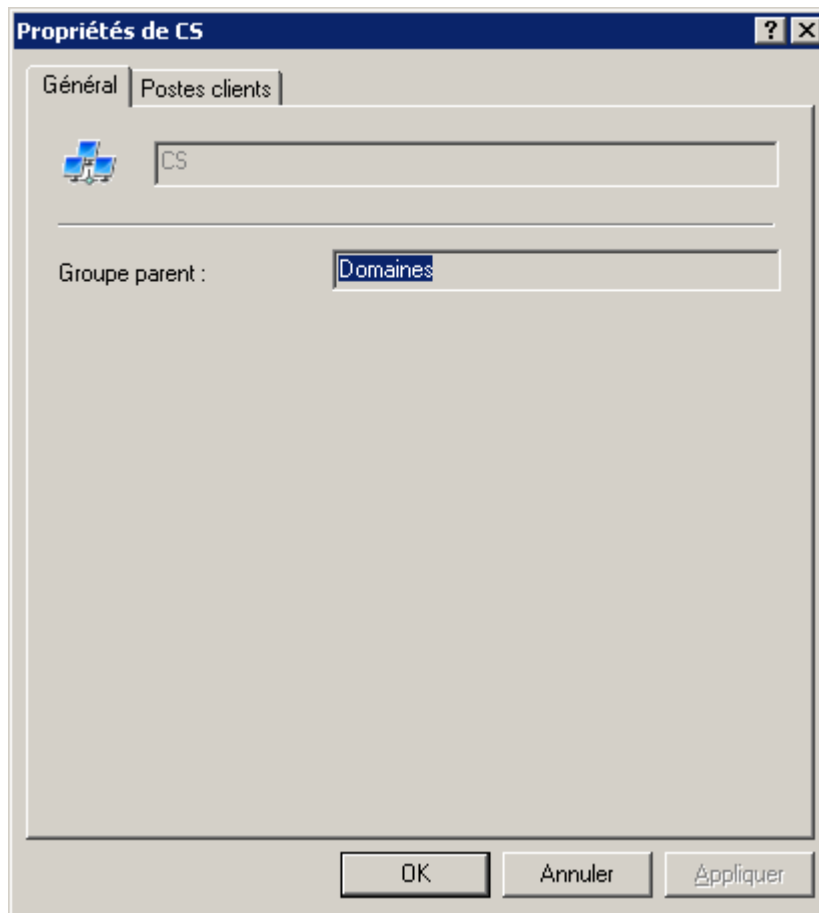


Illustration 203. Affichage des paramètres du domaine. Onglet **Général**

Sur l'onglet **Postes clients** (cf. ill. ci-après), vous pouvez :

- Définir les paramètres de suppression automatique pour les ordinateurs inactifs du dossier **Ordinateurs non définis**.

Pour ce faire, cochez la case **Supprimer du groupe après une période d'inactivité de**. Quand la case est cochée, le Serveur d'administration supprimera des domaines les ordinateurs inactifs pendant une période supérieure à la durée indiquée dans le champ jours. Vous pouvez modifier la valeur du paramètre en désignant une autre valeur ou annuler la suppression des ordinateurs en désélectionnant la case **Supprimer du groupe après une période d'inactivité de**.

- Exclure le domaine du sondage complet du réseau. Pour ce faire, sous l'onglet **Postes clients** décochez la case **Autoriser le sondage de tous les ordinateurs du groupe**.

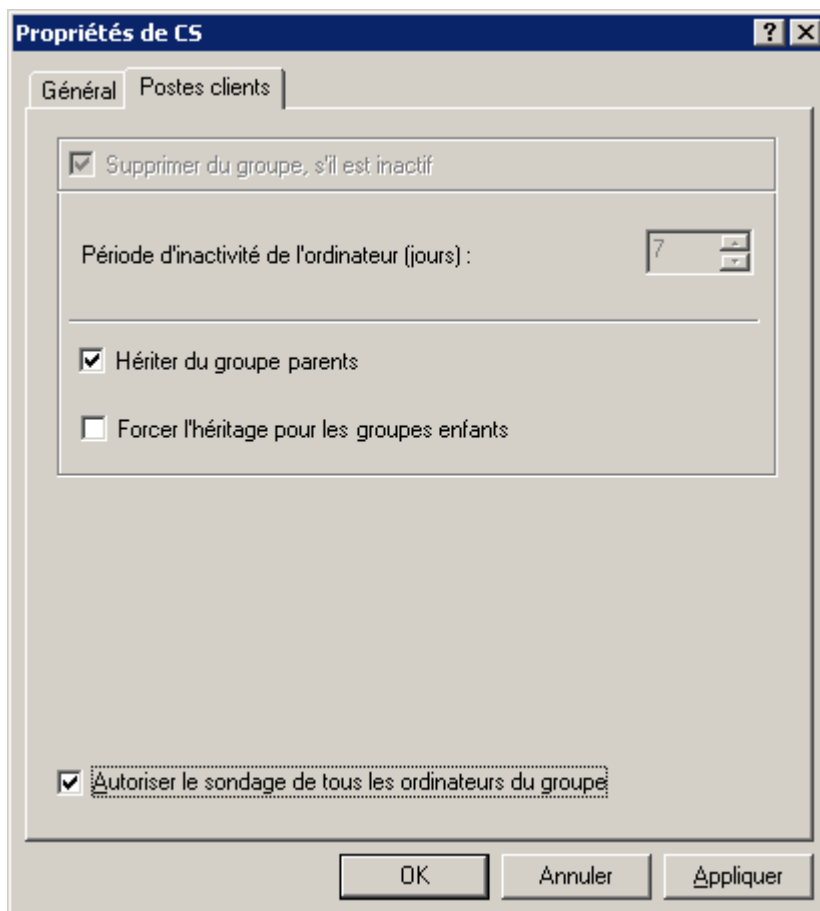


Illustration 204. Affichage des paramètres du domaine. Onglet **Postes clients**

CREATION DE LA PLAGE IP

➤ Pour créer une nouvelle plage IP, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs non définis** → **Plages IP**.
2. Ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Plage IP**.
3. Dans la fenêtre **Nouvelle plage IP** ouverte (cf. ill. ci-après), spécifiez les valeurs des paramètres suivants :
 - Nom du sous-réseau.
 - Méthode de description du sous-réseau et valeurs des paramètres pour la méthode sélectionnée.
 - Vous avez le choix parmi les options suivantes :
 - **Spécifier la plage d'adresses IP en utilisant l'adresse et le masque de sous-réseau** : dans ce cas vous devez indiquer le **Masque de sous-réseau** et l'**Adresse de sous-réseau** dans les champs de saisie correspondants.
 - **Spécifier la plage d'adresses IP en utilisant des adresses de début et de fin** : après cela, précisez les adresses IP de début et de fin.

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

Illustration 205. Création de la plage IP

AFFICHAGE ET MODIFICATION DES PARAMETRES DE PLAGE IP

► Pour modifier les paramètres de plage IP, procédez comme suit :

1. Ouvrez le dossier **Ordinateurs non définis** → **Plages IP**.
2. Sélectionnez le dossier correspondant au sous-réseau requis.
3. Ouvrez le menu contextuel et utilisez la commande **Propriétés**.

Cela entraîne l'ouverture de la boîte de dialogue **Propriétés de <Nom de la plage>** contenant les onglets **Général** et **Intervalles IP**.

Sur l'onglet **Général** (cf. ill. ci-après), vous pouvez :

- modifier le nom de la plage ;
- modifier la valeur de l'intervalle de temps après lequel les données d'un ordinateur inactif seront supprimées de la base de données du Serveur d'administration, dans le champ **Durée de vie de l'adresse IP (heures)** ; par défaut, l'adresse IP a une durée de vie de 24 heures ;

- autoriser ou annuler le sondage normal par le Serveur d'administration des ordinateurs de la plage. Si vous ne souhaitez pas que le Serveur d'administration sonde les ordinateurs deux fois de suite, décochez la case **Autoriser le sondage de la plage IP**.

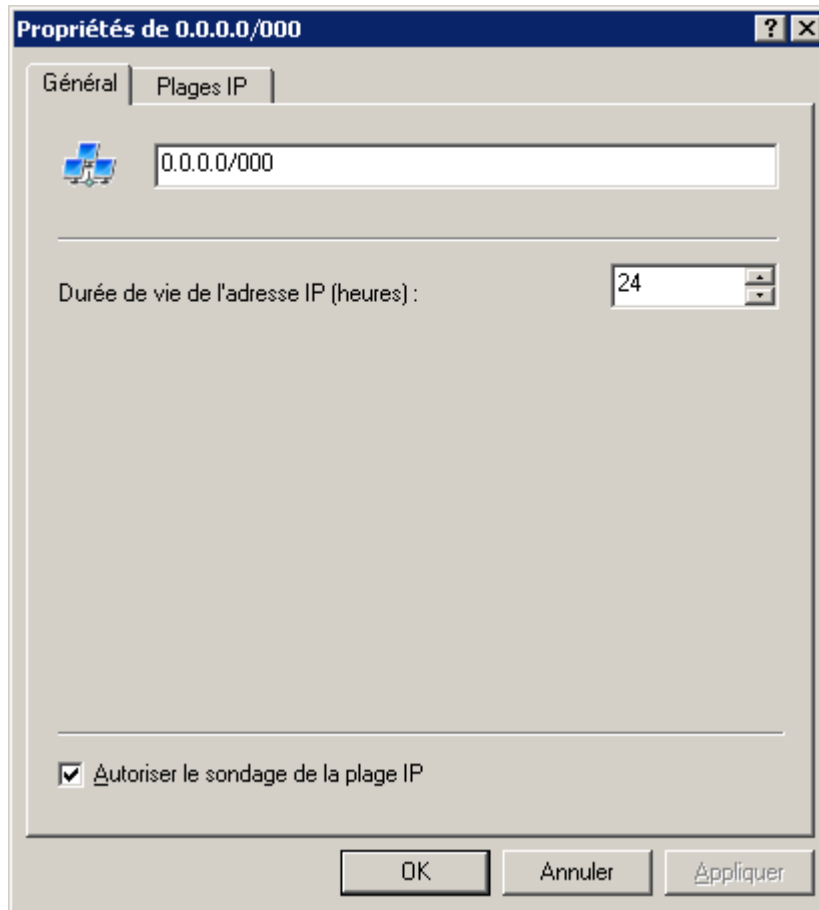


Illustration 206. Affichage des paramètres de la plage IP. Onglet **Général**

Sous l'onglet **Intervalles IP** (cf. ill. ci-après), vous pouvez ajouter ou supprimer des intervalles IP qui définissent la plage et modifier les paramètres des intervalles :

- adresses IP de début et de fin de l'intervalle ;

- masque de sous-réseau et adresse.

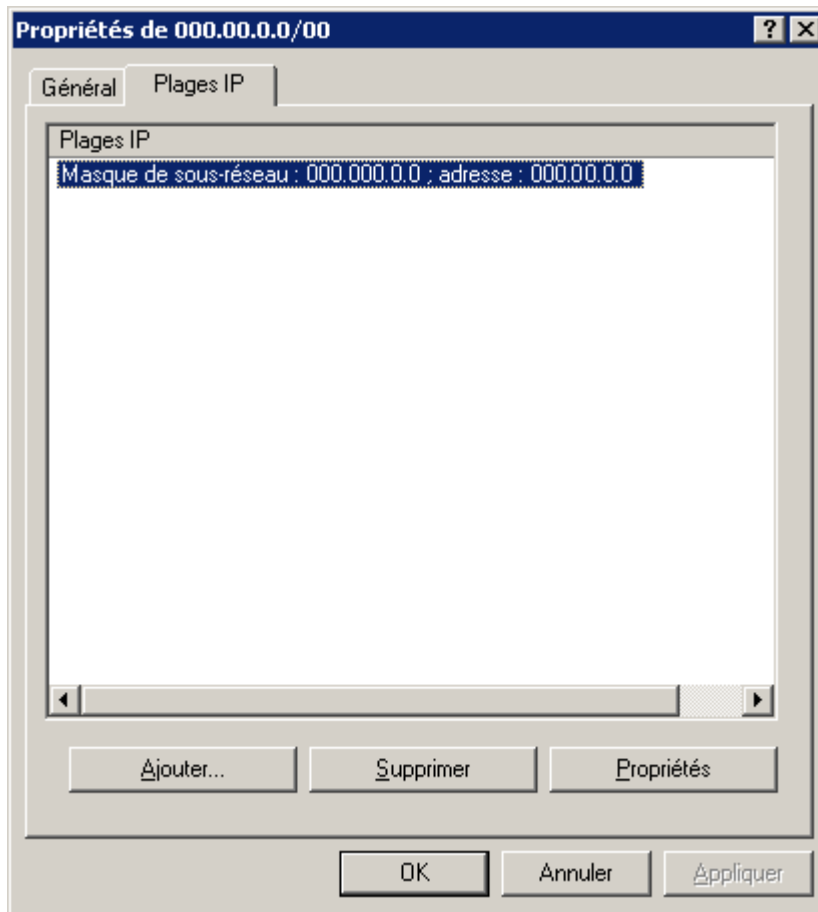


Illustration 207. Affichage des paramètres de la plage IP. Onglet **Plages IP**

Pour ajouter une plage IP définissant la plage, cliquez sur **Ajouter**. Dans la fenêtre **Intervalle IP** (cf. ill. ci-après) ouverte, spécifiez la méthode de description de l'intervalle puis saisissez les valeurs en fonction de la méthode choisie. Vous avez le choix parmi les options suivantes :

- **Définir l'intervalle IP à l'aide d'une adresse et d'un masque de sous-réseau** : saisissez le masque de sous-réseau et l'adresse de sous-réseau dans les champs de saisie correspondants.
- **Définir l'intervalle IP à l'aide d'une adresse de début et de fin** : indiquez les adresses IP de début et de fin.

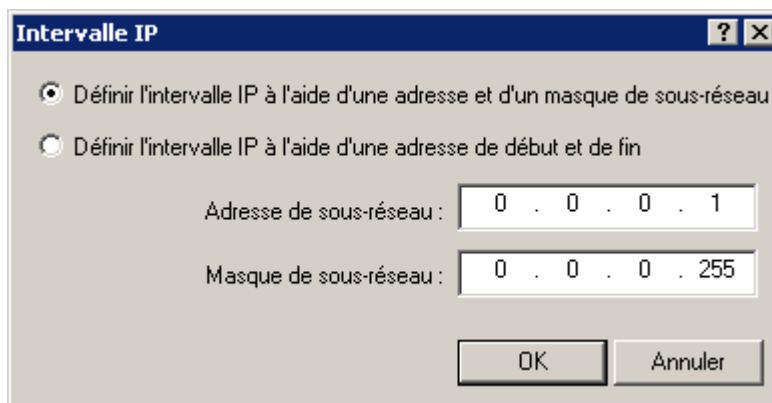


Illustration 208. Ajout de l'intervalle IP

AFFICHAGE ET MODIFICATION DES PARAMETRES DU GROUPE ACTIVE DIRECTORY

➔ Pour modifier les paramètres du groupe Active Directory, procédez comme suit :

1. Ouvrez le dossier **Ordinateurs non définis** → **Active Directory**.
2. Sélectionnez le dossier correspondant au groupe Active Directory requis, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.

Ceci entraîne l'ouverture de la boîte de dialogue **Propriétés de <Nom du groupe Active Directory>** contenant l'onglet **Général** (cf. ill. ci-après).

3. Pour autoriser le sondage du groupe, cochez la case **Activer le sondage**. Pour annuler le sondage, désélectionnez la case.



Illustration 209. Affichage des propriétés du groupe Active Directory

MISE A JOUR

La mise à jour en temps opportun des bases 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.

Pour actualiser les bases et les modules logiciels des applications administrées via Kaspersky Administration Kit, il faut créer une tâche de récupération des mises à jour par le Serveur d'administration. 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.

Avant d'être installées sur les postes clients, les mises à jour récupérées peuvent être analysées (cf. section "Analyse des mises à jour récupérées" à la page [258](#)) pour vérifier qu'elles fonctionnent et qu'elles sont dépourvues d'erreurs sur les ordinateurs d'essai.

DANS CETTE SECTION

Création d'une tâche de téléchargement des mises à jour dans le référentiel	246
Analyse des mises à jour récupérées	258
Affichage des mises à jour récupérées	261
Déploiement de mises à jour automatique	262

CREATION D'UNE TACHE DE TELECHARGEMENT DES MISES A JOUR DANS LE REFERENTIEL

La tâche **Téléchargement des mises à jour dans le référentiel** est créée automatiquement lors de l'exécution de l'Assistant de démarrage rapide. Vous pouvez créer qu'une seule tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.

► *Pour créer la tâche de récupération des mises à jour par le Serveur d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches de Kaspersky Administration Kit**, ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Tâche**.

2. Créez une tâche du Serveur d'administration (cf. section "Création d'une tâche pour le Serveur d'administration" à la page 113). En guise de type de tâche, sélectionnez **Téléchargement des mises à jour dans le référentiel** (cf. ill. ci-après).

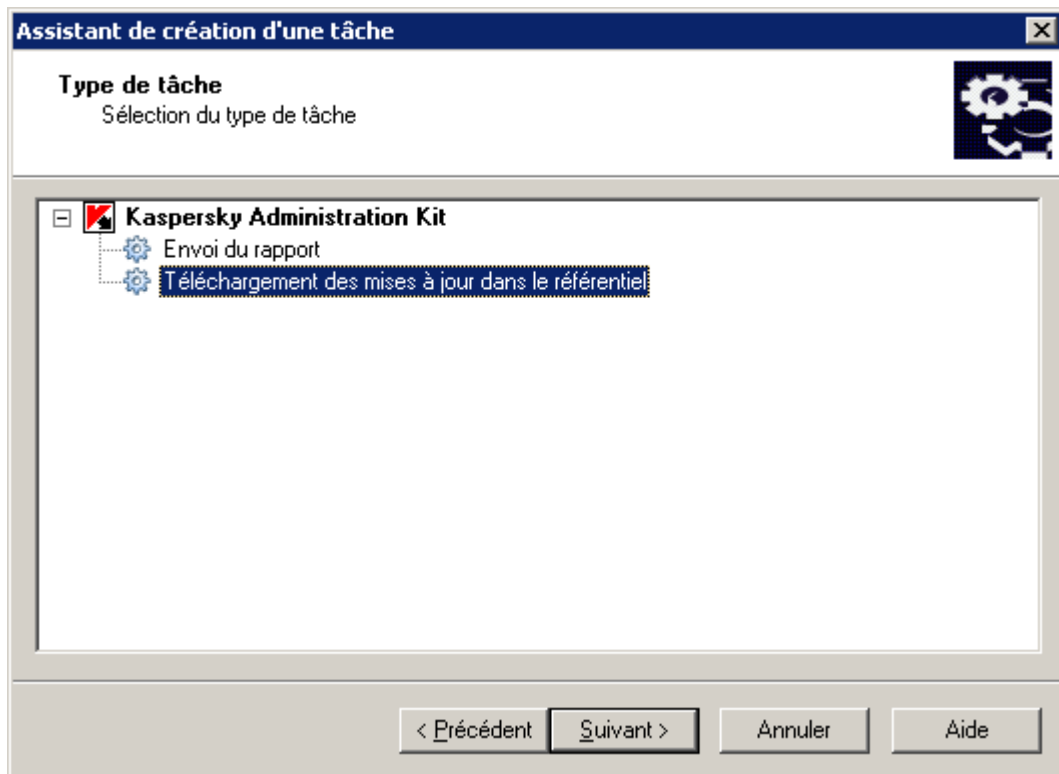


Illustration 210. Création d'une tâche de mise à jour. Sélection du type de la tâche

3. Dans la fenêtre ouverte (cf. ill. ci-après), en passant au lien **Personnaliser**, vous pouvez configurer :
- **Sources des mises à jour** : la liste des sources possibles, dont la mise à jour s'exécute ;
 - **Paramètres de connexion** : les paramètres du serveur proxy et autres paramètres des connexions de réseau installées ;
 - **Autres paramètres** : l'emplacement des mises à jour copiées, les paramètres de la mise à jour automatique, les paramètres des mises à jour des modules de programme, la diffusion des mises à jour sur les Serveurs secondaires.

Cliquez sur **Suivant**.

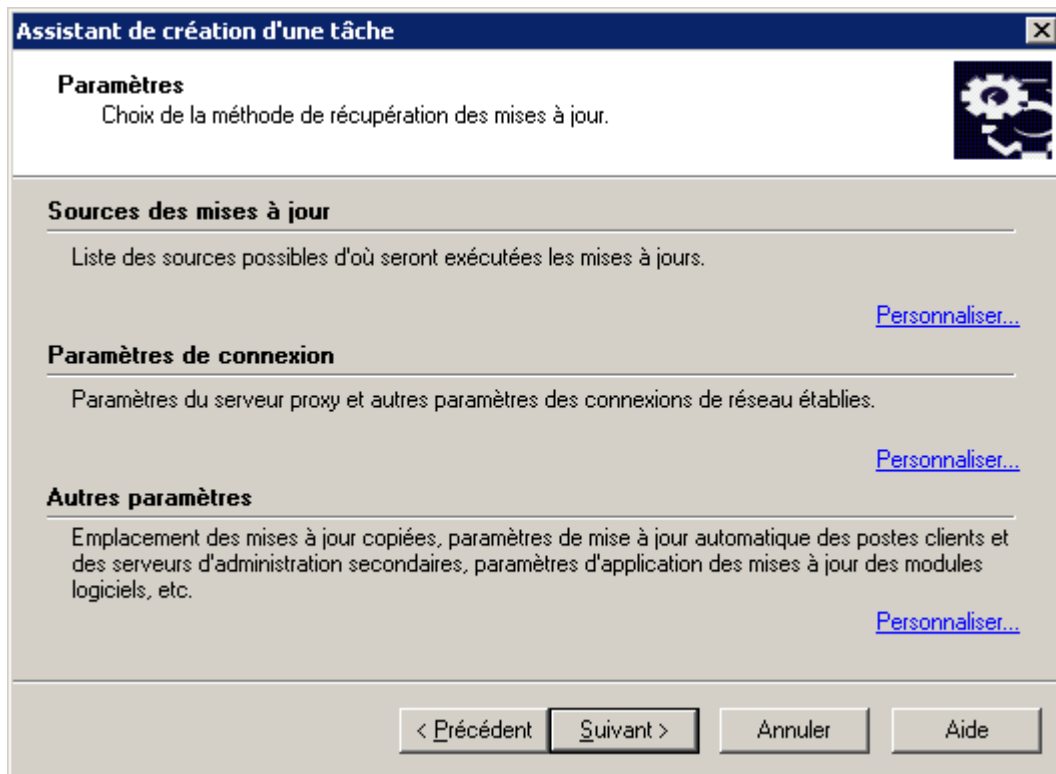


Illustration 211. Configuration des paramètres des sources de mises à jour

- Planifiez la tâche (cf. section "Création d'une tâche de groupe" à la page [101](#)). Cliquez sur **Suivant** (cf. ill. ci-après).

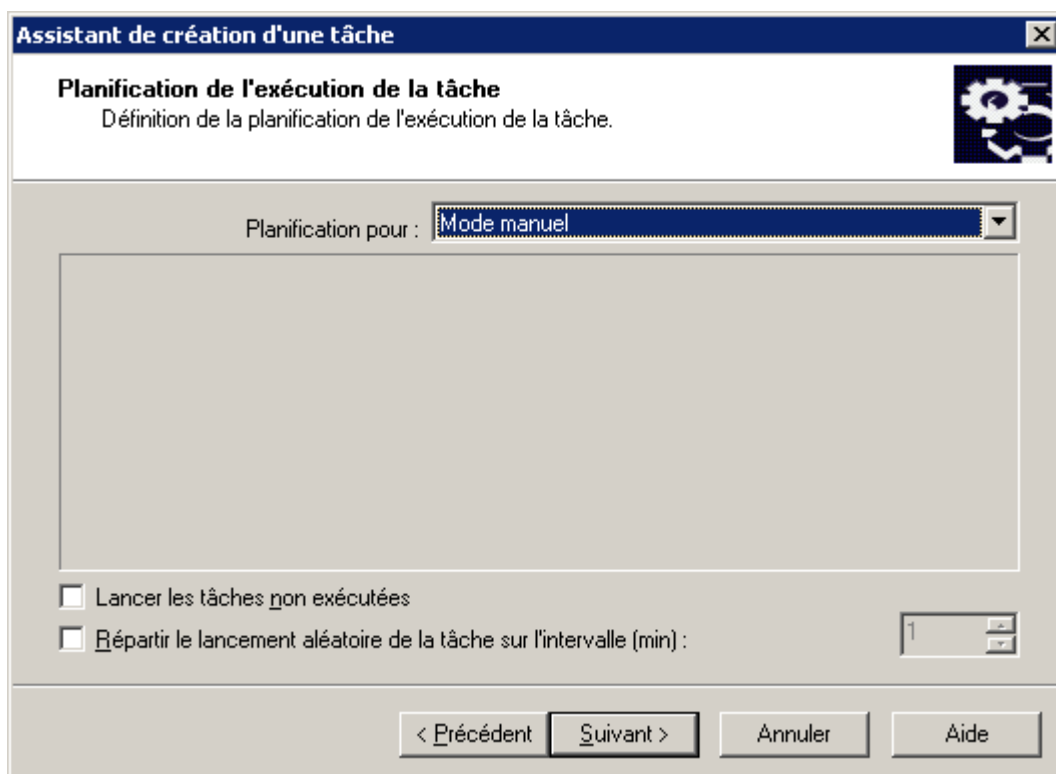


Illustration 212. Programmation de la tâche

- Appuyez sur le bouton **Terminer** (cf. ill. ci-après) pour terminer la création de la tâche.

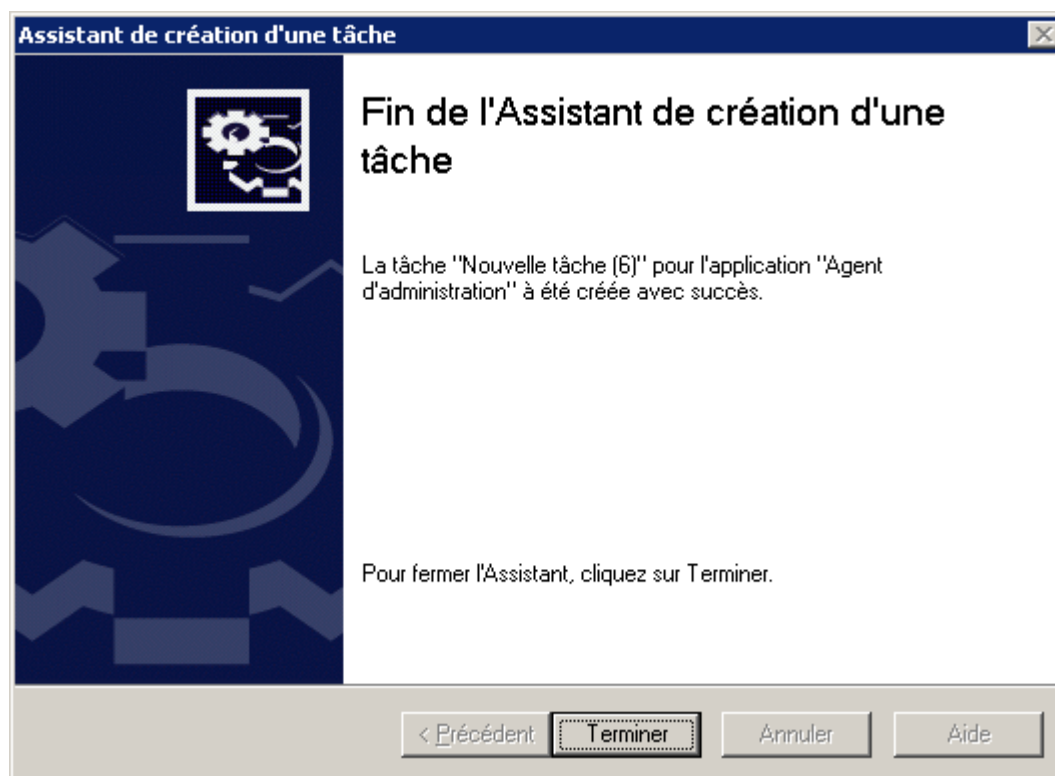


Illustration 213. Fin de la création d'une tâche

AJOUT D'UNE SOURCE DE MISES A JOUR

➔ Pour ajouter une source de mises à jour à la liste, procédez comme suit :

- Sélectionnez dans l'arborescence de la console le dossier **Tâches de Kaspersky Administration Kit**, sélectionnez la tâche **Téléchargement des mises à jour dans le référentiel**. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.

- Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres** (cf. ill. ci-après).

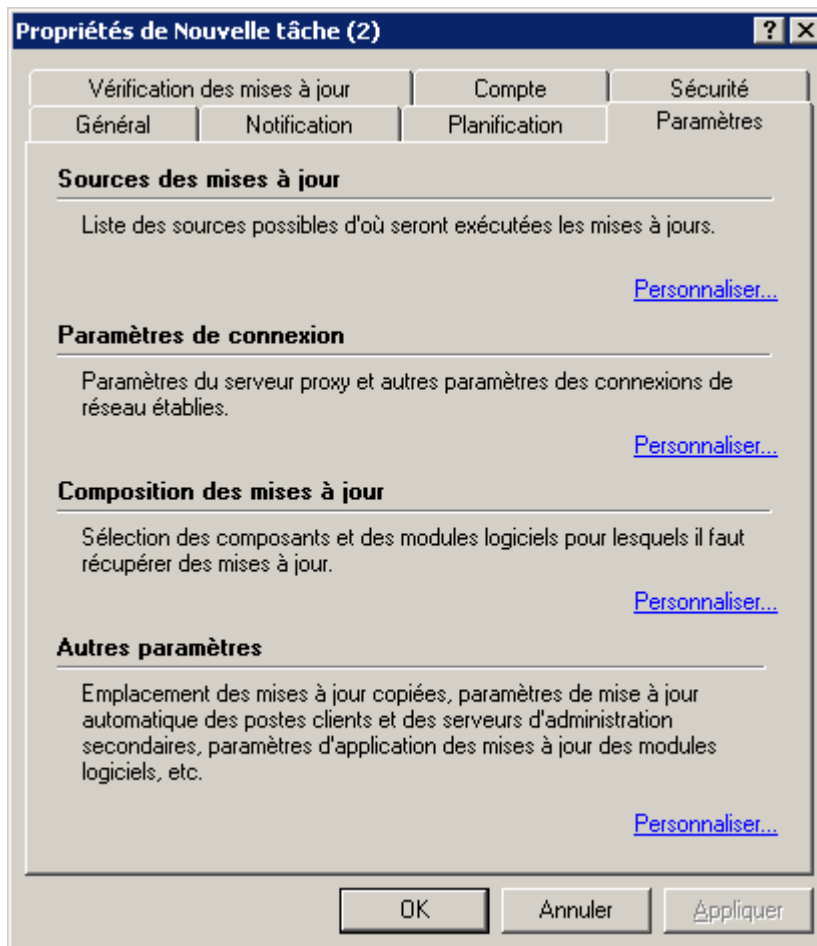




Illustration 214. Configuration des paramètres des sources de mises à jour

- Passez au lien **Personnaliser**, dans le groupe **Sources des mises à jour**.

Dans la fenêtre ouverte (cf. ill. ci-après) vous pouvez ajouter les sources des mises à jour. Le Serveur d'administration récupérera la mise à jour depuis les sources reprises dans la liste et dans l'ordre de celle-ci. Si une source est inaccessible pour une raison quelconque, la mise à jour sera réalisée depuis la source suivante dans la liste, etc. Vous pouvez modifier l'ordre des sources dans la liste à l'aide des boutons  et .

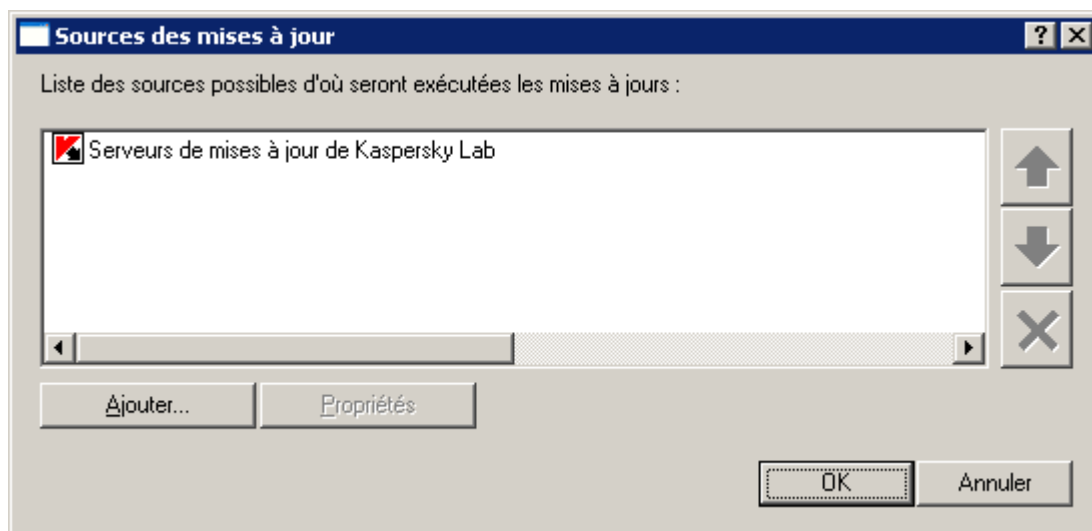


Illustration 215. Ajout d'une source de mises à jour

Cliquez sur le bouton **Ajouter** (cf. ill. ci-dessus). Ceci permet d'ouvrir la fenêtre **Propriétés de la source des mises à jour des bases**.

4. La fenêtre ouverte **Propriétés de la source des mises à jour des bases** (cf. ill. ci-après) permet de spécifier une source de mises à jour de la base antivirus et des modules d'application. Pour ce faire, choisissez une des options suivantes :
 - Les **Serveurs de mises à jour Kaspersky Lab** sont les serveurs Kaspersky Lab où sont déposés les mises à jour de la base antivirus et des modules de programmes.
 - Le **Serveur d'administration principal** est un dossier en accès public situé sur le serveur d'administration principal.
 - **Dossier local ou de réseau** est un serveur FTP ou HTTP ou un dossier local ou de partage réseau ajouté par l'utilisateur, contenant les dernières mises à jour. Si vous cochez cette option, spécifiez l'adresse du dossier de mises à jour, manuellement ou en cliquant sur **Parcourir**. N'oubliez pas que choisissant lors de la sélection du dossier local, il faut indiquer le dossier avec le Serveur d'administration installé.
 - Cochez **Ne pas utiliser de serveur proxy** pour connecter à la source de mise à jour sans utiliser un serveur proxy. Si la case n'est pas cochée, le serveur proxy sera utilisé selon les paramètres de connexion définis dans la fenêtre **Paramètres LAN**.

Cliquez sur le bouton **OK**.

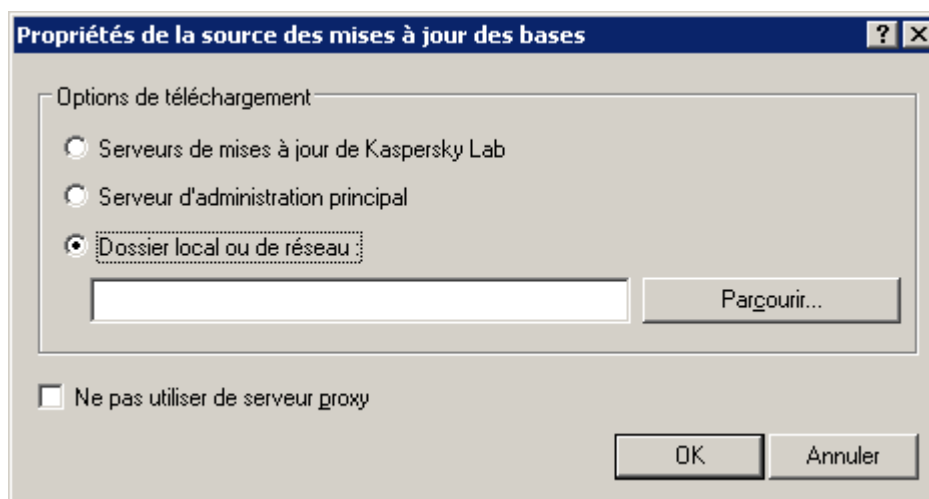


Illustration 216. Sélection d'une source de mises à jour de la base antivirus et des modules d'application

5. Cliquez sur le bouton **OK** pour terminer l'ajout du volet d'informations.

CONFIGURER LA CONNEXION AUX SERVEURS DE MISES A JOUR

- Pour configurer les connexions aux serveurs de mises à jour, procédez comme suit :
1. Sélectionnez dans l'arborescence de la console le dossier **Tâches de Kaspersky Administration Kit**, sélectionnez la tâche **Téléchargement des mises à jour dans le référentiel**. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres** (cf. ill. ci-après).

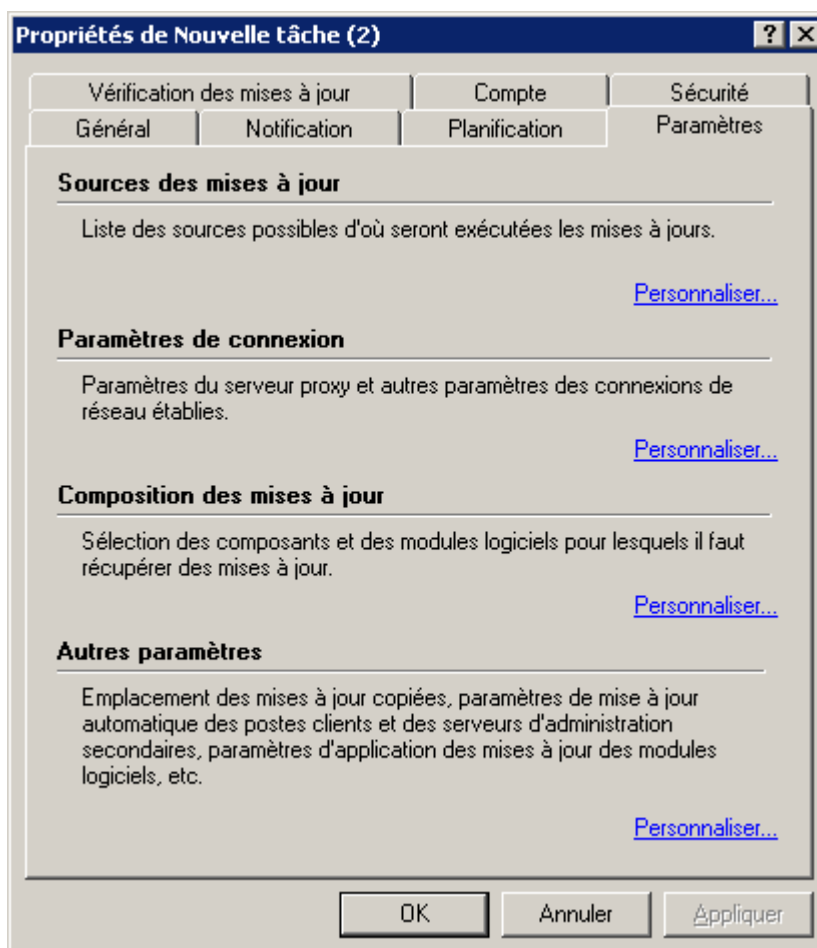


Illustration 217. Configuration des paramètres des sources de mises à jour

3. Dans la fenêtre ouverte (cf. ill. ci-dessus), passez au lien **Personnaliser**, dans le groupe **Paramètres de connexion**.
4. Dans la fenêtre ouverte **Paramètres LAN** établissez les valeurs nécessaires des paramètres de connexion avec les serveurs de mises à jour (cf. ill. ci-après) :
- **Utiliser le serveur proxy** : si la connexion à la source de mise à jour se fait par un serveur proxy. Saisissez l'adresse et le numéro de port pour la connexion au serveur proxy. L'adresse peut être saisie sous la forme qui vous convient le mieux : textuelle (par exemple, **Adresse** : testserver) ou décimale (par exemple, **Adresse** : 125.2.19.1).
 - **Définir automatiquement les paramètres** : pour utiliser les paramètres de connexion au serveur proxy qui ont été définis dans la base de registre système de l'ordinateur du Serveur d'administration.
 - **Authentification du serveur proxy** : si l'accès au serveur proxy est protégé par un mot de passe. Remplissez les champs **Nom d'utilisateur** et **Mot de passe**.
 - **Utiliser le FTP en mode passif** : pour forcer le mode passif lors des mises à jour en utilisant le protocole FTP. Décochez cette case pour utiliser le mode actif. Il est conseillé d'utiliser le mode passif.

- **Délai d'attente de connexion (sec.)** : spécifiez le délai maximum de connexion au serveur de mises à jour. Si la connexion échoue, après un certain délai une nouvelle tentative est faite pour connecter au serveur de mises à jour suivant. Ceci se répète jusqu'à ce qu'une connexion réussisse ou quand tous les serveurs disponibles ont été essayés.

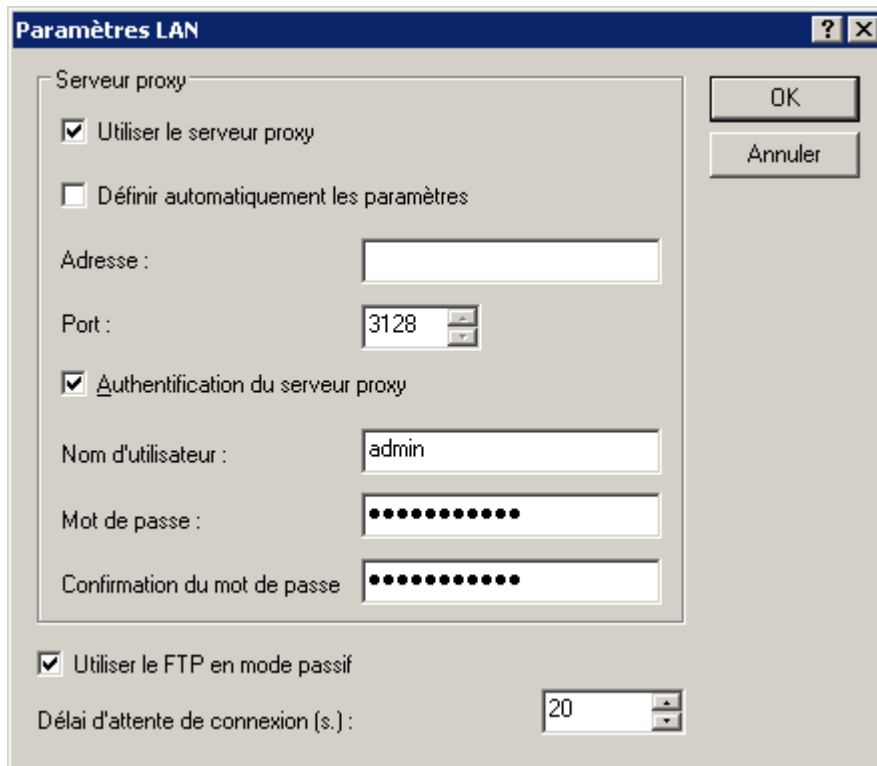


Illustration 218. Configuration des paramètres de connexion aux serveurs de mises à jour

DEFINITION DU CONTENU DES MISES A JOUR

En rédigeant les paramètres de la tâche de mise à jour, vous pouvez définir le contenu des mises à jour, copiées à partir de la source de mises à jour.

➤ Pour modifier le contenu des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches de Kaspersky Administration Kit**, ouvrez le menu contextuel de la tâche **Téléchargement des mises à jour dans le référentiel** et sélectionnez la commande **Propriétés**.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres** (cf. ill. ci-après).

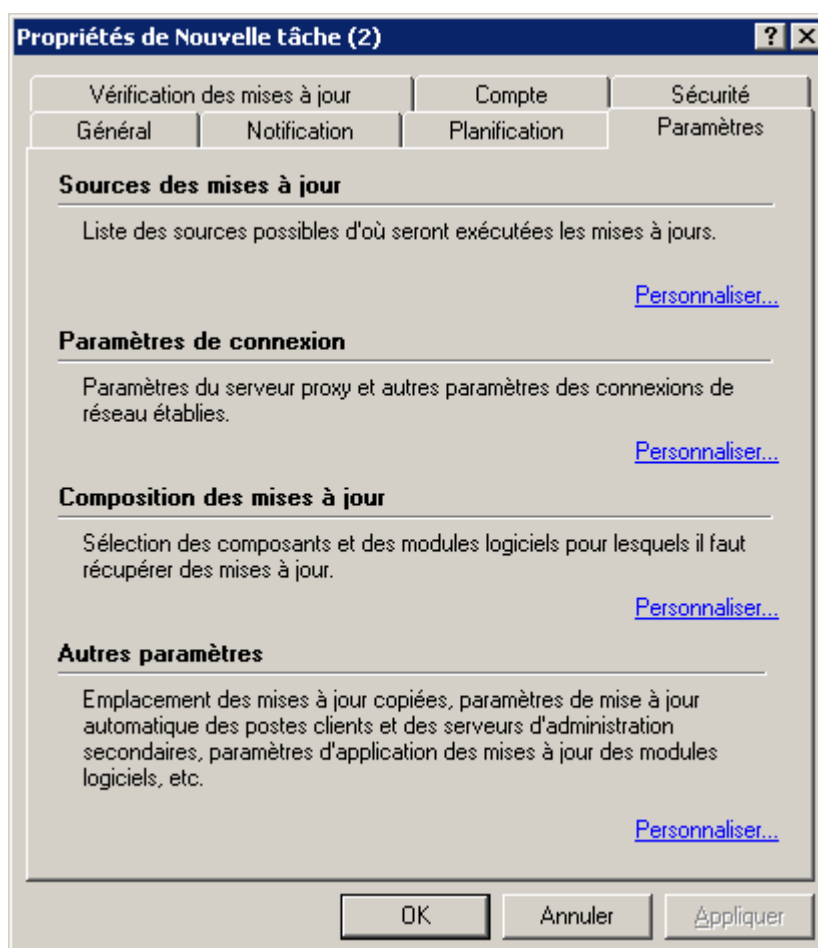


Illustration 219. Modification du contenu des mises à jour. Onglet **Paramètres**

3. Dans le groupe **Composition des mises à jour**, à l'aide du lien **Personnaliser** ouvrez la fenêtre de configuration de la composition des mises à jour et cochez la case en regard des types des mises à jour téléchargées (cf. ill. ci-après). Cette fenêtre vous permet de configurer les paramètres suivants :
- **Définir automatiquement le contenu des mises à jour téléchargées** : télécharger les mises à jour pour toutes les applications de Kaspersky Lab installées sur les ordinateurs connectés au Serveur d'administration.

- **Forcer le téléchargement des types suivants de mises à jour** : sélectionner la composition des mises à jour à télécharger par composant, quelles que soient les applications qui les utilisent et sans qu'elles soient nécessairement installées sur les ordinateurs des groupes d'administration. Pour ce faire, cochez les cases dans le tableau en regard des noms des types nécessaires des mises à jour.

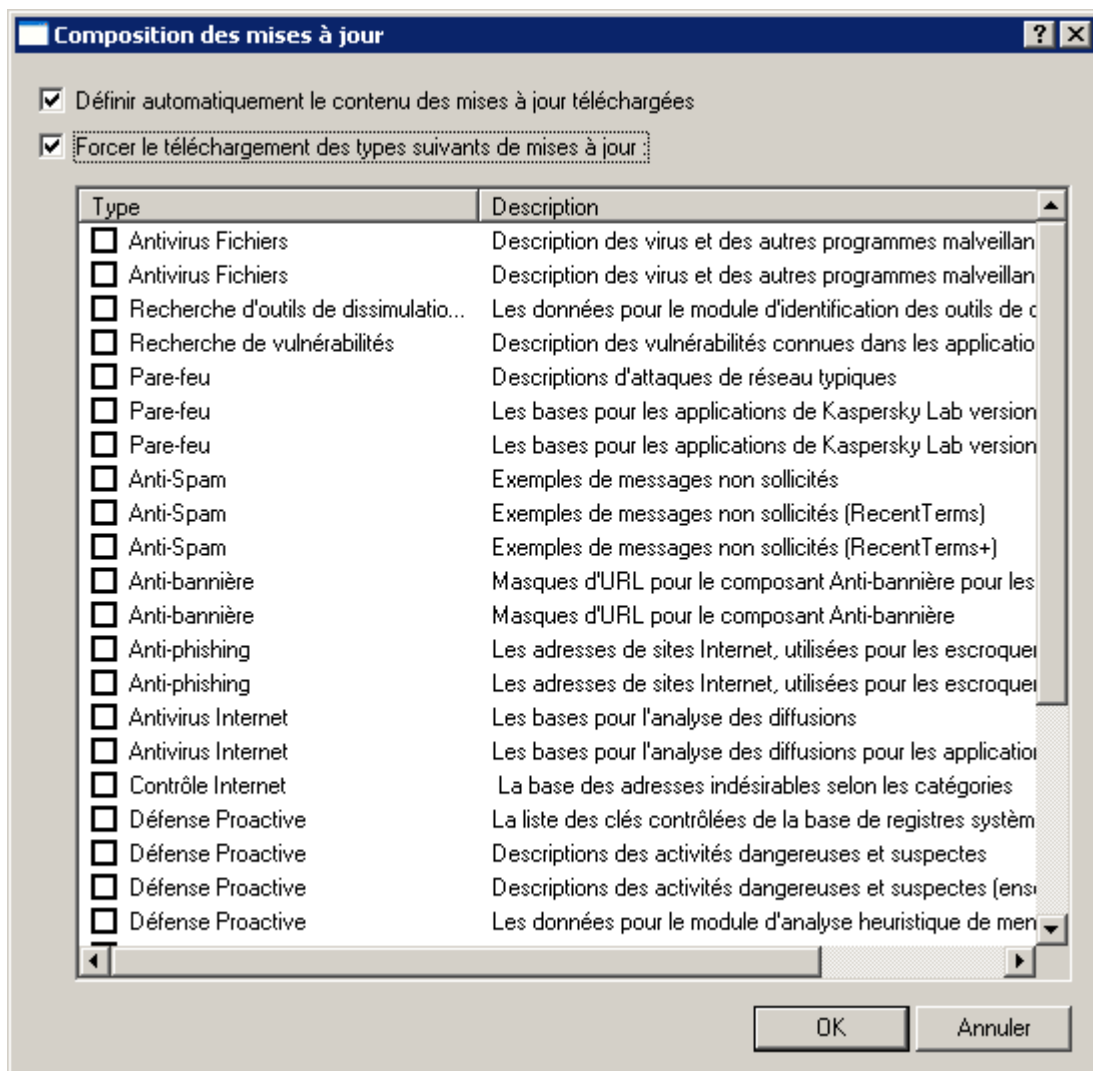


Illustration 220. Sélection des mises à jour

4. Cliquez sur le bouton **OK** pour terminer la définition du contenu des mises à jour.

CONFIGURATION D'AUTRES PARAMETRES DE LA TACHE DE MISE A JOUR

➔ Pour configurer les paramètres de la source de mises à jour, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches de Kaspersky Administration Kit** et sélectionnez **Tâche de téléchargement des mises à jour dans le référentiel**. Ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres** (cf. ill. ci-après).

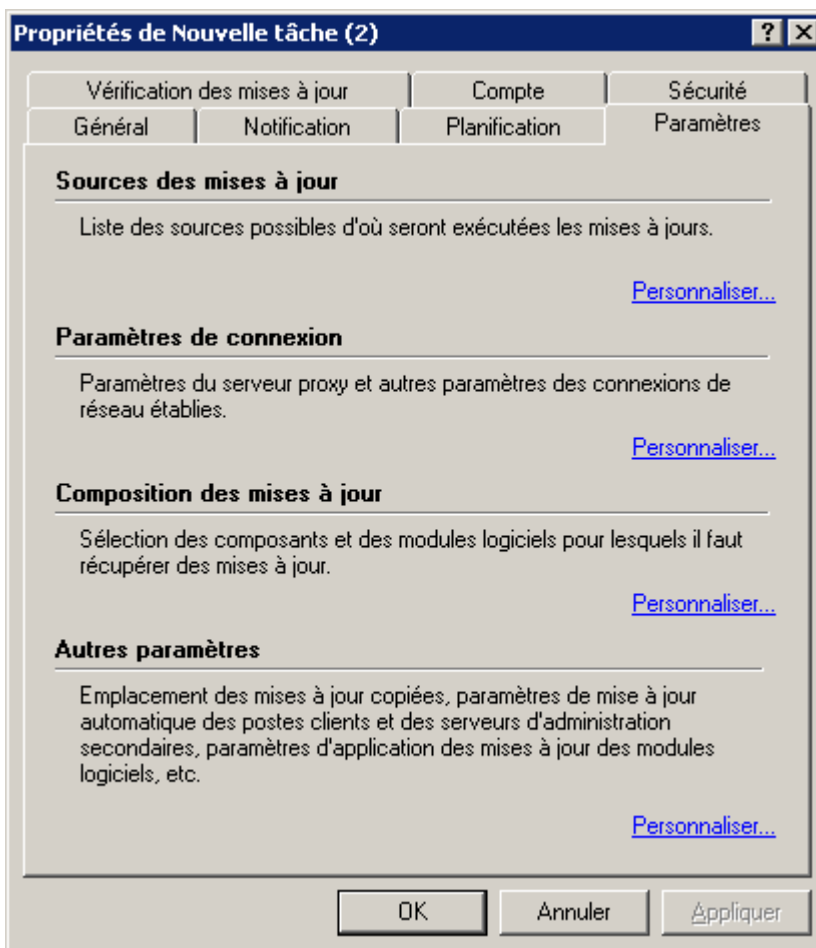


Illustration 221. Configuration d'autres paramètres de la tâche de mise à jour

3. Dans la fenêtre ouverte (cf. ill. ci-dessus), passez au lien **Personnaliser**, dans le groupe **Autres paramètres**.
4. Dans la fenêtre ouverte **Autres paramètres** (cf. ill. ci-après), il est possible de configurer les paramètres suivantes :
- **Forcer la mise à jour des serveurs secondaires.** Pour vous assurer que les tâches de récupération des mises à jour par les Serveurs d'administration sont lancées automatiquement après leur réception par le Serveur d'administration principal, et sans tenir compte de la programmation prévue dans la configuration de ces tâches.
 - **Actualiser les modules des Serveurs d'administration.** Si la case est cochée, les mises à jour des modules du Serveur d'administration, quand elles sont récupérées, sont installées directement après la fin de la tâche de récupération des mises à jour par le Serveur d'administration. Si la case n'est pas sélectionnée, les mises à jour pourront être installées manuellement seulement.
 - **Actualiser les modules des Agents d'administration.** Si la case est cochée, les mises à jour des modules de l'Agent d'administration, quand elles sont récupérées, sont installées après la fin de la tâche de récupération des mises à jour par le Serveur d'administration. Si la case n'est pas sélectionnée, les mises à jour pourront être installées manuellement seulement.
 - **Copier les mises à jour récupérées dans des dossiers complémentaires.** Si la case est cochée, le Serveur d'administration copiera les mises à jour récupérées sur la source dans les répertoires indiqués. Composez la liste des répertoires complémentaires à l'aide des boutons **Ajouter** et **Supprimer**. Celle-ci est décochée par défaut.

Pour que les tâches de récupération des mises à jour par les postes clients et les Serveurs d'administration secondaire soient lancées uniquement après la fin de la copie des mises à jour depuis le répertoire de réseau vers les répertoires complémentaires, cochez la case **Ne pas forcer la mise à jour des postes clients et des serveurs d'administration secondaires avant la fin de la copie**. Cette case doit être cochée si les postes clients et les Serveurs d'administration secondaires téléchargent les mises à jour depuis des répertoires complémentaires.

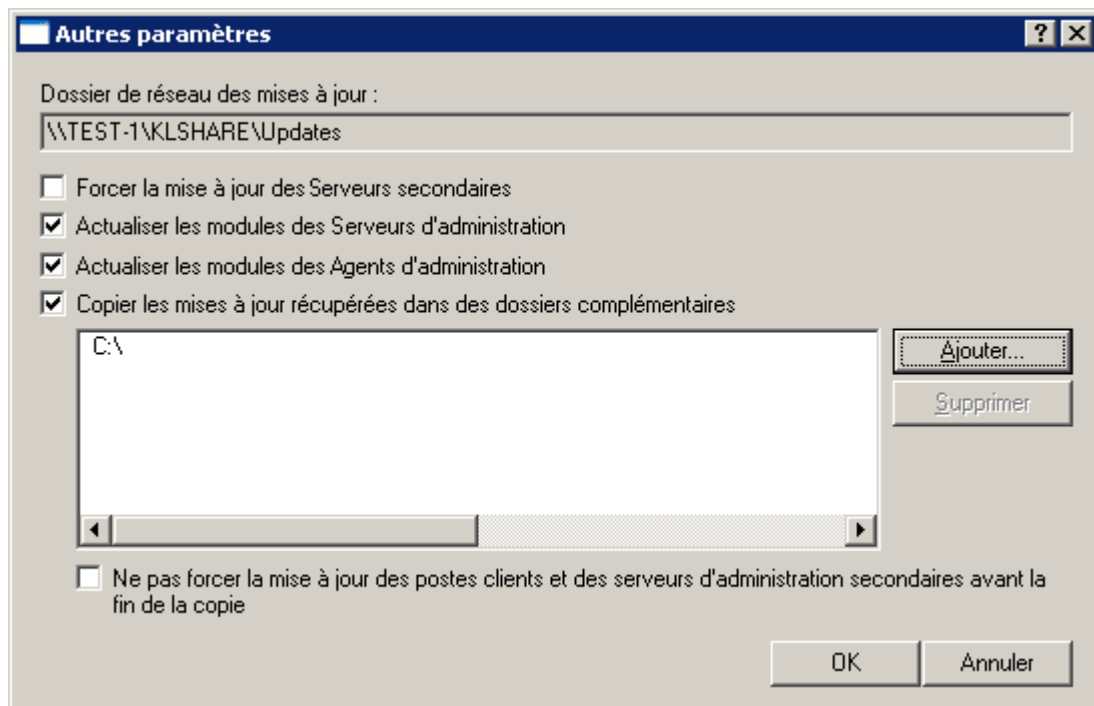


Illustration 222. Configuration des paramètres

5. Cliquez sur le bouton **OK** pour terminer la configuration d'autres paramètres de la tâche de mises à jour.

ANALYSE DES MISES A JOUR RECUPEREES

Le système de la protection antivirus ne fonctionne correctement que dans le cas où les applications antivirus utilisent les versions à jour des bases. Il est donc nécessaire de s'assurer que les tâches de téléchargement des mises à jour dans le référentiel effectuées par le Serveur d'administration et les tâches des mises à jour des bases sur les postes clients fonctionnent correctement.

➤ Pour vérifier la mise à jour des bases, procédez comme suit :

1. Dans la Console d'administration passez au dossier **Tâches de Kaspersky Administration Kit** et sélectionnez la tâche de téléchargement des mises à jour dans le référentiel.
2. Ouvrez la fenêtre des propriétés d'une tâche, en sélectionnant le point **Propriétés** dans le menu contextuel.

3. Sélectionnez l'onglet **Vérification des mises à jour** (cf. ill. ci-après).

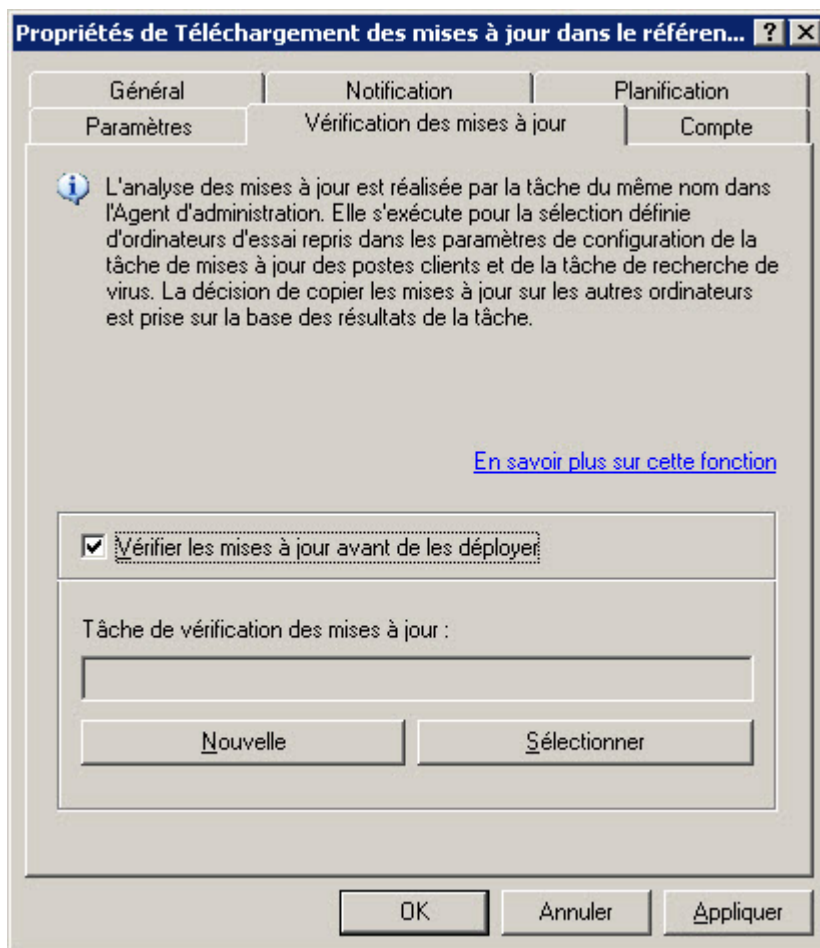


Illustration 223. Configuration de la vérification des mises à jour

4. Cochez la case **Vérifier les mises à jour avant de les déployer**.
5. Dans le champ **Tâche de vérification des mises à jour**, sélectionnez une tâche parmi le nombre des tâches existantes à l'aide du bouton **Sélectionner**. Vous pouvez aussi créer une nouvelle tâche de vérification des mises à jour. Pour ce faire, cliquez sur **Créer** et suivez les consignes de l'Assistant. Lors de la création d'une tâche de vérification des mises à jour, le Serveur d'administration crée des stratégies de vérification, ainsi que des tâches de groupe auxiliaires de mise à jour et d'analyse à la demande.

Pour lancer la tâche de vérification des mises à jour, il est conseillé d'utiliser des ordinateurs bien protégés et présentant la configuration logicielle la plus répandue dans le réseau de l'entreprise. La qualité de la vérification sera ainsi accrue et le risque de faux positifs, ainsi que la probabilité d'identifier des virus lors de la vérification seront réduits (en cas de découverte de virus sur les ordinateurs d'essai, la tâche de vérification des mises à jour est considérée comme un échec).

Après avoir appliqué les paramètres indiqués avant le déploiement des bases, la tâche de vérification des mises à jour est lancée. Avec cela, le Serveur d'administration copie les mises à jour depuis la source, les place dans un dossier temporaire et lance la tâche de vérification des mises à jour. Si l'exécution de cette tâche réussit, les mises à jour seront copiées depuis le dossier temporaire vers le dossier partagé du Serveur d'administration (dossier Share\Updates), puis seront diffusées vers tous les autres ordinateurs pour lesquels le Serveur d'administration est une source de mise à jour.

Si, à la fin de la tâche de vérification des mises à jour placées dans le répertoire temporaire, les mises à jour sont considérées comme incorrectes ou si la tâche se solde sur une erreur, la copie des mises à jour dans le répertoire partagé n'a pas lieu et la version précédente des mises à jour est conservée sur le Serveur d'administration. Les tâches dont la programmation est **Lors du téléchargement des mises à jour dans le référentiel** ne sont pas lancées. Ces

opérations sont réalisées à l'exécution suivante de la tâche de téléchargement des mises à jour dans le référentiel, si la vérification du nouvel ensemble des mises à jour donne un résultat positif.

Si la case **Vérifier les mises à jour avant de les déployer** est cochée, la tâche de téléchargement des mises à jour dans le stockage est considérée comme étant terminée après la fin de la tâche de vérification des mises à jour. N'oubliez pas que dans le cadre de l'exécution de la tâche de vérification des mises à jour, ce sont des tâches spéciales de mise à jour et d'analyse à la demande qui sont lancées. Leur exécution peut durer un certain temps. Il faut tenir compte de cet élément lors de la programmation de la tâche de récupération des mises à jour par le Serveur d'administration.

Vous pouvez modifier les paramètres des stratégies de vérification et des tâches auxiliaires. Cependant, n'oubliez pas que pour une vérification correcte des mises à jour, il faut :

- Enregistrer sur le Serveur d'administration tous les événements correspondant aux niveaux d'importance **Critique** et **Erreur**. Sur la base des événements de ce type, le Serveur d'administration analyse le fonctionnement des applications.
- Utiliser le Serveur d'administration en tant que source des mises à jour.

Si le redémarrage de l'ordinateur est requis après l'installation des mises à jour des modules logiciels, il faut l'exécuter sans attendre. Si l'ordinateur n'est pas redémarré, il sera impossible de vérifier l'exactitude de ce type de mise à jour. Pour certaines applications, l'installation de mises à jour qui requièrent un redémarrage peut être interdites ou réalisées uniquement après confirmation de l'utilisateur. Ces restrictions doivent être désactivées dans les stratégies des tâches ou les paramètres des tâches.

- Ne pas utiliser les technologies iChecker, iSwift et iStream d'accélération de l'analyse.
- Sélectionner les actions sur les objets infectés : **Ne pas demander/Ignorer/Enregistrer l'information dans le rapport**.
- Définir le type de programmation des tâches : **Mode manuel**.

Il est déconseillé de supprimer automatiquement les objets malveillants identifiés car dans ce cas, le fichier à l'origine du faux positif sera supprimé de l'ordinateur et il sera impossible de vérifier le déclenchement d'un faux positif sur ce fichier avec la mise à jour suivante. La mise à jour des bases antivirus sera diffusée sur tous les ordinateurs gérés par le Serveur d'administration.

Le mécanisme de vérification des mises à jour suit le scénario suivant :

1. Après la sauvegarde des mises à jour dans un stockage temporaire, le Serveur d'administration lance les tâches de mise à jour, indiqués dans les paramètres de la tâche d'analyse des mises à jour : les tâches de groupe secondaires des mises à jour ou les tâches des mises à jour formées par l'administrateur pour l'ensemble d'ordinateurs.

Les mises à jour des bases et des modules des applications sont diffusées vers des ordinateurs sélectionnés. Après la récupération des mises à jour, les ordinateurs peuvent être redémarrés pour appliquer les mises à jour des modules logiciels.

2. Une fois que les mises à jour ont été appliquées selon les paramètres de la tâche, les éléments suivants sont vérifiés :
 - l'état de la protection en temps réel des applications antivirus ainsi que l'état de toutes les tâches de protection en temps réel ;
 - le lancement des tâches d'analyse à la demande, indiquées dans les paramètres de la tâche d'analyse des mises à jour : les tâches de groupe secondaires d'analyse à la demande ou les tâches d'analyse à la demande formées par l'administrateur pour l'ensemble d'ordinateurs.
3. Quand toutes les tâches sur tous les ordinateurs définis dans les paramètres de la tâche de vérification des mises à jour sont terminées, une décision est prise sur la qualité des mises à jour.

Les mises à jour sont jugées **incorrectes** si une des conditions suivantes s'est manifestée ne serait-ce que sur un ordinateur :

- une erreur s'est produite pendant l'exécution de la tâche de mise à jour ;
- après l'application des mises à jour, l'état de la protection en temps réel de l'application antivirus a changé ;
- un objet infecté a été identifié durant l'analyse à la demande ;
- une erreur de fonctionnement de l'application de Kaspersky Lab s'est produite.

Si aucune des conditions citées ne s'est manifestée sur aucun des ordinateurs, alors les mises à jour sont considérées comme **correctes** et la tâche de vérification des mises à jour a réussi.

AFFICHAGE DES MISES A JOUR RECUPEREES

Afin d'afficher les mises à jour récupérées par le Serveur d'administration, sélectionnez dans l'arborescence de la console le dossier **Stockages** → **Mises à jour**. La liste des mises à jour enregistrées sur le Serveur d'administration est présentée dans le panneau des résultats.

Pour afficher les propriétés de la mise à jour, sélectionnez la mise à jour souhaitée dans le panneau des résultats puis choisissez l'option **Propriétés** du menu contextuel. Cela entraînera l'ouverture de la fenêtre **Propriétés : <Nom de la mise à jour>** (cf. ill. ci-après).

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

- nom de la mise à jour ;
- nombre d'enregistrements dans les bases (ce champ n'est pas visible pour la mise à jour des modules de l'application) ;
- nom et version de l'application à laquelle la mise à jour est destinée ;
- taille de la mise à jour enregistrée sur le Serveur d'administration ;
- date où la mise à jour a été copiée sur le Serveur d'administration ;

- date de création de la mise à jour.

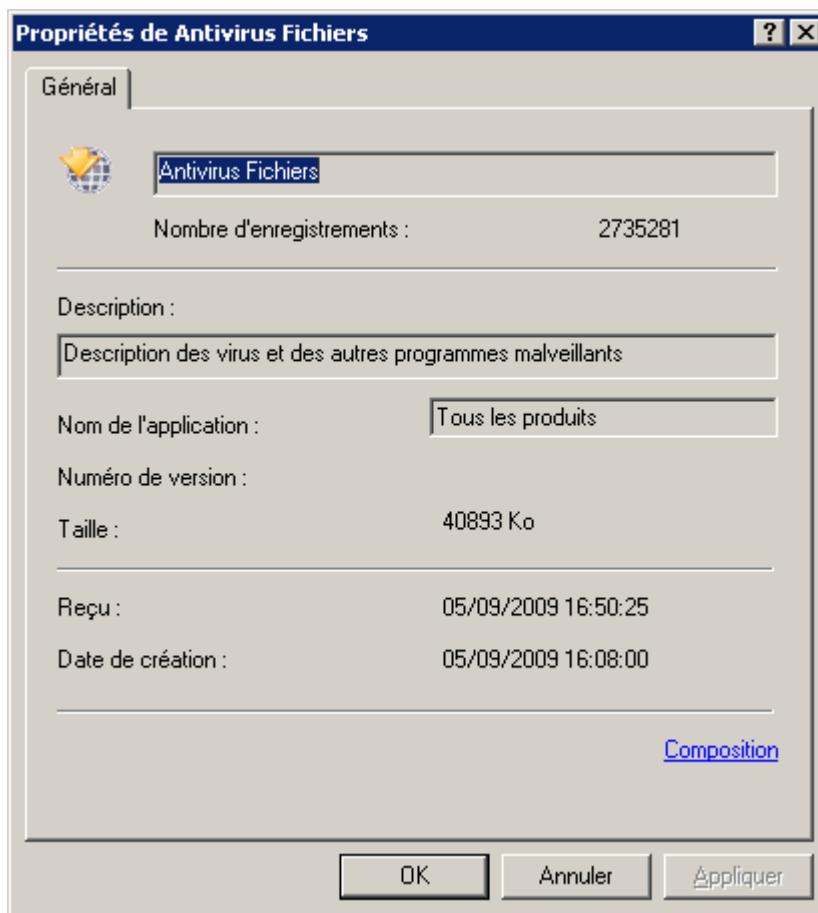


Illustration 224. Affichage des propriétés des mises à jour téléchargées

DEPLOIEMENT DE MISES A JOUR AUTOMATIQUE

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 sont lancées automatiquement après leur réception par le Serveur d'administration principal, et sans tenir compte de la programmation prévue dans la configuration de ces tâches.

DEPLOIEMENT DE MISES A JOUR VERS LES CLIENTS IMMEDIATEMENT APRES LE TELECHARGEMENT

- Pour que le Serveur d'administration puisse transférer les mises à jour vers les clients immédiatement après le téléchargement,

dans les paramètres de la tâche de récupération des mises à jour par une application quelconque de Kaspersky Lab, désignez en tant que source des mises à jour le **Serveur d'administration** et sous l'onglet **Planification**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le référentiel**.

REDISTRIBUTION AUTOMATIQUE DES MISES A JOUR SUR LES SERVEURS SECONDAIRES

- *Pour vous assurer que les tâches de récupération des mises à jour par le Serveur d'administration principal sont redistribuées automatiquement sur les Serveurs secondaires immédiatement après leur réception, procédez comme suit :*

dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Forcer la mise à jour des Serveurs secondaires**.

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

INSTALLATION AUTOMATIQUE DES MISES A JOUR DES MODULES LOGICIELS

- *Pour pouvoir installer automatiquement les mises à jour des modules logiciels sur le Serveur d'administration une fois qu'elles ont été récupérées,*

dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Actualiser les modules des Serveurs d'administration**.

- *Pour pouvoir installer automatiquement les mises à jour des modules logiciels sur l'agents d'administration une fois qu'elles ont été récupérées,*

dans les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Actualiser les modules des Agents d'administration**.

Immédiatement après la réception des mises à jour par le Serveur d'administration principal, des tâches d'installation des mises à jour des modules logiciels seront automatiquement lancées.

CONSTITUTION DE LA LISTE DES AGENTS DE MISE A JOUR ET LEUR CONFIGURATION

- ➔ Pour composer la liste des agents de mise à jour et les configurer pour la diffusion des mises à jour sur les ordinateurs du groupe, procédez comme suit :

Dans la fenêtre des propriétés du groupe, sélectionnez l'onglet **Agents de mise à jour** (cf. ill. ci-après). Grâce aux boutons **Ajouter** et **Supprimer** composez la liste des postes qui rempliront le rôle d'agent de mise à jour dans le cadre du groupe.

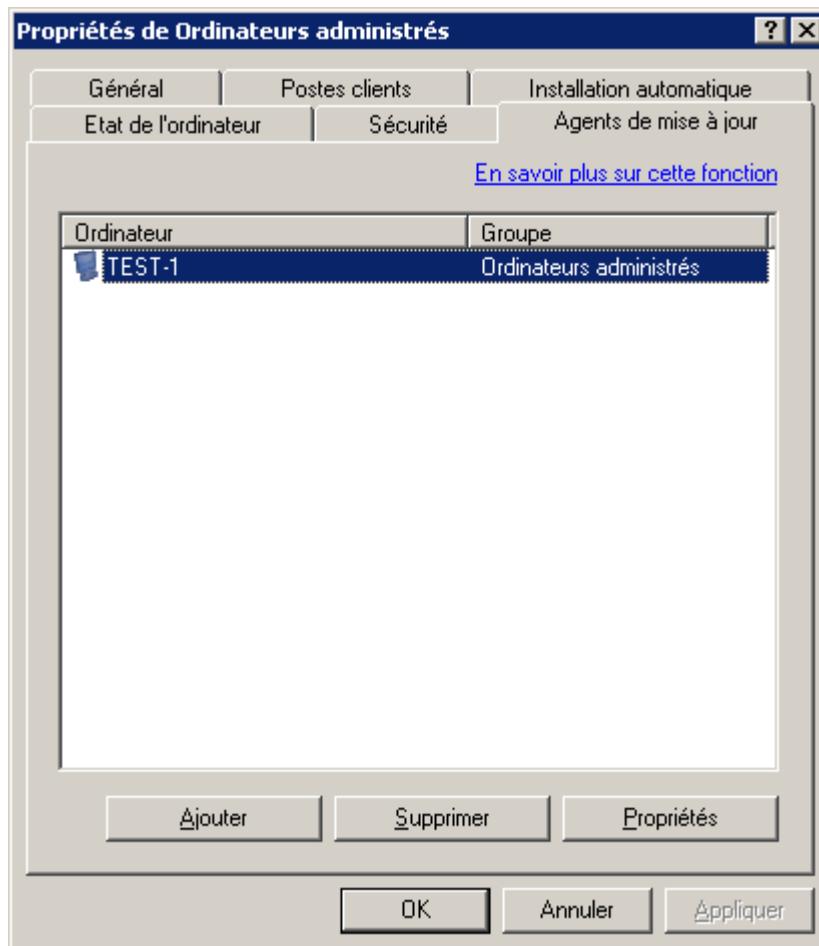


Illustration 225. Création de la liste des agents de mise à jour

Pour modifier les paramètres de l'agent de mise à jour, sélectionnez l'agent dans la liste et cliquez sur **Propriétés**. Dans la fenêtre **<Nom de l'agent de mise à jour> propriétés** (cf. ill. ci-après), vous pouvez :

- indiquer le numéro de port utilisé par le client pour se connecter à l'agent de mise à jour (le numéro de port par défaut est 14000. Si ce port est déjà en service, vous pouvez en changer) ;

Dans le cas où l'agent de mise à jour tourne sur un ordinateur sur lequel est également installé un Serveur d'administration, le numéro de port par défaut pour la connexion est 14001.

- indiquer le numéro de port utilisé par le client pour se connecter de manière sécurisée à l'agent de mise à jour par le biais du protocole SSL (par défaut, il s'agit du port 13000) ;

Dans le cas où l'agent de mise à jour tourne sur un ordinateur sur lequel est également installé un Serveur d'administration, le numéro de port par défaut pour la connexion SSL est 13001.

- activer l'utilisation d'une diffusion IP multiadresse pour la diffusion automatique des paquets d'installation sur les postes clients du groupe. Pour ce faire, cochez la case **Utiliser la multidiffusion** et saisissez les données dans le champ **IP de multidiffusion** et **Numéro du port d'IP-MULTICAST**. Si cette case est cochée, les paramètres des tâches et des stratégies de groupe seront également diffusés sur les postes clients à l'aide d'une diffusion IP multiadresse.

Lors de l'utilisation de la diffusion IP multiadresse, le volume du trafic se réduit à peu près dans N fois, où N - le nombre général des ordinateurs inclus dans le groupe d'administration.

Pour obtenir de plus amples informations sur la diffusion de paquets d'installation à l'aide d'agents de mise à jour, consultez le manuel d'implantation.

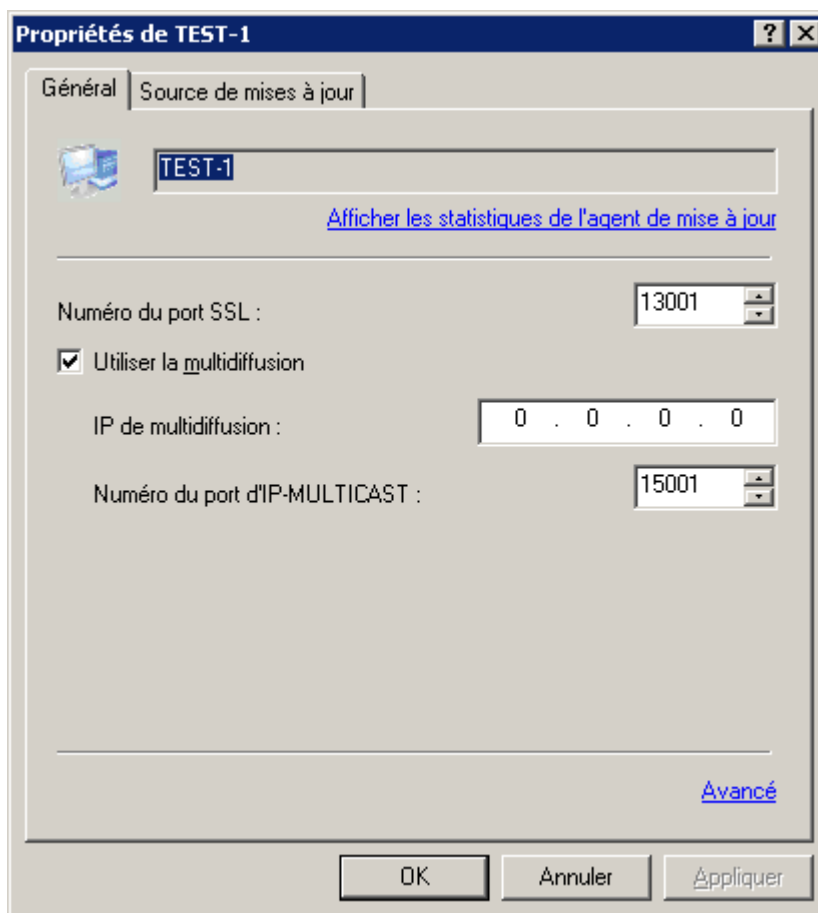


Illustration 226. Fenêtre des propriétés de l'agent de mise à jour. Onglet **Général**

- Pour consulter les statistiques relatives à l'agent de mise à jour,

utilisez le lien **Afficher les statistiques de l'agent de mise à jour**.

Dans la fenêtre qui s'ouvre (cf. ill. ci-après), vous verrez les informations suivantes :

- Données relatives aux bases des applications :
 - Heure de la dernière synchronisation avec le Serveur d'administration** : il s'agit de l'heure de la dernière connexion de l'agent de mises à jour avec le Serveur d'administration pour récupérer les dernières mises à jour.

- **Volume de données reçues par les clients via les distributions multiadresses** : il s'agit du rapport du volume d'information transmise aux postes clients via la diffusion multi-adresses par rapport au volume d'informations récupérées par l'agent de mises à jour depuis le Serveur d'administration.
- **Nombre total de synchronisations avec le Serveur d'administration** : nombre total de connexion de l'agent de mises à jour au Serveur d'administration.
- **Volume de données envoyé par le moyen de distributions multi-adresses** : volume d'informations (en octets) transmises par l'agent de mises à jour sur les postes client via la diffusion multi-adresse des bases de l'application.
- **Volume des données copiées par les clients via le protocole TCP** : volume d'informations (en octets) transmises par l'agent de mises à jour aux postes clients via le protocole TCP.
- **Heure de création** : date et heure de création des bases des applications récupérées du serveur d'administration par l'agent de mises à jour.
- **Dossier de travail** : adresse du dossier de travail de l'agent de mises à jour.
- **Taille du dossier de travail** : taille du dossier de travail de l'agent de mises à jour.
- Les données sur l'installation à distance et la diffusion de stratégies :
 - **Volume de données reçues par les clients via les distributions multiadresses** : il s'agit du rapport du volume d'information transmise aux postes clients via la diffusion multi-adresses par rapport au volume d'informations récupérées par l'agent de mises à jour depuis le Serveur d'administration.
 - **Volume total des stratégies et des paquets d'installation copiés depuis le Serveur d'administration** : il s'agit de la taille de tous les paquets d'installation et de toutes les stratégies récupérés par l'agent de mises à jour depuis le Serveur d'administration.
 - **Volume total des données copiées par les clients depuis les agents de mise à jour** : volume d'informations (en octets) transmises par l'agent de mises à jour aux postes clients via le protocole TCP.

- **Volume de données envoyé par l'agent de mise à jour à l'aide de la distribution multiadresse :** volume d'informations (en octets) transmises par l'agent de mises à jour sur les postes client via la diffusion multi-adresse des bases de l'application.

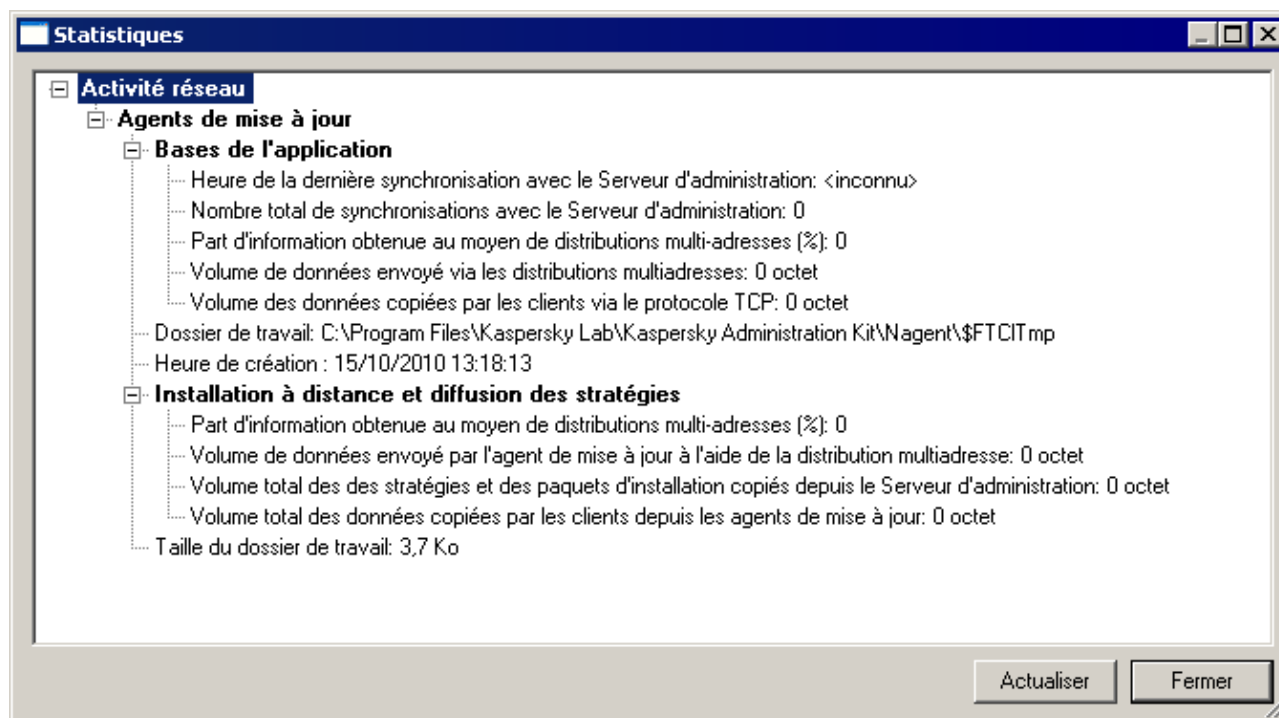


Illustration 227. Fenêtre des statistiques de l'agent de mise à jour

TACHE DE RECUPERATION DES MISES A JOUR PAR LES AGENTS DE MISE A JOUR

Kaspersky Administration Kit offre la possibilité d'obtention des mises à jour par les agents de mise à jour.

► Pour recevoir les mises à jour pour les agents de mise à jour, procédez comme suit :

1. Dans les propriétés du groupe sélectionnez l'onglet **Agents de mise à jour** (cf. ill. ci-après) et cliquez sur le bouton **Propriétés**.

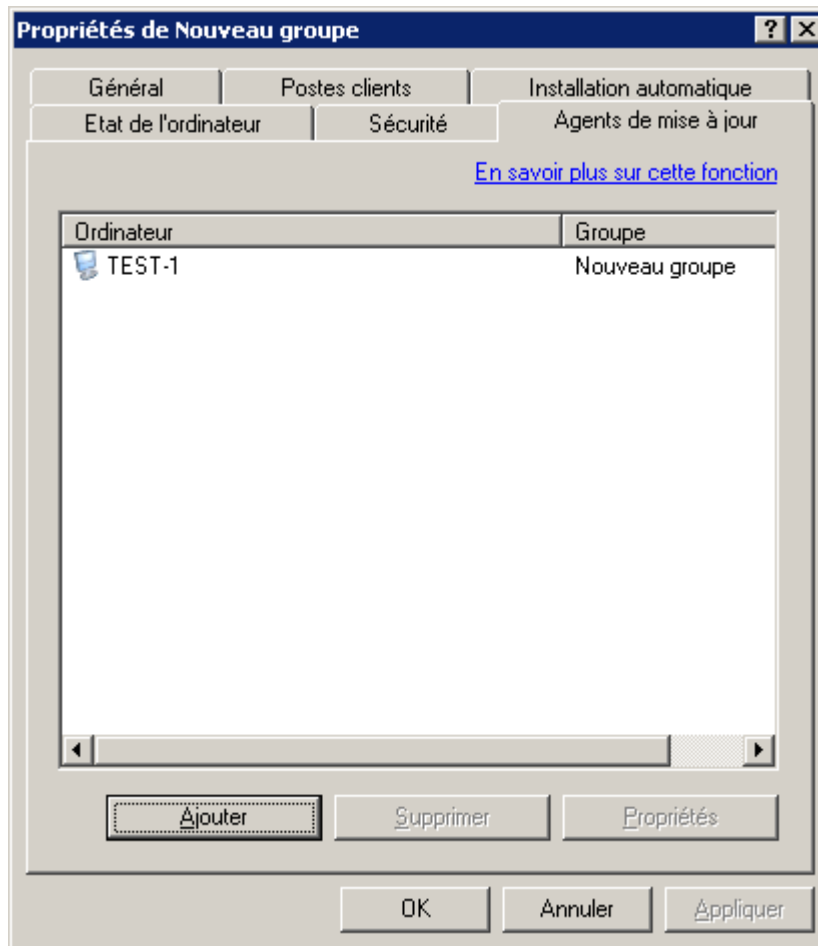


Illustration 228. Sélection de l'agent de mise à jour

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Source de mises à jour** (cf. ill. ci-après).

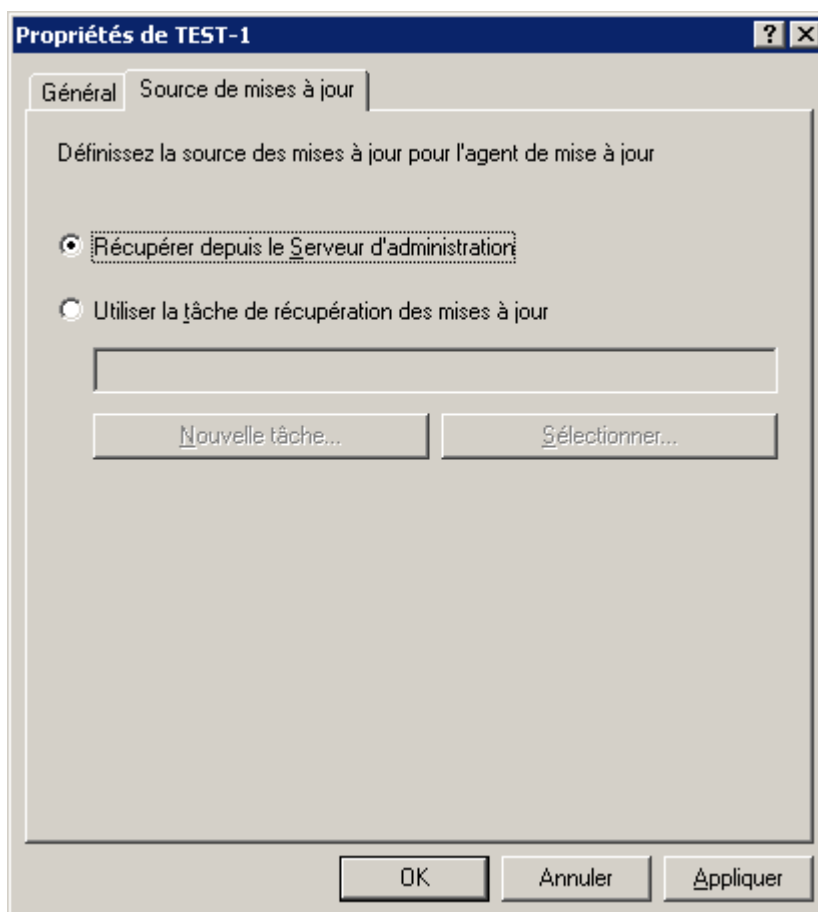


Illustration 229. Sélection de la source des mises à jour pour l'agent de mise à jour

3. Sur cet onglet cochez la case en regard de **Utiliser la tâche de récupération des mises à jour**. Sélectionnez la tâche dans la liste des tâches déjà formées pour la sélection d'ordinateurs à l'aide du bouton **Sélectionner**, ou créez une nouvelle tâche à l'aide du bouton **Nouvelle tâche** (cf. ill. ci-dessus).

ADMINISTRATION DES LICENCES

L'application Kaspersky Administration Kit permet d'installer de façon centralisée les licences sur les postes clients des groupes d'administration, 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.

DANS CETTE SECTION

Affichage des informations sur les licences installées.....	270
Installation d'une licence	273
Lancement de l'Assistant d'installation de la licence	274
Création et affichage de rapports sur les licences.....	275
Réception de la licence par le code d'activation.....	275
Extension automatique de la licence	276

AFFICHAGE DES INFORMATIONS SUR LES LICENCES INSTALLEES


➡ *Pour consulter les informations relatives à toutes les licences installées, procédez comme suit :*


Connectez-vous au Serveur d'administration nécessaire (cf. section "Administration des Serveurs d'administration" à la page [22](#)) et sélectionnez le dossier **Stockages** → **Licences** dans l'arborescence de la console. Le panneau de résultats montrera la liste des licences installées sur les postes clients.


Les informations suivantes sont proposées pour chacune des licences :

- **Numéro** : numéro de la licence.
- **Type** : type de la licence installée, par exemple, commerciale, démonstration.
- **Restriction** : restrictions imposées par la licence.
- **Durée de validité** : période de validité de la licence.
- **Date d'expiration** : date d'expiration de la licence.
- **Application** : nom de l'application pour laquelle la licence est valable.
- **Active** : nombre d'ordinateurs pour lesquels la licence est active.
- **Complémentaire** : nombre d'ordinateurs pour lesquels la licence est complémentaire.

En regard de chaque licence une icône, correspondant au type de son utilisation, s'affiche :

 - l'information sur la licence utilisée est reçue depuis le poste client connecté au Serveur d'administration. Cette licence n'est pas sauvegardée dans le référentiel du Serveur d'administration.

 – la licence se trouve dans le référentiel du Serveur d'administration. L'installation automatique de cette licence n'est pas active.

 – la licence se trouve dans le référentiel du Serveur d'administration. L'installation automatique de cette licence est active (cf. section "Extension automatique de la licence" à la page [276](#)).

➡ *Pour consulter les informations relatives à une licence en particulier,*

sélectionnez la licence souhaitée dans le panneau des résultats et utilisez la commande **Propriétés** du menu contextuel.

Ceci permet d'ouvrir la boîte de dialogue **Propriétés : <Numéro de licence>** contenant les onglets **Général** et **Objets**.

Sur l'onglet **Général**(cf. ill. ci-après), vous retrouverez les informations suivantes :

- numéro ;
- type ;
- nom de l'application pour laquelle la licence est valable ;
- durée de validité ;
- limites définies dans la licence ;
- le nombre d'ordinateurs pour lesquels la licence est active ;
- le nombre d'ordinateurs pour lesquels la licence est complémentaire ;

- les informations relatives à la licence.

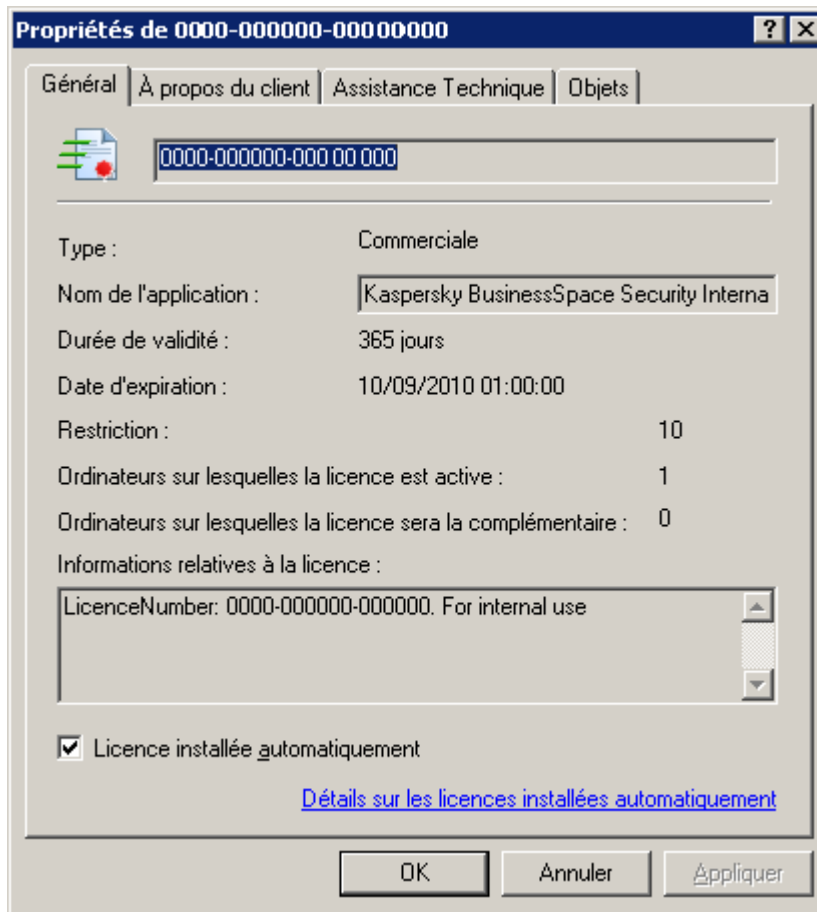


Illustration 230. Propriétés de la licence. Onglet **Général**

Sur l'onglet **Objets** (cf. ill. ci-après) contient la liste des postes clients sur lesquels cette licence est installée. Cet onglet propose les informations suivantes :

- le nom du poste client ;
- le groupe d'administration ;
- si la licence est utilisée (ou pas) en tant que licence active ;
- date de fin de validité de la licence ;

- la date d'activation de la licence sur les postes clients.

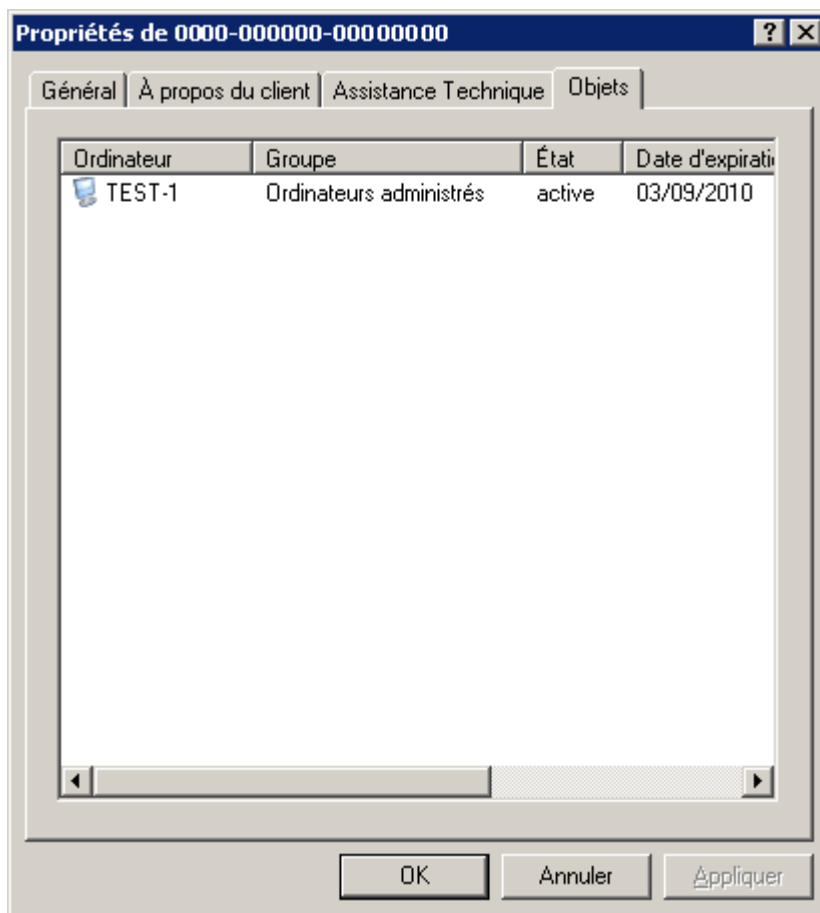


Illustration 231. Propriétés de la licence. Onglet **Objets**

Sur l'onglet **A propos du client** l'information sur le propriétaire, prise du fichier de licence, est accessible.

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.

INSTALLATION D'UNE LICENCE

La licence s'installe à l'aide de la tâche d'installation de la licence. La tâche d'installation de la licence peut être créée en tant que tâche de groupe (cf. section "Création d'une tâche de groupe" à la page [101](#)), une tâche pour les sélections d'ordinateurs (cf. section "Création d'une tâche pour la sélection d'ordinateurs" à la page [114](#)) ou locale (cf. section "Création d'une tâche locale" à la page [115](#)). Lors de la création de cette tâche :

- sélectionnez l'application à laquelle vous affectez la licence en guise d'application pour laquelle la tâche est créée ;
- sélectionnez **Installation du fichier de licence** comme type de tâche.

LANCEMENT DE L'ASSISTANT D'INSTALLATION DE LA LICENCE

➔ Pour démarrer l'Assistant d'installation de la licence,

sélectionnez le dossier **Licences** dans l'arborescence de la console et utilisez la commande **Ajouter une licence** du menu contextuel. Ceci permet de démarrer un assistant de création de tâche pour des sélections d'ordinateurs qui saute l'étape de sélection du type de tâche (indiqué par défaut).

Les tâches créées à l'aide de l'Assistant d'installation de licence sont des tâches pour des sélections d'ordinateurs situées dans le dossier **Tâches pour les sélections d'ordinateurs** de l'arborescence de console.

Quand vous modifiez les paramètres de la tâche d'installation de la licence sur l'onglet **Paramètres** (cf. ill. ci-après), vous pouvez remplacer le fichier de licence à installer, et cocher la case **Ajouter en tant que licence pour une licence complémentaire** pour en faire la licence complémentaire de l'application. Si la case n'est pas cochée, la licence servira de licence active. Des informations supplémentaires sur la licence figurent dans la zone **Informations relatives à la licence**.

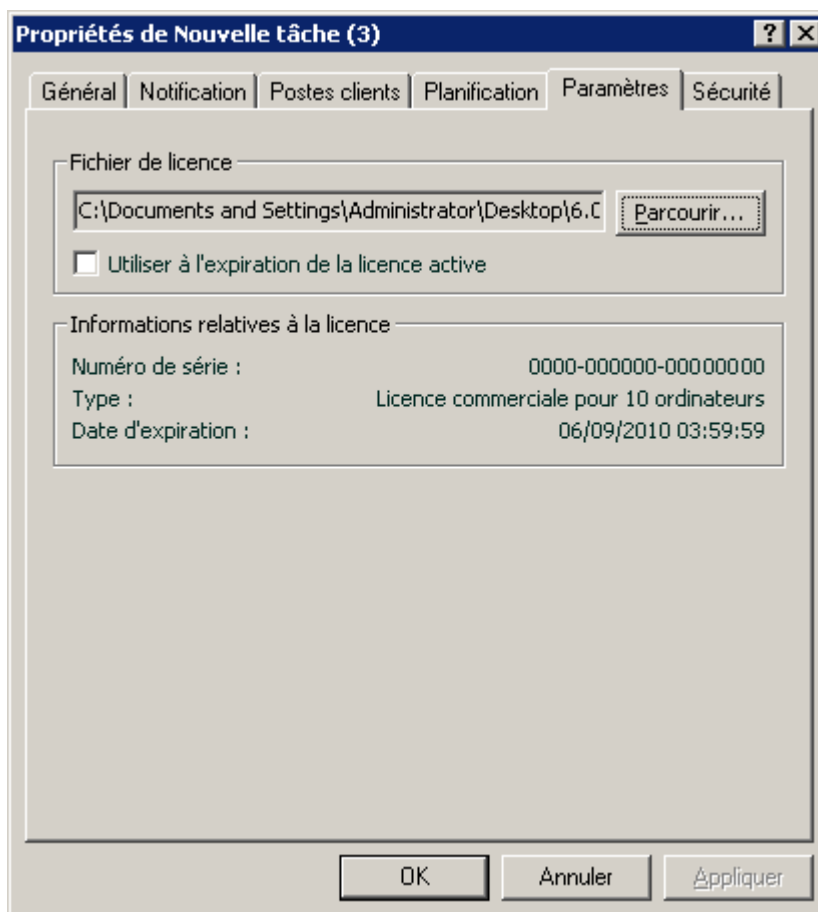


Illustration 232. Configuration d'une tâche d'ajout de licence

CREATION ET AFFICHAGE DE RAPPORTS SUR LES LICENCES

➔ Pour créer un rapport sur l'état des licences installées sur les postes clients,

utilisez le modèle intégré **Rapport de licences** ou créez un nouveau modèle (cf. section "Créer le nouveau rapport" à la page [179](#)) de ce type.

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

RECEPTION DE LA LICENCE PAR LE CODE D'ACTIVATION

➔ Afin de recevoir la licence par le code d'activation, procédez comme suit :

1. Dans le dossier **Stockages** ouvrez le menu contextuel du sous-dossier **Licences** et sélectionnez **Générer** → **Ajouter une licence**. Finalement la fenêtre de l'Assistant d'ajout d'une licence s'ouvre. Cliquez sur **Suivant**.
2. Dans la fenêtre suivante sélectionnez **Saisir le code d'activation**. Cliquez sur **Suivant**.

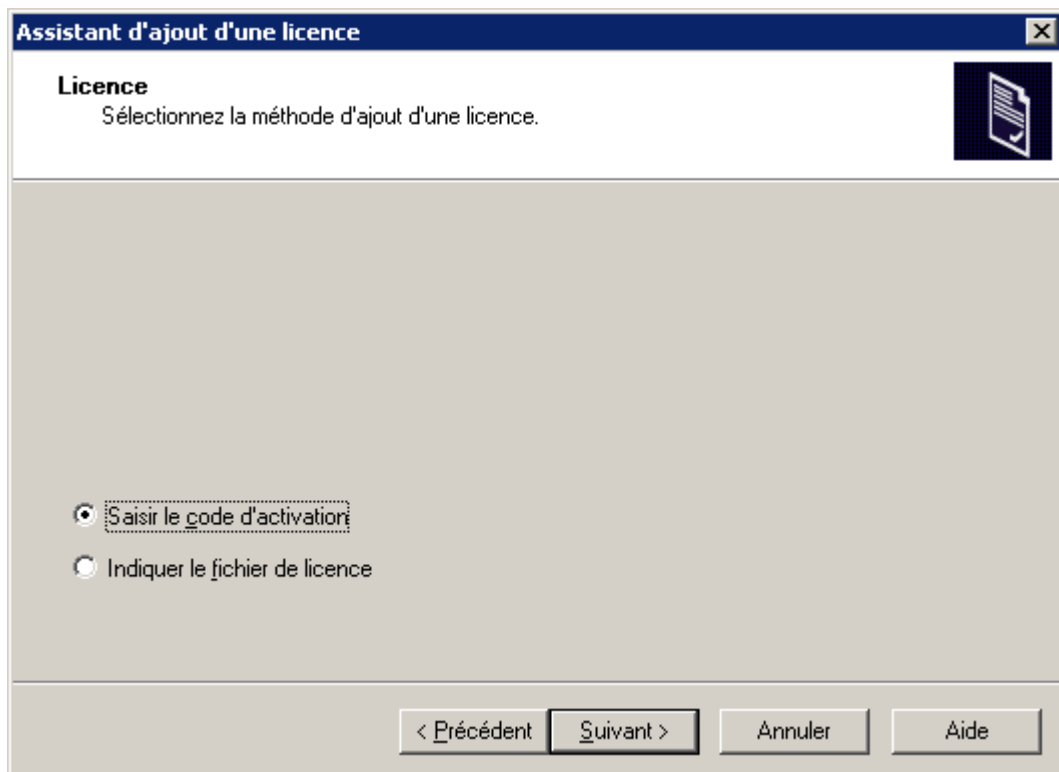


Illustration 233. Réception de la licence par le code d'activation

3. Dans la fenêtre ouverte saisissez le code d'activation reçu lors de l'achat de la version commerciale de l'application. Si vous voulez diffuser automatiquement la licence sur les ordinateurs dans les groupes d'administration, cochez la case dans le champ homonyme. Cliquez sur **Suivant**.

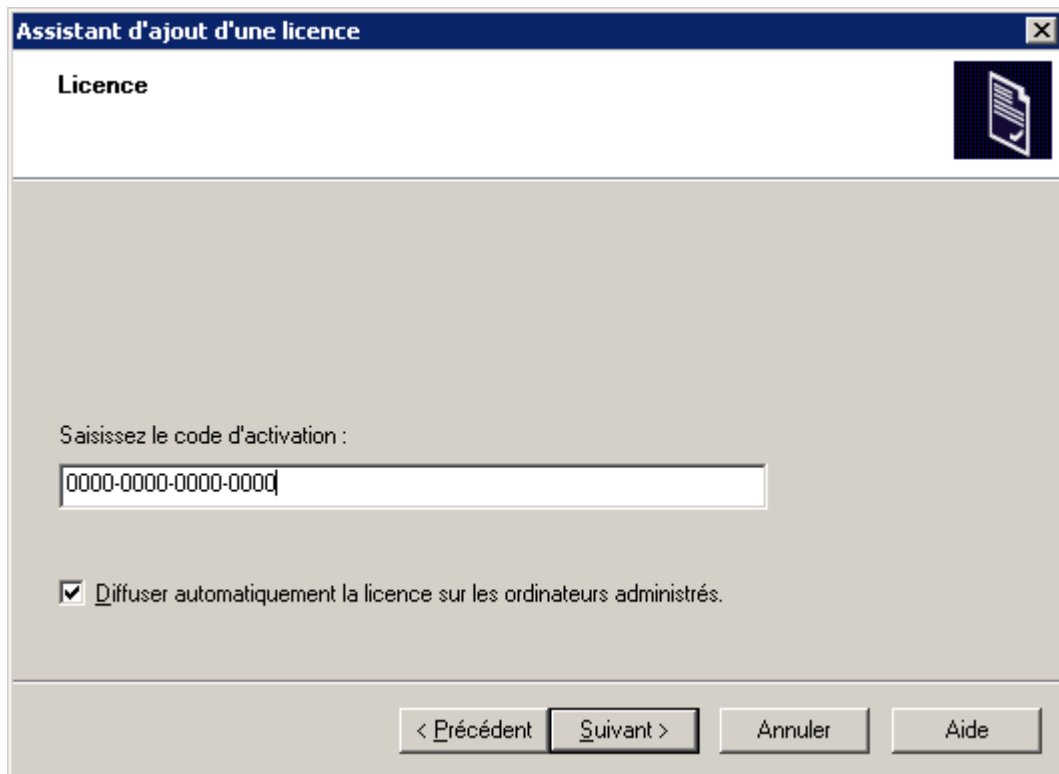


Illustration 234. Insertion du code d'activation

4. Cliquez sur le bouton **Terminer** pour terminer l'opération.

EXTENSION AUTOMATIQUE DE LA LICENCE

Kaspersky Administration Kit offre la possibilité d'extension automatique des licences sur les postes clients, placées dans le stockage des licences sur le Serveur d'administration.

➤ Afin de diffuser automatiquement une licence sur les postes clients, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le dossier **Stockages** → **Licences**.
2. Sélectionnez une licence que vous voulez diffuser.
3. Ouvrez le menu contextuel de la licence et sélectionnez l'élément **Propriétés**.
4. Dans la fenêtre des propriétés ouverte cochez la case **Licence installée automatiquement**.

La licence est diffusée sur ceux postes clients où l'application est installée et il n'y a pas du code d'activation.

L'installation de la licence s'effectuera aux moyens de l'Agent d'administration. Avec cela les tâches auxiliaires d'installation de la licence pour l'application ne se forment pas. La licence s'installe en qualité de la licence active.

Lors de l'installation d'une licence une restriction de licence est tenue en compte. Dans le cas de sa perturbation la licence ne s'installera pas.

STOCKAGES

Le dossier **Stockages** permet de manipuler les objets utilisés pour la surveillance de l'état des postes client et les entretenir. Les informations sont fournies dans les dossiers qui contiennent les listes suivantes :

- les paquets d'installation qui peuvent être utilisés pour l'installation à distance des applications sur les postes clients ;
- les mises à jour récupérées par le Serveur d'administration (cf. section "Mise à jour" à la page [246](#)), qui peuvent être déployées sur les postes client ;
- les licences installées sur les postes clients (cf. section "Administration des licences" à la page [270](#)) ;
- les objets placés par les applications antivirus dans les dossiers de quarantaine des postes client ;
- les copies de sauvegarde des objets placées dans le dossier de sauvegarde ;
- les fichiers pour lesquels les applications antivirus ont décidé d'une analyse ultérieure ;
- les applications installées sur les ordinateurs du réseau de l'entreprise sur lesquels l'Agent d'administration est installé.

DANS CETTE SECTION

Paquets d'installation	277
Quarantaine	277
Dossier de sauvegarde	280
Fichiers avec un traitement différé	282
Registre des applications	283

PAQUETS D'INSTALLATION

Une des possibilités les plus importantes de Kaspersky Administration Kit est l'installation à distance des applications de Kaspersky Lab, aussi que les applications d'autres fabricants. Afin d'installer une application par les moyens de Kaspersky Administration Kit, il est nécessaire de créer un paquet d'installation pour cette application. Le paquet d'installation représente l'ensemble des fichiers, nécessaires pour l'installation, aussi que les paramètres tangentiels au processus de l'installation, aussi que la configuration initiale de l'application à installé (particulièrement, du fichier avec les paramètres d'Anti-virus).

La liste de tous les paquets d'installation est affichée dans le dossier **Stockages** → **Paquets d'installation** de l'arborescence de la console.

L'information détaillée à propos des propriétés des paquets d'installation se trouve dans le Manuel d'implantation.

QUARANTAINE

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, via 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.

CONSULTATION DES PROPRIETES DE L'OBJET PLACE EN QUARANTAINE

➡ *Afin de consulter les propriétés de l'objet placé en quarantaine,*

sélectionnez le dossier **Stockages** dans l'arborescence de la console, puis **Quarantaine**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option Propriétés du menu contextuel.

Dans la fenêtre qui s'ouvre (cf. ill. ci-après), vous verrez les informations suivantes relatives à l'objet :

- nom sous lequel l'objet avait été délivré pour son traitement par l'application antivirus ;
- description de l'objet ;
- action réalisée sur l'objet par l'application antivirus ;
- nom du poste où l'objet est conservé ;
- état attribué à l'objet par l'application antivirus ;
- nom du virus présent ou soupçonné dans l'objet ;
- date de mise en quarantaine ou dans le dossier de sauvegarde ;
- taille de l'objet en octets ;
- chemin d'accès sur le poste client au dossier où se trouvait l'objet à l'origine ;

- nom de l'utilisateur qui a mis l'objet en quarantaine ou dans le dossier de sauvegarde.

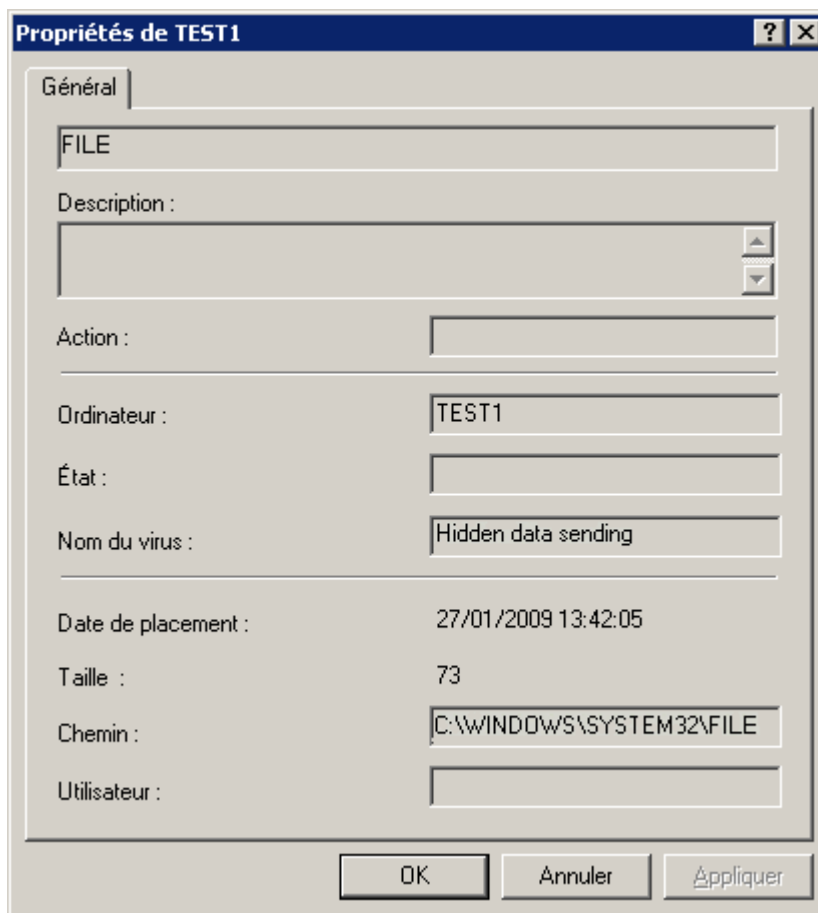


Illustration 235. Affichage des propriétés d'un objet de la quarantaine ou du dossier de sauvegarde

SUPPRESSION D'UN OBJET DE LA QUARANTAINE

- Pour supprimer un objet de la quarantaine,

sélectionnez le dossier **Stockages** → **Quarantaine** dans l'arborescence de la console. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Supprimer** du menu contextuel.

L'application antivirus qui avait stocké cet objet sur le poste client supprimera l'objet de la quarantaine ou du dossier de sauvegarde.

ANALYSE DU DOSSIER DE QUARANTAINE SUR LE POSTE CLIENT

- Pour analyser le dossier de quarantaine sur le poste client, procédez comme suit :

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Quarantaine**, dans le panneau des résultats sélectionnez l'objet que vous souhaitez analyser et utilisez la commande **Analyser les objets en quarantaine** dans le menu contextuel ou son équivalent dans le menu **Action**.

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

RESTAURER UN OBJET DE LA QUARANTAINE

► *Pour restaurer un objet de la quarantaine,*

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Quarantaine**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Restaurer** du menu contextuel.

L'application antivirus qui avait stocké cet objet sur le poste client restaurera l'objet de la quarantaine ou du dossier de sauvegarde dans son dossier d'origine.

SAUVEGARDE D'UN OBJET DE LA QUARANTAINE SUR LE DISQUE

Kaspersky Administration Kit permet à l'administrateur de sauvegarder sur le Serveur d'administration les fichiers, qui sont placés en quarantaine par l'application antivirus sur le poste client. Le fichier est téléchargé sur l'ordinateur, sur lequel Kaspersky Anti-Virus est installé, et puis, sauvegardé là, où l'administrateur a indiqué.

► *Afin de sauvegarder un objet de la quarantaine sur le disque de l'administrateur,*

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Quarantaine**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Enregistrer sur le disque** du menu contextuel.

L'application antivirus qui avait stocké cet objet en quarantaine sur le poste client sauvegardera l'objet dans le dossier indiqué par l'administrateur.

DOSSIER DE SAUVEGARDE

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, via la Console d'administration, d'afficher les propriétés des objets en quarantaine ou dans la sauvegarde sur les ordinateurs locaux, de lancer une analyse antivirus de la sauvegarde ou de la quarantaine ou d'en supprimer les objets.

AFFICHAGE DES PROPRIETES DE L'OBJET PLACE DANS LE DOSSIER DE SAUVEGARDE

► *Pour afficher les propriétés d'un objet stocké,*

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Dossier de sauvegarde**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Propriétés** du menu contextuel.

Dans la fenêtre qui s'ouvre (cf. ill. ci-après), vous verrez les informations suivantes relatives à l'objet :

- nom sous lequel l'objet avait été délivré pour son traitement par l'application antivirus ;
- description de l'objet ;
- action réalisée sur l'objet par l'application antivirus ;
- nom du poste où l'objet est conservé ;
- état attribué à l'objet par l'application antivirus ;
- nom du virus présent ou soupçonné dans l'objet ;
- date de mise en quarantaine ou dans le dossier de sauvegarde ;

- taille de l'objet en octets ;
- chemin d'accès sur le poste client au dossier où se trouvait l'objet à l'origine ;
- nom de l'utilisateur qui a mis l'objet en quarantaine ou dans le dossier de sauvegarde.

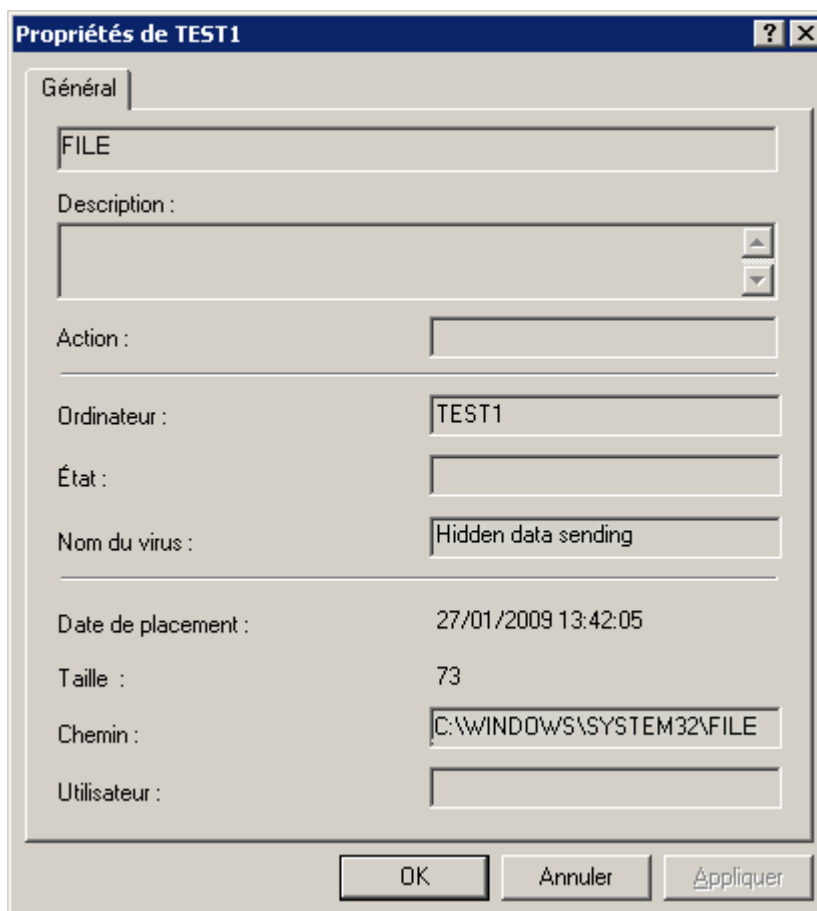


Illustration 236. Affichage des propriétés d'un objet de la quarantaine ou du dossier de sauvegarde

SUPPRESSION D'UN OBJET DEPUIS LE DOSSIER DE SAUVEGARDE

- *Pour supprimer un objet stocké,*

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Dossier de sauvegarde**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Supprimer** du menu contextuel.

L'application antivirus qui avait stocké cet objet sur le poste client supprimera l'objet de la quarantaine ou du dossier de sauvegarde.

RESTAURATION D'UN OBJET DEPUIS LE DOSSIER DE SAUVEGARDE

- *Pour restaurer un objet stocké,*

Dans l'arborescence de la console, sélectionnez le dossier **Stockages** → **Dossier de sauvegarde**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Restaurer** du menu contextuel.

L'application antivirus qui avait stocké cet objet sur le poste client restaurera l'objet de la quarantaine ou du dossier de sauvegarde dans son dossier d'origine.

SAUVEGARDE D'UN OBJET DU DOSSIER DE SAUVEGARDE SUR LE DISQUE

Kaspersky Administration Kit permet à l'administrateur de sauvegarder sur le Serveur d'administration les fichiers, qui sont placés dans le dossier de sauvegarde par l'application antivirus sur le poste client. Le fichier est téléchargé sur l'ordinateur, sur lequel Kaspersky Anti-Virus est installé, et puis, sauvegardé là, où l'administrateur a indiqué.

➤ *Afin de sauvegarder un objet du dossier de sauvegarde sur le disque de l'administrateur,*

sélectionnez le dossier **Stockages** → **Quarantaine** dans l'arborescence de la console. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Enregistrer sur le disque** du menu contextuel.

L'application antivirus qui avait stocké cet objet dans le dossier de sauvegarde sur le poste client sauvegardera l'objet dans le dossier indiqué par l'administrateur.

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.

REPARATION DE L'OBJET DU DOSSIER FICHIERS AVEC UN TRAITEMENT DIFFERE

➤ *Afin de réparer un objet du dossier **Fichiers avec un traitement différé***

sélectionnez le dossier **Stockages** → **Fichiers avec un traitement différé** dans l'arborescence de la console, puis dans le panneau des résultats sélectionnez l'objet que vous voulez réparer, et utilisez la commande **Réparer** du menu contextuel.

Cela entraîne la tentative de réparer l'objet :

- si l'objet est réparé, alors son écriture est supprimée du dossier **Fichiers avec un traitement différé** ;
- si la réparation du fichier est impossible, alors l'objet et son écriture sont supprimés.

LA SAUVEGARDE DE L'OBJET DU FICHIER FICHIERS AVEC UN TRAITEMENT DIFFERE SUR LE DISQUE

Kaspersky Administration Kit permet à l'administrateur de sauvegarder sur le Serveur d'administration les fichiers, placés par l'application antivirus dans le dossier **Fichiers avec un traitement différé** sur le poste client. Le fichier est téléchargé sur l'ordinateur, sur lequel Kaspersky Anti-Virus est installé, et puis, sauvegardé là, où l'administrateur a indiqué.

➤ *Afin de sauvegarder l'objet du dossier **Fichiers avec un traitement différé** sur le disque de l'administrateur,*

sélectionnez dans l'arborescence de la console le dossier **Stockages** → **Fichiers avec un traitement différé**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Enregistrer sur le disque** du menu contextuel.

Finalement, l'application antivirus qui avait placé cet objet dans le dossier **Fichiers avec un traitement différé** sur le poste client sauvegardera l'objet dans le dossier indiqué par l'administrateur.

SUPPRESSION D'UN OBJET DU DOSSIER FICHIERS AVEC UN TRAITEMENT DIFFERE

➤ *Afin de supprimer un objet du dossier **Fichiers avec un traitement différé***

sélectionnez dans l'arborescence de la console le dossier **Stockages** → **Fichiers avec un traitement différé**. Sélectionnez l'objet souhaité dans le panneau des résultats et cliquez sur l'option **Supprimer** du menu contextuel.

L'application antivirus qui avait stocké cet objet sur le poste client supprimera l'objet de la liste du dossier **Fichiers avec un traitement différé**.

REGISTRE DES APPLICATIONS

Les informations relatives aux applications installées dans le réseau sont conservées dans le registre des applications. Les informations relatives aux applications reposent sur les données reçues des postes clients.

Les informations relatives aux applications sur les ordinateurs connectés aux Serveurs d'administration secondaires sont également rassemblées et enregistrées dans le registre des applications du Serveur d'administration principal. Vous pouvez consulter ces informations à l'aide du rapport, en activant la collection des données des Serveurs d'administration secondaires (cf. section "Rapports d'hierarchie des Serveurs d'administration" à la page [204](#)).

➤ *Pour consulter le registre des applications, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le dossier **Stockages**.
2. Ouvrez le dossier **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**.

Les informations relatives aux applications apparaîtront sur le panneau des résultats dans un tableau (cf. ill. ci-après). Le tableau contient les champs suivants :

- **Nom** : nom de l'application ;
- **Versio**n : numéro de la version de l'application ;
- **Editeur** : nom de la société qui produit l'application ;
- **Nombre d'ordinateurs** : 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 d'assistance technique** peuvent rester vides.

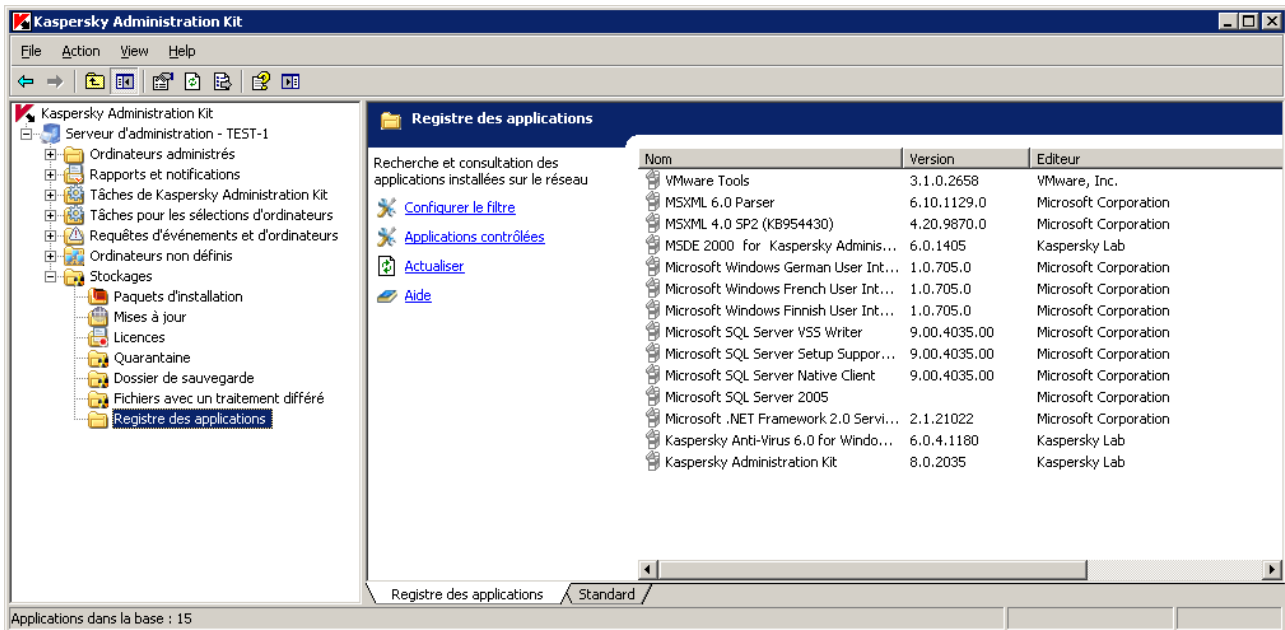


Illustration 237. Affichage du registre des applications

➤ Pour consulter les informations relatives à une application dans une nouvelle fenêtre, procédez comme suit :

1. Sélectionnez l'application dans la liste du panneau des résultats.
2. Ouvrez le menu contextuel et utilisez la commande **Propriétés**.

L'onglet **Général** (cf. ill. ci-après) contient les données relatives à l'application : nom, numéro de version, éditeur, commentaires de l'éditeur, adresse du site Web et numéro de téléphone du service d'assistance technique.

Cochez la case **Annoncer l'événement d'installation** pour que les informations relatives à l'installation de cette application sur les postes clients soient transmises au Serveur d'administration et enregistrées conformément aux paramètres définis pour l'événement **L'application observée a été installée depuis le registre des applications** dans la configuration du Serveur d'administration ou dans la stratégie de l'application Kaspersky Administration Kit.

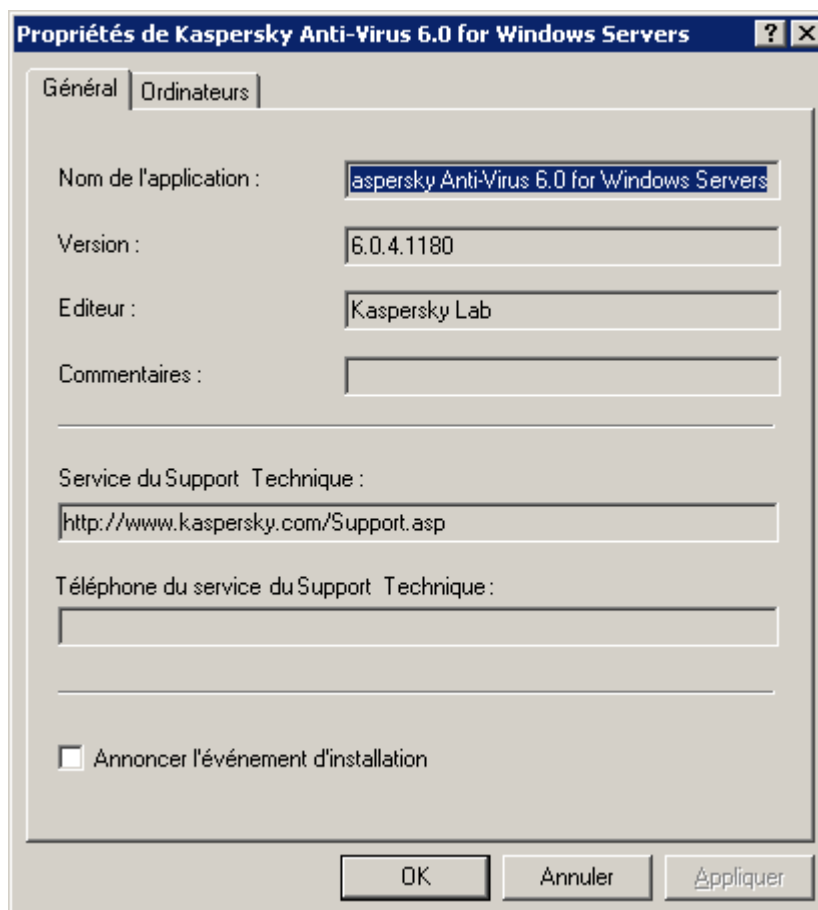


Illustration 238. Fenêtre des propriétés de l'application. Onglet **Général**

L'onglet **Ordinateurs** (cf. ill. ci-après) contient la liste des ordinateurs sur lesquels l'application est installée.

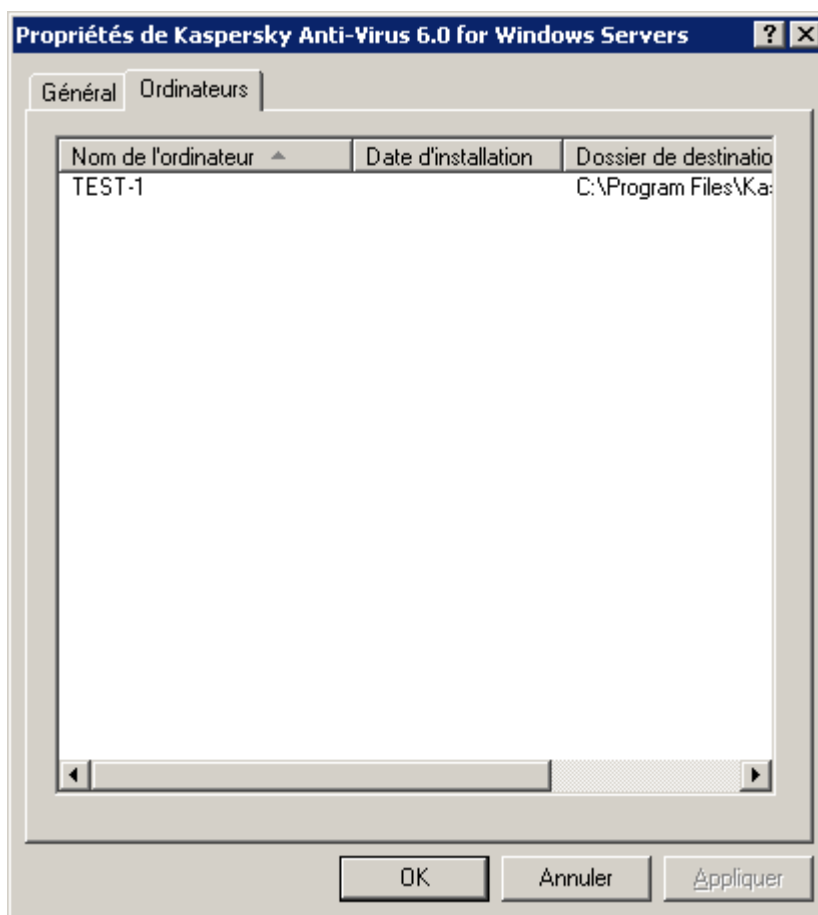


Illustration 239. Fenêtre des propriétés de l'application. Onglet **Ordinateurs**

➔ Pour consulter la liste des applications répondant à des critères définis, vous pouvez utiliser un filtre. Pour ce faire, exécutez les opérations suivantes :

1. Ouvrez le dossier **Registre des applications**.
2. Ouvrez le menu contextuel et utilisez la commande **Filtre**.
3. Dans la fenêtre ouverte (cf. ill. ci-après) sélectionnez l'option **Définir le filtre** et attribuez les valeurs aux paramètres suivants :
 - Saisissez le nom de l'application manuellement ou sélectionnez-la de la liste déroulante. La liste reprend toutes les applications installées sur les postes clients. Les Agents d'administration installés sur les ordinateurs proposent les informations sur la base des données du registre système.
 - Indiquez la version de l'application.

- Saisissez le nom de l'éditeur manuellement ou sélectionnez-le de la liste déroulante. Les informations de la liste sont proposées à tous les agents d'administration installés sur les postes clients.

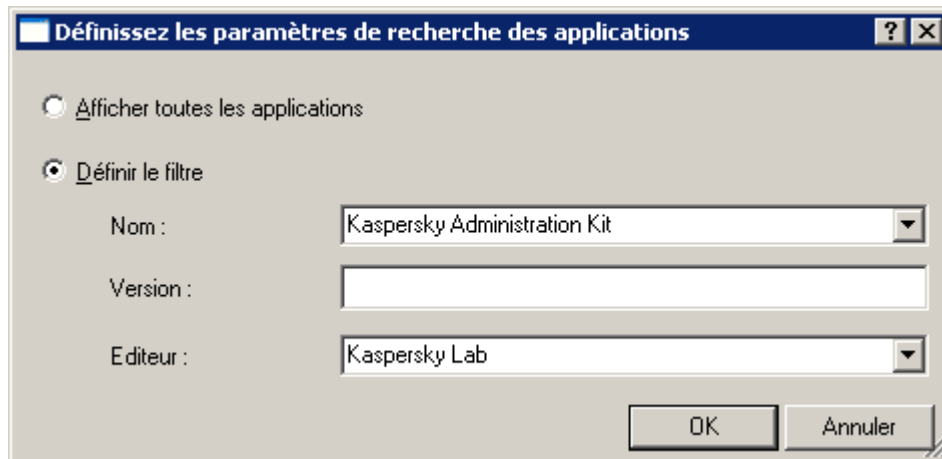


Illustration 240. Fenêtre des paramètres de recherche des applications

4. Pour que le dossier **Registre des applications** reprenne uniquement les informations sur les applications installées, cochez la case **Afficher uniquement les applications installées**.
5. Cliquez sur le bouton **OK**.

La liste des applications validant les paramètres définis apparaît dans le panneau des résultats du dossier **Registre des applications**.

Si le filtrage n'est pas requis, choisissez l'option **Afficher toutes les applications**. Le filtre sera supprimé.

POSSIBILITES COMPLEMENTAIRES

Cette rubrique aborde les possibilités complémentaires de Kaspersky Administration Kit prévues pour étendre les fonctions d'administration centralisée des applications du réseau informatique.

DANS CETTE SECTION

Suivi de l'état de la protection antivirus à l'aide d'informations du registre système.....	288
Utilisateurs nomades.....	289
Recherche.....	298
Copie de sauvegarde des données.....	311
Suivi des épidémies de virus.....	318
Automatisation du fonctionnement de Kaspersky Administration Kit (klakaut).....	323
Outils externes.....	323
Configuration de l'interface.....	323

SUIVI DE L'ETAT DE LA PROTECTION ANTIVIRUS A L'AIDE D'INFORMATIONS DU REGISTRE SYSTEME

Pour afficher l'état de la protection antivirus sur un poste client à l'aide d'informations inscrites par l'Agent d'administration dans le registre système, procédez comme suit :

1. Ouvrez le registre système du poste client (par exemple, à l'aide de la commande **regedit** dans le menu **Démarrer** → **Exécuter**).
2. Rendez-vous dans la section :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVS  
tate
```

Une valeur spécifique, décrite dans le tableau ci-dessous, correspond à chaque état de la protection antivirus.

Tableau 2. Liste des clés du registre et valeurs possibles

CLE (TYPE DE DONNEES)	VALEUR	DESCRIPTION
Protection_AdmServer (REG_SZ)		Nom du Serveur d'administration qui administre cet ordinateur.
Protection_AvInstalled (REG_DWORD)	Différent de 0	L'application antivirus installée sur l'ordinateur.
Protection_AvRunning (REG_DWORD)	Différent de 0	Protection permanente du poste active.
Protection_HasRtp (REG_DWORD)	Différent de 0	Composant de protection en temps réel installé.
	Etat de la protection en temps réel :	

CLE (TYPE DE DONNEES)	VALEUR	DESCRIPTION
	0	Inconnu.
	2	Inactive.
	3	Suspendue.
	4	En cours de démarrage.
	5	Active.
	6	Active, niveau élevé (protection maximale).
	7	Active, paramètres recommandés.
	8	Active, paramètres personnalisés.
	9	Erreur.
Protection_LastFscan (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière analyse achevée.
Protection_BasesDate (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière analyse achevée.
Protection_LastConnected (REG_SZ)	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière connexion au Serveur d'administration.

UTILISATEURS NOMADES

L'application Kaspersky Administration Kit prévoit la possibilité de transférer l'agent administratif sur d'autres Serveurs d'administration en cas de modification des caractéristiques du réseau, par exemple :

- **Présence dans le sous-réseau** : modification de l'adresse et du masque du sous-réseau.
- **Présence dans le domaine DNS** : modification du suffixe DNS du sous-réseau.
- **Adresse de la passerelle principale** : modification de la passerelle principale du réseau.
- **Adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP dans le réseau.
- **Adresse du serveur DNS** : modification de l'adresse IP du serveur DNS dans le réseau.
- **Adresse du serveur WINS** : modification de l'adresse IP du serveur WINS dans le réseau.
- **Accès au domaine Windows** : modification de l'état du domaine Windows auquel le poste client est connecté.

La fonctionnalité est soutenue pour les S.E. suivants : Microsoft Windows XP/Vista ; Microsoft Windows Server 2003/2008.

Paramètres de connexion d'origine de l'Agent d'administration au Serveur lors de l'installation de l'Agent d'administration. Par la suite, quand des règles de permutation sont rédigées, l'Agent d'administration réagit aux modifications des caractéristiques du réseau :



- si elles correspondent à une des règles créées, l'Agent d'administration se connecte au Serveur indiqué dans la règle et, si la règle le prévoit, les applications installées sur les postes clients suivent les stratégies établies pour les utilisateurs nomades ;
- si aucune règle n'est exécutée, l'Agent d'administration revient aux paramètres de connexion d'origine définis lors de l'installation, et les applications installées sur les postes clients reviennent aux stratégies actives ;
- si le Serveur d'administration est inaccessible, l'Agent d'administration utilisera les stratégies nomades.

Les paramètres de connexion de l'Agent d'administration au Serveur sont préservés dans le profil. De plus, les règles de transfert des postes client aux stratégies pour les utilisateurs nomades sont aussi définies dans le profil, l'utilisation du profil est limitée au téléchargement des mises à jour. Par défaut, l'Agent d'administration passe à la stratégie pour les postes nomades si le Serveur d'administration est inaccessible pendant plus de 45 minutes.

Les profils de passage de l'Agent d'administration sont configurés dans la stratégie ou les paramètres de l'Agent d'administration.

La liste des profils créés pour l'agent figure dans le groupe **Profils de connexion au Serveur d'administration** de l'onglet **Connexion**. Il est possible d'ajouter et de supprimer des profils ainsi que de modifier les valeurs des paramètres du profil à l'aide des boutons **Ajouter**, **Supprimer** et **Propriétés**.

La liste des règles formées pour le profil se trouve dans le groupe **Permutation des profils** de l'onglet **Connexion**. Il est possible d'ajouter et de supprimer des règles ainsi que de modifier les valeurs des paramètres du règles à l'aide des boutons **Ajouter**, **Supprimer** et **Propriétés**.

La vérification de la correspondance entre les règles et les caractéristiques du réseau s'opère dans l'ordre de présentation dans la liste. Si les caractéristiques du réseau correspondent à plusieurs règles, c'est la première d'entre elles qui sera appliquée. Pour modifier l'ordre de consultation des règles de la liste, utilisez les boutons  et .

CREATION DU PROFIL POUR LES UTILISATEURS NOMADES

➤ Afin d'ajouter le nouveau profil de connexion au Serveur d'administration, procédez comme suit :

1. Sélectionnez la stratégie de l'Agent d'administration dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Ouvrez la fenêtre **Propriétés <Nom de la stratégie>** sous l'onglet **Réseau**.

4. A l'aide du lien **Profils des connexions** passez à la fenêtre de configuration des paramètres de permutation de l'Agent d'administration (cf. ill. ci-après).

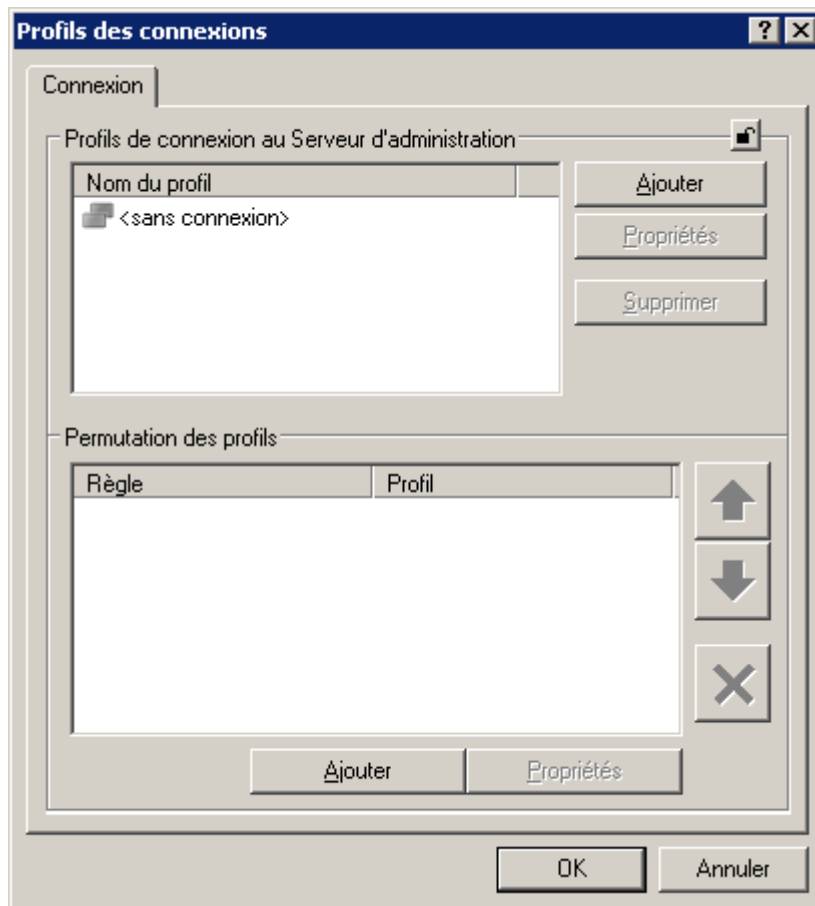


Illustration 241. Onglet **Connexion**

5. Cliquez sur le bouton **Ajouter** situé dans le groupe **Profils de connexion au Serveur d'administration** (cf. ill. ci-dessus). Ceci permet d'ouvrir la boîte de dialogue de configuration du profil (cf. ill. ci-après).

Illustration 242. Fenêtre **Nouveau profil**

6. Indiquez les valeurs des paramètres du profil de l'Agent d'administration suivants (cf. ill. ci-dessus) :
- Nom du profil.
 - Adresse de l'ordinateur sur lequel est installé le Serveur d'administration.
 - Numéro du port utilisé pour la connexion.
 - Numéro de port utilisé pour la connexion par protocole SSL. Si vous souhaitez vous connecter à travers un port sécurisé (utilisant le protocole SSL), cochez la case **Utiliser la connexion SSL**.
 - Configuration du serveur proxy. Pour ce faire, utilisez le lien **Configurer la connexion via le serveur proxy**.

Si la case **Activer les stratégies mobiles** est cochée, les applications installées sur le poste client utiliseront les stratégies pour les utilisateurs nomades, même si le Serveur d'administration repris dans le profil est accessible. Si aucune stratégie n'est définie pour les utilisateurs nomades, c'est la stratégie active normale qui sera utilisée. Si la case est désélectionnée, les applications utiliseront les stratégies actives.

Si la case **Utiliser uniquement pour récupérer les mises à jour** est cochée, le profil sera utilisé uniquement lors du téléchargement des mises à jour par les applications installées sur le poste client. Pour les autres opérations, la connexion au Serveur d'administration sera réalisée selon les paramètres de connexion d'origine définis lors de l'installation de l'Agent d'administration.

7. Cliquez sur le bouton **OK** pour terminer l'opération.

Liste contient uniquement par défaut le profil <Sans connexion>. Ce profil ne peut être modifié ou supprimé. Il ne contient pas de Serveur pour la connexion et en cas de sélection de ce profil, l'Agent d'administration ne tentera pas de se connecter à un serveur quelconque tandis que les applications installées sur les postes clients utilisent les stratégies pour les utilisateurs nomades. Le profil <Sans connexion> peut être invoqué quand les ordinateurs sont déconnectés du réseau.

CREATION DE LA REGLE DE PERMUTATION DE L'AGENT D'ADMINISTRATION

► Afin de créer la règle de permutation de l'Agent d'administration d'un Serveur d'administration sur un autre, lors de la modification des caractéristiques du réseau, procédez comme suit :

1. Sélectionnez la stratégie de l'Agent d'administration dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Ouvrez la fenêtre **Propriétés <Nom de la stratégie>** sous l'onglet **Réseau**.
4. En cliquant sur le lien **Profils des connexions**, ouvrez la fenêtre du même nom. Cette action entraîne l'ouverture de la fenêtre de configuration des paramètres de permutation de l'Agent d'administration (cf. ill. ci-après).

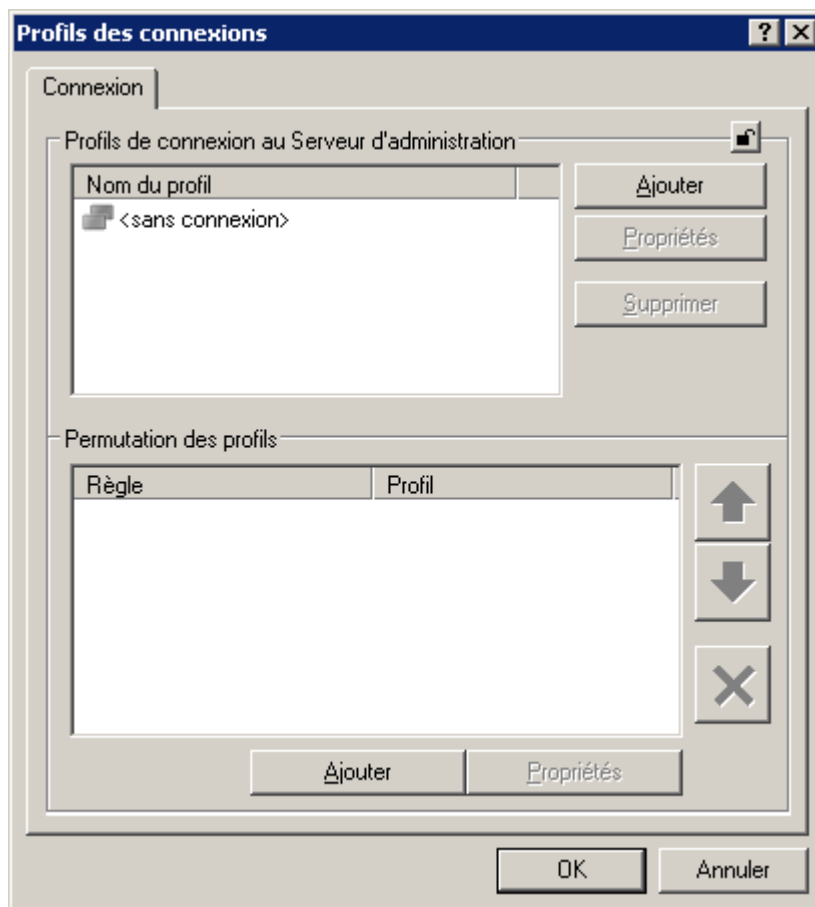


Illustration 243. Onglet **Connexion**

5. Cliquez sur **Ajouter** situé dans le groupe **Permutation des profils**.
6. Dans la fenêtre ouverte (cf. ill. ci-après) :
 - saisissez le nom de la règle dans le champ du dessus ;

- dans la liste déroulante **Utiliser le profil de connexion** sélectionnez le profil créé ;
- dans la groupe **Conditions de permutation** composez la liste des conditions de la règle à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Les conditions dans la règles sont réunies via l'opérateur logique "et".

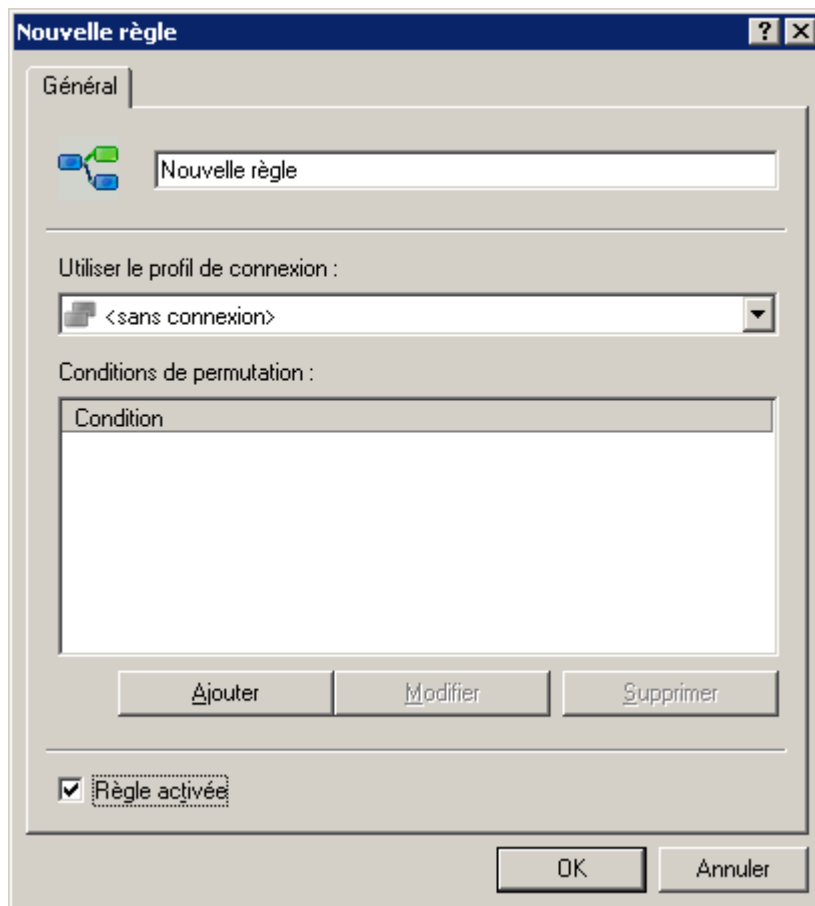


Illustration 244. Fenêtre **Nouvelle règle**

7. Cochez la case **Règle activée** pour activer l'utilisation de la règle (cf. ill. ci-dessus).
8. Appuyer sur **OK** pour terminer le fonctionnement de la règle.

AJOUT D'UNE CONDITION DANS LA REGLE

➔ Afin d'ajouter une condition dans la règle, procédez comme suit :

1. Sélectionnez la stratégie de l'Agent d'administration dans l'arborescence de la console.
2. Ouvrez le menu contextuel et sélectionnez l'élément **Propriétés**.
3. Ouvrez la fenêtre **Propriétés <Nom de la stratégie>** sous l'onglet **Réseau**.

4. A l'aide du lien **Profils des connexions** passez à la fenêtre de configuration des paramètres de permutation de l'Agent d'administration (cf. ill. ci-après).

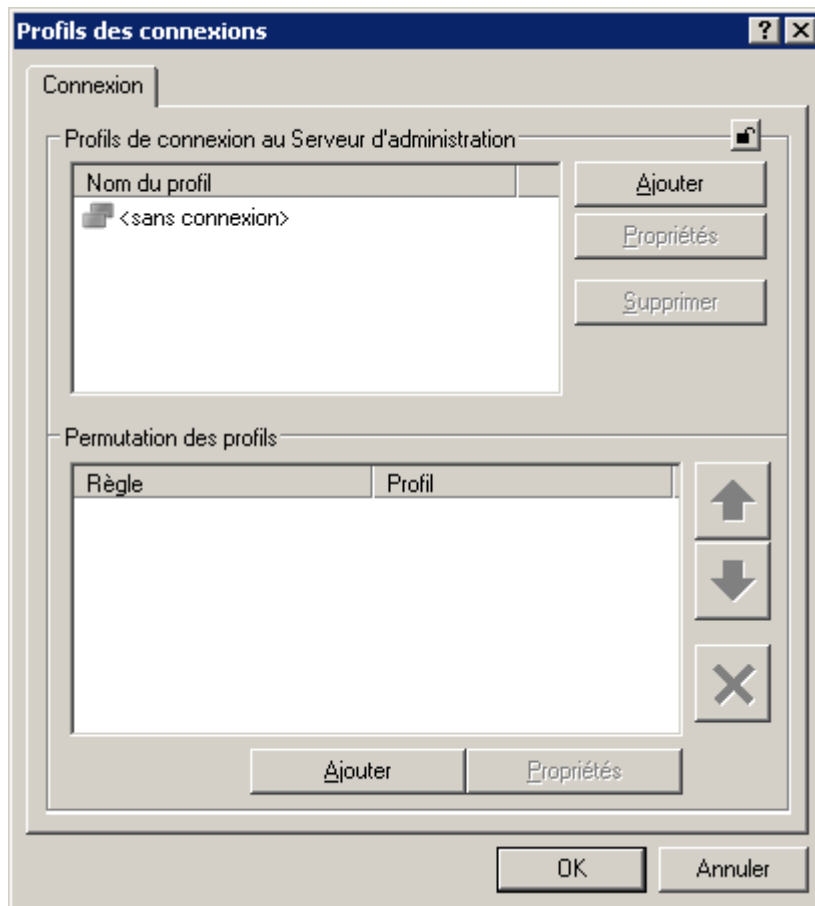


Illustration 245. Onglet **Connexion**

5. Cliquez sur **Ajouter** situé dans le groupe **Permutation des profils**.

6. Dans la groupe **Conditions de permutation** cliquez sur **Ajouter** (cf. ill. ci-après).

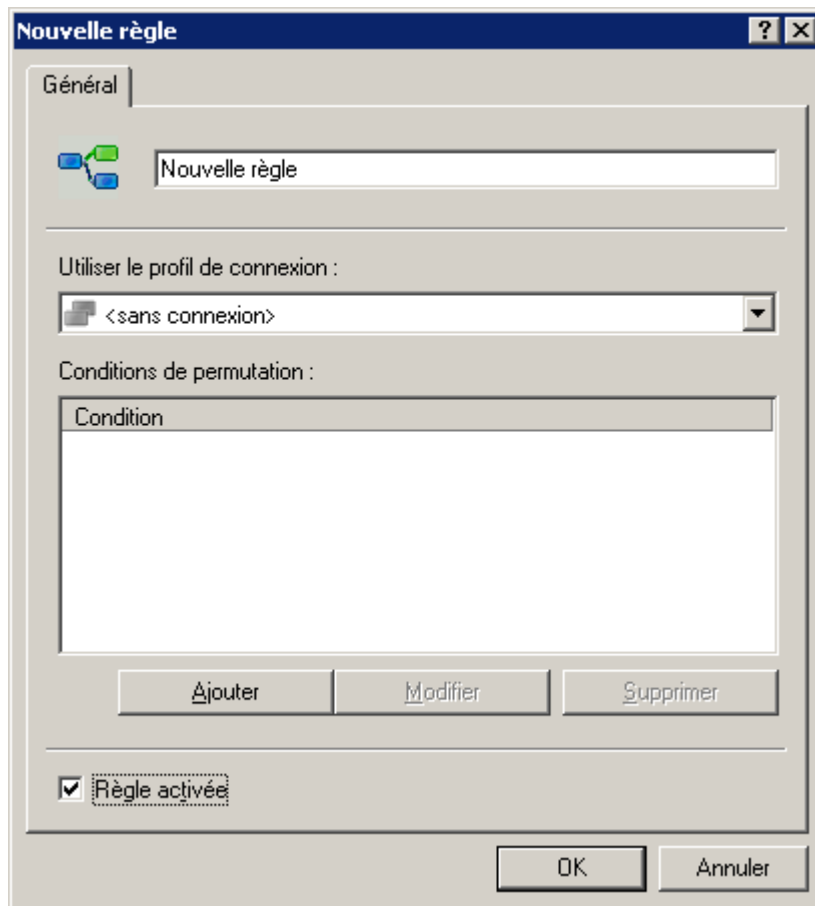


Illustration 246. Fenêtre **Nouvelle règle**

7. De la liste déroulante sélectionnez la valeur qui correspond à la modification de la caractéristique du réseau auquel le poste client est branché (cf. ill. ci-après) :

- **Présence dans le sous-réseau** : modification de l'adresse et du masque du sous-réseau ;
- **Présence dans le domaine DNS** : modification du suffixe DNS du sous-réseau ;
- **Adresse de la passerelle principale** : modification de la passerelle principale du réseau ;
- **Adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP dans le réseau ;
- **Adresse du serveur DNS** : modification de l'adresse IP du serveur DNS dans le réseau ;
- **Adresse du serveur WINS** : modification de l'adresse IP du serveur WINS dans le réseau ;

- **Accès au domaine Windows** : modification de l'état du domaine Windows auquel le poste client est connecté.

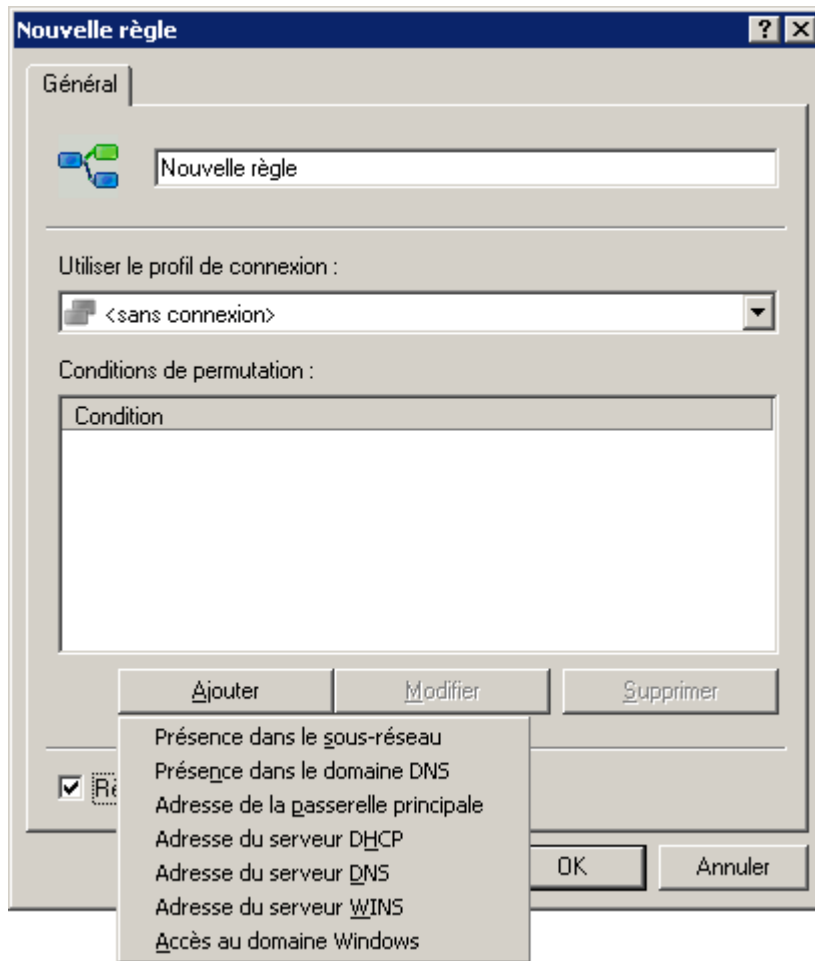


Illustration 247. Liste des caractéristiques du réseau

8. Cliquez sur **Ajouter** et établissez la valeur, avec laquelle la condition de permutation de l'agent sur un autre Serveur d'administration s'effectuera. Définissez autant de valeurs que nécessaire pour la condition à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer** (cf. ill. ci-après).

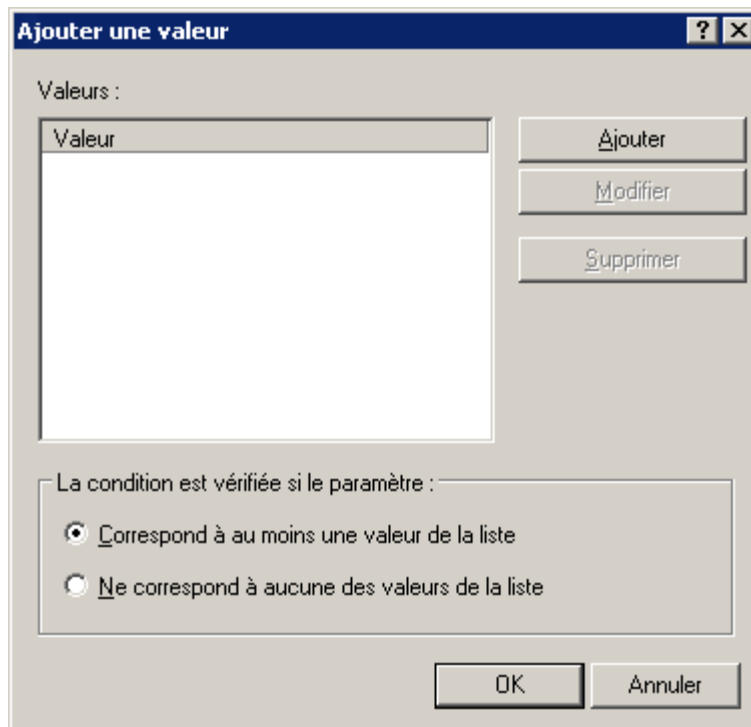


Illustration 248. Ajout d'une valeur

9. Sélectionnez les cas qui vérifieront la condition :
- **Correspond à au moins une valeur de la liste.**
 - **Ne correspond à aucune des valeurs de la liste.**
10. Cliquez sur le bouton **OK** pour terminer l'opération.

RECHERCHE

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 dans les groupes d'administration du Serveur d'administration et de ses 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.

Pour rechercher des ordinateurs, vous pouvez également utiliser les liens : **Rechercher des ordinateurs non définis** (situé dans la barre d'état du dossier **Ordinateurs non définis**) ou **Rechercher des ordinateurs** (sous l'onglet **Groupes** sur la barre des tâches du dossier **Ordinateurs administrés**).

Lors de la recherche d'ordinateurs, vous pouvez utiliser les termes suivants :

- * – n'importe quelle ligne d'une longueur de 0 ou plus de symboles ;
- ? – un n'importe quel symbole ;
- [<intervalle>] – un symbole de la plage définie ou de la multitude, par exemple, [0–9] – n'importe quel chiffre ou [abcdef] – un des symboles a, b, c, d, e, f.

RECHERCHE D'UN POSTE

► Pour rechercher un ordinateur qui vérifie les critères spécifiés, procédez comme suit :

1. Dans le menu contextuel du nœud **Serveur d'administration**, du dossier **Ordinateurs non définis** ou des groupes d'administration, sélectionnez le point **Recherche**.
2. En haut, à droit de la fenêtre, dans la liste déroulante, sélectionnez l'élément **Rechercher des postes clients**.

Dans la boîte de dialogue, spécifiez les critères de recherche sous les onglets suivants : **Réseau**, **Activité réseau**, **Application**, **Etat du poste**, **Protection antivirus**, **Registre des applications** et **Hiérarchie des Serveurs d'administration**.

3. Dans la fenêtre ouverte **Recherche**, indiquez les critères de recherche qui vous intéressent. Sous les onglets de la fenêtre, les critères de recherche suivants sont disponibles :
 - Sous l'onglet **Réseau** (cf. ill. ci-après) :
 - **Nom de poste** dans le réseau de l'entreprise ou l'adresse IP ;
 - **Domaine** auquel appartient le poste client ;
 - **Intervalle d'adresses IP** : l'adresse IP de début et de fin ;

- **L'ordinateur se trouve dans la &division Active Directory.** En cochant cette case, vous pouvez sélectionner l'ordinateur depuis le groupe Active Directory. Si l'ordinateur fait partie d'une unité particulière d'Active Directory, il est possible de cocher la case **Compris les divisions filles**.

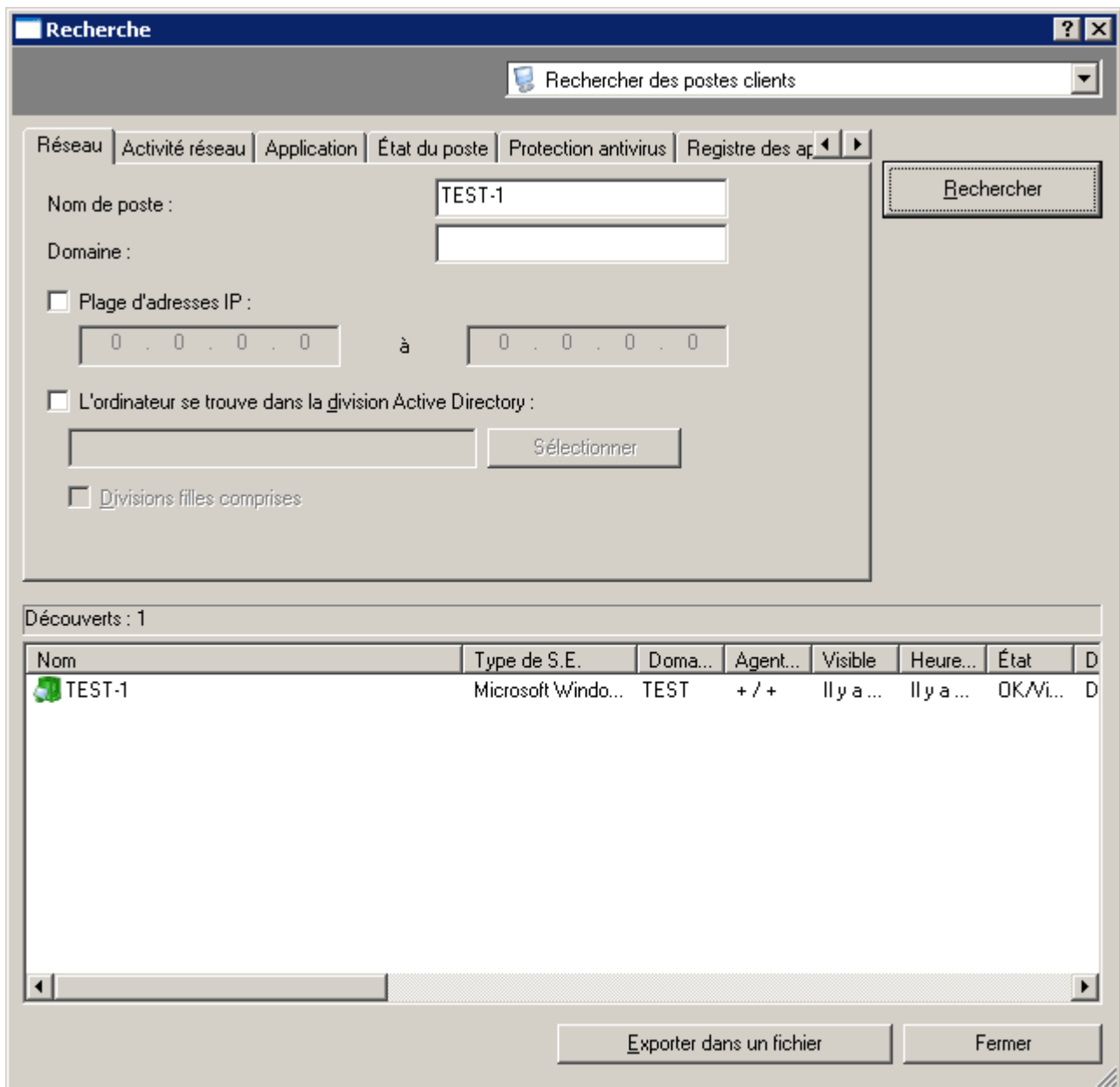


Illustration 249. Recherche d'un poste. Onglet Réseau

- Sous l'onglet **Activité réseau** (cf. ill. ci-après) :
 - L'ordinateur est-il un agent de mises à jour. Pour utiliser le critère dans la ligne **Est l'agent de mise à jour**, il faut sélectionner la valeur nécessaire (**Oui** ou **Non**).
 - La case **Maintenir la connexion avec le Serveur d'administration** est-elle cochée dans les propriétés de l'ordinateur. Pour utiliser le paramètre dans la ligne **Paramètre "Maintenir la connexion avec le Serveur d'administration"**, il faut sélectionner la valeur requise (**Activé** ou **Désactivé**).
 - L'ordinateur, est-il connecté au Serveur d'administration par suite de l'action du profil de connexion. Pour utiliser le paramètre dans la ligne **Changement du profil de connexion**, il faut sélectionner la valeur nécessaire (**Oui** ou **Non**).

- L'heure de dernière connexion du poste client au Serveur d'administration. Pour définir l'intervalle de temps, il faut cocher la case dans le champ **Intervalle après connexion précédente**.

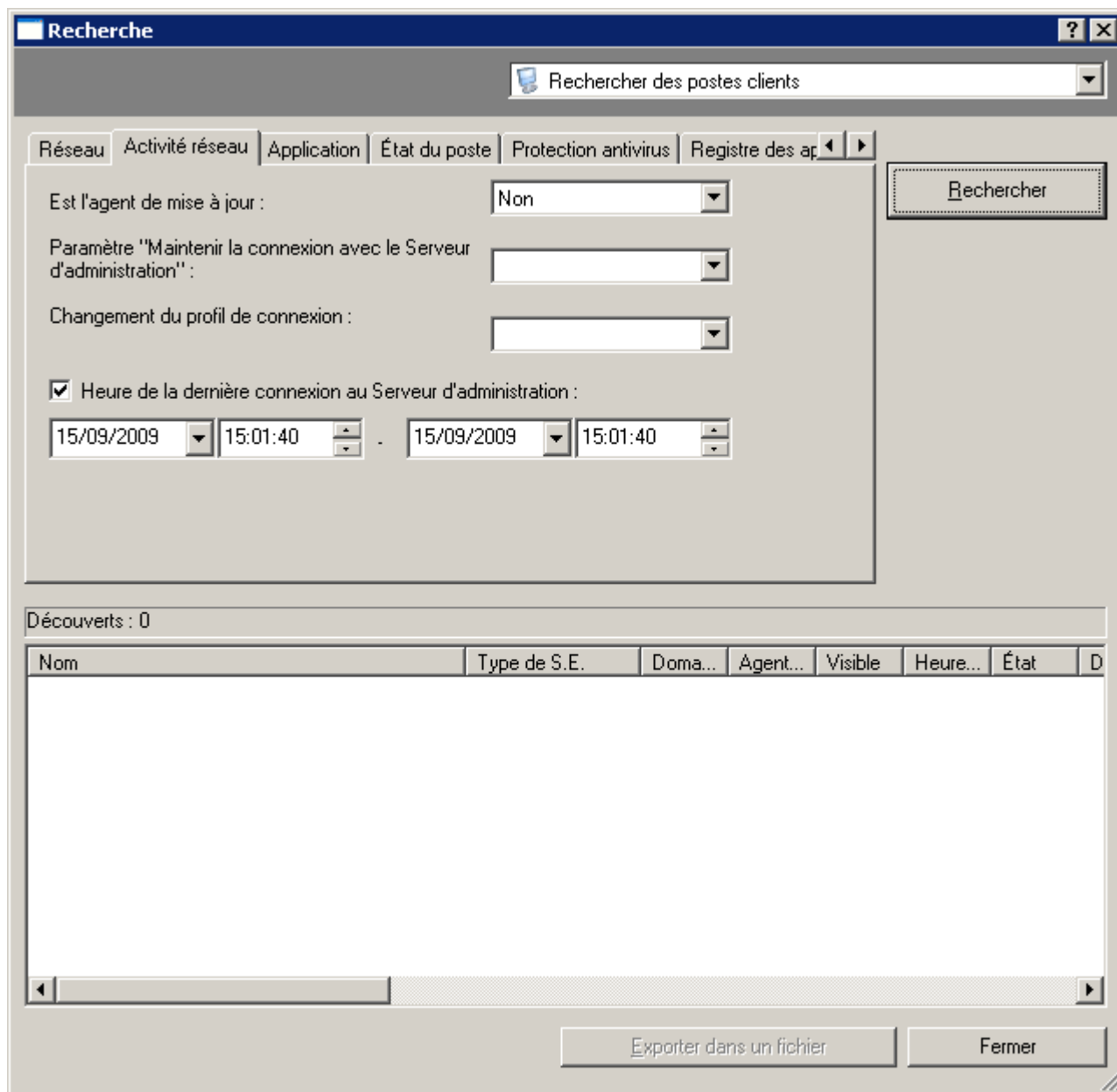


Illustration 250. Recherche de poste. Onglet **Activité réseau**

- Sous l'onglet **Application** (cf. ill. ci-après) :
 - **Nom de l'application** : le nom de l'application de Kaspersky Lab installée sur le poste client. Il est possible de sélectionner la valeur dans la liste déroulante. La liste ne fournit que le nom des applications disposant de plug-ins de contrôle installés dans l'espace de travail de l'administrateur.
 - **Versión de l'application** installée sur le poste client.
 - **Nom de la mise à jour critique** : le numéro ou le nom du paquet de mises à jour installé pour l'application.
 - **Dernière mise à jour des modules de l'application** : l'intervalle de temps de la dernière mise à jour des modules des applications installées sur le poste client.

- **Version du système d'exploitation** installé sur le poste.

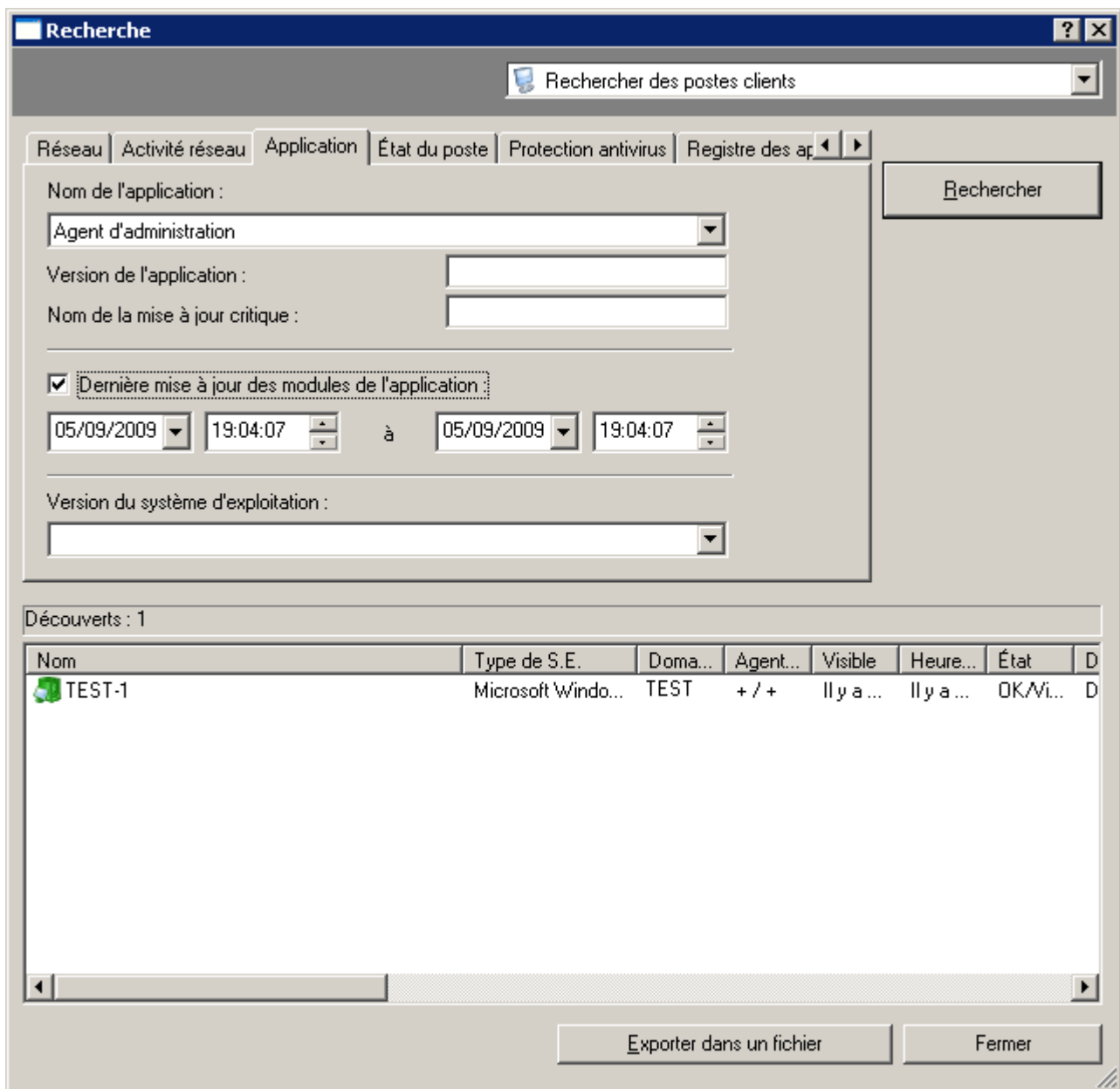


Illustration 251. Recherche de poste. Onglet **Application**

- Sous l'onglet **Etat du poste** (cf. ill. ci-après) :
 - **Etat du poste** : l'état actuel du poste : *OK*, *Critique* ou *Avertissement*.
 - **Description de l'état du poste**. Dans ce groupe, il est possible de cocher des conditions en fonction desquelles le poste client reçoit cet état.

- **Etat de la protection en temps réel** ; l'état actuel de protection en temps réel du poste client que vous souhaitez trouver dans la liste déroulante.

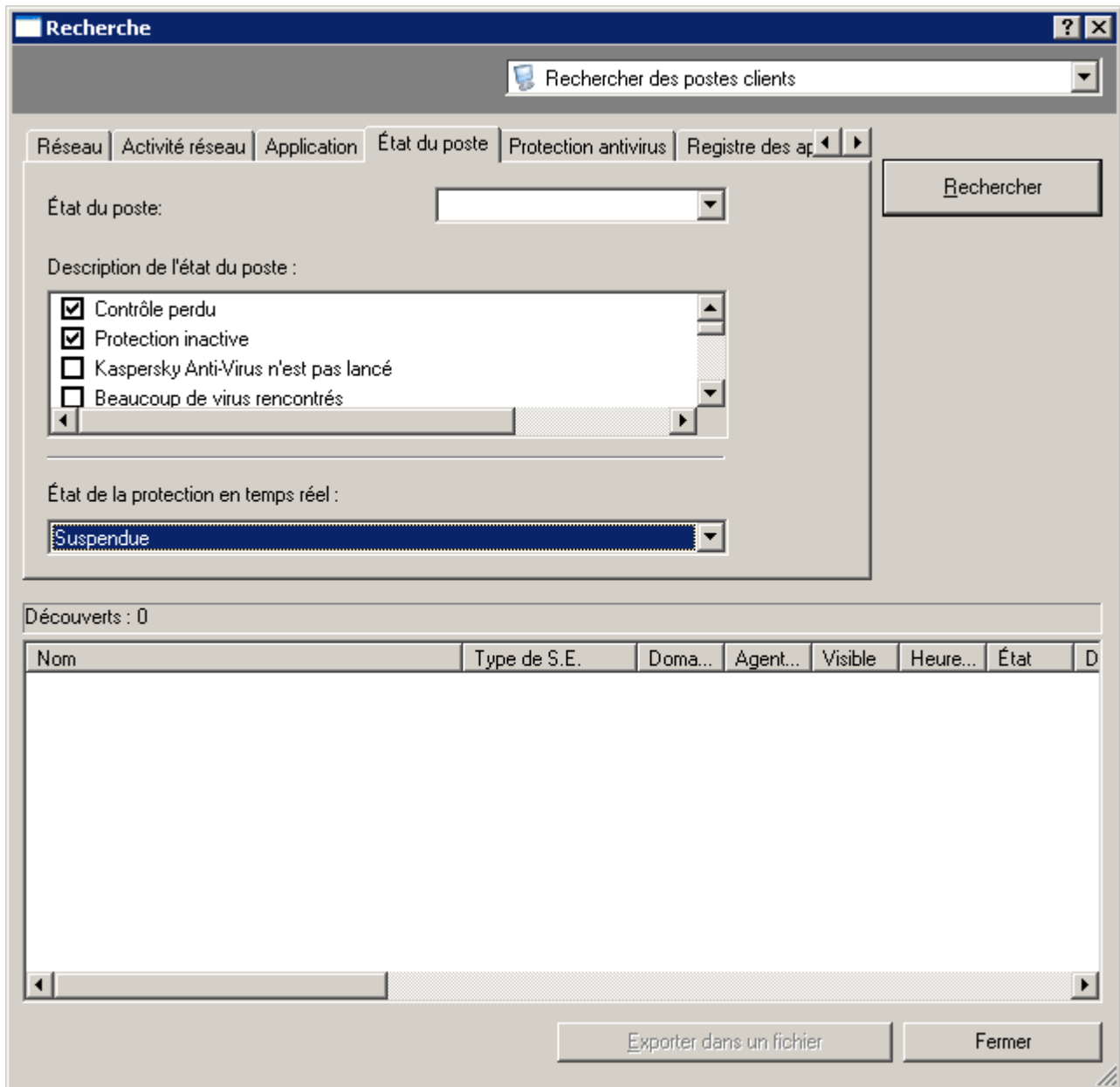


Illustration 252. Recherche de poste. Onglet **Etat du poste**

- Sous l'onglet **Protection antivirus** (cf. ill. ci-après) :
 - **Date des bases antivirus** : l'intervalle de temps pendant lequel les bases ont été publiées.
 - **Nombre d'enregistrements dans les bases** : la plage numérique comprenant le nombre d'enregistrements dans les bases.
 - **Dernière recherche de virus** : l'intervalle de temps pendant lequel une analyse complète du poste client s'est déroulée pour la dernière fois.

- **Virus trouvés** : la plage numérique comprenant le nombre de virus trouvés.

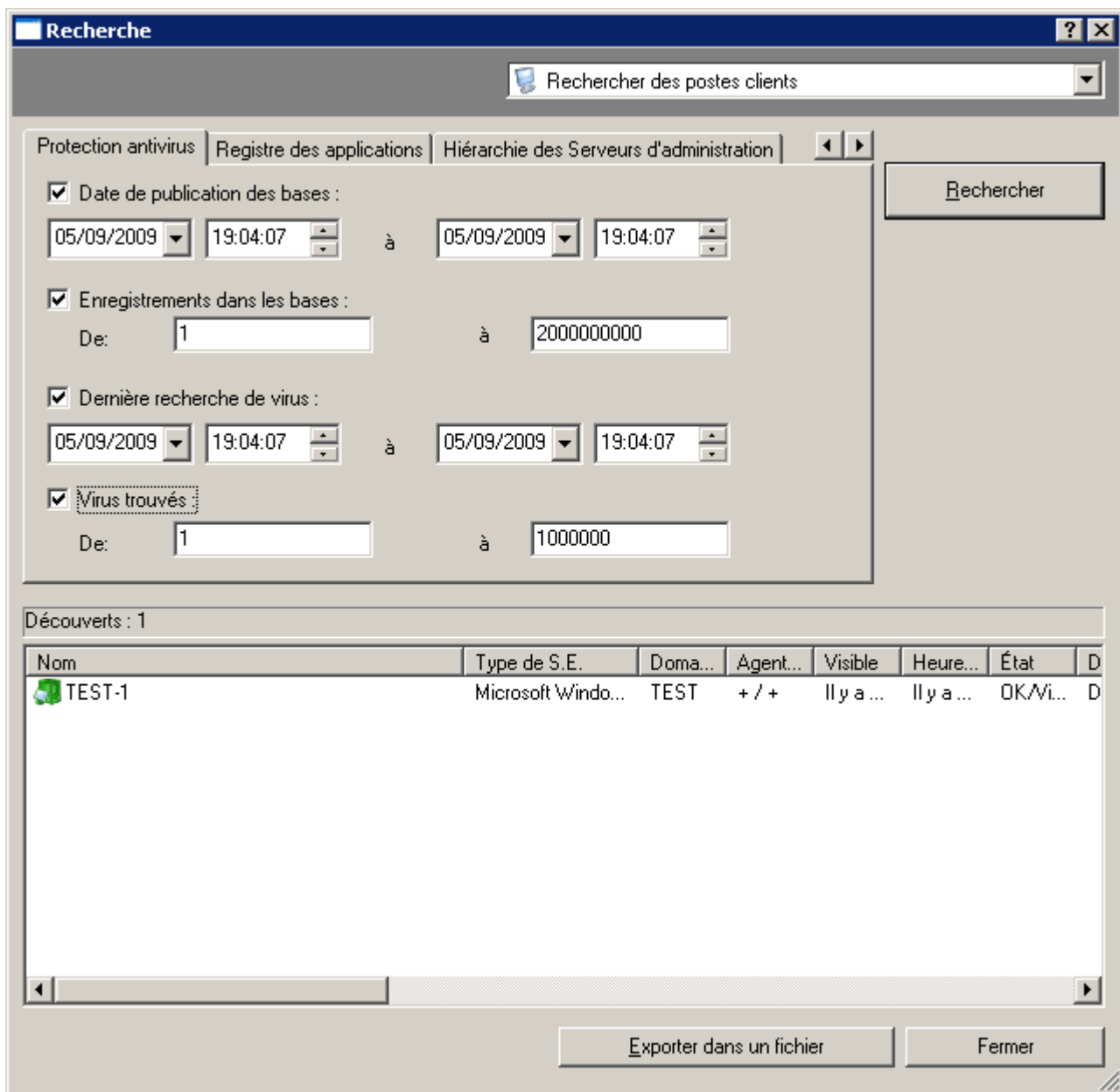


Illustration 253. Recherche de poste. Onglet **Protection antivirus**

- Sous l'onglet **Registre des applications** (cf. ill. ci-après) :
 - Afin que la recherche s'opère selon les données sur l'application, indiquez les paramètres qui vous intéressent une fois que la case **Rechercher selon la mise à jour** est décochée : **Nom de l'application** ; **Version de l'application** ; **Editeur**.
 - Pour que la recherche s'opère selon les données relatives à la mise à jour, installée sur une application quelconque, cochez la case **Rechercher selon la mise à jour** et désignez les paramètres qui vous intéressent : **Nom de la mise à jour** ; **Version de la mise à jour** ; **Editeur**.

- **Nom de l'application de sécurité incompatible** : l'application de sécurité d'un éditeur tiers (il faut sélectionner dans la liste).

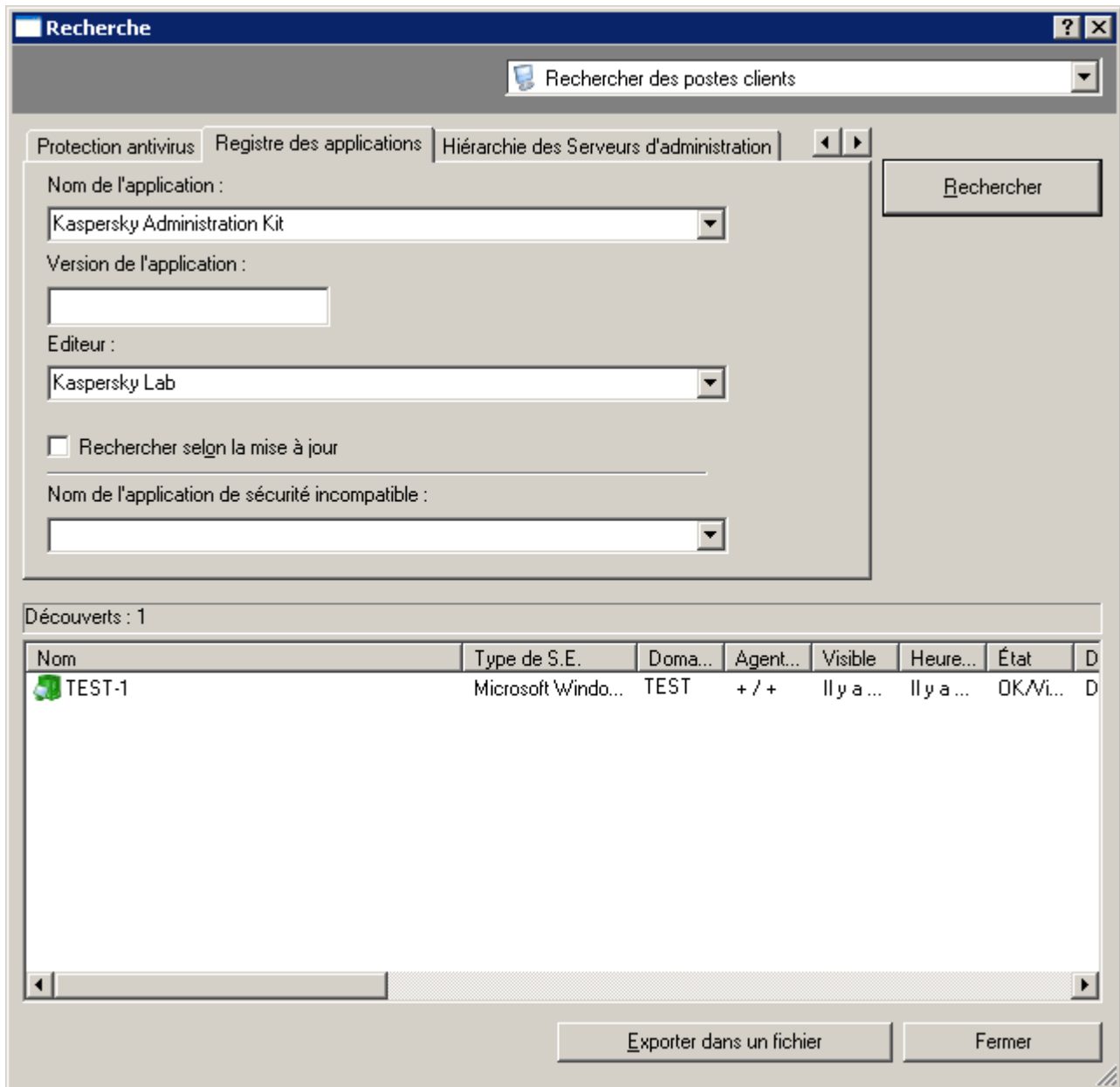


Illustration 254. Recherche de poste. Onglet **Registre des applications**

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

- L'onglet **Hiérarchie des Serveurs d'administration** vous permet de définir si les informations reprises sur les Serveurs d'administration secondaires seront prises en compte lors de la recherche des ordinateurs (cf. ill. ci-après).

Pour que ces informations soient prises en compte, cochez la case **Y compris les données des Serveurs secondaires jusqu'au niveau**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

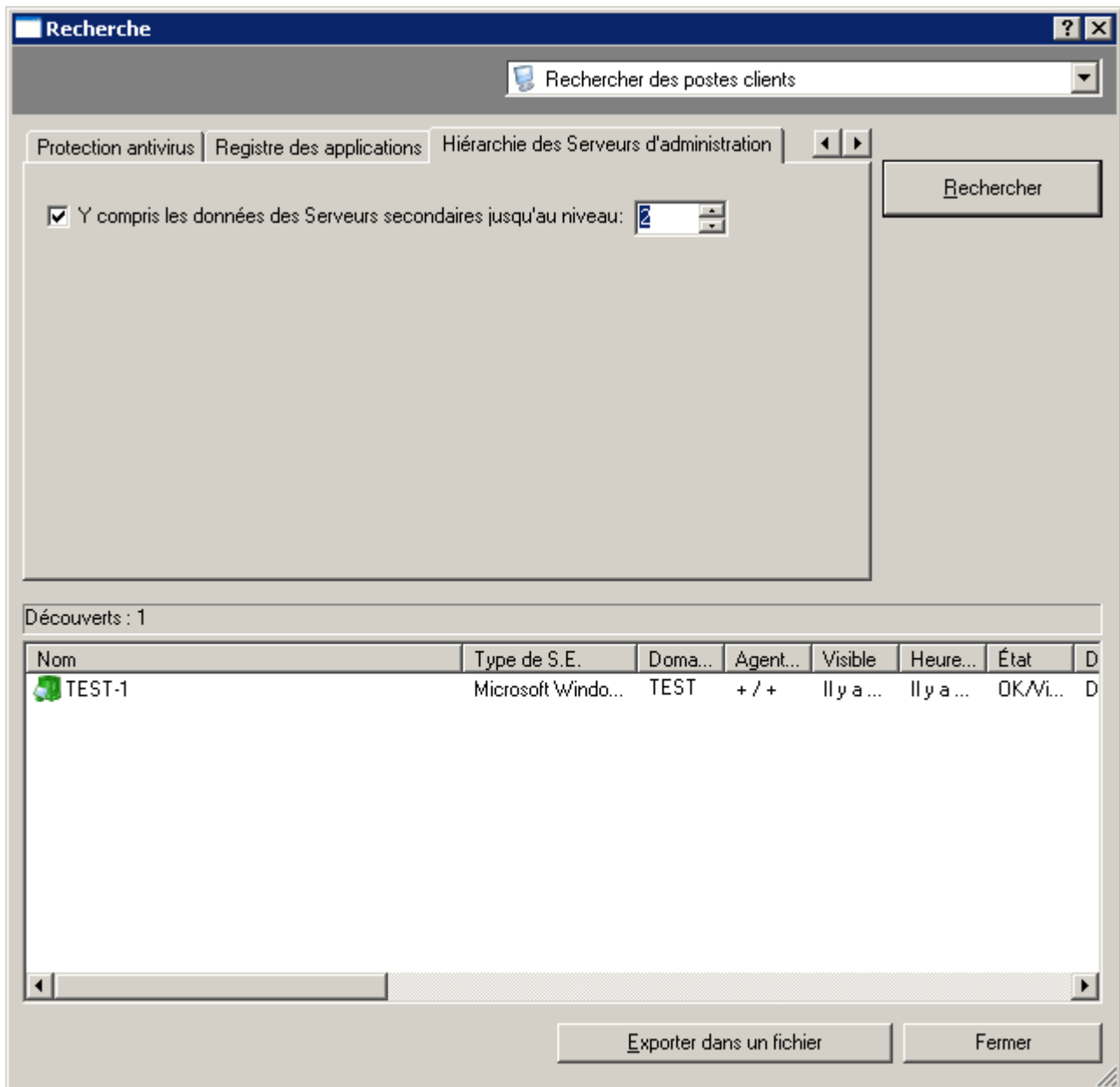


Illustration 255. Recherche d'un poste. Onglet **Hiérarchie des Serveurs d'administration**

- Une fois les critères définis, cliquez sur **Rechercher**. La liste des ordinateurs vérifiant les critères de recherche est affichée au bas de la boîte de dialogue. La liste contient des informations générales sur les ordinateurs détectés.
- Pour enregistrer les résultats de la recherche dans un fichier texte, cliquez sur le bouton **Exporter dans un fichier** et dans la fenêtre qui s'ouvre, indiquez le fichier pour l'enregistrement.

RECHERCHE DE GROUPES D'ADMINISTRATION

➤ Afin de rechercher un groupe d'administration qui vérifie les critères spécifiés, procédez comme suit :

1. Dans le menu contextuel de l'entrée **Serveur d'administration** ou du groupe d'administration sélectionnez le point **Recherche**.
2. En haut, à droite de la fenêtre, dans la liste déroulante, sélectionnez l'élément **Rechercher des groupes d'administration**.

Dans la boîte de dialogue, spécifiez les critères de recherche sous les onglets suivants : **Général** et **Hiérarchie des Serveurs d'administration**.

3. Sur l'onglet **Général** indiquez le nom du groupe (cf. ill. ci-après).

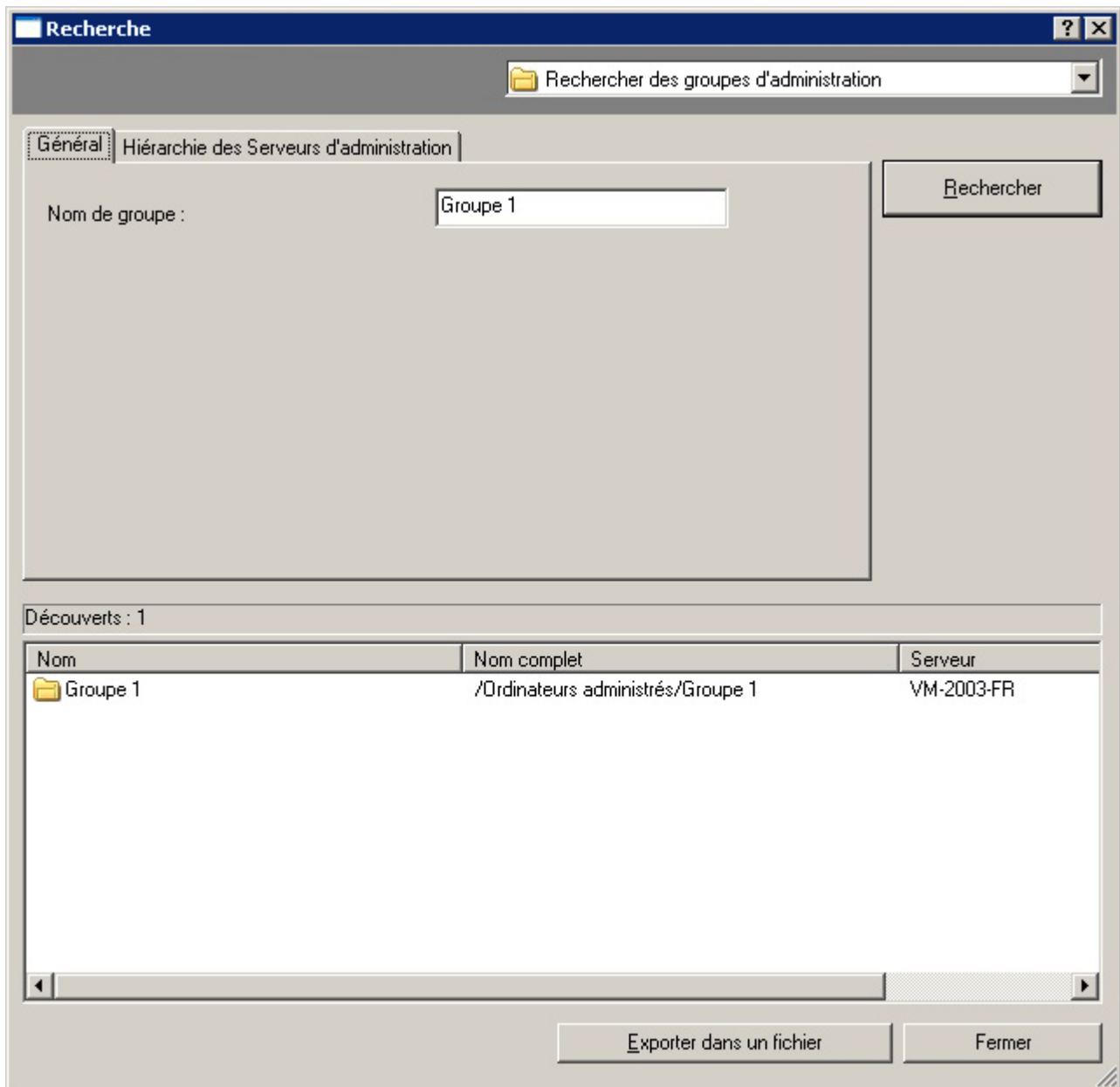


Illustration 256. Recherche d'un groupe d'administration. Onglet **Général**

4. L'onglet **Hiérarchie des Serveurs d'administration** vous permet de définir si les informations reprises sur les Serveurs d'administration secondaires seront prises en compte ou non lors de la recherche des ordinateurs.

Pour que ces informations soient prises en compte, cochez la case **Y compris les données des Serveurs secondaires jusqu'au niveau**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

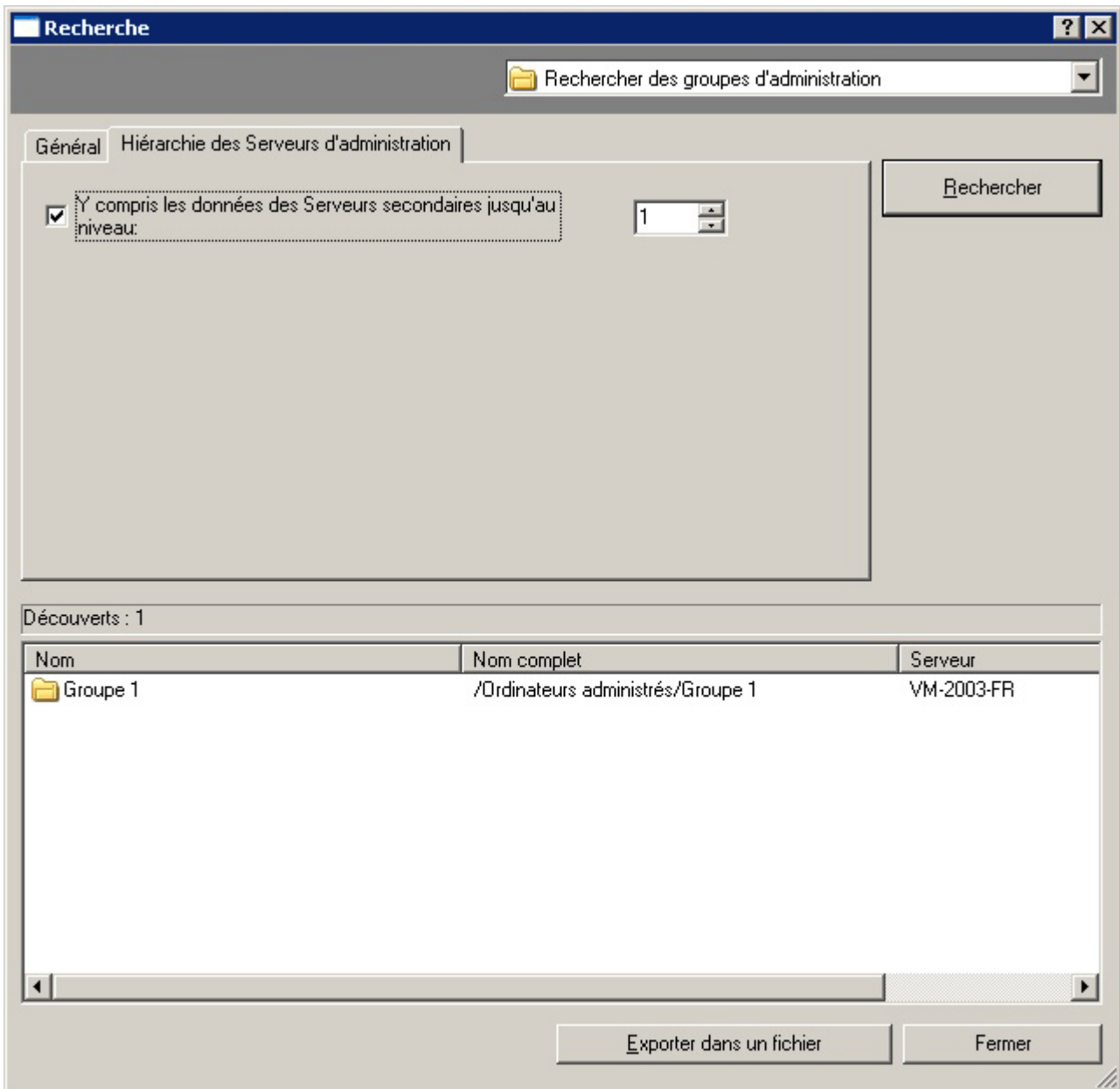


Illustration 257. Recherche d'un groupe d'administration. Onglet **Hiérarchie des Serveurs d'administration**

5. Une fois les critères définis, cliquez sur **Rechercher**. La liste des ordinateurs vérifiant les critères de recherche est affichée au bas de la boîte de dialogue. La liste contient des informations générales sur les ordinateurs détectés.
6. Pour enregistrer les résultats de la recherche dans un fichier texte, cliquez sur le bouton **Exporter dans un fichier** et dans la fenêtre qui s'ouvre, indiquez le fichier pour l'enregistrement.

RECHERCHE DE SERVEURS D'ADMINISTRATION SECONDAIRES

➤ Afin de rechercher le Serveur d'administration secondaire qui vérifie les critères spécifiés, procédez comme suit :

1. Dans le menu contextuel de l'entrée **Serveur d'administration** ou du groupe d'administration sélectionnez le point **Recherche**.
2. En haut, à gauche de la fenêtre, dans la liste déroulante, sélectionnez l'élément **Rechercher des Serveurs d'administration secondaires**.

Dans la boîte de dialogue, spécifiez les critères de recherche sous les onglets suivants : **Général** et **Hiérarchie des Serveurs d'administration**.

3. Sur l'onglet **Général** indiquez le nom du Serveur (cf. ill. ci-après).

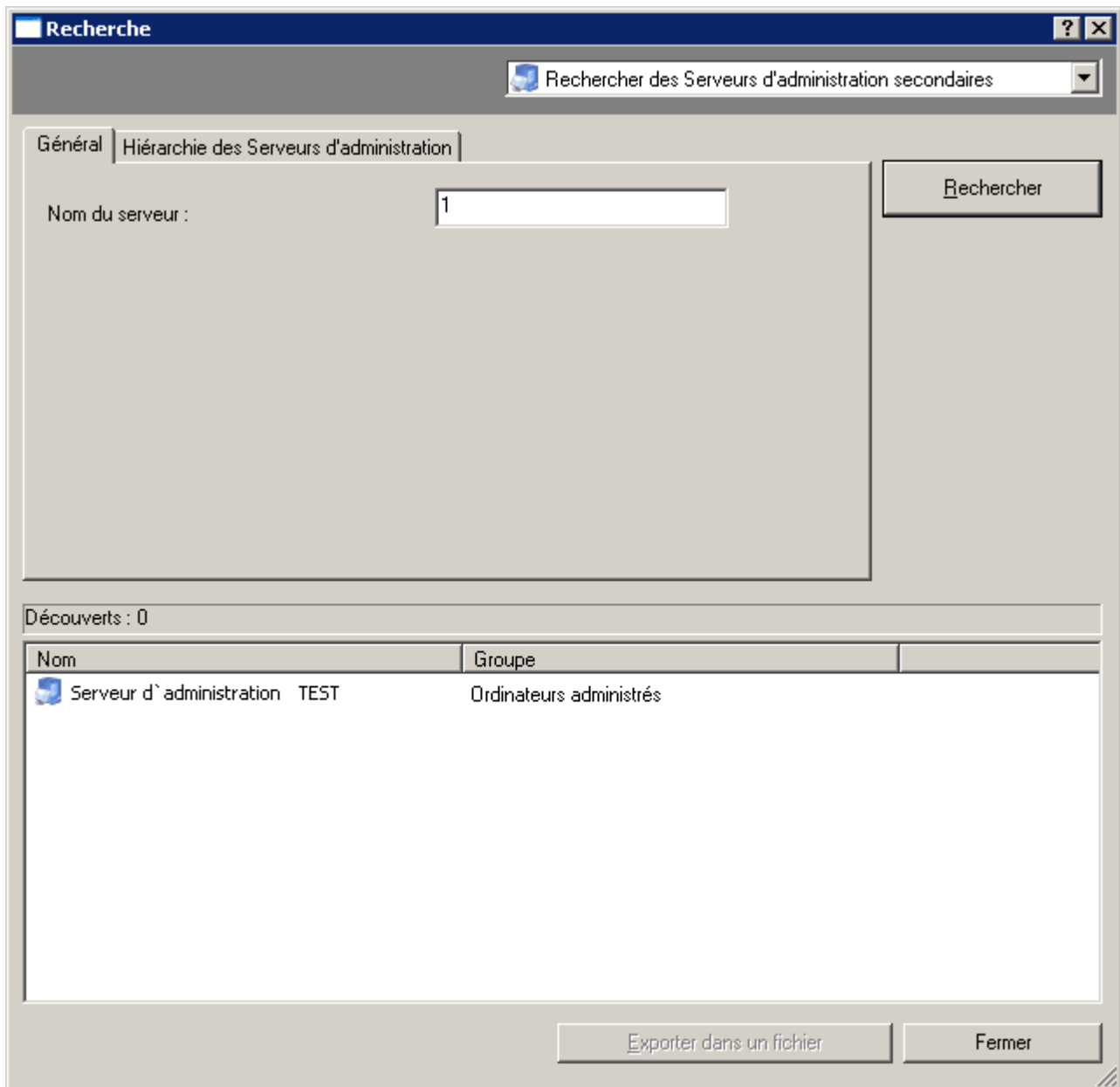


Illustration 258. Recherche d'un Serveur d'administration secondaire. Onglet **Général**

4. L'onglet **Hiérarchie des Serveurs d'administration** vous permet de définir si les informations reprises sur les Serveurs d'administration secondaires seront prises en compte ou non lors de la recherche des ordinateurs.

Pour que ces informations soient prises en compte, cochez la case **Y compris les données des Serveurs secondaires jusqu'au niveau**. Spécifiez ensuite le niveau d'imbrication maximum que la recherche doit couvrir.

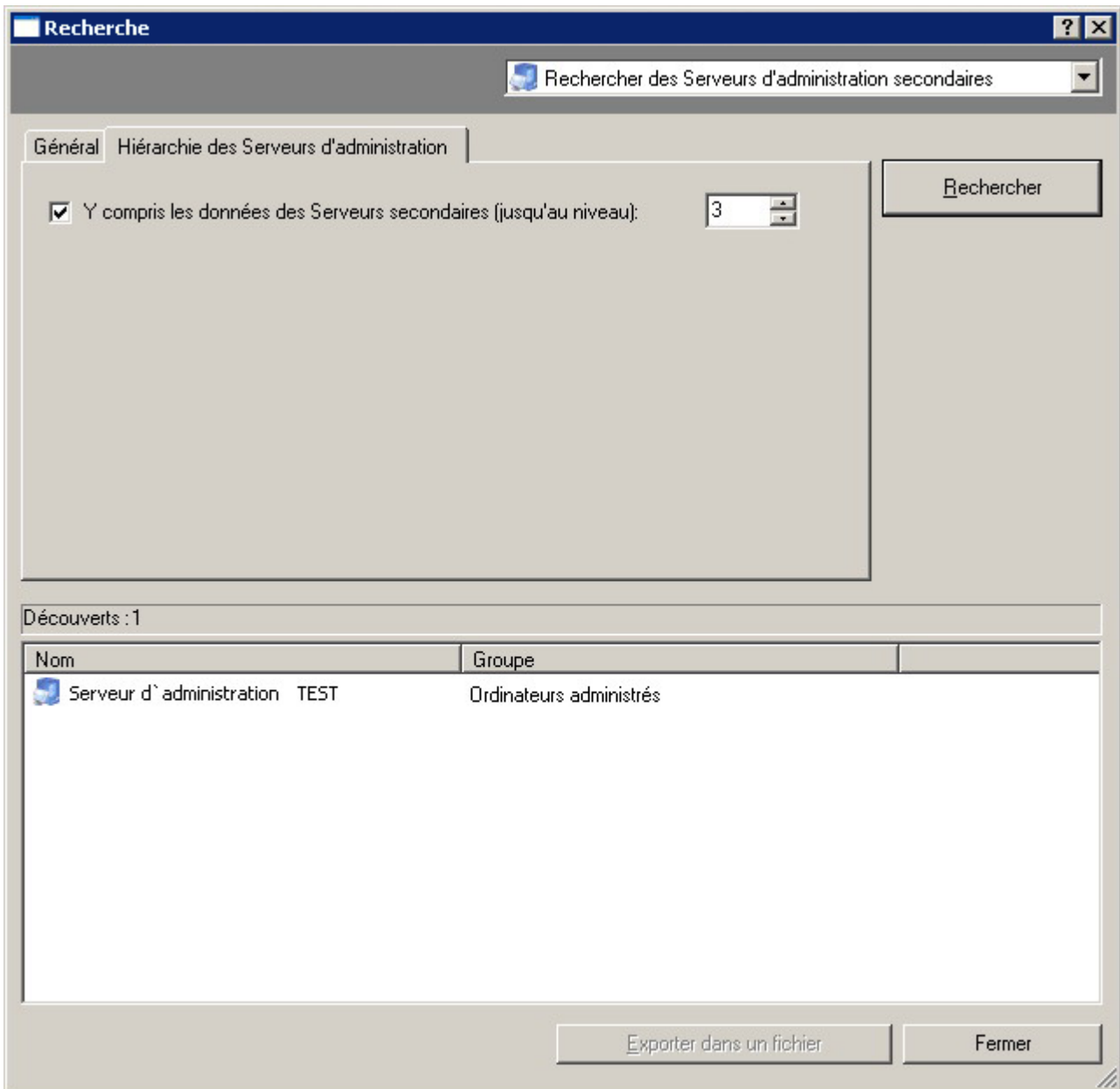


Illustration 259. Recherche d'un Serveur d'administration secondaire. Onglet **Hiérarchie des Serveurs d'administration**

5. Une fois les critères définis, cliquez sur **Rechercher**. La liste des ordinateurs vérifiant les critères de recherche est affichée au bas de la boîte de dialogue. La liste contient des informations générales sur les ordinateurs détectés.
6. Pour enregistrer les résultats de la recherche dans un fichier texte, cliquez sur le bouton **Exporter dans un fichier** et dans la fenêtre qui s'ouvre, indiquez le fichier pour l'enregistrement.

COPIE DE SAUVEGARDE DES DONNEES

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.

- *Pour créer une copie de sauvegarde des données du Serveur d'administration, utilisez une des options suivantes :*
 - A l'aide de la Console d'administration, créez et lancez une tâche pour la copie de sauvegarde des données (cf. section "Tâche de copie de sauvegarde des données" à la page [311](#)).
 - Lancez l'utilitaire klbackup sur l'ordinateur avec le serveur d'administration installé (cf. section "Utilitaire de copie de sauvegarde et de restauration des données (klbackup)" à la page [314](#)). Cet outil est fourni avec le paquet de distribution Kaspersky Administration Kit et se trouve à la racine du dossier d'installation indiqué après l'installation du Serveur d'administration.

- *Pour rétablir les données du Serveur d'administration,*

lancez l'utilitaire klbackup sur l'ordinateur avec le Serveur d'administration installé.

Le nom de la base de données de l'ancien serveur et du nouveau doit correspondre.

TACHE DE COPIE DE SAUVEGARDE DES DONNEES

La tâche de copie de sauvegarde est une des tâches du Serveur d'administration qui est créée par l'Assistant de configuration initiale (cf. section "Assistant de configuration initiale" à la page [14](#)) ou manuellement et elle se place dans le dossier **Tâches de Kaspersky Administration Kit**.

- *Pour créer une tâche de sauvegarde des données du Serveur d'administration, procédez comme suit :*
 1. Dans l'arborescence de la console, sélectionnez l'entrée **Tâches de Kaspersky Administration Kit**, ouvrez le menu contextuel et sélectionnez la commande **Générer** → **Tâche**.
 2. Créez une tâche du Serveur d'administration (cf. section "Création d'une tâche pour le Serveur d'administration" à la page [113](#)). Lors de la création d'une tâche, spécifiez les valeurs suivantes pour les paramètres :

- En guise de type de tâche, indiquez **Sauvegarde des données du Serveur d'administration** (cf. ill. ci-après).

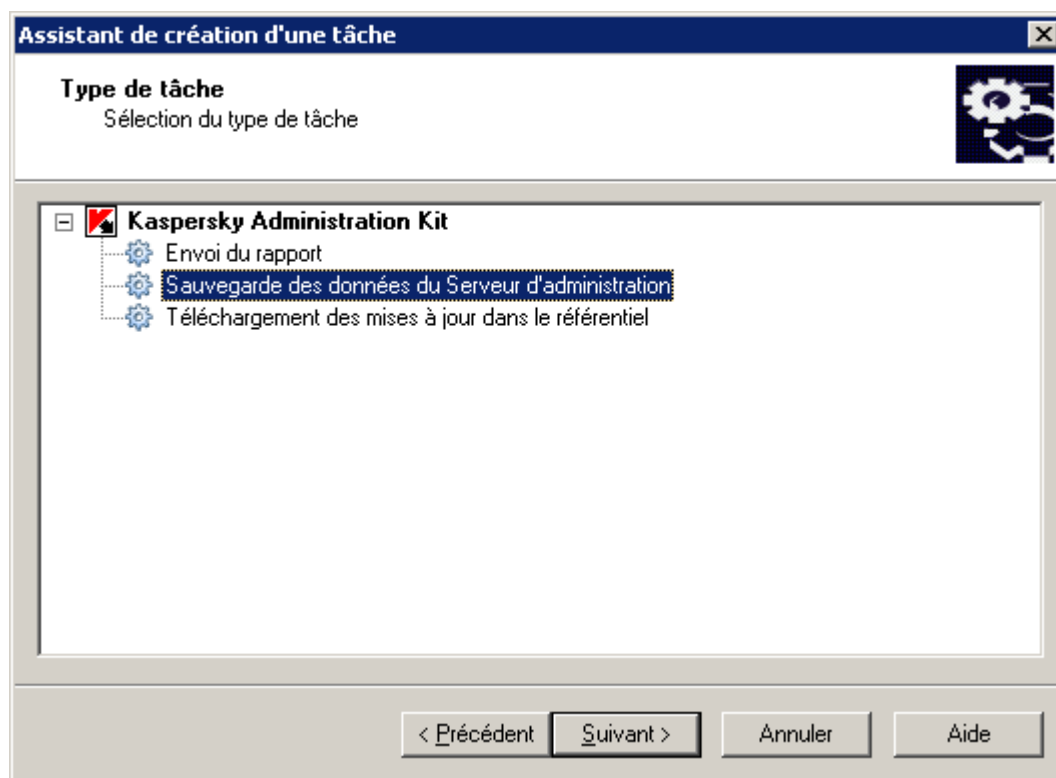


Illustration 260. Création d'une tâche. Sélection du type de la tâche

- Au moment de configurer les paramètres de la tâche (cf. ill. ci-après), indiquez :
 - le dossier destination des données de sauvegarde ; ce dossier doit être disponible en écriture à la fois pour le Serveur d'administration et pour le serveur SQL sur lequel se trouve installée la base de données du Serveur d'administration ;

- le mot de passe à utiliser pour coder et décoder le certificat du Serveur d'administration ; retapez le mot de passe dans le champ ci-dessous.

Illustration 261. Création d'une tâche de Sauvegarde. Configuration des paramètres

La copie de sauvegarde des données est créée dans le dossier indiqué dans un sous-dossier portant un nom qui indique la date et l'heure système actuelles au format `klbackup AAAA-MM-JJ # HH-MM-SS` (où AAAA représente l'année, MM, le mois, JJ, le jour, HH, l'heure, MM, les minutes, SS, les secondes). On y retrouve :

- la base de données 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 ;
- l'entrepôt des paquets de déploiement des applications (le contenu du dossier Packages) ;
- le certificat du Serveur d'administration.

Le cas échéant, vous pouvez réduire le nombre de copies de sauvegarde - c'est à dire, le nombre maximum de sous-dossiers pouvant figurer dans le dossier de sauvegarde. Pour ce faire cochez la case **Limiter le nombre de copies de sauvegarde conservées** et spécifiez le nombre de copies requis. Une fois la limite définie atteinte, la copie la plus ancienne placée dans le dossier de sauvegarde sera supprimée au moment de la création d'une nouvelle copie.

➔ Pour configurer une tâche de sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Sélectionnez la tâche requise dans le panneau des résultats pour le dossier **Tâches de Kaspersky Administration Kit**, ouvrez le menu contextuel et sélectionnez la commande **Propriétés**.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres** (cf. ill. ci-après). Cet onglet affiche les mêmes paramètres définis lors de la création de la tâche :
 - dossier destination des copies de sauvegarde ;

- le mot de passe à utiliser pour coder et décoder le certificat du Serveur d'administration ; retapez le mot de passe dans le champ ci-dessous ;
- limitation du nombre de copies de sauvegarde.

Spécifiez les valeurs requises des paramètres.

3. Lorsque la configuration est terminée, cliquez sur **Appliquer** ou **OK**.

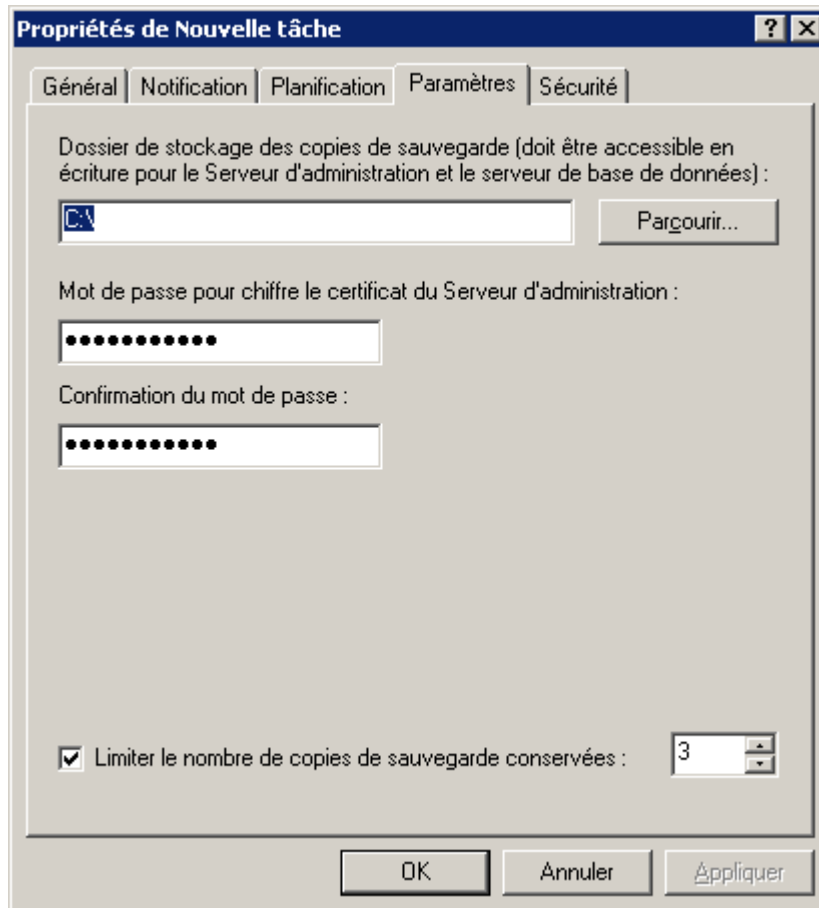


Illustration 262. Configuration de la tâche de copie de sauvegarde des données

UTILITAIRE DE COPIE DE SAUVEGARDE ET DE RESTAURATION DES DONNEES (KLBACKUP)

La copie des données du Serveur d'administration pour la copie de sauvegarde et la restauration ultérieure peut être réalisée non seulement à l'aide de la tâche du Serveur d'administration (cf. section "Tâche de copie de sauvegarde des données" à la page [311](#)), mais aussi 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, qui peut fonctionner en deux modes :

- interactif (cf. section "Mode interactif de création de copie de sauvegarde et de restauration des données" à la page [315](#)) ;
- non interactif (cf. section "Mode non interactif de création de copie de sauvegarde et de restauration des données" à la page [316](#)).

MODE INTERACTIF DE CREATION DE COPIE DE SAUVEGARDE ET DE RESTAURATION DES DONNEES

➔ Pour le mode de création de copie de sauvegarde des données du Serveur d'administration en mode interactif, procédez comme suit :

1. Exécutez l'utilitaire klbackup, situé dans le dossier C:\Program Files\Kaspersky Lab\Kaspersky Administration Kit.
2. Dans la fenêtre ouverte de l'Assistant sélectionnez l'action (cf. ill. ci-après) :
 - Réaliser la copie de sauvegarde des données du Serveur d'administration.
 - Rétablir les données du Serveur d'administration.

En cochant la case **Exécuter la copie de sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**, seulement le certificat du Serveur d'administration sera sauvegardé ou restauré.

Cliquez sur **Suivant**.

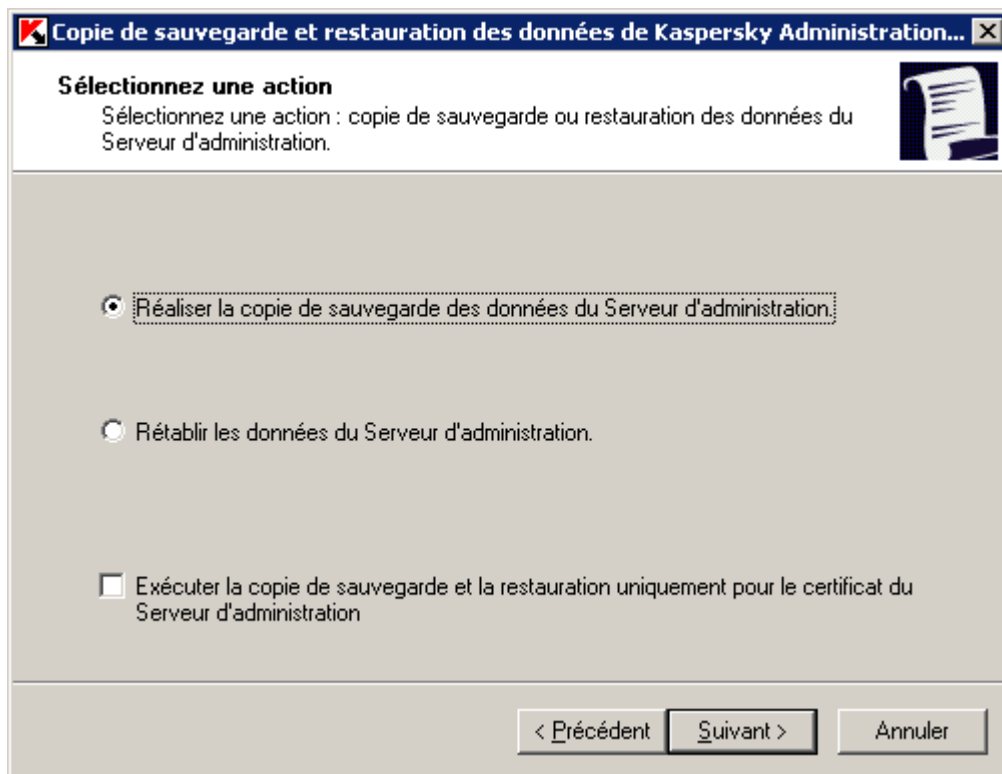


Illustration 263. Sauvegarde

3. Dans la fenêtre suivante, saisissez **Mot de passe** et **Dossier cible pour la copie de sauvegarde** (cf. ill. ci-après). Cliquez sur **Suivant** pour exécuter la copie de sauvegarde.

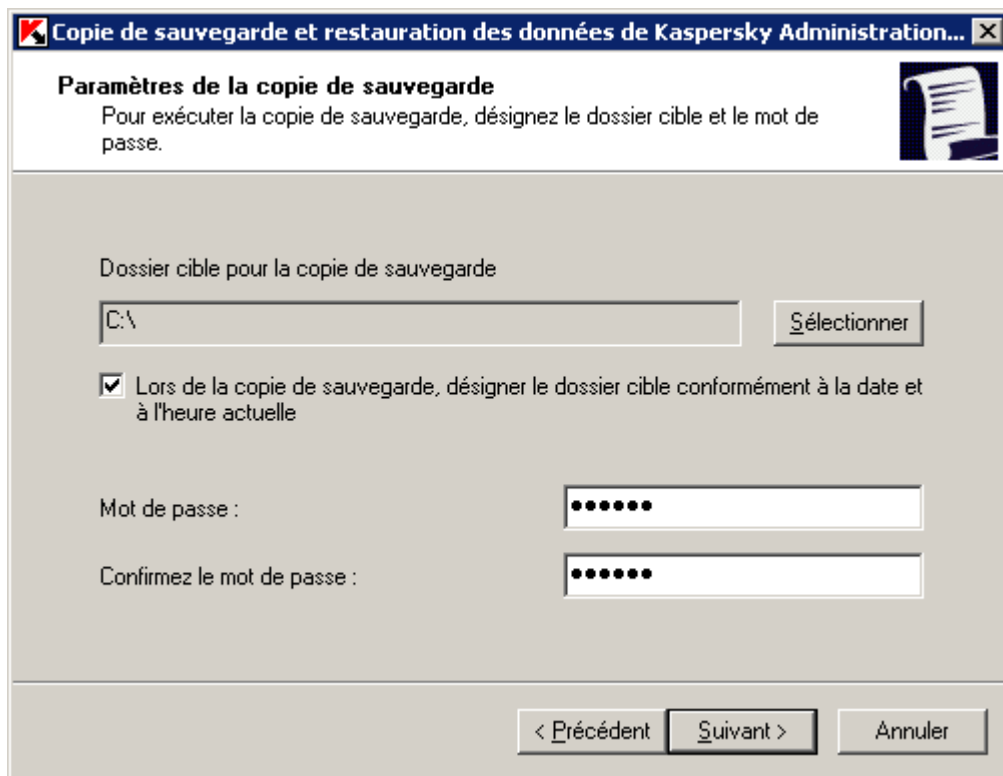


Illustration 264. Création du dossier cible pour la copie de sauvegarde

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

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.

MODE NON INTERACTIF DE CREATION DE COPIE DE SAUVEGARDE ET DE RESTAURATION DES DONNEES

- Pour la création manuelle de copie de sauvegarde des données du Serveur d'administration en mode non-interactif,

exécutez l'outil klbackup sur le poste où le Serveur d'administration se trouve installé, avec les paramètres correspondants de la ligne de commande.

Syntaxe de l'utilitaire :

```
klbackup [-logfile LOGFILE] -path BACKUP_PATH [-use_ts] | [-restore] -savecert PASSWORD
```

Si le mot de passe n'est pas saisi dans la ligne de commande de l'utilitaire klbackup, l'utilitaire demandera son entrée interactivement.

Description des paramètres :

- -logfile LOGFILE - enregistre un rapport d'exécution de la tâche de copie/restauration des données du Serveur d'administration ;

- `-path BACKUP_PATH` - enregistre les données dans le dossier `BACKUP_PATH`/restaure à partir des données du dossier `BACKUP_PATH` (paramètre obligatoire) ;

Le compte du serveur de base de données et l'outil `klbackup` doivent posséder les droits pour modifier les données dans le dossier `BACKUP_PATH`.

- `-use_ts` : lors de l'enregistrement des données, copier les informations dans le sous-dossier `BACKUP_PATH` dossier avec un nom représentant la date et l'heure système au format `klbackup AAAA-MM-JJ # HH-MM-SS`. Si aucun paramètre de ligne de commande n'est spécifié, les données seront enregistrées à la racine du dossier `BACKUP_PATH`.

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

L'utilisation du paramètre `-use_ts` permet de gérer les archives de données du Serveur d'administration. Par exemple, si le dossier `C:\KLBackups` a été spécifié en utilisant le paramètre `-path`, alors les données sur l'état du Serveur d'administration datant du 19 juin 2006, à 11 heures 30 et 18 secondes, seront enregistrées dans le dossier `klbackup 2006-06-19 # 11-30-18`.

- `-restore` : restaurer les données du Serveur d'administration. La restauration des données se fera en fonction des informations conservées dans le dossier `BACKUP_PATH`. Si le paramètre n'est pas utilisé, la copie de sauvegarde des données se fera dans le dossier `BACKUP_PATH`.
- `-savecert PASSWORD` : la fonction Enregistrer/Restaurer le Certificat du Serveur d'administration utilise le mot de passe spécifié par le paramètre `PASSWORD` pour coder ou décoder le certificat.

La restauration complète des données du système d'administration nécessite une sauvegarde impérative du certificat du Serveur d'administration.

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

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.

DEPLACEMENT DU SERVEUR D'ADMINISTRATION SUR UN AUTRE ORDINATEUR

➔ Pour déplacer le Serveur d'administration sur un autre ordinateur, procédez comme suit :

1. Créez une copie de sauvegarde des données du Serveur d'administration.
2. Installez le nouveau Serveur d'administration.

Pour simplifier le transfert des groupes d'administration, il est souhaitable que l'adresse du nouveau Serveur coïncide avec l'adresse de l'ancien Serveur. L'adresse (nom de l'ordinateur dans le réseau Windows ou adresse IP) est définie dans les paramètres de connexion de l'Agent d'administration au Serveur.

3. Sur le nouveau Serveur d'administration, restaurez les données de l'ancien Serveur au départ de la copie de sauvegarde.
4. Si les adresses (nom de l'ordinateur dans le réseau Windows ou adresse IP) du nouveau et de l'ancien Serveur ne coïncident pas, sur l'ancien Serveur créez la tâche **de modification du Serveur d'administration** pour le groupe **Ordinateurs administrés**.

Si les adresses correspondent, la tâche de changement de Serveur n'est pas nécessaire. La connexion s'effectuera selon les paramètres définis pour l'adresse du Serveur sans aucun problème.

5. Supprimez l'ancien Serveur d'administration.

➤ *Pour transférer un Serveur d'administration sur un autre ordinateur et remplacer la base de données du Serveur d'administration, procédez comme suit :*

1. Créez une copie de sauvegarde des données du Serveur d'administration.

2. Installez un nouveau serveur SQL.

Pour un transfert correct des données sur un nouveau serveur SQL, celui-ci doit avoir les mêmes fusions que le serveur SQL précédent.

3. Installez le nouveau Serveur d'administration. Le nom de la base de données de l'ancien serveur et du nouveau doit correspondre.

Pour simplifier le transfert des groupes d'administration, il est souhaitable que l'adresse du nouveau Serveur coïncide avec l'adresse de l'ancien Serveur. L'adresse (nom de l'ordinateur dans le réseau Windows ou adresse IP) est définie dans les paramètres de l'Agent d'administration qui régulent la connexion au Serveur.

4. Sur le nouveau Serveur d'administration, restaurez les données de l'ancien Serveur au départ de la copie de sauvegarde.

5. Si les adresses (nom de l'ordinateur dans le réseau Windows ou adresse IP) du nouveau et de l'ancien Serveur ne coïncident pas, sur l'ancien Serveur créez la tâche **de modification du Serveur d'administration** pour le groupe **Ordinateurs administrés**.

Si les adresses correspondent, la tâche de changement de Serveur n'est pas nécessaire. La connexion s'effectuera selon les paramètres définis pour l'adresse du Serveur sans aucun problème.

6. Supprimez l'ancien Serveur d'administration.

SUIVI DES 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.

ACTIVATION DU MECANISME D'IDENTIFICATION D'UNE ATTAQUE DE VIRUS

➤ *Pour identifier les événements de type **Attaque de virus** dans les limites des groupes d'administration et les notifier, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration souhaité, ouvrez le menu contextuel et utilisez la commande **Propriétés**. Cela entraîne l'ouverture de la boîte de dialogue **Propriétés de <Nom du Serveur d'administration>**.

2. Sur l'onglet **Attaque de virus** (cf. ill. ci-après), cochez la case en regard du nom des applications antivirus concernées et configurez leurs paramètres qui déterminent le seuil d'activité viral au-delà duquel l'événement Attaque de virus est attribué. Le dépassement du seuil sera considéré comme une augmentation de l'activité virale et le déclenchement de l'événement **Attaque de virus**.

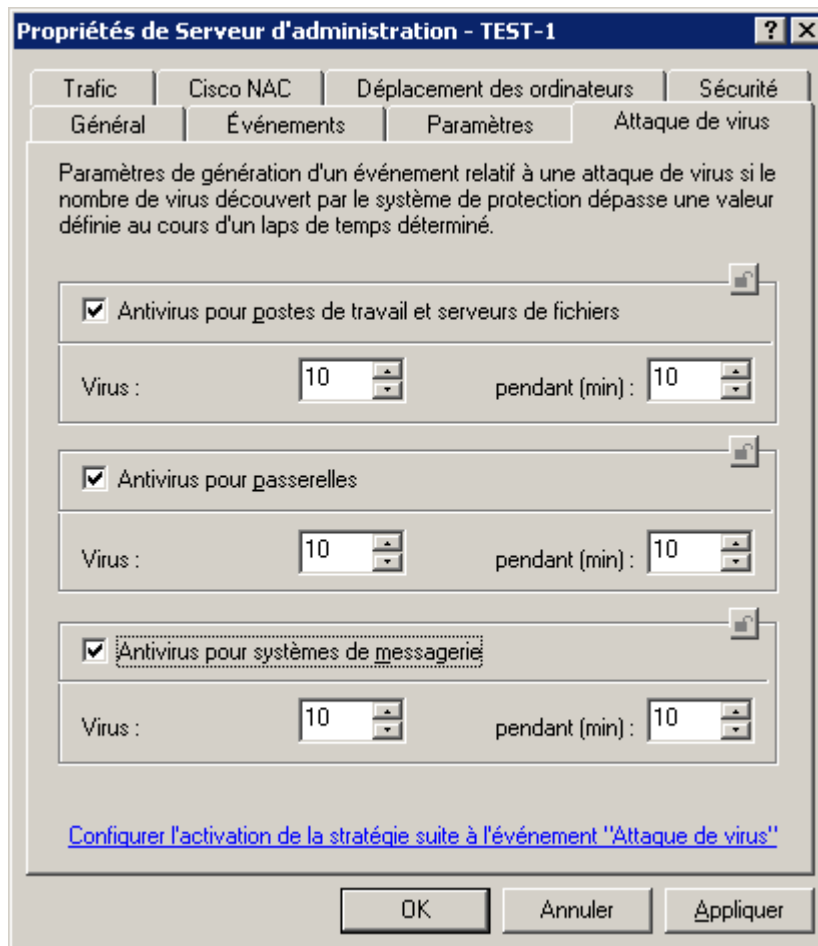


Illustration 265. Affichage des propriétés du Serveur d'administration. Onglet **Attaque de virus**

3. Sur l'onglet **Événements** (cf. ill. ci-après) lors de la configuration des événements du niveau Critique, sélectionnez le type d'événement **Attaque de virus** et configurez les paramètres des notifications requis.

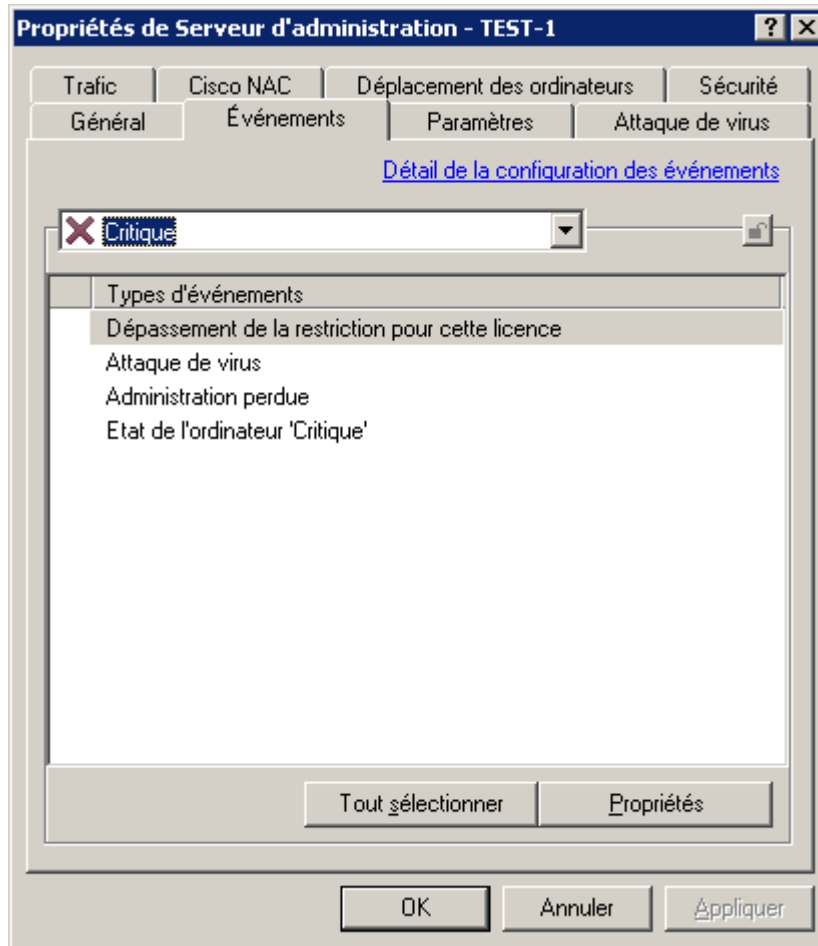


Illustration 266. Affichage des propriétés du Serveur d'administration. Onglet **Événements**

4. Dans les stratégies pour toutes les applications antivirus sur l'onglet **Evénements** (cf. ill. ci-après) lors de la configuration des événements du niveau d'importance **Critique**, sélectionnez le type d'événement **Objet infecté découvert** et dans la fenêtre des propriétés de cet événement, cochez la case **Sur le Serveur d'administration pendant (jours)**.

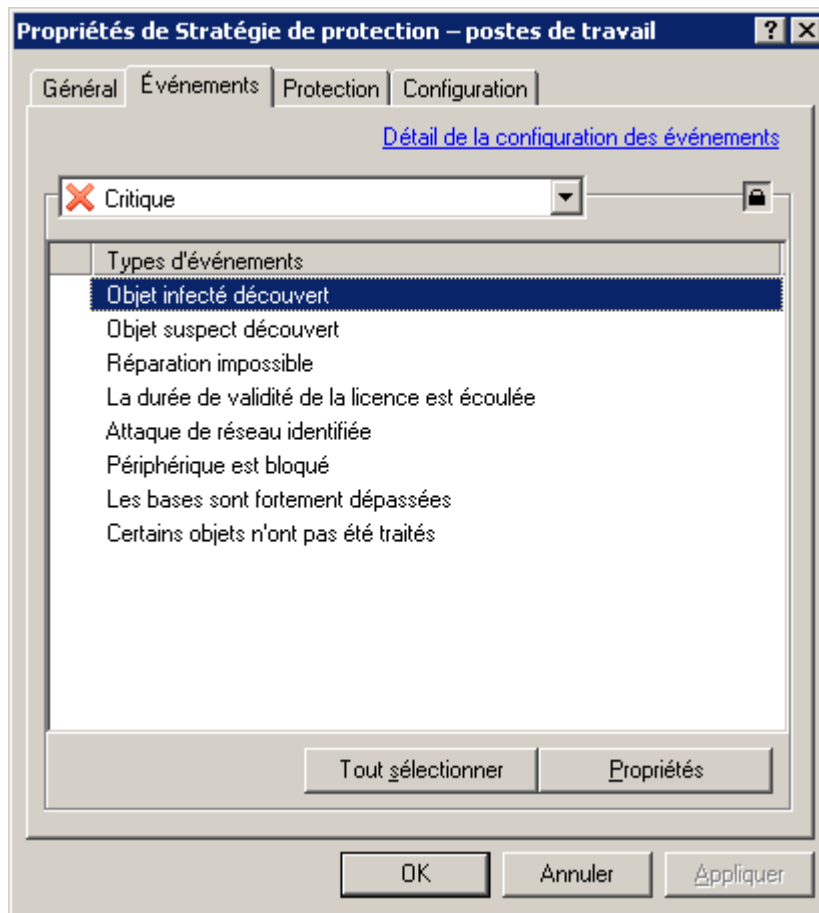


Illustration 267. Modification d'une stratégie. Onglet **Evénements**

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.

CHANGEMENT DE STRATEGIE POUR L'APPLICATION LORS DE L'ENREGISTREMENT DE L'EVENEMENT ATTAQUE DE VIRUS

- Afin de remplacer la stratégie actuelle pour l'application en cas d'événement **Attaque de virus**, procédez comme suit :
 1. Ouvrez la fenêtre des propriétés du Serveur d'administration.
 2. Sélectionnez l'onglet **Attaque de virus**.
 3. Cliquez sur le lien **Configurer l'activation de la stratégie suite à l'événement "Attaque de virus"** et dans la fenêtre ouverte (cf. ill. ci-après) :

- Sélectionnez le type d'attaque de virus selon le type d'application : antivirus pour les postes de travail et les serveurs, antivirus pour les serveurs de messagerie, antivirus de protection du périmètre.

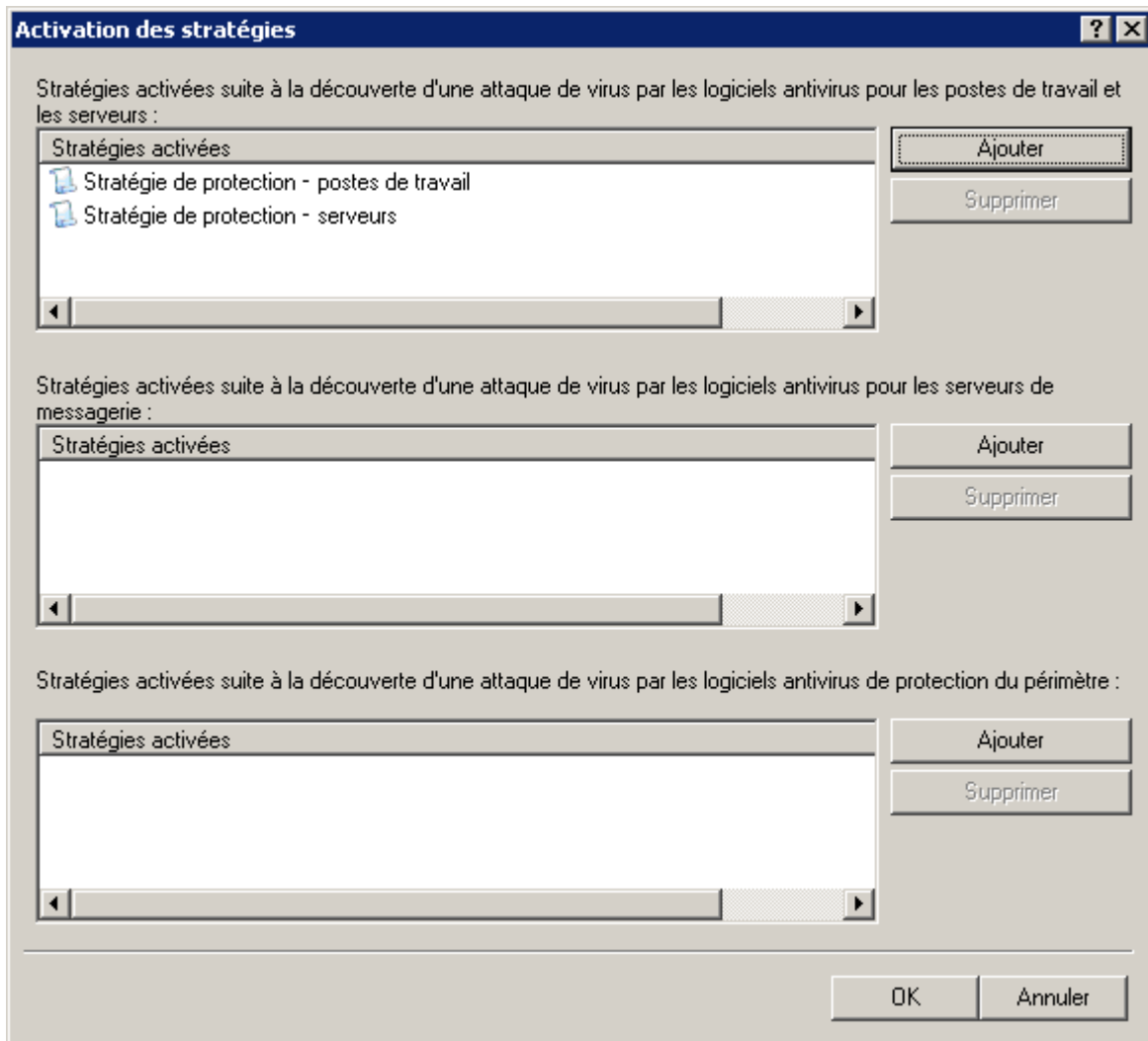


Illustration 268. Paramètres de l'événement **Attaque de virus**. Sélection des stratégies pour l'activation

- Dans le champ correspondant, composez la liste des stratégies à l'aide des boutons situés à droite du champ :
 - Pour ajouter une stratégie à la liste, cliquez sur le bouton **Ajouter** et dans la fenêtre **Choisissez une stratégie** (cf. ill. ci-après), cochez la case en regard de la stratégie dans l'arborescence proposée. Si vous cochez la case en regard du nom du groupe d'administration, alors toutes les stratégies du groupe seront marquées pour l'ajout.

- Pour supprimer une stratégie de la liste, sélectionnez-la et cliquez sur **Supprimer** (cf. ill. ci-dessus).

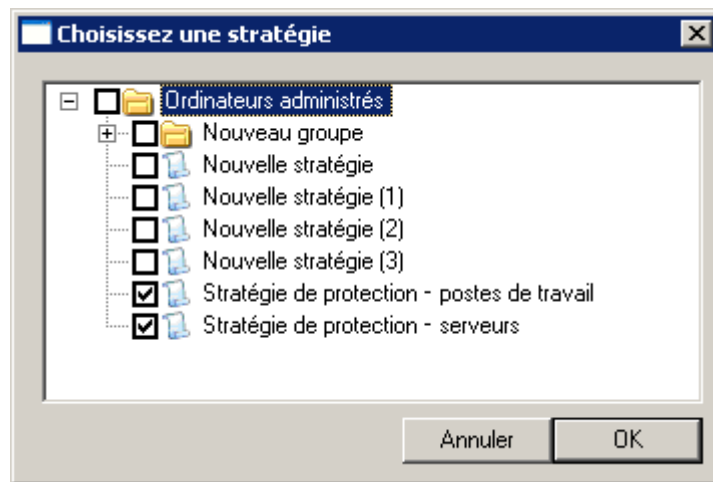


Illustration 269. Fenêtre de sélection des groupes

AUTOMATISATION DU FONCTIONNEMENT DE KASPERSKY ADMINISTRATION KIT (KLAKAUT)

Il est possible d'automatiser le fonctionnement de Kaspersky Administration Kit à l'aide de l'objet d'automatisation klakaut. L'utilitaire le système d'aide sont situés dans le dossier d'installation de l'application dans le sous-dossier klakaut.

OUTILS EXTERNES

Kaspersky Administration Kit permet de configurer une liste des outils externes : des applications qui seront appelées pour le poste client depuis la Console d'administration à l'aide du groupe du menu contextuel **Outils externes**. Pour chaque outil de la liste, une commande de menu est créée, ce qui permet à la console d'administration de lancer l'application qui correspond à l'outil.

L'application est lancée sur le poste de travail de l'administrateur : sur l'ordinateur où la Console d'administration est installée. L'application peut accepter en guise d'arguments de la ligne de commande les attributs du poste client distant (nom NetBIOS, nom DNS, adresse IP). La connexion à l'ordinateur peut être exécutée à l'aide d'une connexion en tunnel spécialement ouverte.

Par défaut, la liste des outils externes contient les services suivants pour chaque poste client :

- **Diagnostic à distance** : utilitaire de diagnostic à distance Kaspersky Administration Kit.
- **Bureau distant** : composant standard de Windows "Connexion en cours au poste de travail distant".
- **Administration de l'ordinateur** : composant Windows standard.

Vous pouvez ajouter ou supprimer des outils externes ainsi que modifier leurs paramètres à l'aide des boutons **Ajouter**, **Supprimer** et **Modifier**.

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).

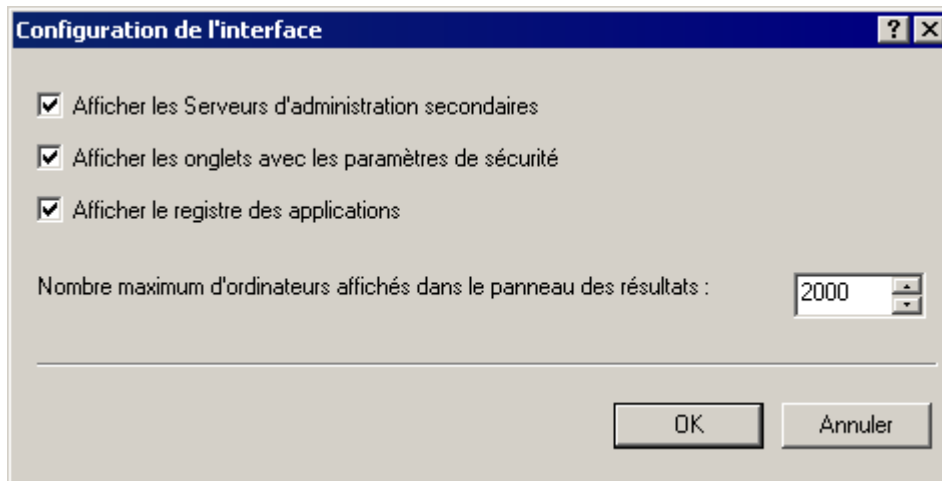


Illustration 270. Affichage des propriétés du groupe. Fenêtre **Configuration de l'interface**

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.

AIDE

Les tableaux de cette rubrique reprennent des informations sur les éléments du menu contextuel des objets de la Console d'administration, des objets du panneau des résultats ainsi que des informations sur la valeur des états des objets du réseau et des groupes d'administration.

DANS CETTE SECTION

Menu contextuel.....	325
Panneau des résultats.....	327
Etats des ordinateurs, des tâches et des stratégies.....	333

MENU CONTEXTUEL

Le tableau ci-après contient une liste des objets de la Console d'administration et la sélection des commandes du menu contextuel qui leur correspond.

Tableau 3. Eléments du menu contextuel des entrées de la Console d'administration

OBJET	ELEMENT	FONCTION DE LA COMMANDE
Points généraux du menu contextuel	Actualiser	Renouveler l'objet sélectionné.
	Exporter la liste	Exporter la liste courante dans le fichier.
	Propriétés	Ouvrir la fenêtre des propriétés de l'objet sélectionné.
Kaspersky Administration Kit	Générer → Serveur d'administration	Ajouter un Serveur d'administration à l'arborescence de la console.
<Nom du Serveur d'administration>	Connecter au Serveur d'administration	Connecter au Serveur d'administration.
	Déconnecter du Serveur d'administration	Déconnecter du Serveur d'administration.
	Installer une application	Exécuter l'Assistant d'installation à distance.
	Recherche	Ouvrir la fenêtre de recherche d'ordinateurs.
	Vue → Configuration de l'interface	Modifier les paramètres de l'interface.
	Supprimer	Supprimer le Serveur d'administration de l'arborescence de la console.
Ordinateurs administrés	Installer une application	Créer et lancer une tâche d'installation à distance pour un groupe.
	Recherche	Recherche d'ordinateurs, de groupes et de Serveurs d'administration qui vérifient le critère spécifié.
	RAZ compteur de virus	Réinitialiser le compteur de virus des hôtes de groupes.
	Activité virale	Créer le rapport d'activité virale des postes clients, qui font partie du groupe.
	Générer → Groupe	Créer le groupe d'administration.


OBJET	ELEMENT	FONCTION DE LA COMMANDE
	Toutes les tâches → Créer la structure du groupe	Créer la structure des groupes sur la base de la structure des domaines ou d'Active Directory.
	Toutes les tâches → Forcer la synchronisation	Forcer la synchronisation pour les ordinateurs qui font partie du groupe d'administration.
	Toutes les tâches → Afficher le message	Afficher le message à l'utilisateur.
Ordinateurs administrés → Stratégies	Importer	Importer une stratégie depuis un fichier.
	Générer → Stratégie	Créer une stratégie.
	Toutes les tâches → Importer	Importer une stratégie depuis un fichier.
	Vue → Stratégies héritées	Afficher les stratégies héritées dans le panneau des résultats.
Ordinateurs administrés → Tâches de groupe	Générer → Tâche	Créer une tâche de groupe.
	Toutes les tâches → Importer	Importer une tâche depuis un fichier.
	Vue → Tâches héritées	Afficher les tâches de groupe héritées dans le panneau des résultats.
Ordinateurs administrés → Postes clients	Générer → Ordinateur	Ajouter un poste client dans un groupe.
Ordinateurs administrés → Serveurs d'administration	Vue → Serveur d'administration	Passer au Serveur d'administration principal.
Rapports et notifications	Générer → Rapport	Créer un modèle de rapport.
Tâches de Kaspersky Administration Kit	Générer → Tâche	Créer une tâche effectuée uniquement par le Serveur d'administration.
	Toutes les tâches → Importer	Importer une tâche depuis un fichier.
Tâches pour les sélections d'ordinateurs	Générer → Tâche	Créer une tâche pour les sélections aléatoires des postes clients.
	Toutes les tâches → Importer	Importer une tâche depuis un fichier.
Requêtes d'événements et d'ordinateurs → Sélections d'ordinateurs	Générer → Nouvelle requête	Créer une requête pour la recherche d'ordinateurs.
	Toutes les tâches → Importer	Importer une tâche depuis un fichier.
Requêtes d'événements → Evénements	Générer → Nouvelle requête	Créer une requête pour la recherche d'ordinateurs.
	Toutes les tâches → Importer	Importer une sélection depuis un fichier.


OBJET	ELEMENT	FONCTION DE LA COMMANDE
Ordinateurs non définis	Recherche	Recherche d'ordinateurs, de groupes et de Serveurs d'administration qui vérifient le critère spécifié.
Ordinateurs non définis → Domaines	Toutes les tâches → Activité des ordinateurs	Configurer les paramètres de la réaction du Serveur d'administration à la recherche d'activité d'ordinateurs dans le réseau.
Ordinateurs non définis → Active Directory	Vue → Rechercher un ordinateur	Recherche d'un ordinateur situé dans la division Active Directory.
Ordinateurs non définis → Plages IP	Générer → Plage IP	Ajouter une plage IP dans le réseau.
Stockages → Paquets d'installation	Générer → Paquet d'installation	Créer un paquet d'installation.
Stockages → Mises à jour	Télécharger les mises à jour	Lancer la récupération des mises à jour par le Serveur d'administration.
	Paramètres de mise à jour	Configurer les paramètres de la tâche de récupération des mises à jour par le Serveur d'administration.
	Rapport de versions de base	Créer et importer le rapport de versions des bases.
	Toutes les tâches → Purger le stockage des mises à jour	Purger le référentiel des mises à jour sur le Serveur d'administration.
Stockages → Licences	Ajouter une licence	Installer une nouvelle licence.
	Rapport de licences	Créer et consulter le rapport de licences installées sur les postes clients.
	Installer une licence	Créer une tâche d'installation d'une nouvelle licence pour une application de Kaspersky Lab administrée par Kaspersky Administration Kit.



PANNEAU DES RESULTATS



Le tableau ci-après contient une liste des objets de la Console d'administration et des colonnes qui leur correspondent dans le panneau des résultats standards.



Tableau 4. Eléments du panneau des résultats

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
Ordinateurs administrés	Nom	Noms des dossiers, intégrés dans le dossier Ordinateurs administrés .
Ordinateurs administrés → Stratégies	Nom	Nom de la stratégie.
	Etat	Etat de la stratégie. Si la stratégie est active, la valeur Active est affichée. Si la stratégie est inactive, alors le champ est vide.
	Application	Nom de l'application pour laquelle la stratégie a été créée.
	Héritée	Nom du groupe duquel la stratégie a été héritée. Si la stratégie n'est pas héritée, le champ est vide. L'icône  apparaît à côté du nom d'une

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
		stratégie héritée.
	Modifiée	Date et heure de la dernière modification des paramètres de la stratégie.
Ordinateurs administrés → Tâches de groupe	Nom	Nom de tâche.
	Type de tâche	Type de tâche.
	Application	Nom de l'application pour laquelle la tâche a été créée.
	Modifiée	Date et heure de la dernière modification des paramètres de la tâche.
	En exécution	Nombre d'ordinateurs sur lesquels la tâche est exécutée.
	Terminée	Nombre d'ordinateurs sur lesquels la tâche est terminée.
	Terminée avec une erreur	Nombre d'ordinateurs sur lesquels l'exécution de la tâche s'est soldée sur une erreur.
	En attente d'exécution	Nombre d'ordinateurs sur lesquels la tâche attend d'être exécutée.
	Suspendu(e)	Nombre d'ordinateurs sur lesquels la tâche est suspendue.
	Héritée	Nom du groupe duquel la tâche a été héritée. Si la tâche n'est pas héritée, le champ est vide. L'icône  apparaît à côté du nom d'une tâche héritée.
Ordinateurs administrés → Postes clients	Nom	Nom de l'ordinateur (nom NETBIOS ou adresse IP de l'ordinateur).
Ordinateurs administrés → Serveurs d'administration	Nom	Nom de l'ordinateur (nom NETBIOS ou adresse IP de l'ordinateur).
Rapports et notifications	Nom	Nom du rapport ou de la notification.
Tâches de Kaspersky Administration Kit	Nom	Nom de tâche.
	Type de tâche	Type de tâche.
	Application	Nom de l'application pour laquelle la tâche a été créée.
	Modifiée	Date et heure de la dernière modification des paramètres de la tâche.
	En attente d'exécution	Nombre d'ordinateurs sur lesquels la tâche attend d'être exécutée.
	Suspendu(e)	Nombre d'ordinateurs sur lesquels la tâche est suspendue.
	En exécution	Nombre d'ordinateurs sur lesquels la tâche est exécutée.
	Terminée	Nombre d'ordinateurs sur lesquels la tâche est terminée.
	Terminée avec une erreur	Nombre d'ordinateurs sur lesquels l'exécution de la tâche s'est soldée sur une erreur.

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
Tâches pour les sélections d'ordinateurs	Nom	Nom de tâche.
	Type de tâche	Type de tâche.
	Application	Nom de l'application pour laquelle la tâche a été créée.
	Modifiée	Date et heure de la dernière modification des paramètres de la tâche.
	En attente d'exécution	Nombre d'ordinateurs sur lesquels la tâche attend d'être exécutée.
	Suspendu(e)	Nombre d'ordinateurs sur lesquels la tâche est suspendue.
	En exécution	Nombre d'ordinateurs sur lesquels la tâche est exécutée.
	Terminée	Nombre d'ordinateurs sur lesquels la tâche est terminée.
	Terminée avec une erreur	Nombre d'ordinateurs sur lesquels l'exécution de la tâche s'est soldée sur une erreur.
Extraction des événements et des ordinateurs	Nom	Nom de la sélection.
Ordinateurs non définis → Domaines	Nom	Nom de l'ordinateur (nom NETBIOS ou adresse IP de l'ordinateur).
	Type de S.E.	Nom du système d'exploitation installé sur le poste. En fonction du type de système d'exploitation, une des icônes suivantes apparaît à côté du nom de l'ordinateur :  – pour un serveur,  – pour une station de travail.
	Domaine	Domaine Windows ou groupe de travail auquel appartient l'ordinateur.
	Agent/Antivirus	Etat des applications installées sur l'ordinateur. Pour l'agent réseau ou l'application antivirus dont l'administration est possible via Kaspersky Administration Kit, l'icône "+" (plus) apparaît s'il est installé sur l'ordinateur. Si les applications ne sont pas installées, le signe "-" (moins) apparaît.
	Visible	Date à laquelle l'ordinateur a été observé pour la dernière fois par le Serveur dans le réseau.
	Heure de dernière mise à jour	Date de la dernière mise à jour des bases ou des applications sur l'ordinateur.
	Etat	Etat actuel de l'ordinateur (<i>OK/Avertissement/Critique</i>), octroyé sur la base de critères définis par l'administrateur. Les parenthèses reprennent la condition qui a donné cet état.
	Description de l'état	La raison, pourquoi tel ou tel état était attribué au poste client.

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
	Mise à jour d'information	Date de la dernière mise à jour des informations relatives à l'ordinateur sur le Serveur d'administration.
	Nom DNS	Nom DNS de l'ordinateur.
	Adresse IP	Adresse IP de l'ordinateur.
	Connexion avec le Serveur	Heure de la dernière connexion de l'Agent d'administration installé sur le poste client avec le Serveur d'administration.
Ordinateurs non définis → Active Directory	Nom	Nom de l'ordinateur (nom NETBIOS ou adresse IP de l'ordinateur).
	Type de S.E.	Nom du système d'exploitation installé sur le poste. En fonction du type de système d'exploitation, une des icônes suivantes apparaît à côté du nom de l'ordinateur :  – pour un serveur,  – pour une station de travail.
	Domaine	Domaine Windows ou groupe de travail auquel appartient l'ordinateur.
	Agent/Antivirus	Etat des applications installées sur l'ordinateur. Pour l'agent réseau ou l'application antivirus dont l'administration est possible via Kaspersky Administration Kit, l'icône "+" (plus) apparaît s'il est installé sur l'ordinateur. Si les applications ne sont pas installées, le signe "-" (moins) apparaît.
	Visible	Date à laquelle l'ordinateur a été observé pour la dernière fois par le Serveur dans le réseau.
	Heure de dernière mise à jour	Date de la dernière mise à jour des bases ou des applications sur l'ordinateur.
	Etat	Etat actuel de l'ordinateur (<i>OK/Avertissement/Critique</i>), octroyé sur la base de critères définis par l'administrateur. Les parenthèses reprennent la condition qui a donné cet état.
	Description de l'état	La raison, pourquoi tel ou tel état était attribué au poste client.
	Mise à jour d'information	Date de la dernière mise à jour des informations relatives à l'ordinateur sur le Serveur d'administration.
	Nom DNS	Nom DNS de l'ordinateur.
	Adresse IP	Adresse IP de l'ordinateur.
	Connexion avec le Serveur	Heure de la dernière connexion de l'Agent d'administration installé sur le poste client avec le Serveur d'administration.

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
Ordinateurs non définis → Plages IP	Nom	Nom de l'ordinateur (nom NETBIOS ou adresse IP de l'ordinateur).
	Type de S.E.	Nom du système d'exploitation installé sur le poste. En fonction du type de système d'exploitation, une des icônes suivantes apparaît à côté du nom de l'ordinateur :  – pour un serveur,  – pour une station de travail.
	Domaine	Domaine Windows ou groupe de travail auquel appartient l'ordinateur.
	Agent/Antivirus	Etat des applications installées sur l'ordinateur. Pour l'agent réseau ou l'application antivirus dont l'administration est possible via Kaspersky Administration Kit, l'icône "+" (plus) apparaît s'il est installé sur l'ordinateur. Si les applications ne sont pas installées, le signe "-" (moins) apparaît.
	Visible	Date à laquelle l'ordinateur a été observé pour la dernière fois par le Serveur dans le réseau.
	Heure de dernière mise à jour	Date de la dernière mise à jour des bases ou des applications sur l'ordinateur.
	Etat	Etat actuel de l'ordinateur (<i>OK/Avertissement/Critique</i>), octroyé sur la base de critères définis par l'administrateur. Les parenthèses reprennent la condition qui a donné cet état.
	Description de l'état	La raison, pourquoi tel ou tel état était attribué au poste client.
	Mise à jour d'information	Date de la dernière mise à jour des informations relatives à l'ordinateur sur le Serveur d'administration.
	Nom DNS	Nom DNS de l'ordinateur.
	Adresse IP	Adresse IP de l'ordinateur.
	Connexion avec le Serveur	Heure de la dernière connexion de l'Agent d'administration installé sur le poste client avec le Serveur d'administration.
Stockages → Paquets d'installation	Nom	Nom du paquet d'installation.
	Application	Application pour qui le paquet d'installation est destiné.
	Numéro de version	Numéro de version d'installation.
Stockages → Mises à jour	Nom	Nom de la mise à jour.
	Description	Description de la mise à jour.
	Date de création	Date de publication des bases de Kaspersky Lab.
	Reçu	Date de réception de la mise à jour du Serveur d'administration.



















OBJET	COLONNE	DESCRIPTION DE LA COLONNE
	Taille	Taille de la mise à jour reçue.
Stockages → Licences	Numéro de série	Numéro de la licence.
	Type	Type de la licence installée (par exemple, commerciale ou démonstration).
	Limite	Limites définies par la licence (par exemple, nombre d'ordinateurs sur lesquels la licence peut être installée).
	Durée de validité	Durée de validité de la licence.
	Date d'expiration	Date d'expiration de validité de la licence.
	Application	Application pour qui la licence est activée.
	Active	Le nombre d'ordinateurs pour lesquels la licence est active.
	Complémentaire	Le nombre d'ordinateurs pour lesquels la licence est complémentaire.
	A propos du client	Information sur le propriétaire, prise du fichier de la clé.
Stockages → Quarantaine	Ordinateur	Poste client sur lequel l'objet a été découvert.
	Nom	Nom du fichier placé en quarantaine.
	Etat	Etat de l'objet attribué par le logiciel antivirus.
	Action en cours	Action sélectionnée sur un objet lors du placement en quarantaine.
	Date de placement	Date de placement d'un objet détecté en quarantaine.
	Nom du virus	Nom de la menace telle qu'elle apparaît dans l'Encyclopédie des virus de Kaspersky Lab.
	Description	Description du fichier, indiqué par l'utilisateur.
	Chemin de restauration	Dossier, où le fichier se trouvait avant d'être placé en quarantaine.
	Utilisateur	Utilisateur qui a placé le fichier en quarantaine.
	Taille	Taille du fichier.
Stockages → Dossier de sauvegarde	Ordinateur	Poste client sur lequel l'objet a été découvert.
	Nom	Nom du fichier placé en quarantaine.
	Etat	Etat de l'objet attribué par le logiciel antivirus.
	Action en cours	Action sélectionnée sur un objet lors du placement en quarantaine.
	Date de placement	Date de placement d'un objet détecté en quarantaine.

OBJET	COLONNE	DESCRIPTION DE LA COLONNE
	Nom du virus	Nom de la menace telle qu'elle apparaît dans l'Encyclopédie des virus de Kaspersky Lab.
	Description	Description du fichier, indiqué par l'utilisateur.
	Chemin de restauration	Dossier, où le fichier se trouvait avant d'être placé dans la Dossier de sauvegarde.
	Utilisateur	Utilisateur qui a placé le fichier dans la Dossier de sauvegarde.
	Taille	Taille du fichier.
Stockages → Fichiers avec un traitement différé	Ordinateur	Poste client sur lequel l'objet a été découvert.
	Nom	Nom du fichier placé en quarantaine.
	Etat	Etat de l'objet attribué par le logiciel antivirus.
	Action en cours	Action sélectionnée sur un objet lors du placement en quarantaine.
	Date de placement	Date de placement d'un objet détecté en quarantaine.
	Nom du virus	Nom de la menace telle qu'elle apparaît dans l'Encyclopédie des virus de Kaspersky Lab.
	Description	Description du fichier, indiqué par l'utilisateur.
	Chemin de restauration	Dossier, où le fichier se trouvait avant d'être placé dans le dossier Fichiers avec un traitement différé.
	Utilisateur	Utilisateur qui a placé le fichier dans le dossier Fichiers avec un traitement différé .
	Taille	Taille du fichier.

ÉTATS DES ORDINATEURS, DES TACHES ET DES STRATEGIES

Le tableau ci-après reprend la liste des icônes qui apparaissent dans l'arborescence de la console et dans le panneau des résultats de la Console d'administration à côté des noms des postes clients, des tâches et des stratégies. Ces icônes définissent l'état des objets.

Tableau 5. Etats des ordinateurs, des tâches et des stratégies

ICONE	ETAT
	Ordinateur avec un système d'exploitation pour poste de travail a été découvert dans le réseau mais n'appartient à aucun groupe d'administration.
	Ordinateur avec un système d'exploitation pour poste de travail, appartenant à un groupe d'administration et correspondant à l'état <i>Avertissement</i> .
	Ordinateur avec un système d'exploitation pour poste de travail, appartenant à un groupe d'administration et correspondant à l'état <i>Avertissement</i> .
	Ordinateur avec un système d'exploitation pour poste de travail, appartenant à un groupe d'administration et correspondant à l'état <i>Avertissement</i> .
	Ordinateur avec un système d'exploitation pour poste de travail, appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	Ordinateur avec un système d'exploitation pour serveurs a été découvert dans le réseau mais n'appartient à aucun groupe d'administration.
	Ordinateur avec un système d'exploitation pour poste serveurs, appartenant à un groupe d'administration et correspondant à l'état <i>OK</i> .
	Ordinateur avec un système d'exploitation pour poste serveurs, appartenant à un groupe d'administration et correspondant à l'état <i>OK</i> .
	Ordinateur avec un système d'exploitation pour poste serveurs, appartenant à un groupe d'administration et correspondant à l'état <i>OK</i> .
	Ordinateur avec un système d'exploitation pour poste serveurs, appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	La grappe, faisant partie du groupe d'administration, avec l'état <i>OK</i> .
	Stratégie active.
	Stratégie inactive.
	La stratégie active héritée depuis le Serveur d'administration principal.
	Tâche (de groupe, du Serveur d'administration ou pour une sélection d'ordinateurs) dans l'état Planifiée pour ou Terminée .
	Tâche (de groupe, du Serveur d'administration ou pour une sélection d'ordinateurs) dans l'état En exécution .
	Tâche (de groupe, du Serveur d'administration ou pour une sélection d'ordinateurs) dans l'état Terminée avec une erreur .
	La tâche héritée depuis le Serveur d'administration principal.

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)

INDEX

A

Administration	
postes clients	154
stratégies	76
ADMINISTRATION	
GROUPE D'ADMINISTRATION	58
LICENCES	270
SERVEUR D'ADMINISTRATION	22
ADMINISTRATION DE L'APPLICATION	76
Agent d'administration	137
Agents de mise à jour	75, 264
Ajout	
poste client	139
Serveur d'administration	26
Serveur secondaire	54
Assistant de conversion des stratégies et des tâches	97, 126
Attaque de virus	
identification	318
stratégie	321

C

Cisco Network Admission Control	51
Copie de sauvegarde	
tâche	311
utilitaire	314

E

Exportation	
stratégies	96
tâche	124

G

Groupes	
paramètres	68
structure	60

I

Importation	
stratégie	97
tâche	125

K

KASPERSKY LAB	340
---------------------	-----

L

Licence	
diffusion	276
installation	273
rapport	275
réception du fichier clé	275
LICENCE	270

M

Menu contextuel.....	325
Mise à jour	
affichage.....	261
analyse.....	258
diffusion.....	262, 263, 264
réception.....	246
Modèle du rapport	
création.....	179
modification.....	191

N

Notifications.....	207
Notifications	
configuration des paramètres.....	18
limite.....	207

P

Panneaux d'informations	
modification.....	190
Permutation entre les Serveurs.....	26
Plage IP	
création.....	241
modification.....	238, 242
Postes clients	
allumer.....	154
arrêt.....	157
connexion au Serveur.....	167
message à l'utilisateur.....	164
redémarrage.....	160
surveillance.....	72
Protection antivirus.....	288

Q

Quarantaine	
restauration d'un objet.....	281
suppression d'un objet.....	281

R

Rapport	
consultation.....	197
Rapports	
création.....	197
diffusion.....	200
hiérarchie des Serveurs d'administration.....	204
licences.....	275
Requête d'événements	
configuration.....	216
création.....	215
Restriction du trafic.....	53

S

Sélections d'événements	
consultation du journal.....	214
Serveur d'administration.....	54
Serveurs secondaires	
affichage.....	56
ajout.....	54
configuration.....	55

Sondage	
groupes Active Directory.....	237
plages IP.....	238
réseau Windows.....	235
Sondage de réseau.....	234
Statistiques.....	182, 183
STOCKAGE	
LICENCES.....	270
Stockages	
dossier de sauvegarde.....	280
paquets d'installation.....	277
quarantaine.....	280
registre des applications.....	283
STOCKAGES	
MISE A JOUR.....	246
Stratégie	
création.....	76
Stratégies	
activation.....	84
configuration des paramètres.....	79
copie.....	87
exportation.....	96
importation.....	97
suppression.....	87
utilisateurs nomades.....	289
Suppression	
objet.....	281
Serveur d'administration.....	29
stratégie.....	87
T	
Tâches	
administration des postes clients.....	154
affichage de l'historique.....	128
copie de sauvegarde.....	311
de groupe.....	101
diffusion des rapports.....	200
exécution.....	127
exportation.....	124
importation.....	125
installation d'une licence.....	273
locales.....	115
modification du Serveur d'administration.....	151
sélection d'ordinateurs.....	101
Serveurs d'administration.....	101
Tâches de groupe	
filtre.....	129
héritage.....	123
U	
Utilisateurs nomades	
conditions de permutation.....	294
profil.....	290
règles de permutation.....	293
V	
Volets d'informations	
création.....	186