Kaspersky Security 8.0 for SharePoint Server

Manuel d'administrateur

VERSION DE L'APPLICATION : 8.0

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (puis dans le texte 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, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois de la France.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

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

Ce document peut être modifié sans un avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.ru/fr/docs.

Kaspersky Lab ne pourra être tenue 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. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Date d'édition : 13/01/2012

© 2012 Kaspersky Lab ZAO

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

TABLE DES MATIERES

PRESENTATION DU GUIDE 6
Dans ce document 6
Conventions 7
SOURCES D'INFORMATIONS SUR L'APPLICATION 9
Sources d'informations pour une aide autonome 9
Discussion sur les logiciels de Kaspersky Lab sur le forum 10
Contacter le service des ventes 10
Département localisation et élaboration de la documentation technique 10
KASPERSKY SECURITY 8.0 FOR SHAREPOINT SERVER 11
Configurations logicielles et matérielles 11
LICENCE DE L'APPLICATION 13
Présentation du contrat de licence 13
Présentation de la licence 13
Présentation du fichier de licence 14
Administration des clés dans Kaspersky Security 14
Obtention d'informations sur la clé 15
Ajout d'une clé 16
Remplacement d'une clé 16
Suppression d'une clé 17
Notification sur l'expiration de la durée de validité de la licence 17
INTERFACE DE L'APPLICATION 18
Fenêtre principale 18
LANCEMENT DE L'APPLICATION 20
ETAT DE LA PROTECTION PAR DEFAUT 21
PREMIERE UTILISATION 22
Lancement de la Console d'administration 22
Connexion de la console d'administration au serveur 22
Activation et désactivation de la protection antivirus et du filtrage de contenu 23
MISE A JOUR DES BASES 24
Présentation de la mise à jour des bases 24
Consultation des informations sur la mise à jour des bases antivirus 25
Mise à jour automatique des bases 26
Configuration des paramètres locaux de la mise à jour sur les serveurs de la ferme 27
Diffusion des paramètres globaux de la mise à jour des bases 27
Sélection de la source de la mise à jour 28
Configuration des paramètres de connexion 28
ANALYSE AU MOMENT DE L'ACCES 30
A propos de l'analyse au moment de l'accès 30
Fonctionnement de Kaspersky Security suivant les paramètres du serveur SharePoint 30
Paramètres de l'analyse au moment de l'accès 31
Configuration des paramètres généraux de l'analyse au moment de l'accès 32
Configuration des règles de traitement des objets lors de l'analyse au moment de l'accès 33

Création d'exclusions de l'analyse au moment de l'accès 35
Paramètres du filtrage de contenu 37
Paramètres de détermination du contenu indésirable 37
Création d'exclusions du filtrage de contenu 39

ANALYSE A LA DEMANDE 40
A propos de l'analyse à la demande 40
Lancement et arrêt de la tâche d'analyse à la demande 41
Visualisation du rapport relatif à l'analyse à la demande 42
Paramètres de la tâche d'analyse à la demande 42
Sélection du serveur pour lancer la tâche 43
Configuration des paramètres généraux d'une tâche d'analyse à la demande 43
Création de la planification du lancement de la tâche d'analyse à la demande 45
Configuration des règles de traitement des objets lors de l'analyse à la demande 46
Sélection des zones d'analyse 47
Définition des domaines de SharePoint en mode manuel 49
Création d'exclusions de l'analyse à la demande 49
Paramètres du filtrage de contenu 51
Création d'une nouvelle tâche d'analyse à la demande 51
Suppression de la tâche d'analyse à la demande 52

FILTRAGE DE CONTENU 53
A propos du filtrage de contenu 53
Paramètres du filtrage de contenu 53
Configuration des catégories d'utilisateurs de mots et expressions indésirables 54
Modification des mots et expressions inclus dans le contenu des catégories d'utilisateurs 55
Importation d'une liste de mots et d'expressions indésirables 56
Utilisation des symboles dans les mots et les phrases au nombre des catégories d'utilisateurs 56
Masques des noms de fichiers indésirables 57
Modification de l'ensemble de masques des noms de fichiers indésirables 58
Utilisation des masques des noms de fichiers indésirables 59

ESPACE DE SAUVEGARDE 60
A propos de l'Espace de sauvegarde 60
Actions sur les objets placés dans l'Espace de sauvegarde 61
Consultation de la liste des objets placés dans l'Espace de sauvegarde 61
Recherche des objets dans l'Espace de sauvegarde 64
Recherche des objets dans l'Espace de sauvegarde : recherche rapide 64
Recherche des objets dans l'Espace de sauvegarde : filtre avancé 66
Restauration des objets de la Espace de sauvegarde 68
Restauration de fichiers du même nom 69
Enregistrement des objets placés dans l'Espace de sauvegarde sur le disque 70
Suppression des fichiers de la Espace de sauvegarde 71
Nettoyage de l'Espace de sauvegarde 72

NOTIFICATIONS 73
A propos des notifications 73
Paramètres des notifications sur les événements liés aux clés 73
Paramètres des notifications sur les infractions aux stratégies de protection 74
Paramètres de notifications des événements système 74

RAPPORTS 76
Présentation des rapports....76
Tâches de composition des rapports....76
Lancement de la tâche sélectionnée de composition des rapports....77
Configuration des paramètres de tâche de composition des rapports 77
Création d'une nouvelle tâche de composition des rapports....78
Suppression d'une tâche de composition des rapports....78
Consultation des rapports prêts....78
Création de rapports rapides 78
Envoi des rapports par courrier électronique 79
CONFIGURATION DES PARAMETRES DU FONCTIONNEMENT DE L'APPLICATION 80
Configuration des paramètres d'envoi des messages électroniques 80
Configuration des paramètres de diagnostic 81
Configuration des paramètres de l'Espace de sauvegarde 81
CONTACTER LE SUPPORT TECHNIQUE 82
Modes d'obtention d'une assistance technique 82
Assistance technique par téléphone....82
Obtention d'une assistance technique via votre espace personnel 82
Utilisation du fichier de trace et du script AVZ 83
INFORMATIONS SUR LE CODE TIERS....85
GLOSSAIRE 86
KASPERSKY LAB ZAO 88
NOTIFICATIONS SUR LES MARQUES COMMERCIALES 89
INDEX 90

PRESENTATION DU GUIDE

Ce document présente le Guide de l'administrateur de Kaspersky Security.

Le guide est destiné aux techniciens, responsables de l'installation et de l'administration de Kaspersky Security, à l'assistance des entreprises, utilisant Kaspersky Security.

Ce guide poursuit les objectifs suivants :

- Fournir une aide pour configurer et utiliser Kaspersky Security.
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

Dans ce document 6

Conventions 7

DANS CE DOCUMENT

Le Manuel de l'administrateur de Kaspersky Security 8.0 pour SharePoint® Server comprend les chapitres suivants :

- A propos de ce manuel (à la page 6). Le chapitre décrit la structure du Manuel d'administrateur.
- Sources d'informations sur l'application (à la page 9). Le chapitre décrit différentes sources d'informations sur l'acquisition, l'installation et l'utilisation de Kaspersky Security.
- Kaspersky Security 8.0 for SharePoint Server (à la page 11). Le chapitre décrit les fonctions de base de l'application.
- Licence de l'application (à la page 13). Le chapitre décrit les types de licences et la procédure d'installation, remplacement et suppression de clés.
- Interface de l'application (à la page 18). Le chapitre décrit l'interface utilisateur de Kaspersky Security.
- Lancement de l'application (à la page 20). Le chapitre reprend les informations sur le lancement et l'arrêt de l'application.
- Etat de la protection par défaut (à la page 21). Le chapitre détaille les caractéristiques de fonctionnement de Kaspersky Security avec les paramètres par défaut.
- Première utilisation (à la page 22). Le chapitre reprend les informations sur la première utilisation de Kaspersky Security, l'activation de la protection du serveur de messagerie et la création de la liste des serveurs protégés.
- Mise à jour des bases (à la page 24). Le chapitre détaille la configuration des paramètres de la mise à jour des bases de Kaspersky Security.
- Analyse au moment de l'accès (à la page 30). Le chapitre décrit la procédure d'analyse des documents lorsqu'ils sont envoyés vers le serveur SharePoint ou téléchargés sur l'ordinateur depuis le serveur.

- Analyse à la demande (à la page 40). Le chapitre reprend les informations sur l'analyse à la demande des documents stockés sur le serveur SharePoint.
- Filtrage de contenu (à la page 53). Le chapitre décrit la configuration des paramètres du filtrage de contenu.
- Espace de sauvegarde (à la page 60). Le chapitre décrit les fonctions de l'Espace de sauvegarde, les modes de restauration des objets de l'Espace de sauvegarde, ainsi que la configuration des paramètres de l'Espace de sauvegarde.
- Notifications (à la page 73). Le chapitre décrit les modes de réception de notifications sur les évènements de Kaspersky Security.
- Rapport (à la page 76). Le chapitre reprend les informations sur la création et la consultation des rapports dans l'application, ainsi que sur leur réception par courrier électronique.

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Ils comportent des informations sur les actions indésirables éventuelles susceptibles d'entraîner une perte de données, ainsi que des dysfonctionnements de l'équipement ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les annotations contiennent de l'aide et des renseignements. Les remarques peuvent contenir des conseils utiles, des recommandations, des paramètres importants ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés dans les blocs sous le titre "Exemple".
La *mise à jour*, c'est... L'événement *Bases dépassées* se présente.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **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. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
➡ *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
Dans la ligne de commande, saisissez le texte: `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants du texte apparaissent dans un style spécial (Courier) : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<Nom d'utilisateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace celle-ci dans chaque cas. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

Sources d'informations pour une aide autonome 9

Discussion sur les logiciels de Kaspersky Lab dans le forum 10

Contacter le service des ventes 10

Département localisation et élaboration de la documentation technique 10

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du support technique (base de connaissances) ;
- aide électronique ;
- documentation.

Vous ne trouvez pas la réponse à votre question, il est recommandé de contacter le "Support technique de Kaspersky Lab" (cf. la rubrique "Assistance technique par téléphone" à la page 82).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

Page du site de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page particulière pour chaque application.

La page (http://www.kaspersky.com/fr/security-sharepoint) fournit des informations générales sur l'application, ces possibilités et ses particularités.

Page sur le site du support technique (banque de solutions)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/servers/kssp) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur l'assistance technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle contient des informations sur chaque fenêtre de l'application, à savoir la liste et la description des paramètres, ainsi que des liens vers les tâches dans lesquelles ces paramètres sont utilisés.

L'aide complète contient des informations sur la gestion de la protection, sur la configuration des paramètres de l'application et sur la résolution des problèmes principaux de l'utilisateur.

Documentation

La distribution de l'application comprend la documentation qui vous permet d'installer, d'activer l'application sur les ordinateurs de l'entreprise et de configurer les paramètres de fonctionnement ainsi que de recevoir des informations sur l'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications sur notre forum (http://forum.kaspersky.com).

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

CONTACTER LE SERVICE DES VENTES

Pour toute question sur le choix, sur l'acquisition ou sur le renouvellement du délai d'utilisation de l'application, vous pouvez vous adresser à nos spécialistes du service des ventes par l'un des moyens suivants :

- En téléphonant à notre siège principal à Moscou. (http://www.kaspersky.com/fr/contacts).
- En envoyant une question par courrier électronique.

Le service est assuré en russe et en anglais.

DEPARTEMENT LOCALISATION ET ELABORATION DE LA DOCUMENTATION TECHNIQUE

Si vous avez des questions concernant la documentation de l'application, vous pouvez vous adresser aux experts du Groupe chargé de l'élaboration de la documentation. Vous pouvez par exemple envoyer une partie de la documentation à nos experts.

KASPERSKY SECURITY 8.0 FOR SHAREPOINT SERVER

Kaspersky Security 8.0 for SharePoint Server est une application qui protège les serveurs Microsoft® SharePoint Server contre les objets malveillants et le contenu indésirable.

Kaspersky Security permet d'effectuer les actions suivantes :

- Analyser à la demande les documents placés sur le serveur SharePoint pour détecter d'éventuels objets malveillants et le contenu indésirable. En fonction des paramètres sélectionnés, Kaspersky Security répare ou supprime les documents infectés ou le contenu indésirable.
- Analyser les documents au moment de l'accès. Kaspersky Security analyse les documents pour détecter d'éventuels objets malveillants et le contenu indésirable lorsque l'utilisateur essaie d'envoyer le document sur le serveur ou de le télécharger du serveur vers l'ordinateur. Les règles de traitement des documents où les objets malveillants ou le contenu indésirable ont été découverts varient en fonction des paramètres définis du serveur SharePoint.
- Analyser à la demande les éléments des listes SharePoint pour détecter un contenu indésirable éventuel.
- Définir les zones de la structure du serveur SharePoint à analyser. L'application permet d'exclure des zones de l'analyse afin de réduire la charge du serveur.
- Configurer les règles de traitement des documents où les objets malveillants ou le contenu indésirable ont été découverts.
- Stocker les copies de sauvegarde des documents avant leur réparation ou suppression dans l'Espace de sauvegarde.
- Produire des rapports avec les résultats de l'analyse des documents. Les rapports peuvent être créés automatiquement selon l'horaire défini ou à la demande.
- Mettre à jour des bases de Kaspersky Security en mode automatique ou manuel. Vous pouvez utiliser en tant que sources de la mise à jour des bases les serveurs de mise à jour FTP et HTTP du Kaspersky Lab sur le Web ou un dossier local / réseau avec une sélection de dernières versions des mises à jour, ainsi que les serveurs d'utilisateur FTP et HTTP.
- Administration des clés.

DANS CETTE SECTION

Configurations logicielles et matérielles 11

CONFIGURATIONS LOGICIELLES ET MATERIELLES

Configuration matérielle

La configuration matérielle de Kaspersky Security est celle de Microsoft SharePoint Server. En fonction des paramètres de l'application et du mode de son utilisation, vous pouvez avoir besoin d'un espace disque considérable pour l'Espace de sauvegarde et les autres dossiers du service.

Configuration logicielle

L'installation de Kaspersky Security nécessite un des systèmes d'exploitation suivants :

- Pour SharePoint® Server 2007 x86/x64 :

  Windows Server® 2003/Windows Server 2003 x64/Windows Server 2003 R2/Windows Server 2003 R2 x64/Windows Server 2008 /Windows Server 2008 x64/Windows Server 2008 R2.

- Pour SharePoint Server 2010 :

  Windows Server 2008 x64/Windows Server 2008 R2.

Pour réussir l'installation, les composants suivants sont requis :

- Microsoft SharePoint Server 2007 ou Microsoft SharePoint 2010 ;

  Pour installer uniquement la Console d'administration, Microsoft SharePoint Server n'est pas nécessaire.

- Microsoft .NET Framework 3.5 Service Pack 1 ;
- Microsoft Management Console 3.0.

L'installation de la seule console d'administration nécessite un des systèmes d'exploitation suivants :

- Windows Server 2003 ;
- Windows Server 2003 x64 ;
- Windows Server 2003 R2 ;
- Windows Server 2003 R2 x64 ;
- Windows Server 2008 ;
- Windows Server 2008 x64 ;
- Windows Server 2008 R2 ;
- Microsoft Windows® XP x64 Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft Windows Vista® Service Pack 2 ;
- Microsoft Windows Vista x64 Service Pack 2 ;
- Windows 7 Professional ;
- Windows 7 Professional x64 ;
- Windows 7 Enterprise ;
- Windows 7 Enterprise x64 ;
- Windows 7 Ultimate ;
- Windows 7 Ultimate x 64.

LICENCE DE L'APPLICATION

Cette section présente les principaux concepts liés à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

DANS CETTE SECTION

Présentation du contrat de licence 13

Présentation de la licence 13

Présentation du fichier de licence 14

Administration des clés dans Kaspersky Security 14

PRESENTATION DU CONTRAT DE LICENCE

Le Contrat de licence est un contrat juridique entre vous et Kaspersky Lab ZAO dans lequel les conditions d'utilisation de l'application sont décrites.

Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.

Vous pouvez faire connaissance avec les conditions du Contrat de licence lors de l'installation de l'application de Kaspersky Lab.

Vous êtes censé accepter les conditions du Contrat de licence en étant d'accord avec le texte du Contrat de licence lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les conditions du Contrat de licence, vous devez interrompre l'installation de l'application.

PRESENTATION DE LA LICENCE

La *licence* est un droit d'utilisation de l'application octroyé pour une durée définie sur la base du Contrat de licence.

La licence inclut le droit de bénéficier des types de services suivants :

- Utilisation de l'application sur un ou plusieurs appareils.

  La quantité d'appareils sur lesquels vous pouvez utiliser l'application est définie par les conditions du Contrat de licence.

- Recours au service d'assistance technique de Kaspersky Lab.
- Accès à l'ensemble des services offerts par Kaspersky Lab.

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite qui permet de prendre connaissance de l'application.

La licence d'évaluation a en général une durée de validité réduite. Une fois que la licence d'évaluation de Kaspersky Security arrive à échéance, toutes les fonctions sont désactivées. Pour pouvoir continuer à utiliser l'application, vous devez acheter une licence commerciale.

- *Commerciale* : licence payante octroyée lors de l'achat de l'application.

  Quand la licence commerciale arrive à échéance, l'application continue à fonctionner, mais avec certaines restrictions. Vous pouvez toujours soumettre les fichiers à une analyse antivirus et utiliser les autres modules de l'application, mais uniquement à l'aide des bases installées avant la date d'expiration de la licence. Pour continuer à utiliser toutes les fonctionnalités de Kaspersky Security, vous devez prolonger la durée de validité de la licence commerciale.

  Il est conseillé de prolonger la durée de validité de la licence au plus tard à la date d'expiration pour que l'appareil nomade bénéficie d'une protection optimale.

PRESENTATION DU FICHIER DE LICENCE

Fichier de licence : fichier xxxxxxxx.key qui permet d'utiliser l'application de Kaspersky Lab selon les conditions de la licence d'évaluation ou commerciale. Kaspersky Lab offre une fichier clé lors de l'achat de Kaspersky Security. Vous ne pouvez pas utiliser l'application sans fichier de clé.

Si le fichier clé a été supprimé par hasard, vous pouvez envoyer une demande au service du Support technique pour le restaurer (cf. la rubrique "Contacter le Support technique" à la page 82).

Le fichier clé contient les informations suivantes :

- La clé est un numéro unique utilisé, par exemple, pour recevoir le support technique de Kaspersky Lab.
- Limite du nombre d'ordinateurs : nombre maximal d'ordinateurs sur lesquels vous pouvez activer l'application à l'aide de ce fichier de licence.
- Durée de validité du fichier de licence : durée définie depuis la création du fichier de licence. Le type d'application dépend de la durée de validité de la licence (cf. la rubrique "Présentation de la licence" à la page 13).
- Date de création du fichier de licence : date de création du fichier clé, utilisée pour le décompte de la durée de validité du fichier de licence.
- Durée de validité de la licence : durée fixée à partir de la création du fichier de licence par les spécialistes de Kaspersky Lab. La durée de validité de la licence peut être autorisée pour plusieurs années. Activation de l'application est possible jusqu'à la fin de cette période.
- Date de fin de validité du fichier de licence : date après laquelle il est impossible d'utiliser le fichier de licence pour activer l'application. La date de fin de validité du fichier de licence est calculée à partir de la date d'utilisation du fichier de licence, en plus de la durée de validité du fichier de licence, mais pas au-delà de la fin de la conservation de la licence.

  Si la date de fin de validité du fichier de licence est antérieure à la fin de validité de la licence, la durée de conservation de la licence est limitée à la date de fin de validité du fichier de licence.

- Informations sur l'assistance technique.

ADMINISTRATION DES CLES DANS KASPERSKY SECURITY

Dans l'application Kaspersky Security, vous pouvez ajouter, modifier ou supprimer les clés d'activation ou complémentaires.

DANS CETTE SECTION

Obtention d'informations sur la clé 15

Ajout d'une clé 16

Remplacement d'une clé 16

Suppression d'une clé 17

Notification sur l'expiration de la durée de validité de la licence 17

OBTENTION D'INFORMATIONS SUR LA CLE

Pour visualiser les informations sur la clé, procédez comme suit :

1. Lancez la Console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le nœud **Licence** dans le nœud du serveur qui vous intéresse (cf. ill. ci-après).

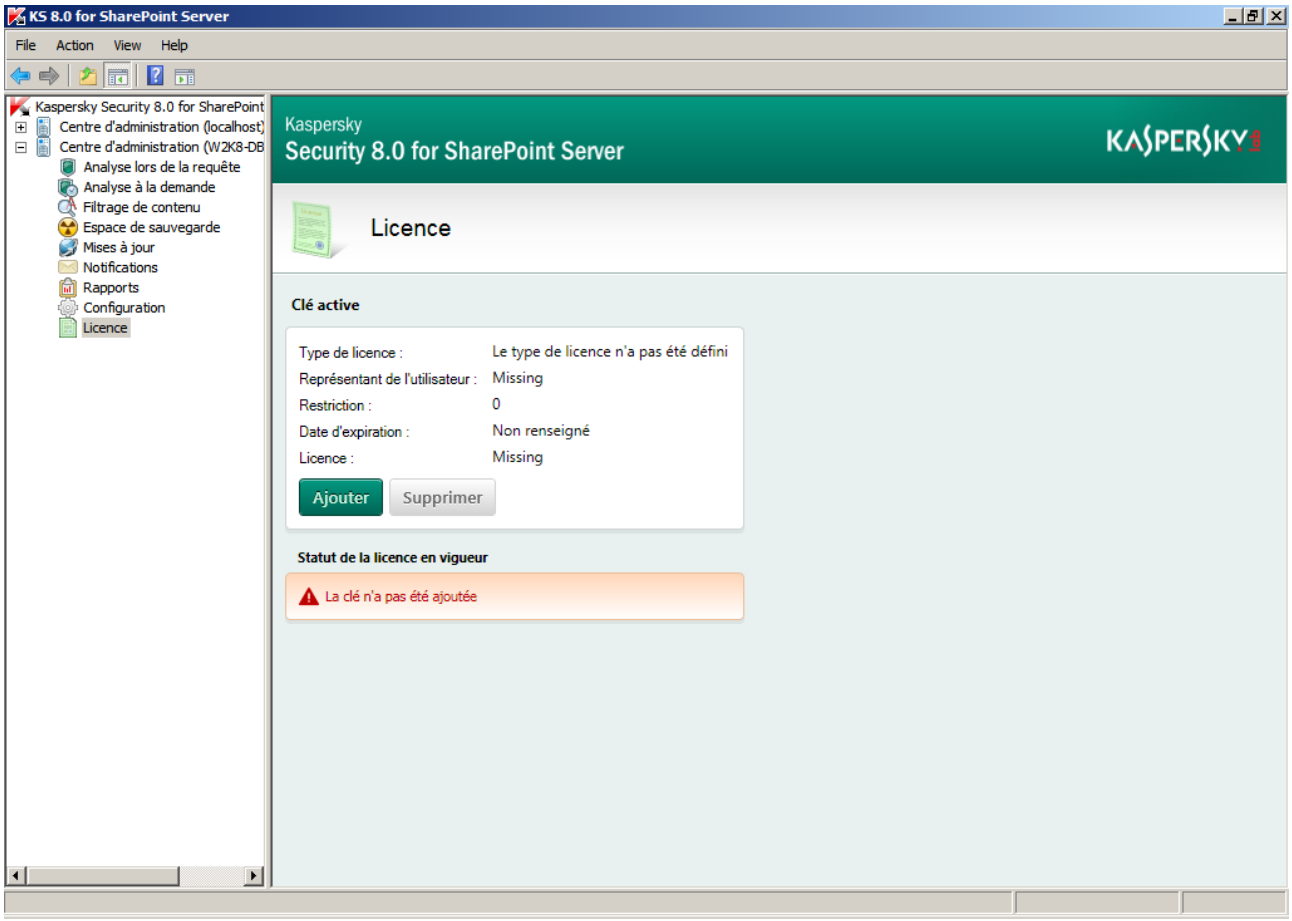

*Figure 1. Nœud **Licence***

Dans le panneau de résultats, vous pouvez visualiser les informations sur les clés ajoutées. Pour l'affichage, les données suivantes sur les clés d'activation et complémentaires sont accessibles :

- **Type de licence**. Description du type de licence.
- **Identificateur de l'utilisateur**. Affiche l'identificateur de l'utilisateur.
- **Restriction**. Indique le nombre autorisé de serveurs protégés.
- **Date d'expiration**. Affiche la date d'expiration de la licence.
- **Clé**. Affiche la clé.

Le tableau contient les informations sur le statut de la clé sur tous les serveurs de la ferme.

Si Kaspersky Security est installé sur le serveur autonome, les informations sur l'état de la clé seront affichées dans le groupe général des données.

AJOUT D'UNE CLE

Pour ajouter une clé Kaspersky Security, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Licence**.
2. Dans le panneau de résultats, cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur le bouton **Ouvrir**.

Toute clé ajoutée à un des serveurs de la ferme est propagée sur la totalité d'entre eux.

Une fois la clé principale ajoutée, vous pouvez ajouter une clé complémentaire.

Pour ajouter une clé complémentaire, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Licence**.
2. Dans le panneau de résultats, dans le groupe **Clé complémentaire**, cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur le bouton **Ouvrir**.

REMPLACEMENT D'UNE CLE

Pour remplacer une clé de Kaspersky Security, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Licence**.
2. Dans le panneau de résultats, cliquez sur le bouton **Remplacer**.
3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur le bouton **Ouvrir**.

Pour remplacer une clé complémentaire, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Licence**.

2. Dans le panneau de résultats, dans le groupe **Clé complémentaire**, cliquez sur le bouton **Remplacer**.

3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur le bouton **Ouvrir**.

SUPPRESSION D'UNE CLE

Pour supprimer une clé de Kaspersky Security, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Licence**.

2. Dans le panneau de résultats, dans le bloc **Clé d'activation** ou **Clé complémentaire**, cliquez sur **Supprimer**.

Toute clé supprimée d'un des serveurs de la ferme est également supprimée de la totalité d'entre eux.

NOTIFICATION SUR L'EXPIRATION DE LA DUREE DE VALIDITE DE LA LICENCE

L'application vérifie les licences après chaque mise à jour des bases. Au cours de l'analyse, vous pouvez détecter des problèmes suivants concernant la licence et les clés :

- la clé est ajoutée ;
- la validité de la licence expire dans quelques jours ;
- la validité de la licence est écoulée ;
- la clé active se trouve sur la liste noire.

Dans ces cas-là dans les journaux de l'application une entrée est consignée et si les paramètres de notification sont configurés un message électronique sera envoyé à l'adresse indiquée pendant la configuration. Par défaut, la notification est envoyée 30 jours avant la fin de validité de la licence. Vous pouvez définir un délai plus long ou plus court.

Pour configurer les paramètres de notification sur l'expiration de la licence de Kaspersky Security, procédez comme suit :

1. Dans la console d'administration, choisissez le nœud **Notifications**.

2. Dans le panneau des résultats, pour le champ **Signaler l'expiration de la durée de validité de licence**, définissez, à l'aide du menu déroulant, combien de jours avant l'expiration vous souhaitez recevoir la notification sur l'expiration de la licence.

   Par défaut, la notification est envoyée 30 jours avant la fin de validité de la licence.

3. Cliquez sur le bouton **Enregistrer**.

INTERFACE DE L'APPLICATION

L'interface de gestion de l'application est assurée par la Console d'administration. Il s'agit d'un composant logiciel enfichable spécifique et isolé qui est intégré dans MMC (Microsoft Management Console).

DANS CETTE SECTION

Fenêtre principale 18

FENETRE PRINCIPALE

La fenêtre principale de la Console inclut les sections suivantes (cf. ill. ci-après) :

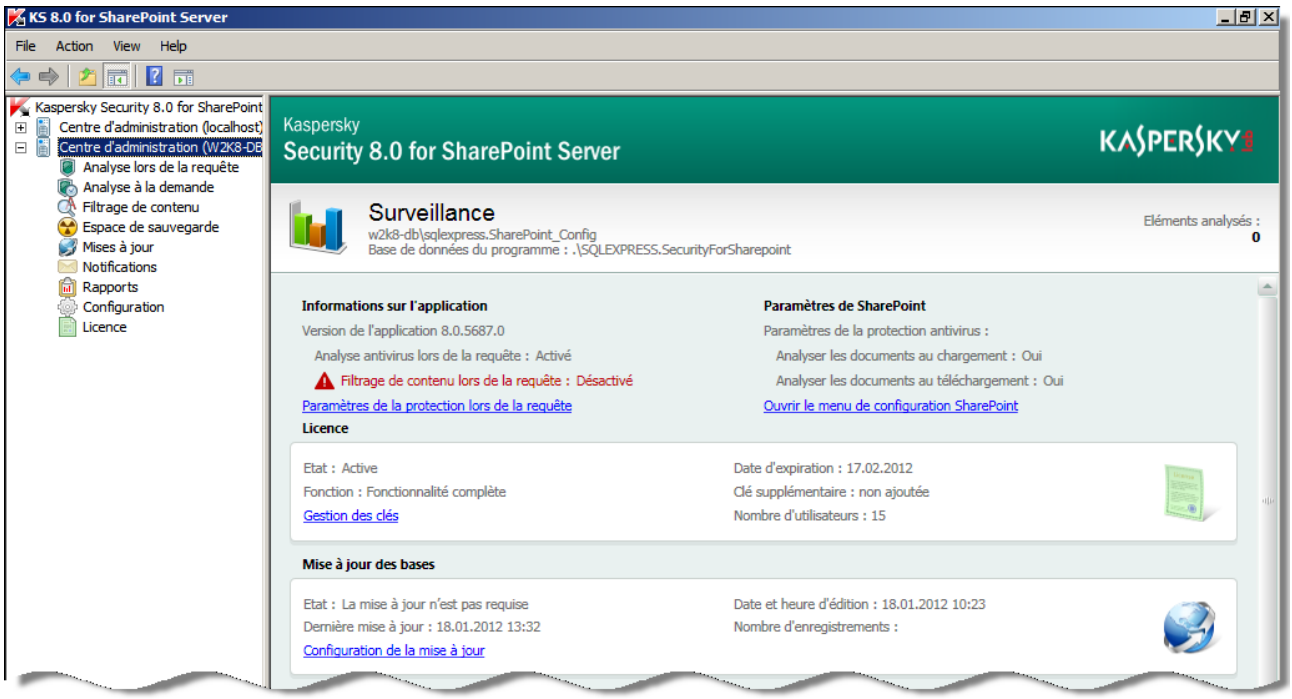

Figure 2. La fenêtre principale de Kaspersky Security

- **Barre d'outils**. Elle se trouve dans la partie supérieure de la fenêtre principale. L'ensemble de boutons de la barre d'outils permet d'accéder directement à quelques fonctions les plus utilisées de l'application.

- **Menu**. Se trouve directement au-dessus de la barre d'outils. Le menu assure la gestion des fichiers et des fenêtres et l'accès au système d'aide.

- **Arborescence de la console**. Se trouve dans la partie gauche de la fenêtre principale. L'arborescence de la console sert à consulter les serveurs SharePoint connectés et les paramètres de Kaspersky Security. Les serveurs connectés et les paramètres de Kaspersky Security sont affichés sous forme de nœuds. Vous pouvez ouvrir les nœuds parents en cloquant sur le symbole plus. Le nœud ouvert est affiché avec le symbole minus.

- **Panneau de résultats**. Se trouve dans la partie droite de la fenêtre principale. Affiche le contenu du nœud sélectionné dans l'arborescence.

Le nœud racine de l'arborescence de la console est **Kaspersky Security 8.0 pour SharePoint Server**. En double-cliquant sur ce nœud dans l'arborescence de la console, vous ouvrez la liste des serveurs connectés SharePoint avec

Kaspersky Security installé. Le panneau de résultats affiche les serveurs connectés et le bouton **Ajouter un serveur**. Lorsque vous cliquez avec le bouton gauche de la souris sur le nœud **Centre de gestion** du serveur connecté, le panneau des résultats affiche des informations générales sur les composants de l'application installés sur le serveur sélectionné, le type de licence, l'état des mises à jour et les statistiques de fonctionnement de l'application. En cliquant sur le symbole plus correspondant au serveur connecté, vous ouvrez dans l'arborescence de la console la liste des paramètres configurés de Kaspersky Security pour le serveur en question. Vous pouvez consulter et configurer les paramètres suivants de Kaspersky Security :

- **Analyse au moment de l'accès** : consultation et configuration des paramètres d'analyse des documents au moment de l'envoi sur le serveur et du téléchargement depuis le serveur vers l'ordinateur de l'utilisateur.
- **Analyse à la demande** : consultation et configuration des paramètres des tâches d'analyse des documents placés sur le serveur SharePoint.
- **Filtrage de contenu** : consultation et configuration des règles du filtrage de contenu.
- **Espace de sauvegarde** : consultation de l'Espace de sauvegarde.
- **Mises à jour** : consultation et configuration des paramètres de la mise à jour des bases antivirus et des bases du filtrage de contenu.
- **Notifications** : consultation et configuration des paramètres d'envoi des notifications sur les événements survenant lors du fonctionnement de l'application.
- **Rapports** : consultation et configuration des paramètres des rapports antivirus, ainsi que des rapports du filtrage de contenu.
- **Configuration** : consultation et configuration des paramètres d'envoi des notifications, de l'Espace de sauvegarde, de diagnostic, des rapports et des statistiques.
- **Licence** : ajout et suppression de clés ; consultation des données sur la licence.

Pendant la sélection d'un nœud de l'application dans l'arborescence de la console, le panneau de résultat affiche les paramètres configurés du nœud en question.

LANCEMENT DE L'APPLICATION

Les services de Kaspersky Security sont lancés automatiquement lors du lancement du système d'exploitation.

Pour lancer la console d'administration,

Cliquez sur le menu **Démarrer** → **Tous les programmes** → **Kaspersky Security 8.0 for SharePoint Server** → **KS 8.0 for SharePoint Server.**

ETAT DE LA PROTECTION PAR DEFAUT

L'état de la protection du serveur par défaut dépend des paramètres définis lors de l'exécution de l'assistant de configuration de l'application.

Si pendant l'installation de l'application sur le premier serveur la case **Activer la protection antivirus** dans la fenêtre de l'Assistant de configuration de l'application a été cochée, l'analyse pour les virus existant au moment de l'accès est activée par défaut.

Par défaut, l'option de réparation des fichiers infectés et potentiellement infectés est activée. Les fichiers protégés par mot de passe et les fichiers endommagés sont bloqués.

PREMIERE UTILISATION

Cette section indique comment lancer la console d'administration et ajouter des serveurs à celle-ci.

DANS CETTE SECTION

Lancement de la Console d'administration 22

Connexion de la console d'administration au serveur 22

Activation et désactivation de la protection antivirus et du filtrage de contenu 23

LANCEMENT DE LA CONSOLE D'ADMINISTRATION

Pour lancer la console d'administration, procédez comme suit :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programme**s.
2. Dans la liste de programmes, sélectionnez **Kaspersky Security 8.0 for SharePoint Server**.
3. Dans le menu, sélectionnez l'option **KS 8.0 for SharePoint Server**.

Lors du lancement de la console d'administration, le composant Kaspersky Security se connecte à MMC, et l'icône de l'application apparaît dans l'arborescence de la console avec le nœud **Kaspersky Security 8.0 for SharePoint Server**.

Après le lancement de la console d'administration, vous pouvez ajouter un serveur à celle-ci (cf. la rubrique "Connexion de la console d'administration au serveur" à la page 22).

CONNEXION DE LA CONSOLE D'ADMINISTRATION AU SERVEUR

Pour connecter la console d'administration au serveur SharePoint, procédez comme suit :

1. Sélectionnez le nœud **Kaspersky Security 8.0 for SharePoint Server** dans l'arborescence de la Console d'administration.
2. Dans le panneau de résultats, cliquez sur le bouton **Ajouter un serveur**.
3. Dans la fenêtre affichée, sélectionnez l'option nécessaire :
   - **Poste local**. La console d'administration et connectée au poste sur lequel elle est installée (localhost).
   - **Autre poste**. La console d'administration est connectée au serveur SharePoint indiqué pour l'administration de l'application. Lors du choix de cette option, indiquez le nom du serveur par l'une des méthodes suivantes :
     - Choisissez l'ordinateur de la liste dans la fenêtre accessible via le bouton **Parcourir**.
     - Indiquez manuellement le nom du serveur en définissant son adresse IP (dans la version IPv4 ou IPv6) ou son nom DNS.
4. Cliquez sur le bouton **OK**.

Le serveur indiqué est ajouté à la Console d'administration et apparaît dans l'arborescence de celle-ci.

ACTIVATION ET DESACTIVATION DE LA PROTECTION ANTIVIRUS ET DU FILTRAGE DE CONTENU

Pour activer/désactiver l'analyse de la présence de virus au moment de l'accès, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.
2. Sous l'onglet **Général**, cochez/décochez la case de **lancement de l'analyse antivirus**.
3. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre.

Pour activer/désactiver le filtrage de contenu au moment de l'accès, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.
2. Sous l'onglet **Général**, cochez/décochez la case **Exécuter le filtrage de contenu**.
3. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre.

MISE A JOUR DES BASES

Cette section contient des informations sur la configuration des paramètres de mise à jour des bases de Kaspersky Security : planification de la mise à jour automatique, sélection de la source de mise à jour et paramètres de connexion. La section contient des informations sur la configuration des paramètres de chaque serveur de la ferme séparément et sur la distribution des paramètres globaux sur tous les serveurs de la ferme.

DANS CETTE SECTION

Présentation de la mise à jour des bases 24

Consultation des informations sur la mise à jour des bases antivirus 25

Mise à jour automatique des bases 26

Configuration des paramètres locaux de la mise à jour sur les serveurs de la ferme 27

Diffusion des paramètres globaux de la mise à jour des bases 27

Sélection de la source de la mise à jour 28

Configuration des paramètres de connexion 28

PRESENTATION DE LA MISE A JOUR DES BASES

Kaspersky Lab offre à ses utilisateurs la possibilité de mettre à jour les bases antivirus ainsi que les catégories de filtrage de contenu de Kaspersky Security qui recherche des programmes malveillants, répare les objets infectés et effectue le filtrage de contenu. Les fichiers de bases contiennent une description de tous les programmes malveillants actuellement connus, ainsi que les moyens pour traiter les objets infectés, une description du programme pouvant être utilisé par des intrus pour nuire à votre ordinateur ou à un utilisateur spécifique, ainsi que les catégories de filtrage de contenu créées par Kaspersky Lab et utilisées pour vérifier le contenu des fichiers.

Il est primordial de maintenir toutes les bases à jour. Il est conseillé de réaliser la mise à jour directement après l'installation de l'application, car les bases présentes dans la distribution sont dépassées au moment de l'installation. Les bases stockées sur les serveurs de Kaspersky Lab sont mises à jour toutes les heures. Il est conseillé de configurer la même périodicité de mise à jour automatique.

La mise à jour des bases peut avoir lieu depuis les sources suivantes :

- des serveurs de mise à jour de Kaspersky Lab sur le Web ;
- une source de mise à jour locale (dossier local ou de réseau) ;
- un autre serveur HTTP/FTP (par exemple, votre serveur Intranet).

La mise à jour peut se dérouler manuellement ou automatiquement selon un horaire défini. Après avoir copié les fichiers depuis la source des mises à jour indiquée, l'application établit la connexion avec les nouvelles bases en mode automatique.

Lors de l'installation de l'application sur certains serveurs, vous pouvez indiquer des paramètres locaux (cf. la rubrique "Configuration des paramètres locaux de la mise à jour sur les serveurs de la ferme" à la page 27)de mise à jour individuelle pour chaque serveur et diffuser les paramètres globaux (cf. la rubrique "Diffusion des paramètres globaux de la mise à jour des bases" à la page 27) de la mise à jour sur tous les serveurs.

CONSULTATION DES INFORMATIONS SUR LA MISE A JOUR DES BASES ANTIVIRUS

Pour consulter les informations relatives à la mise à jour des bases, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour**.

2. Dans le panneau de résultats, allez sur l'onglet **Paramètres de mise à jour des serveurs**.

   Si Kaspersky Security est installé sur un serveur autonome, les informations sur la mise à jour n'apparaissent pas sous un onglet, mais dans le panneau des résultats, dans le bloc **Paramètres de mise à jour des bases**.

   Les informations sur la mise à jour des bases sur chacun des serveurs de la ferme sont présentées dans un tableau :

   - **Nom du serveur.** Nom du serveur inclus dans la ferme.
   - **Date de sortie des bases**. Heure d'édition des bases utilisées actuellement par l'application sur le serveur de Kaspersky Lab.
   - **Dernière mise à jour des bases**. Heure de la dernière mise à jour des bases sur le serveur.
   - **Paramètres**. Ce graphique montre les paramètres globaux et locaux de la mise à jour utilisés sur le serveur.
   - **Statut de la dernière mise à jour**. Informations sur le résultat de la dernière mise à jour des bases.

MISE A JOUR AUTOMATIQUE DES BASES

Pour réaliser la mise à jour des bases de l'Anti-Virus automatiquement, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour** (cf. ill. ci-après).

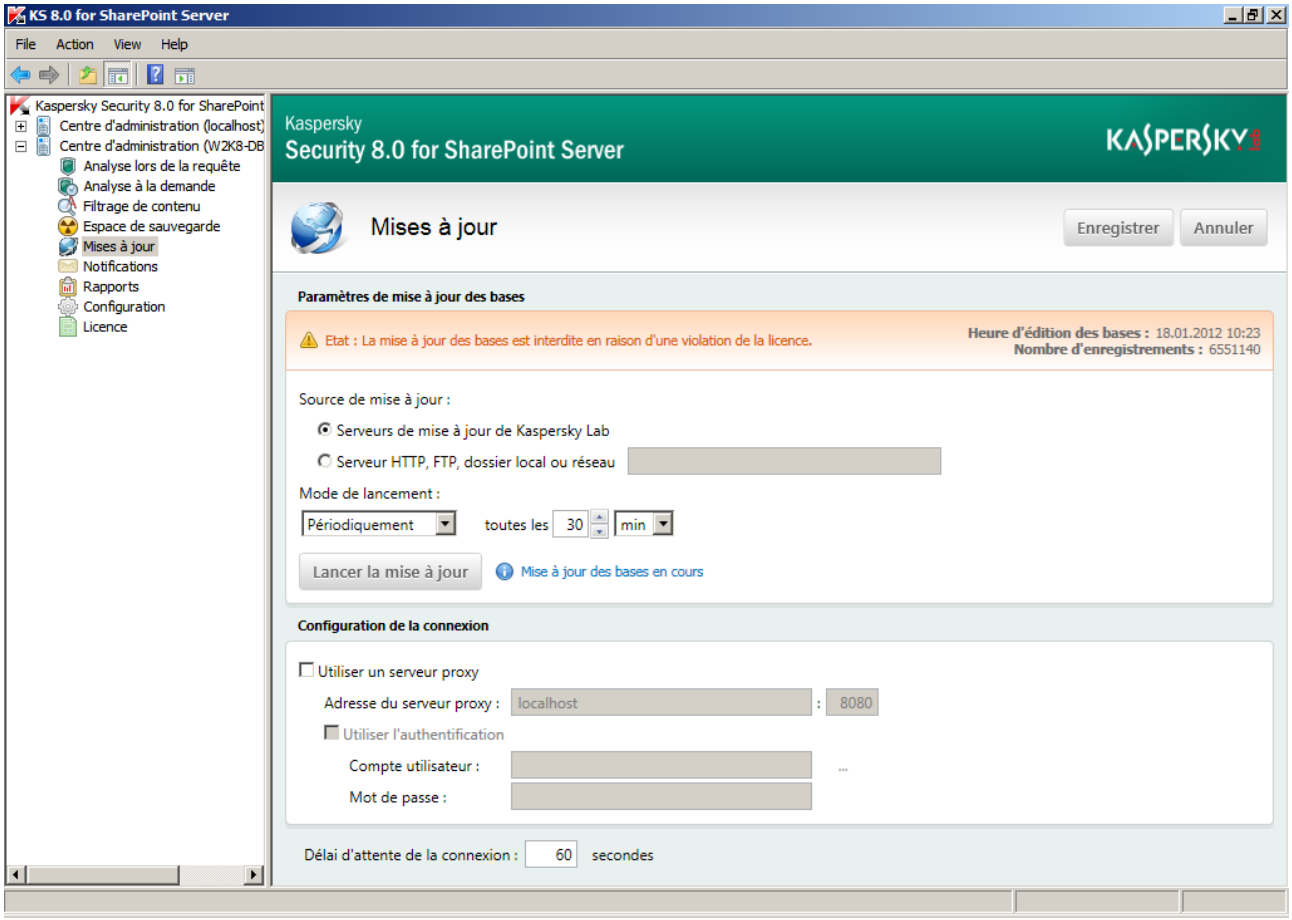

*Figure 3. Nœud **Mise à jour***

2. Dans le panneau de résultats, allez sur l'onglet **Général** et dans le bloc **Paramètres de mise à jour des bases** dans le menu déroulant **Mode de lancement**, sélectionnez une des options :

   - **Périodiquement**. Dans le menu déroulant, définissez la valeur du champ **toutes les N minutes, heures, jours** pour la fréquence d'exécution de la mise à jour.

   - **Chaque jour**. Indiquez l'heure exacte dans le champ **au format HH**:**MM** (heure locale).

   - **Le jour sélectionné**. Cochez la case en regard des jours de la semaine quand vous souhaitez réaliser la mise à jour des bases. Indiquez également l'heure de la mise à jour.

3. Cliquez sur le bouton **Enregistrer**.

CONFIGURATION DES PARAMETRES LOCAUX DE LA MISE A JOUR SUR LES SERVEURS DE LA FERME

Pour configurer les paramètres locaux de mise à jour des bases sur un serveur faisant partie d'une ferme, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour**.

2. Dans le tableau de résultats, allez sur l'onglet **Paramètres de mise à jour des serveurs,** sélectionnez le serveur nécessaire dans le tableau et cliquez sur **Modifier les paramètres locaux**.

3. La fenêtre **Paramètres du serveur** apparaît. Dans le bloc **Paramètres de mise à jour des bases**, sélectionnez la source de mise à jour :

   - **Serveurs de mise à jour de Kaspersky Lab**, si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab.

   - **Serveur HTTP, FTP, dossier local ou réseau** si vous souhaitez télécharger les mises à jour depuis une des sources de mises à jour citées.

     Pour sélectionner cette option, saisissez dans le champ de saisie l'adresse du serveur, du dossier local ou de réseau.

4. Dans le bloc **Paramètres de mise à jour des bases** dans le menu déroulant **Mode de lancement**, indiquez le mode de lancement de mise à jour :

   - **Périodiquement**. Dans le menu déroulant, définissez la valeur du champ **toutes les N minutes, heures, jours** pour la fréquence d'exécution de la mise à jour.

   - **Chaque jour**. Indiquez l'heure exacte dans le champ **au format HH**:**MM** (heure locale).

   - **Le jour sélectionné**. Cochez la case en regard des jours de la semaine quand vous souhaitez réaliser la mise à jour des bases. Indiquez également l'heure de la mise à jour.

5. Dans le bloc **Paramètres de connexion**, indiquez les paramètres de connexion :

   - Si la connexion à Internet s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy** et définissez les paramètres de connexion : adresse du serveur proxy et numéro du port pour la connexion. Le numéro du port du serveur proxy est **8080** par défaut.

   - Si l'accès au serveur proxy requiert un mot de passe, définissez les paramètres d'authentification de l'utilisateur. Pour ce faire, cochez la case **Utiliser l'authentification** et remplissez les champs **Compte utilisateur** et **Mot de passe**.

   - Indiquez le délai d'attente de la connexion dans le champ **Délai d'attente de la connexion**. Par défaut, le délai d'attente de la connexion est de **60** s.

DIFFUSION DES PARAMETRES GLOBAUX DE LA MISE A JOUR DES BASES

Pour diffuser les paramètres globaux de mise à jour des bases sur tous les serveurs de la ferme, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour**.

2. Dans le tableau de résultats, allez sur l'onglet **Paramètres de mise à jour des serveurs,** sélectionnez le serveur nécessaire dans le tableau et cliquez sur **Diffuser les paramètres globaux**.

SELECTION DE LA SOURCE DE LA MISE A JOUR

Pour sélectionner la source des mises à jour des bases de l'Antivirus, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour**.

2. Dans l'onglet **Général** dans le bloc **Paramètres de mise à jour des bases**, sélectionnez une des options :

   - **Serveurs de mise à jour de Kaspersky Lab**, si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab.

   - **Serveur HTTP, FTP, dossier local ou réseau** si vous souhaitez télécharger les mises à jour depuis une des sources de mises à jour citées.

     Pour sélectionner cette option, saisissez dans le champ de saisie l'adresse du serveur, du dossier local ou de réseau.

   Si Kaspersky Security est installé sur un serveur autonome, le choix de la source de la mise à jour est effectué dans le groupe **Paramètres de mise à jour des bases** du panneau des résultats lorsque vous sélectionnez le nœud **Mise à jour dans l'arborescence de la console**.

3. Cliquez sur le bouton **Enregistrer**.

CONFIGURATION DES PARAMETRES DE CONNEXION

Pour consulter ou modifier les paramètres de la connexion de réseau, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Mises à jour**.

2. Dans le panneau de résultats, allez sur l'onglet **Général** et dans le bloc **Paramètres de connexion** (cf. ill. ci-après), indiquez les paramètres de connexion nécessaires.

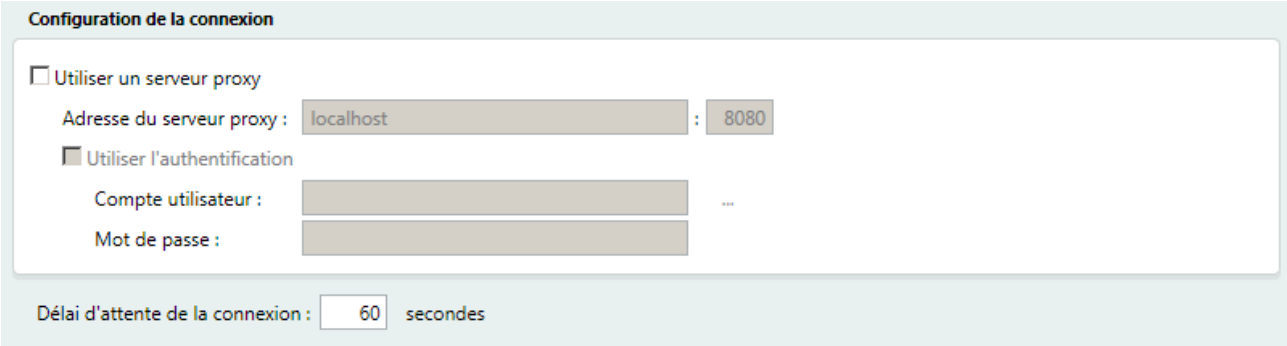

*Figure 4. Groupe **Configuration de la connexion***

Si Kaspersky Security est installé sur un serveur autonome, la configuration des paramètres de connexion est effectuée dans le groupe **Configuration de connexion** du panneau des résultats lorsque vous sélectionnez le nœud **Mise à jour** dans l'arborescence de la console.

3. Si la connexion à Internet s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy** et indiquez les paramètres de connexion : adresse du serveur proxy et numéro du port pour la connexion. Le numéro du port du serveur proxy est **8080** par défaut.

4. Si l'accès au serveur proxy requiert un mot de passe, indiquez les paramètres d'authentification de l'utilisateur. Pour ce faire, cochez la case **Utiliser l'authentification** et remplissez les champs **Compte utilisateur** et **Mot de passe**.

5. Si vous ne souhaitez pas utiliser le serveur proxy pour télécharger la mise à jour depuis les adresses locales, cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.

6. Indiquez le délai d'attente de la connexion dans le champ **Délai d'attente de la connexion**. Par défaut, le délai d'attente de la connexion est de **60** s.

ANALYSE AU MOMENT DE L'ACCES

Cette section contient des informations sur l'analyse des fichiers pour les virus existants et un contenu indésirable avant d'envoyer les fichiers vers le serveur SharePoint et avant de les télécharger vers l'ordinateur de l'utilisateur. Cette section décrit le fonctionnement de Kaspersky Security en fonction des paramètres définis pour le serveur SharePoint, ainsi que les instructions de configuration des paramètres d'analyse.

DANS CETTE SECTION

A propos de l'analyse au moment de l'accès 30

Fonctionnement de Kaspersky Security suivant les paramètres du serveur SharePoint 30

Paramètres de l'analyse au moment de l'accès 31

A PROPOS DE L'ANALYSE AU MOMENT DE L'ACCES

Kaspersky Security permet d'analyser les fichiers pour les virus existants et un contenu indésirable au moment de l'accès à ces fichiers. Cette analyse est effectuée lorsqu'on essaie d'envoyer le fichier vers le serveur SharePoint ou de télécharger le fichier depuis le serveur sur l'ordinateur de l'utilisateur.

Lors de l'analyse au moment de l'accès, Kaspersky Security analyse les fichiers pour les virus existants et contenus indésirables en respectant la séquence suivante :

1. analyse du type de fichier conformément aux paramètres du filtrage de contenu ;
2. analyse du fichier pour les virus existants ;
3. recherche du contenu interdit dans le fichier.

Si au cours de l'analyse, le fichier doit être bloqué conformément aux paramètres définis, l'analyse ne sera pas poursuivie. Le fichier est bloqué.

FONCTIONNEMENT DE KASPERSKY SECURITY SUIVANT LES PARAMETRES DU SERVEUR SHAREPOINT

Le fonctionnement de Kaspersky Security pendant l'analyse des fichiers au moment de l'accès dépend des valeurs des paramètres du serveur SharePoint.

L'analyse avant d'envoyer le fichier sur le serveur SharePoint ne sera effectuée que si, dans les paramètres du serveur, la case **Rechercher les virus dans les documents lors de l'envoi** est cochée.

En cas de détection de virus ou d'un contenu indésirable dans les fichiers lorsqu'on essaie d'envoyer ces fichiers vers le serveur SharePoint, Kaspersky Security va agir en fonction des paramètres de SharePoint :

- **Bloquer**. Le fichier sera bloqué, si :
  - la case **Essayer d'effacer les documents infectés** dans les paramètres SharePoint est décochée ;
  - dans les règles de traitement des objets Kaspersky Security l'action **Bloquer** a été sélectionnée ;

    - dans les règles de traitement des objets, l'action **Réparer** a été sélectionnée, mais le fichier ne peut pas être réparé.

- **Réparer**. Kaspersky Security essai de réparer le fichier si dans les paramètres SharePoint est cochée la case **Essayer d'effacer les documents infectés** et dans les règles de traitement des objets l'action **Réparer** a été sélectionnée.

- **Ignorer**. Kaspersky Security va ignorer un fichier infecté ou avec un contenu indésirable si dans les règles de traitement des objets Kaspersky Security l'action **Ignorer** a été sélectionnée.

L'analyse lors du téléchargement du fichier depuis le serveur SharePoint vers l'ordinateur de l'utilisateur ne sera effectuée que si, dans les paramètres du serveur, la case **Rechercher les virus dans les documents lors du téléchargement** est cochée.

En cas de détection de virus ou d'un contenu indésirable dans les fichiers lorsqu'on essaie de télécharger ces fichiers depuis le serveur SharePoint, Kaspersky Security va agir en fonction des paramètres de SharePoint :

- **Bloquer**. Le fichier sera bloqué si l'utilisateur qui essaie de télécharger le fichier vers le serveur ne fait pas partie de l'équipe d'administrateurs du serveur SharePoint et si une des conditions suivantes sera réalisée :

    - la case **Essayer d'effacer les documents infectés** dans les paramètres SharePoint est décochée ;

    - dans les règles de traitement des objets Kaspersky Security l'action **Bloquer** a été sélectionnée ;

    - dans les règles de traitement des objets, l'action **Réparer** a été sélectionnée, mais le fichier ne peut pas être réparé et la case **Autoriser les utilisateurs à télécharger les documents infectés** dans les paramètres de SharePoint est décochée.

- **Réparer**. Kaspersky Security essai de réparer le fichier si dans les paramètres SharePoint est cochée la case **Essayer d'effacer les documents infectés** et dans les règles de traitement des objets l'action Réparer a été sélectionnée.

- **Avertir en cas de téléchargement d'un fichier malveillant.** Kaspersky Security affichera le message sur l'extraction d'un fichier contenant un virus ou un contenu indésirable si l'utilisateur qui essaie d'extraire ce fichier malveillant fait partie de l'équipe d'administrateurs du serveur SharePoint ou si dans les paramètres SharePoint est cochée la case **Autoriser les utilisateurs à télécharger les documents infectés** et en même temps une des conditions suivantes sera réalisée :

    - la case **Essayer d'effacer les documents infectés** dans les paramètres SharePoint est décochée ;

    - dans les règles de traitement des objets Kaspersky Security l'action **Bloquer** a été sélectionnée ;

    - dans les règles de traitement des objets, l'action **Réparer** a été sélectionnée, mais le fichier ne peut pas être réparé.

PARAMETRES DE L'ANALYSE AU MOMENT DE L'ACCES

La fonction d'analyse au moment de l'accès permet de configurer les paramètres suivants :

- paramètres généraux ;

- règles de traitement des objets ;

- exclusions du scan antivirus ;

- paramètres du filtrage de contenu.

DANS CETTE SECTION

Configuration des paramètres généraux de l'analyse au moment de l'accès 32

Configuration des règles de traitement des objets lors de l'analyse au moment de l'accès 33

Création d'exclusions de l'analyse au moment de l'accès 35

Paramètres du filtrage de contenu 37

CONFIGURATION DES PARAMETRES GENERAUX DE L'ANALYSE AU MOMENT DE L'ACCES

Pour définir des paramètres généraux de l'analyse au moment de l'accès, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau des résultats, sélectionnez l'onglet **Général** et définissez les paramètres souhaités (cf. ill. ci-après).:

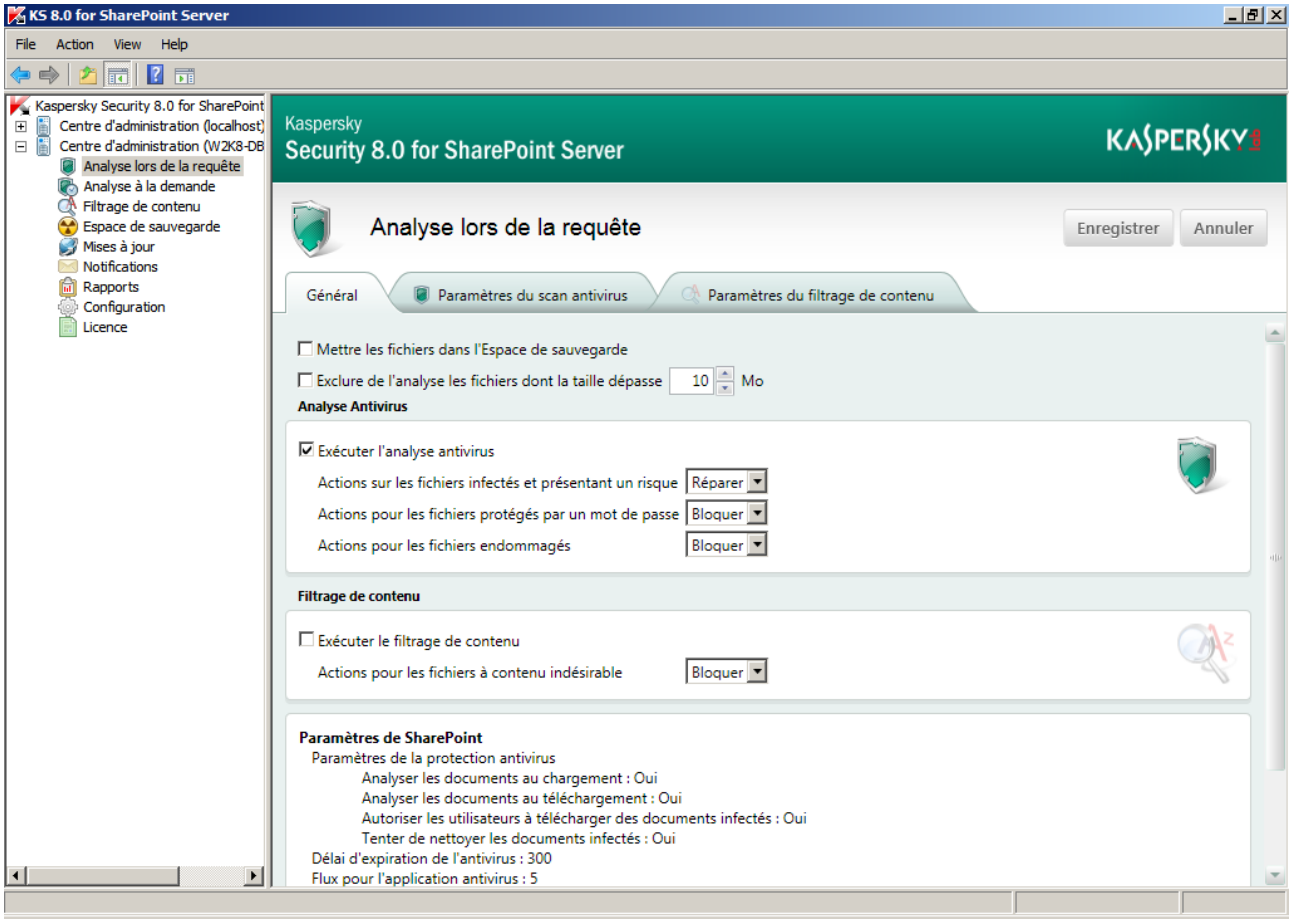

Figure 5. Paramètres généraux de l'analyse au moment de l'accès

- Si vous souhaitez effectuer le scan antivirus lors de l'exécution de la tâche, cochez la case **Lancer l'analyse pour les virus existants**.

- Si vous souhaitez exécuter le filtrage du contenu des fichiers, cochez la case **Exécuter le filtrage de contenu**.
- Si vous souhaitez que Kaspersky Security copie les fichiers dans l'Espace de sauvegarde avant de les traiter, cochez la case **Mettre les fichiers dans l'Espace de sauvegarde**.
- Si vous souhaitez limiter la taille des fichiers analysés, cochez la case **Exclure de l'analyse les fichiers dont la taille dépasse** et spécifiez la taille limite du fichier (en Mo). La valeur définie par défaut est de 10 Mo.

3. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer.**

CONFIGURATION DES REGLES DE TRAITEMENT DES OBJETS LORS DE L'ANALYSE AU MOMENT DE L'ACCES

Kaspersky Security traite les fichiers infectés, potentiellement infectés, endommagés et protégés par un mot de passe suivant les paramètres du serveur SharePoint (cf. la rubrique "Fonctionnement de Kaspersky Security suivant les paramètres du serveur SharePoint" à la page 30).

Pour créer des règles de traitement des objets lors du scan antivirus, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès** et sélectionnez dans le panneau des résultats l'onglet **Général**.
2. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers infectés et potentiellement infectés**, sélectionnez l'action à appliquer (cf. ill. ci-après):

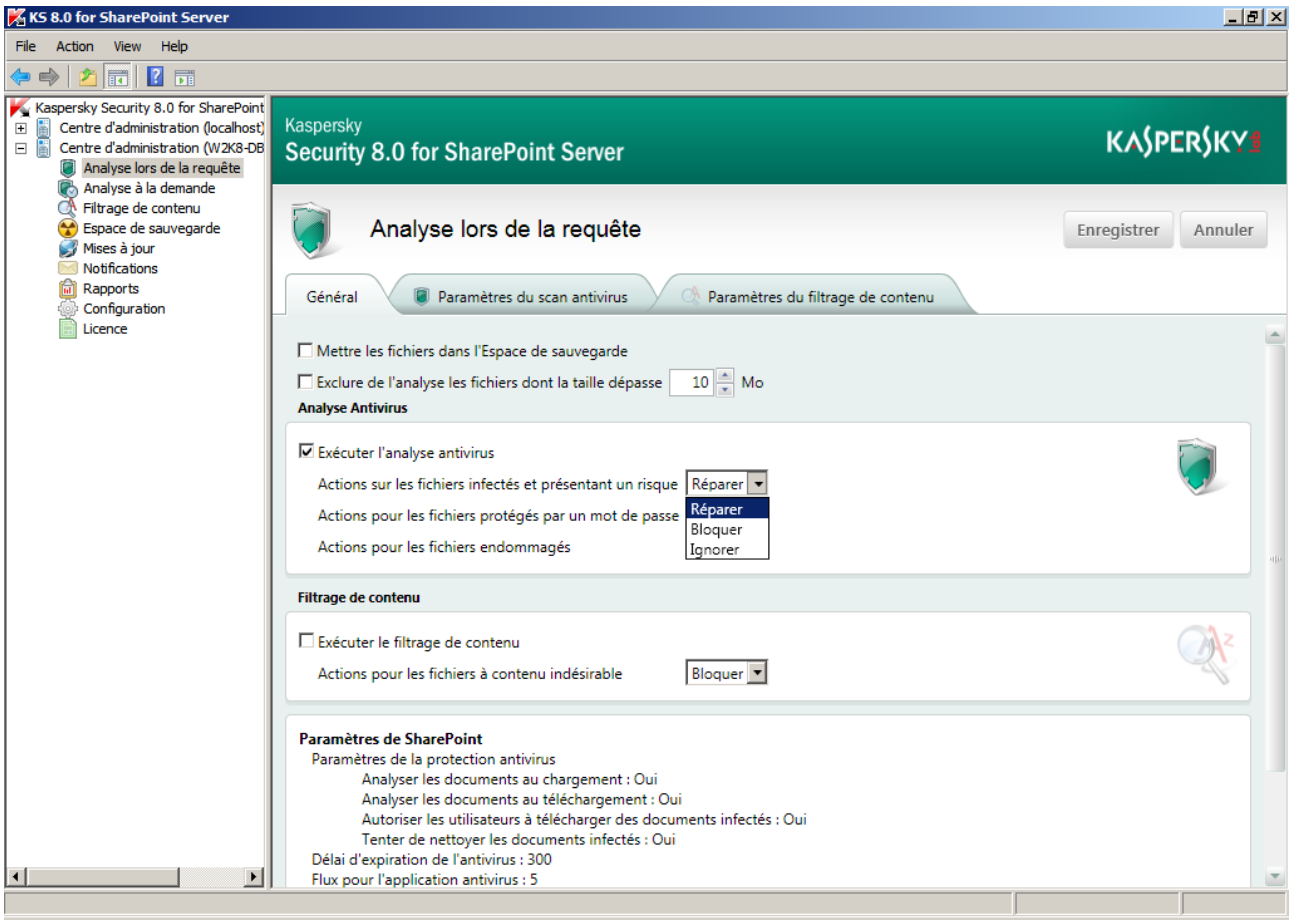

Figure 6. Règles de traitement des objets lors du scan antivirus

- **Réparer**. Kaspersky Security va essayer de réparer le fichier. Si le fichier est irréparable, il sera bloqué.
- **Bloquer**. Kaspersky Security va bloquer le fichier. Le fichier ne sera pas envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.
- **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier. Le fichier sera envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.

3. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers protégés par un mot de passe**, sélectionnez l'action à appliquer :
   - **Bloquer**. Kaspersky Security va bloquer le fichier. Le fichier ne sera pas envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.
   - **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier. Le fichier sera envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.
4. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers endommagés**, sélectionnez l'action à appliquer :
   - **Bloquer**. Kaspersky Security va bloquer le fichier. Le fichier ne sera pas envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.
   - **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier. Le fichier sera envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.
5. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer**.

Si l'option **Ignorer** est sélectionnée, aucune action ne sera effectuée sur le fichier, mais l'un des statuts lui sera attribué en fonction des résultats de l'analyse. Les informations sur le fichier seront consignées dans des rapports et dans des statistiques.

Pour créer des règles de traitement des objets lors du filtrage de contenu, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès** et sélectionnez dans le panneau des résultats l'onglet **Général**.

2. Dans le groupe **Filtrage de contenu** dans la liste déroulante **Actions pour les fichiers à contenu indésirable**, sélectionnez l'action à appliquer (cf. ill. ci-après):

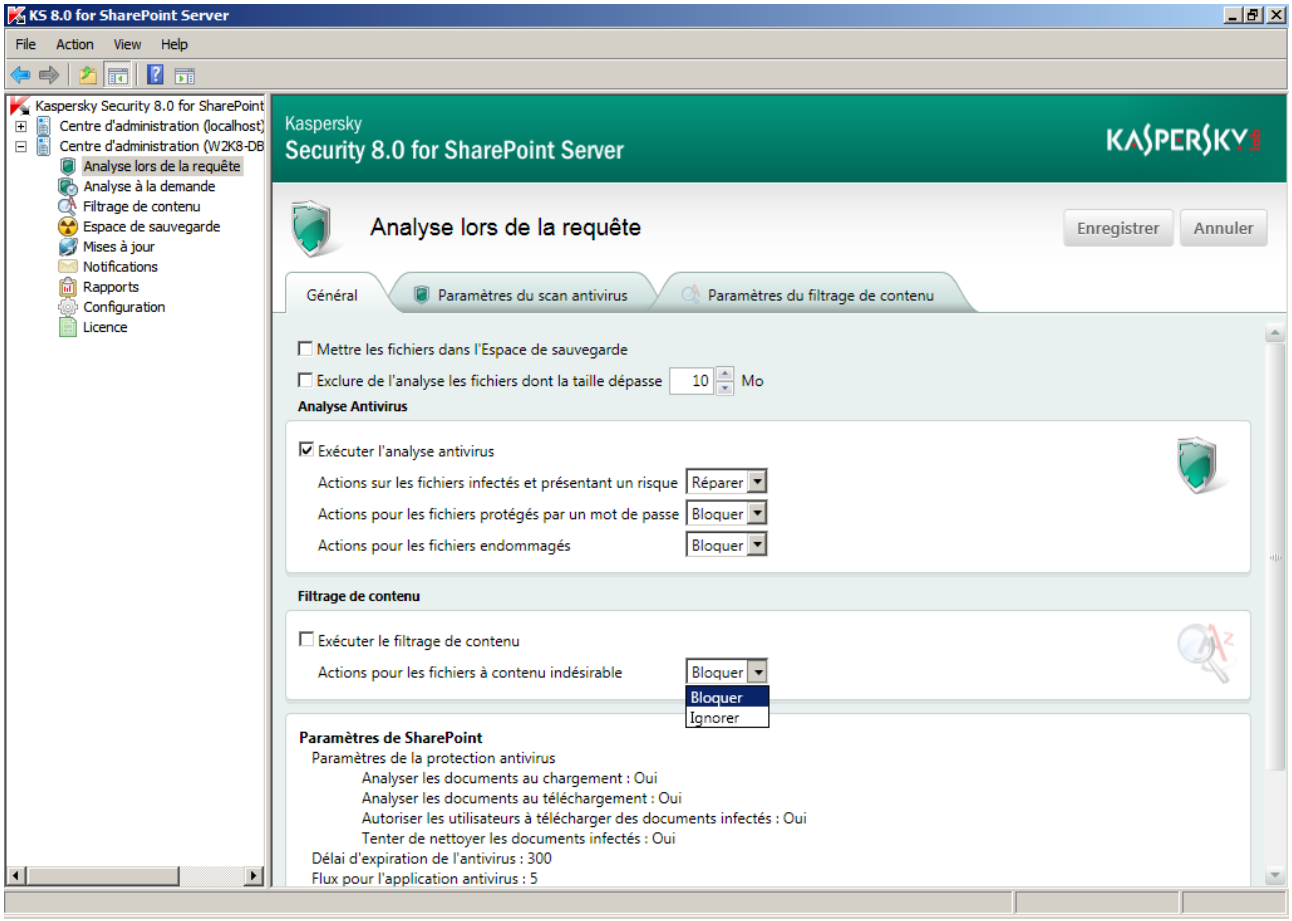

Figure 7. Règles de traitement des objets lors du filtrage de contenu

- **Bloquer**. Kaspersky Security va bloquer le fichier. Le fichier ne sera pas envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.

- **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier. Le fichier sera envoyé vers le serveur SharePoint ou téléchargé depuis le serveur vers l'ordinateur de l'utilisateur.

3. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer.**

Si l'option **Ignorer** est sélectionnée, aucune action ne sera effectuée sur le fichier, mais l'un des statuts lui sera attribué en fonction des résultats de l'analyse. Les informations sur le fichier seront consignées dans des rapports et dans des statistiques.

CREATION D'EXCLUSIONS DE L'ANALYSE AU MOMENT DE L'ACCES

Pour réduire la charge du serveur pendant l'analyse lors de la requête, vous pouvez définir au moment de l'accès les types ou les masques de fichiers à ignorer, limiter la taille des fichiers à analyser, ainsi que désactiver l'analyse des archives et des conteneurs imbriqués.

➡ *Pour exclure de l'analyse antivirus les fichiers de certains formats, procédez comme suit :*

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau de résultats, sélectionnez l'onglet **Paramètres du scan antivirus** (cf. ill. ci-après).

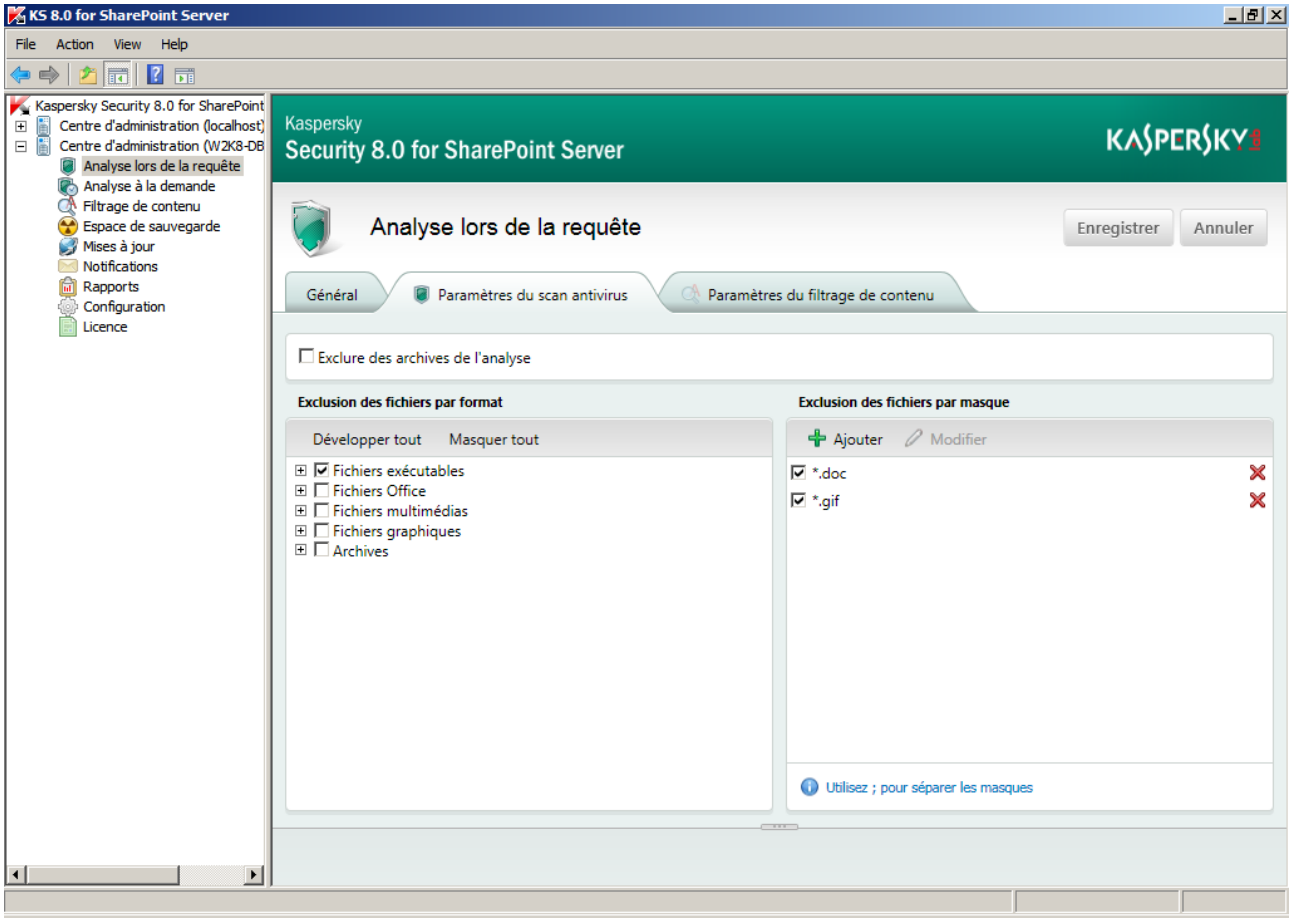

Figure 8. Création d'exclusions de l'analyse antivirus au moment de l'accès

3. Dans le champ **Exclusion des fichiers par format**, cochez les cases des éléments de l'arborescence des formats des fichiers qui correspondent aux formats requis.

   Pour votre confort, vous pouvez administrer la structure avec des boutons suivants **Développer tout** et **Masquer tout**.

4. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

Pour exclure de l'analyse des fichiers par masque, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau de résultats, sélectionnez l'onglet **Paramètres du scan antivirus**.

3. Dans le champ **Exclure des fichiers par masque**, cochez les cases correspondant aux masques à exclure de l'analyse.

4. Pour ajouter un masque sur la liste, ouvrez la fenêtre **Ajout d'un masque** en cliquant sur le bouton **Ajouter** et spécifiez le masque dans le champ de saisie. Pour quitter la fenêtre, cliquez sur le bouton **OK**.

   Si vous souhaitez définir plusieurs masques, utilisez dans le champ de saisie le point-virgule, pour les séparer.

5. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

Pour imposer d'autres restrictions relatives aux fichiers analysés, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Définissez les paramètres suivants sous les onglets du panneau des résultats :

   - Si vous souhaitez que Kaspersky Security n'analyse pas les archives, sous l'onglet **Paramètres du scan antivirus** cochez la case **Exclure des archives de l'analyse**.

   - Si vous souhaitez limiter la taille des fichiers analysés, sous l'onglet **Général** cochez la case **Exclure de l'analyse les fichiers dont la taille dépasse** et spécifiez la taille limite du fichier (en Mo) dans le champ de saisie défilement. La valeur du champ par défaut est de 10 Mo.

3. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

PARAMETRES DU FILTRAGE DE CONTENU

Kaspersky Security vous permet de définir des formats de fichiers, des noms de fichiers et des formes de mots indésirables.

Pour augmenter la vitesse d'exécution, vous pouvez exclure des fichiers de grande taille de l'analyse.

DANS CETTE SECTION

Paramètres de détermination du contenu indésirable 37

Création d'exclusions du filtrage de contenu 39

PARAMETRES DE DETERMINATION DU CONTENU INDESIRABLE

Pour définir les formats indésirables de fichiers, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau de résultats, sélectionnez l'onglet **Paramètres du filtrage de contenu** (cf. ill. ci-après).

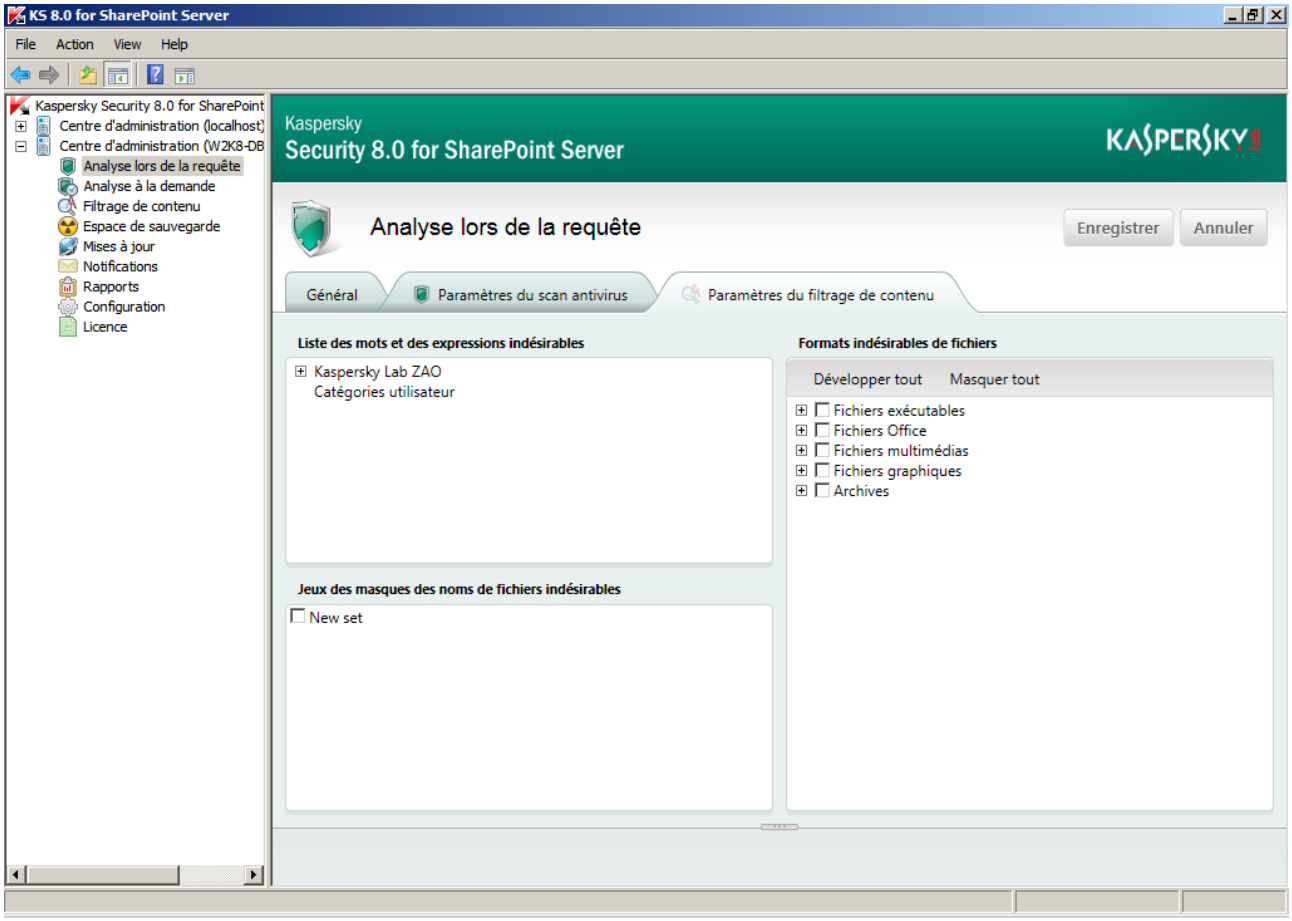

Figure 9. Paramètres du filtrage de contenu lors de l'analyse lors d'une requête

3. Dans le champ **Formats indésirables des fichiers**, cochez les cases des éléments de l'arborescence des formats des fichiers qui correspondent aux formats requis.

   Pour votre confort, vous pouvez administrer l'arborescence des formats avec des boutons suivants :

   - **Dérouler tout**. Ce bouton déroule tous les nœuds imbriqués de l'arborescence des formats.
   - **Réduire tout**. Le bouton réduit l'arborescence des formats.

4. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

➡ *Pour définir les masques des noms indésirables de fichiers, procédez comme suit :*

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau de résultats, sélectionnez l'onglet **Paramètres du filtrage de contenu**.

3. Dans le champ **Jeux des masques des noms de fichiers indésirables**, cochez les cases correspondant aux masques des listes requises.

   Vous pouvez ajouter et modifier les jeux de masques des noms de fichiers indésirables dans le nœud **Filtrage de contenu** sous l'onglet **Masques des noms de fichiers indésirables** (à la page 57).

4. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

Pour définir les mots indésirables et les formes de mots, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau de résultats, sélectionnez l'onglet **Paramètres du filtrage de contenu**.

3. Dans le champ **Liste des mots et des expressions indésirables**, cochez les cases à côté des catégories requises.

   Vous pouvez ajouter et modifier les catégories utilisateur de mots et expressions indésirables dans le nœud **Filtrage de contenu** sous l'onglet **Mots et expressions** (cf. la rubrique "**Modification des mots et expressions inclus dans le contenu des catégories d'utilisateurs**" à la page 55).

4. Pour enregistrer les modifications, cliquez sur le bouton **Enregistrer**.

CREATION D'EXCLUSIONS DU FILTRAGE DE CONTENU

Pour réduire la charge du serveur et pour augmenter la vitesse d'exécution de Kaspersky Security, vous pouvez exclure des fichiers de grande taille de l'analyse.

Pour exclure du filtrage de contenu les fichiers dont la taille dépasse la valeur spécifiée, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse au moment de l'accès**.

2. Dans le panneau des résultats, sélectionnez l'onglet **Général**.

3. Cochez la case **Exclure de l'analyse les fichiers dont la taille dépasse** et spécifiez la taille requise (en méga-octets) dans le champ de saisie avec défilement à droite. La valeur du champ par défaut est de 10 Mo.

ANALYSE A LA DEMANDE

Cette section contient des informations sur les tâches d'analyse à la demande, les instructions sur la création des tâches d'analyse à la demande, la configuration des paramètres et la planification du lancement des tâches.

DANS CETTE SECTION

A propos de l'analyse à la demande 40

Lancement et arrêt de la tâche d'analyse à la demande 41

Visualisation du rapport relatif à l'analyse à la demande 42

Paramètres de la tâche d'analyse à la demande 42

Création d'une nouvelle tâche d'analyse à la demande 51

Suppression de la tâche d'analyse à la demande 52

A PROPOS DE L'ANALYSE A LA DEMANDE

Kaspersky Security effectue le scan antivirus et le filtrage du contenu des fichiers stockés sur le serveur SharePoint.

Pour gérer l'analyse à la demande, Kaspersky Security utilise les tâches d'analyse personnalisées.

Vous pouvez définir pour chacune des tâches des paramètres d'analyse et de filtrage, ainsi qu'une planification de l'analyse.

Lors de l'analyse à la demande, Kaspersky Security analyse les fichiers pour les virus existants et les contenus indésirables en fonction des paramètres définis.

1. analyse du fichier pour les virus existants ;
2. analyse du type de fichier conformément aux paramètres du filtrage de contenu ;
3. recherche du contenu interdit dans le fichier.

Si au cours de l'analyse, le fichier doit être supprimé conformément aux paramètres définis, l'analyse ne sera pas poursuivie et l'application supprimera le fichier.

L'application analyse uniquement les dernières versions des fichiers stockés sur le serveur.

Lorsque vous ouvrez le nœud **Analyse à la demande**, le panneau des résultats affiche un tableau avec la liste des tâches et des paramètres d'exécution.

Pour chacune des tâches sélectionnez, vous pouvez effectuer les actions suivantes :

- lancer ;
- arrêter ;
- copier ;
- reconfigurer ;

- consulter le rapport d'avancement ;
- supprimer.

Vous pouvez également créer une nouvelle tâche (v. section "Création d'une nouvelle tâche d'analyse à la demande" à la page 51).

Lors de l'analyse à la demande, Kaspersky Security peut également analyser les fichiers de service SharePoint. Vous pouvez activer/désactiver l'analyse de ces fichiers lors de la configuration de la tâche d'analyse à la demande.

LANCEMENT ET ARRET DE LA TACHE D'ANALYSE A LA DEMANDE

Pour lancer la tâche d'analyse à la demande manuellement :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche dans la liste du panneau des résultats (cf. ill. ci-après).

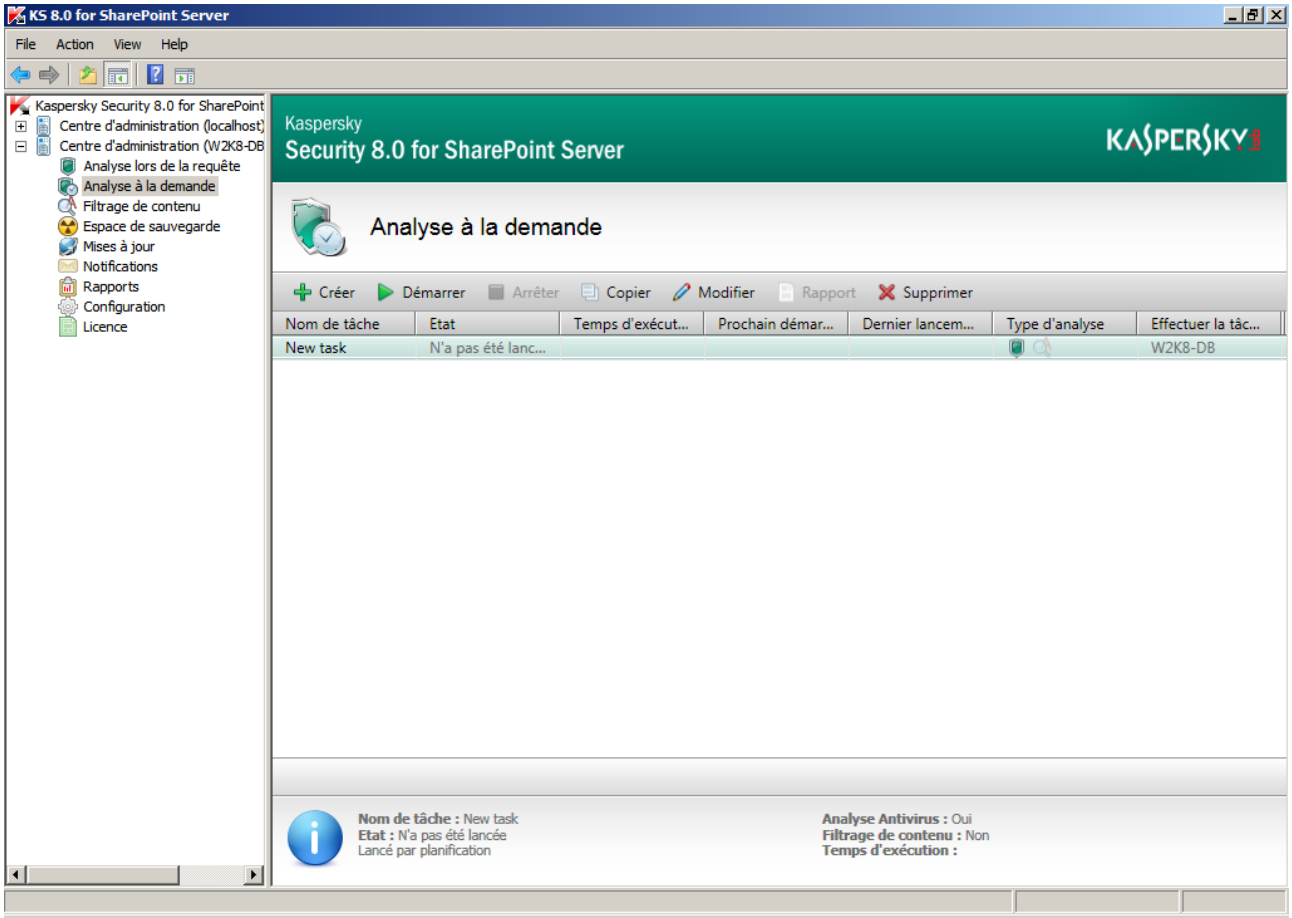

Figure 10. Administration les tâches d'analyse à la demande

3. Cliquez sur le bouton **Démarrer**.

Pour arrêter la tâche d'analyse à la demande :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche dans la liste du panneau des résultats.
3. Cliquez sur le bouton **Arrêter**.

Pour pouvoir lancer la tâche d'analyse à la demande en mode automatique :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche dans la liste du panneau des résultats.
3. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche**.
4. Passez à l'onglet **Général** et créer une planification (v. section "Création de la planification du lancement de la tâche d'analyse à la demande" à la page 45) du lancement de la tâche d'analyse à la demande.

VISUALISATION DU RAPPORT RELATIF A L'ANALYSE A LA DEMANDE

Pour visualiser le rapport sur la dernière l'exécution de la tâche à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche depuis la liste dans le panneau de résultats et cliquez sur **Rapport**. Le rapport est affiché dans un nouveau fenêtre du navigateur Web.

Le bouton **Rapport** est inaccessible pour la tâche en cours et pour la tâche qui n'a jamais été lancée.

PARAMETRES DE LA TACHE D'ANALYSE A LA DEMANDE

Les tâches d'analyse à la demande vous permettent :

- de définir les paramètres lors de la création d'une nouvelle tâche d'analyse à la demande ;
- de modifier les paramètres d'une tâche d'analyse à la demande qui existe déjà.

Vous pouvez configurer les paramètres suivants :

- paramètres généraux ;
- mode de lancement de l’analyse ;
- zone de l'analyse ;
- règles de traitement des objets ;
- exclusions de l'analyse ;
- paramètres du filtrage de contenu.

L'analyse de toutes les zones de SharePoint peut s'effectuer uniquement lorsque le compte utilisateur sous lequel les services de l'application sont lancés dispose des droits de l'administrateur du serveur SharePoint et de l'administrateur de la ferme.

DANS CETTE SECTION

Sélection du serveur pour lancer la tâche 43

Configuration des paramètres généraux d'une tâche d'analyse à la demande 43

Création de la planification du lancement de la tâche d'analyse à la demande 45

Configuration des règles de traitement des objets lors de l'analyse à la demande 46

Sélection des zones d'analyse 47

Création d'exclusions de l'analyse à la demande 49

Paramètres du filtrage de contenu 51

SELECTION DU SERVEUR POUR LANCER LA TACHE

Pour sélectionner le serveur sur lequel l'analyse à la demande sera exécutée, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.
2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Général**.
3. Dans la liste **Exécuter la tâche sur le serveur**, sélectionnez le serveur requis.
4. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

CONFIGURATION DES PARAMETRES GENERAUX D'UNE TACHE D'ANALYSE A LA DEMANDE

Pour définir des paramètres généraux de la tâche d'analyse à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Général** et définissez les paramètres requis (cf. ill. ci-après):

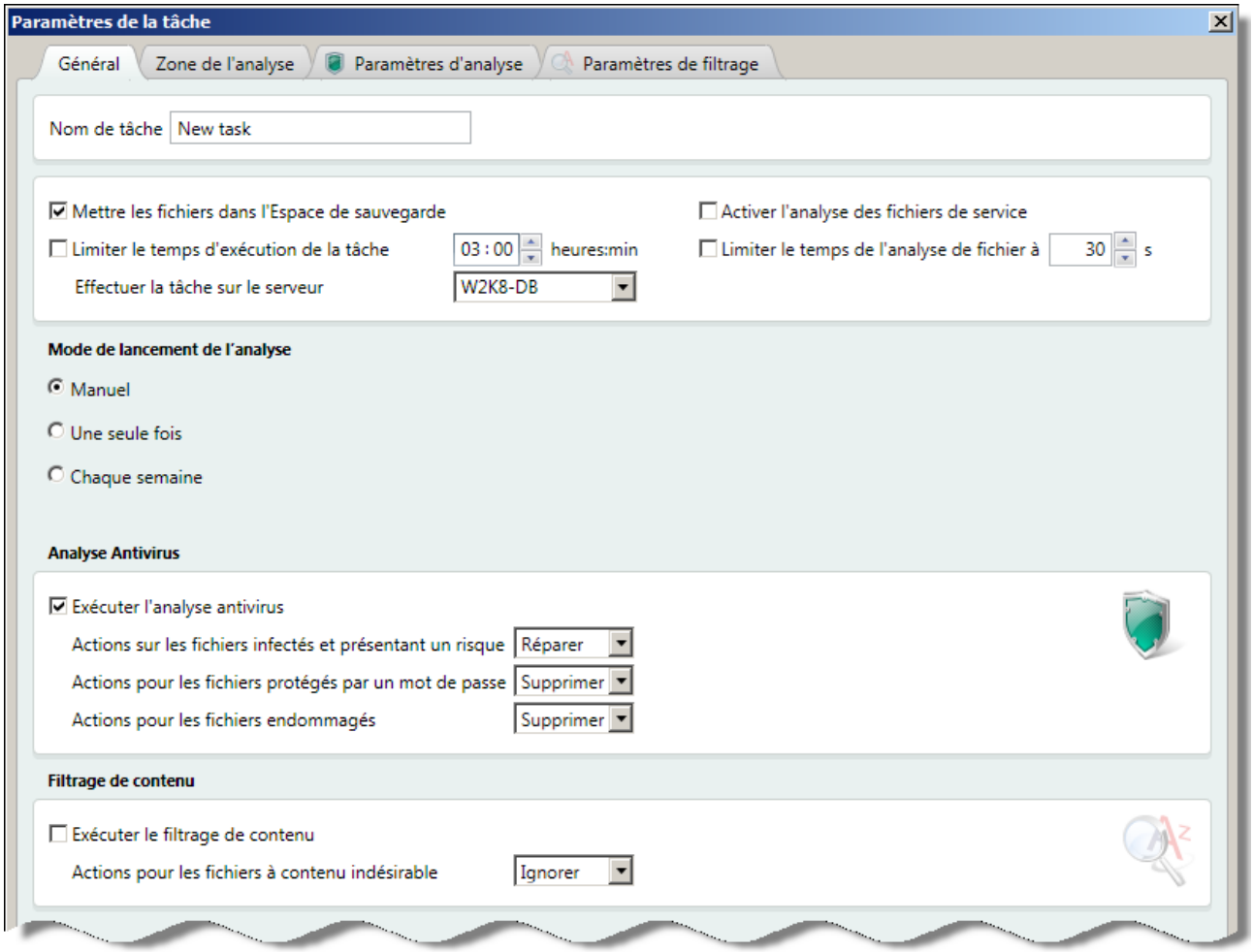

Figure 11. Paramètres de la tâche d'analyse à la demande

- Si vous souhaitez modifier le nom de la tâche, modifiez-le dans le champ **Nom de tâche**.
- Si vous souhaitez que Kaspersky Security copie les fichiers dans l'Espace de sauvegarde avant de les traiter, cochez la case **Mettre les fichiers dans l'Espace de sauvegarde**.
- Si vous souhaitez limiter le temps de l'exécution de la tâche d'analyse à la demande, cochez la case **Limiter le temps de l'exécution de la tâche** et spécifiez la valeur dans le champ à droit.
- Si vous souhaitez analyser les fichiers de service SharePoint lors de l'exécution de la tâche, cochez la case **Activer l'analyse des fichiers de service**.
- Si vous souhaitez limiter le temps de l'analyse de chaque fichier, cochez la case **Limiter le temps de l'analyse de chaque fichier à ... s** et spécifiez la valeur (en secondes) dans le champ à droit.
- Si vous voulez que la tâche soit exécutée sur un autre serveur, sélectionnez-le dans le menu déroulant **Exécuter la tâche sur le serveur**.
- Si vous souhaitez effectuer le scan antivirus lors de l'exécution de la tâche, cochez la case **Exécuter l'analyse antivirus** et spécifiez les règles de traitement des objets (cf. la rubrique "Configuration des règles de traitement des objets lors de l'analyse à la demande" à la page 46).

- Si vous souhaitez effectuer le scan antivirus lors de l'exécution de la tâche, cochez la case **Exécuter le filtrage de contenu** et spécifiez les règles de traitement des objets (cf. la rubrique "Configuration des règles de traitement des objets lors de l'analyse à la demande" à la page 46).

- En cas de besoin, créez une planification de l'exécution de la tâche d'analyse à la demande (cf. la rubrique "Création de la planification du lancement de la tâche d'analyse à la demande" à la page 45).

3. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

CREATION DE LA PLANIFICATION DU LANCEMENT DE LA TACHE D'ANALYSE A LA DEMANDE

Pour programmer le lancement automatique de la tâche d'analyse à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Général**.

3. Dans le groupe **Mode de lancement de l'analyse**, sélectionnez la variante requise du lancement de la tâche d'analyse à la demande :

   - Si vous souhaitez lancer la tâche d'analyse en temps voulu, sélectionnez **Manuel**.

   - Si vous ne souhaitez lancer la tâche d'analyse qu'une seule fois en temps voulu, sélectionnez **Une seule fois** et spécifiez le jour et l'heure du lancement de la tâche (cf. ill. ci-après).

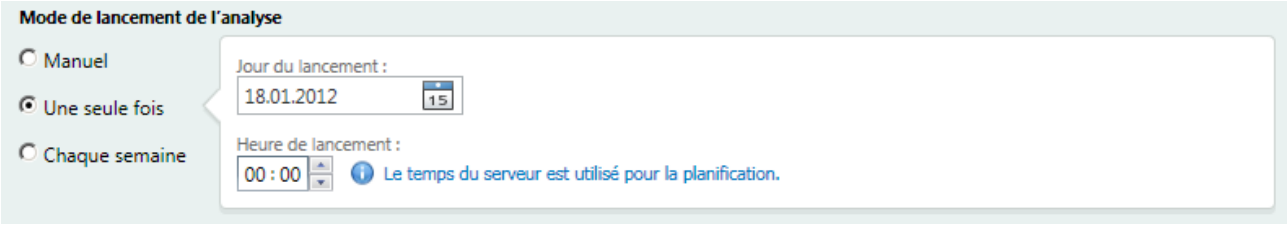

Figure 12. La planification ne s'exécute qu'une seule fois

   - Si vous souhaitez lancer la tâche d'analyse en mode automatique chaque semaine, sélectionnez **Chaque semaine** et spécifiez les dates et l'heure du lancement de la tâche (cf. ill. ci-après).

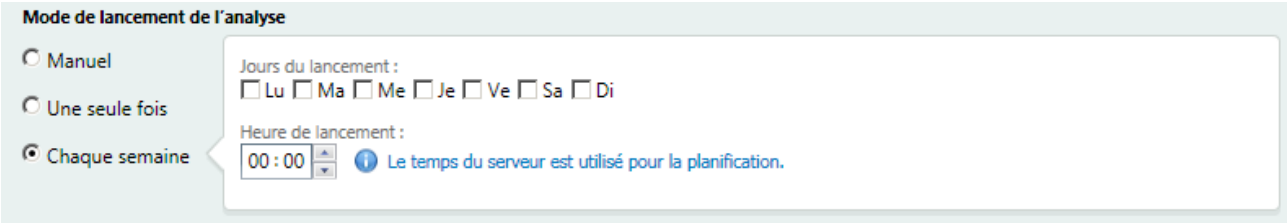

Figure 13. La planification ne s'exécute chaque semaine

Si vous sélectionnez le lancement automatique de la tâche d'analyse en temps voulu, l'application va utiliser l'heure du serveur défini dans les paramètres de la tâche (cf. la rubrique "Sélection du serveur pour lancer la tâche" à la page 43).

4. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

CONFIGURATION DES REGLES DE TRAITEMENT DES OBJETS LORS DE L'ANALYSE A LA DEMANDE

Pour créer des règles de traitement des objets lors de l'analyse à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Général**.

3. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers infectés et potentiellement infectés**, sélectionnez le type de l'action à appliquer (cf. ill. ci-après):

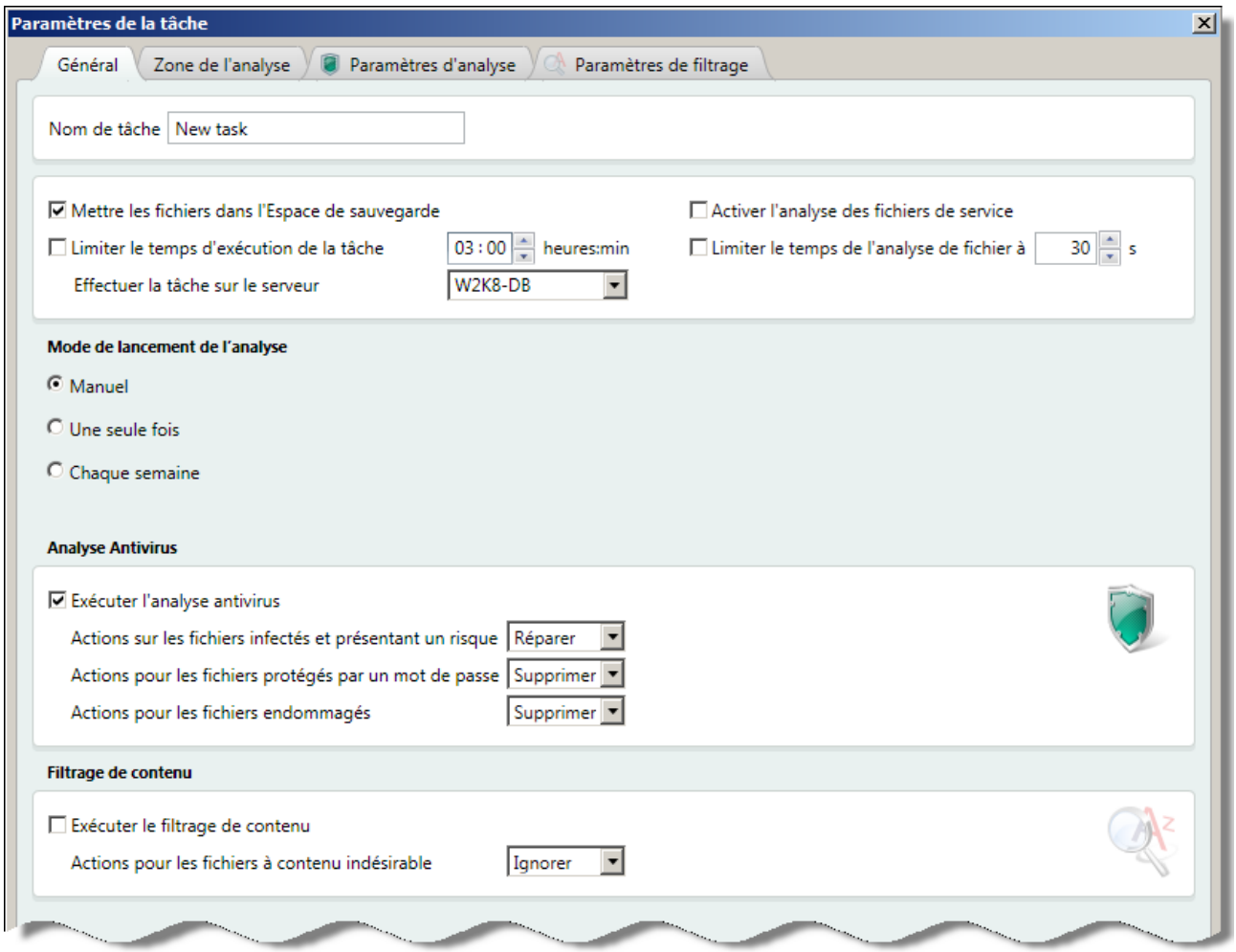

Figure 14. Paramètres de la tâche d'analyse à la demande

- **Réparer**. Kaspersky Security va essayer de réparer le fichier. S'il est impossible de réparer le fichier, l'application le remplace par un fichier texte qui explique la cause de la suppression.

- **Supprimer**. Kaspersky Security remplace tout fichier infecté ou suspect par un fichier texte qui explique la cause de la suppression.

- **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier.

4. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers protégés par un mot de passe**, sélectionnez le type de l'action à appliquer :

   - **Supprimer**. Kaspersky Security replace tout fichier protégé par un mot de passe par un fichier texte qui explique la cause de la suppression.

   - **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier.

5. Dans le groupe **Scan Antivirus** dans la liste déroulante **Actions pour les fichiers endommagés**, sélectionnez le type de l'action à appliquer :

   - **Supprimer**. Kaspersky Security remplace tout fichier endommagé par un fichier texte qui explique la cause de la suppression.

   - **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier.

Si l'option **Ignorer** est sélectionnée, aucune action ne sera effectuée sur le fichier, mais l'un des statuts lui sera attribué en fonction des résultats de l'analyse. Les informations sur le fichier seront consignées dans des rapports et dans des statistiques.

Pour créer des règles de traitement des objets lors du filtrage de contenu, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Général**.

3. Dans le groupe **Filtrage de contenu** dans la liste déroulante **Actions pour les fichiers à contenu indésirable**, sélectionnez le type de l'action à appliquer :

   - **Supprimer**. Kaspersky Security remplace tout fichier à contenu indésirable par un fichier texte qui explique la cause de la suppression.

   - **Ignorer**. Kaspersky Security n'appliquera aucune action pour le fichier.

Si l'option **Ignorer** est sélectionnée, aucune action ne sera effectuée sur le fichier, mais l'un des statuts lui sera attribué en fonction des résultats de l'analyse. Les informations sur le fichier seront consignées dans des rapports et dans des statistiques.

SELECTION DES ZONES D'ANALYSE

Vous pouvez indiquer les zones de la structure de SharePoint qui seront analysées pendant l'exécution de la tâche d'analyse à la demande. Vous pouvez également exclure de l'analyse certaines zones de la structure SharePoint.

Pour définir les zones de l'analyse, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Zone de l'analyse** (cf. ill. ci-après).

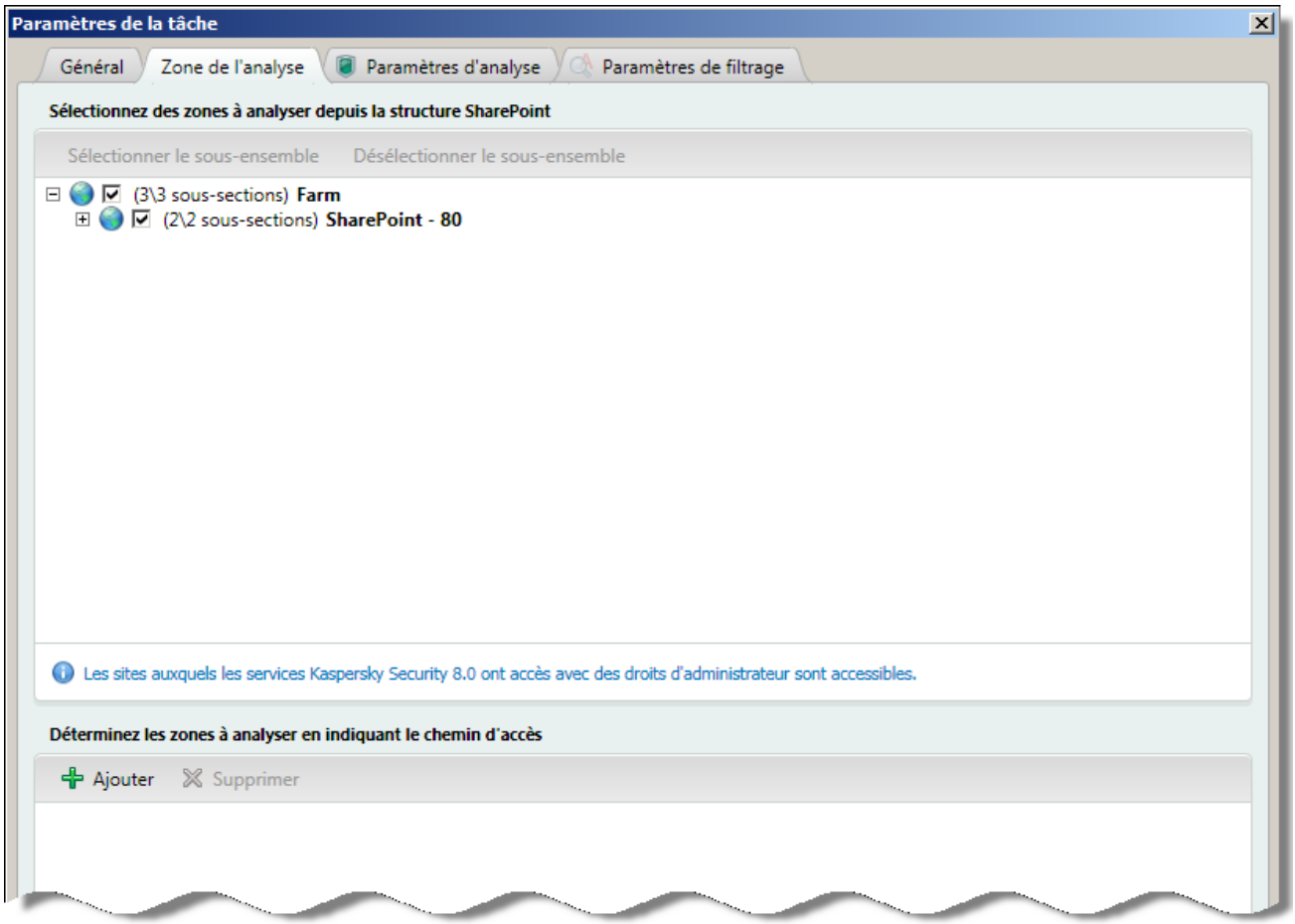

Figure 15. Sélection de zone d'analyse

3. Définissez les zones de l'analyse avec l'une des méthodes suivantes :

   - Dans l'arborescence de la structure du serveur SharePoint cochez les cases pour les zones que vous souhaitez ajouter à l'analyse. Par défaut, toutes les cases sont cochées. En d'autres termes, lors d'une tâche d'analyse à la demande, toutes les zones accessibles de SharePoint sont traitées.

     L'arborescence contient uniquement les zones SharePoint pour lesquelles le compte utilisateur de lancement des services dispose des droits d'administrateur.

   - Dans le champ **Désignez la zone en indiquant le chemin d'accès**, cochez les cases des zones définies manuellement que vous souhaitez inclure dans l'analyse. Dans le menu déroulant, sélectionnez l'action **Ajouter le chemin d'accès**.

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

4. Pour enregistrer les modifications et quitter la fenêtre, cliquez sur le bouton **OK**.

➡ *Pour exclure de l'analyse certaines zones, procédez comme suit :*

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Zone de l'analyse**.

3. Pour exclure des zones de l'analyse, utilisez un des procédés suivants :

   - Dans l'arborescence de la structure du serveur SharePoint, désélectionnez les zones que vous souhaitez exclure de l'analyse.

   - Dans le champ **Désignez la zone en indiquant le chemin d'accès**, cochez les cases des zones définies manuellement que vous souhaitez exclure de l'analyse. Dans les listes affichées, sélectionnez l'action **Exclure le chemin d'accès.**

4. Pour enregistrer les modifications et quitter la fenêtre, cliquez sur le bouton **OK**.

DEFINITION DES DOMAINES DE SHAREPOINT EN MODE MANUEL

Pour définir manuellement un domaine de SharePoint, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Zone de l'analyse**.

3. Dans le champ **Désignez la zone en indiquant le chemin d'accès**, cliquez sur **Ajouter** et, dans la fenêtre affichée, indiquez le chemin d'accès au domaine de SharePoint requis.

4. Définissez l'inclusion/l'exclusion du domaine :

   - Pour inclure un domaine dans l'analyse, cochez le chemin d'accès à ce domaine et, dans la liste affichée, sélectionnez **Ajouter le chemin d'accès**.

   - Pour exclure un domaine de l'analyse, cochez le chemin d'accès à ce domaine et, dans la liste affichée, sélectionnez **Exclure le chemin d'accès**.

5. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

CREATION D'EXCLUSIONS DE L'ANALYSE A LA DEMANDE

Pour réduire la charge du serveur, vous pouvez exclure de l'analyse à la demande certains types, formats ou masques des noms de fichiers, limiter le temps de l'analyse de chaque fichier et désactiver l'analyse des archives.

Pour exclure de l'analyse à la demande certains types de fichiers, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Paramètres d'analyse**.

3. Dans le champ **Exclusion des fichiers par format**, cochez les cases à côté des formats de fichiers que vous souhaitez exclure de l'analyse (cf. ill. ci-après).

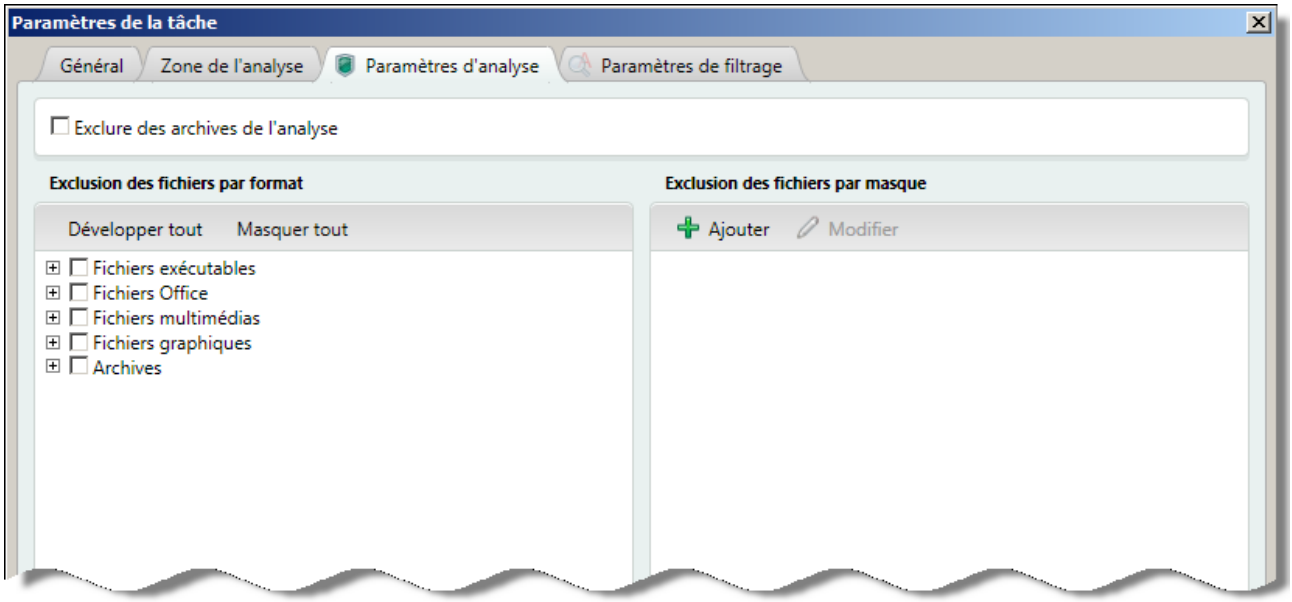

Figure 16. Exclusions de fichiers de l'analyse à la demande

Pour votre confort, vous pouvez administrer l'arborescence de la structure avec des boutons suivants **Développer tout** et **Masquer tout**.

4. Pour enregistrer les modifications et quitter la fenêtre, cliquez sur le bouton **OK**.

Pour exclure de l'analyse des fichiers par masque, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Paramètres d'analyse**.

3. Dans le champ **Exclure des fichiers par masque**, cochez les cases correspondant aux masques à exclure de l'analyse.

4. Pour ajouter un masque sur la liste, ouvrez la fenêtre **Ajout d'un masque** en cliquant sur le bouton **Ajouter** et spécifiez le masque dans le champ de saisie. Pour quitter la fenêtre, cliquez sur le bouton **OK**.

   Si vous souhaitez définir plusieurs masques, utilisez dans le champ de saisie le point-virgule, pour les séparer.

5. Pour enregistrer les modifications et quitter la fenêtre, cliquez sur le bouton **OK**.

Pour exclure de l'analyse à la demande des archives, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier** ouvrez la fenêtre **Paramètres de la tâche** et sous l'onglet **Paramètres de la tâche** cochez la case **Exclure des archives de l'analyse**.

3. Pour enregistrer les modifications et quitter la fenêtre, cliquez sur le bouton **OK**.

PARAMETRES DU FILTRAGE DE CONTENU

Lors de l'analyse à la demande, vous pouvez indiquer un format de fichier, des masques de nom de fichier incorrects ainsi que des catégories de mots et expressions indésirables.

Pour définir les paramètres de filtrage de contenu lors d'une analyse à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez dans la liste des tâches du panneau des résultats la tâche d'analyse à la demande dont vous souhaitez modifier les paramètres. En cliquant sur le bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche** sous l'onglet **Paramètres CF**.

3. Sélectionnez et définissez les paramètres de filtrage de contenu :

   - Dans le champ **Listes des mots et des expressions indésirables**, cochez les rubriques de Kaspersky Lab et les catégories d'utilisateurs à inclure dans la tâche d'analyse à la demande.

   - Dans le champ **Formats indésirables des fichiers**, cochez les formats et les extensions de fichiers qui feront l'objet d'une recherche. Pour développer/réduire la liste complète des formats et des extensions, cliquez sur **Développer tout** et **Réduire tout**.

   - Dans le champ des **jeux de masques de noms de fichiers indésirables**, cochez les jeux de masques qui doivent faire l'objet d'une recherche lors de l'analyse à la demande.

4. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

Vous pouvez définir la composition des listes de mots, d'expressions, de formats et de masques indésirables des noms de fichier dans le nœud Filtrage de contenu (cf. la rubrique "Paramètres du filtrage de contenu" à la page 53).

CREATION D'UNE NOUVELLE TACHE D'ANALYSE A LA DEMANDE

Pour créer une nouvelle tâche d'analyse à la demande, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. En cliquant sur le bouton **Créer** dans le panneau des résultats, ouvrez la fenêtre **Paramètres de la tâche** (cf. ill. ci-après).

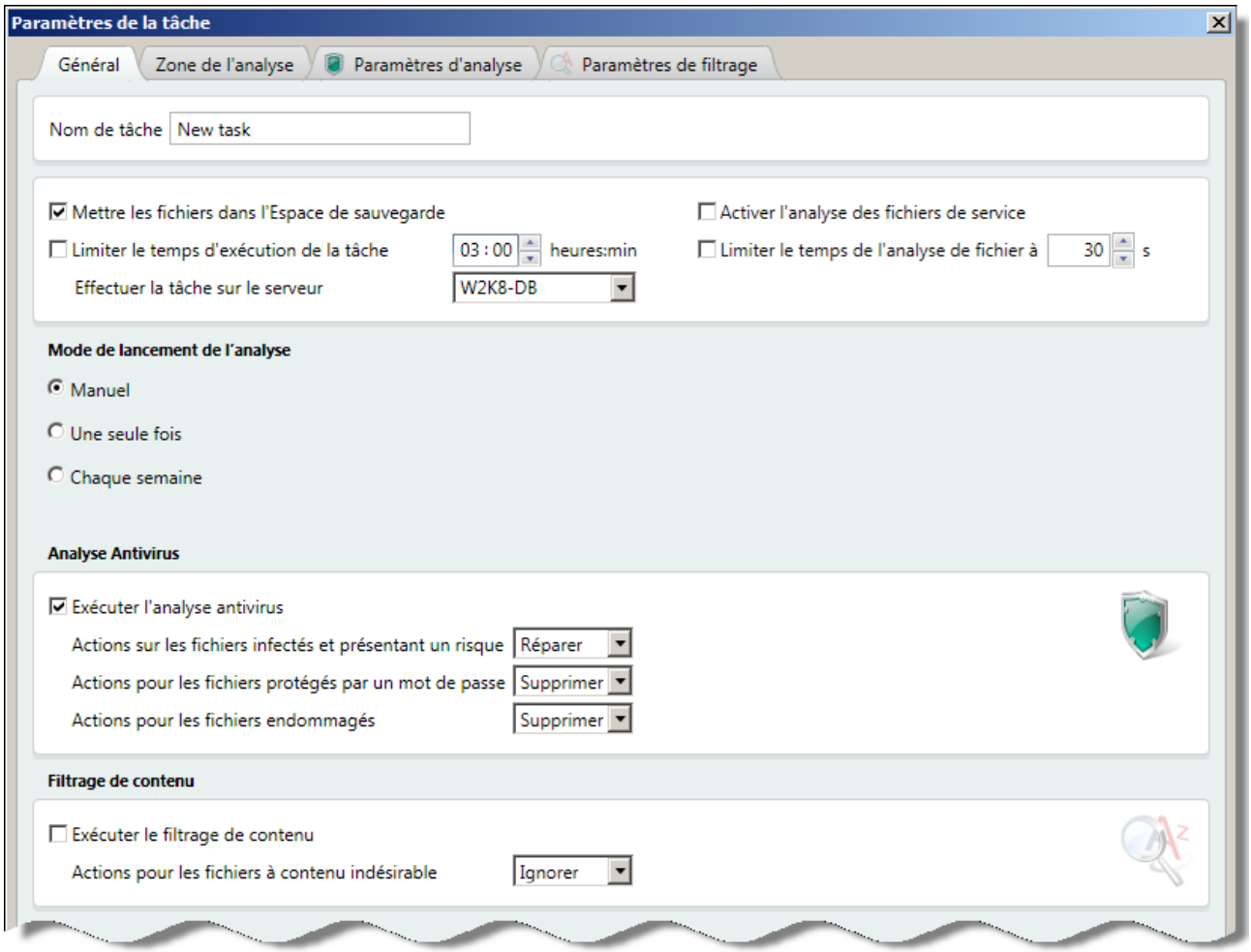

Figure 17. Paramètres d'une nouvelle tâche d'analyse à la demande

3. Définissez tous les paramètres requis de la tâche d'analyse et cliquez sur le bouton **OK**.

   La tâche créée sera ajoutée sur la liste des tâches dans le panneau des résultats. Si nécessaire, vous pouvez modifier les paramètres de la tâche.

SUPPRESSION DE LA TACHE D'ANALYSE A LA DEMANDE

➡ *Pour supprimer une tâche d'analyse à la demande, procédez comme suit :*

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Analyse à la demande**.

2. Dans le panneau des résultats, sélectionnez sur la liste la tâche que vous souhaitez supprimer et cliquez sur le bouton **Supprimer**.

FILTRAGE DE CONTENU

Cette section reprend les informations sur la configuration des règles du filtrage de contenu, effectuée lors de la vérification à la demande ou sur requête.

DANS CETTE SECTION

A propos du filtrage de contenu 53

Paramètres du filtrage de contenu 53

A PROPOS DU FILTRAGE DE CONTENU

Kaspersky Security fournit un filtrage de contenu des fichiers, stockés sur le serveur SharePoint.

Pour le filtrage des fichiers, procédez comme suit :

- selon les formats des fichiers ;
- selon les masques de noms de fichiers ;
- selon le contenu texte des fichiers et les noms des fichiers.

Lors de l'utilisation avec le serveur Microsoft SharePoint Server 2007 SP2 installé sur Windows 2003 Server SP2, Kaspersky Security extrait et analyse le contenu des fichiers texte et des fichiers au format RTF seulement si le panneau de recherche Windows Search 4.0 est installé.

Conformément aux paramètres spécifiés, le filtrage de contenu peut être effectué lors de l'analyse à la demande (cf. la rubrique "Analyse à la demande" à la page 40), ou sur requête (cf. la rubrique "Analyse au moment de l'accès" à la page 30).

Vous pouvez sélectionner un masque de noms et de formats de fichiers indésirables et créer une catégorie de mots et expressions indésirables.

Kaspersky Security contient un ensemble prédéfini de catégories de mots et d'expressions indésirables, créé par les spécialistes de Kaspersky Lab. Cet ensemble de catégories est mis à jour depuis les serveurs de Kaspersky Lab. La liste prédéfinie de mots et d'expressions indésirables ne peut pas être modifiée.

PARAMETRES DU FILTRAGE DE CONTENU

Lors de la configuration du filtrage de contenu, vous pouvez spécifier les paramètres suivants de la définition du contenu indésirable :

- mots et expressions;
- masques des noms de fichiers interdits.

CONFIGURATION DES CATEGORIES D'UTILISATEURS DE MOTS ET EXPRESSIONS INDESIRABLES

Pour créer une nouvelle catégorie de mots et expressions indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite **Filtrage de contenu** (cf. ill. ci-après).

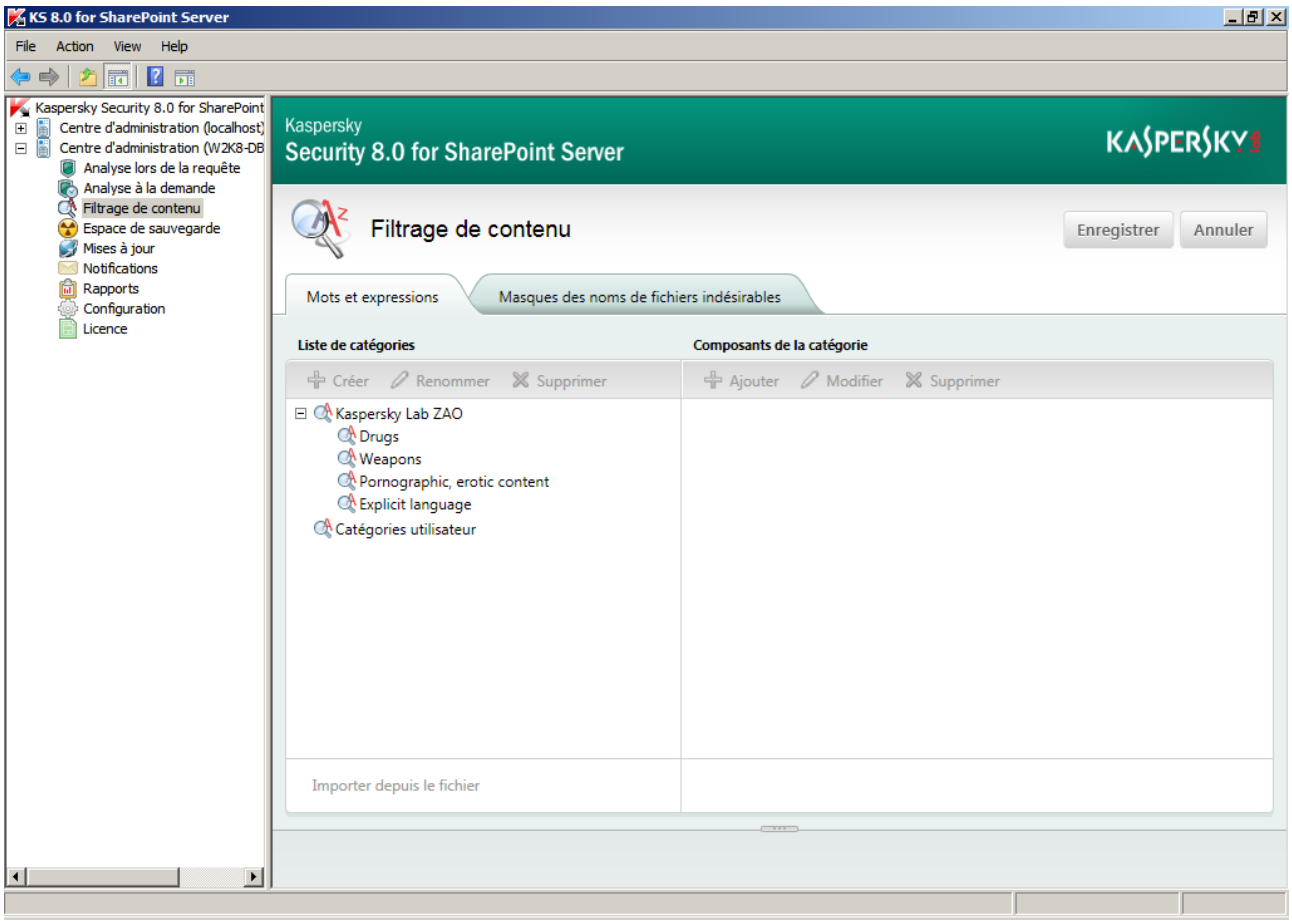

*Figure 18. Ensuite, sélectionnez le nœud **Filtrage de contenu**.*

2. Dans le panneau de résultats, sélectionnez l'onglet **Mots et expressions** et cliquez sur **Créer** dans le bloc **Liste de catégories**.

3. Dans la fenêtre d'**ajout de catégorie,** saisissez le nom de la nouvelle catégorie.

4. Cliquez sur le bouton **OK**.

Pour renommer une catégorie de mots et expressions indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats, sélectionnez **Mots et expressions,** choisissez la catégorie que vous souhaitez renommer, puis cliquez sur **Renommer**.

3. Dans la fenêtre **Modification de catégorie**, spécifiez le nouveau nom de la catégorie, puis cliquez sur **OK**.

Pour supprimer une nouvelle catégorie de mots et expressions indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Puis, sélectionnez **Règles du filtrage de contenu**.

2. Dans le panneau de résultats, sélectionnez **Mots et expressions,** Dans le bloc **Liste de catégories** choisissez la catégorie que vous souhaitez supprimer, puis cliquez sur **Supprimer**. La catégorie sélectionnée sera supprimée de la liste.

Vous pouvez créer, renommer et supprimer uniquement des catégories d'utilisateurs. Vous ne pouvez pas modifier l'ensemble préinstallé des rubriques, offert par Kaspersky Lab.

MODIFICATION DES MOTS ET EXPRESSIONS INCLUS DANS LE CONTENU DES CATEGORIES D'UTILISATEURS

Pour ajouter dans le contenu de la catégorie des mots et expressions indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats **Mots et expressions**, dans le champ **Liste de catégories**, sélectionnez les catégories d'utilisateurs pour laquelle vous souhaitez ajouter un mot ou une expression.

3. Dans le champ **Composition de la catégorie** cliquez sur **Ajouter**. Dans la fenêtre qui apparaît, saisissez dans le champ le mot ou l'expression.

   L'application considère tout symbole qui n'est pas une lettre ou un chiffre comme espace.

4. Si vous le souhaitez, pour rechercher un mot ou expression qui respecte la casse, cochez la case **Respect de la casse**. Cliquez sur le bouton **OK**.

   Vous pouvez spécifier plusieurs mots ou expressions. En les séparant par " | ".

Pour modifier un mot ou expression, inclus dans le contenu de la catégorie sélectionnée, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats **Mots et expressions**, dans le champ **Liste de catégories**, sélectionnez les catégories d'utilisateurs pour laquelle vous souhaitez modifier un mot ou une expression.

3. Dans le champ **Contenu de la catégorie** sélectionnez le mot ou expression que vous souhaitez modifier, puis cliquez sur **Modifier**.

4. Dans la fenêtre qui apparaît, modifiez le mot ou expression. Demandez le respect de la casse, si nécessaire. Cliquez sur le bouton **OK**.

Pour supprimer un mot ou une expression, inclus dans le contenu de la catégorie sélectionnée, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats **Mots et expressions**, dans le champ **Liste de catégories**, sélectionnez le contenu de la catégorie d'utilisateurs pour lequel vous souhaitez supprimer un mot ou une expression.

Vous pouvez sélectionner plusieurs mots ou expressions inclus dans le contenu de la catégorie en appuyant sur la touche **SHIFT** du clavier.

3. Dans le champ **Contenu de la catégorie** sélectionnez le mot ou expression que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Vous pouvez créer, renommer, éditer et supprimer uniquement des catégories d'utilisateurs. L'ensemble prédéfini de rubriques fourni par Kaspersky Lab n'est pas modifiable.

IMPORTATION D'UNE LISTE DE MOTS ET D'EXPRESSIONS INDESIRABLES

Dans une catégorie d'utilisateurs, vous pouvez importer une liste de mots et d'expressions indésirables d'un fichier texte.

Les mots et les phrases d'un tel fichier doivent respecter les conditions suivantes :

- Une ligne ne doit contenir qu'un seul terme avec les formes associées.
- Le terme doit être séparé des formes associées par le symbole " | ".
- La longueur du terme ne doit pas dépasser 127 symboles.

Dans le cas d'utilisation des symboles spéciaux dans le terme ou des symboles du cryptage multioctet, par exemple, UTF-8 (lors du cryptage par trois octets ou plus), la longueur du terme ne doit pas dépasser 64 symboles.

Pour supprimer une liste de mots et expressions indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.
2. Dans le panneau de résultats **Mots et expressions**, dans le champ **Liste de catégories**, sélectionnez la catégorie pour laquelle vous souhaitez Importer la liste.
3. Dans le champ **Liste de catégories**, cliquez sur **Importer depuis le fichier**. Dans la fenêtre qui apparaît, indiquez le chemin d'accès au fichier requis.

   Le bouton **Importer depuis un fichier** n'est accessible que pour les catégories utilisateur de mots et expressions indésirables.

4. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer**.

UTILISATION DES SYMBOLES DANS LES MOTS ET LES PHRASES AU NOMBRE DES CATEGORIES D'UTILISATEURS

Lors de la recherche des mots et des phrases dans les documents, les symboles suivants seront ignorés : ,, ., :, ;, ', ", -, –, —, ..., (,), [,], {, }, <, >, \, /, ®, ¦, °, ™, ", ", v, ©, №.

Les symboles suivants seront considérés comme des mots séparés : !, ?, ~, @, $, #, %, ^, &, *, _, +, =, |, `.

Les symboles suivants sont des symboles interdits : ,•!!.

MASQUES DES NOMS DE FICHIERS INDESIRABLES

Pour créer un nouvel ensemble de masques des noms de fichiers indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite **Filtrage de contenu** (cf. ill. ci-après).

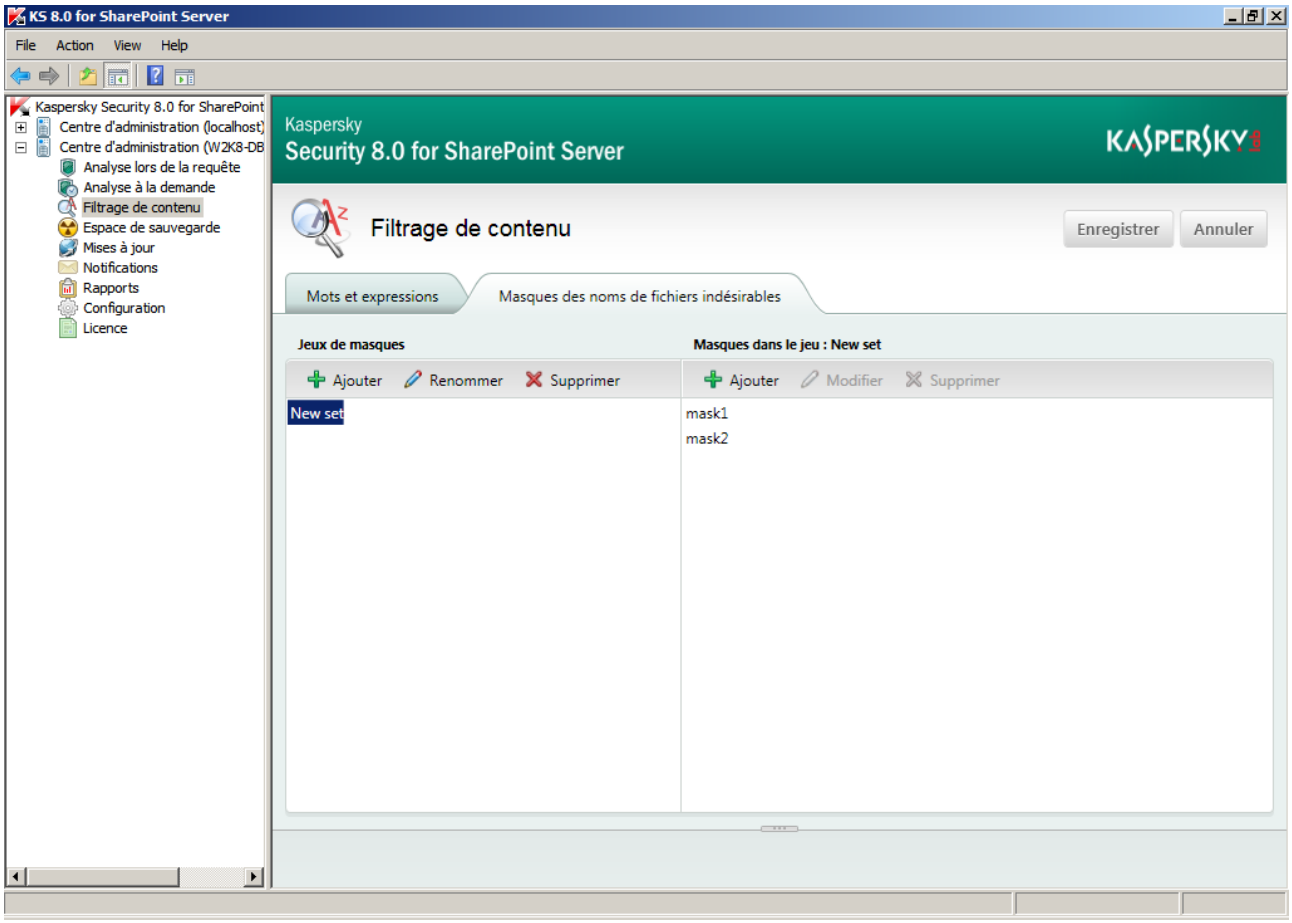

Figure 19. Masques des noms de fichiers indésirables

2. Dans le panneau des résultats sous l'onglet **Masques des noms de fichiers indésirables**, cliquez sur le bouton **Ajouter.** Fenêtre d'**ajout d'un nom d'ensemble de masques de fichiers.**

3. Dans la fenêtre qui apparaît, saisissez le nom du nouvel ensemble de masques.

4. Cliquez sur le bouton **OK**.

Pour renommer un nouvel ensemble de masques des noms de fichiers indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau des résultats sous l'onglet **Masques des noms de fichiers indésirables**, sélectionnez l'ensemble des masques à donner un autre nom, puis cliquez sur le bouton **Donner un autre nom**.

3. Dans la fenêtre qui apparaît, spécifiez le nouveau nom de l'ensemble des masques, puis cliquez sur **OK**.

Pour supprimer l'ensemble de masques des noms de fichiers indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau des résultats sous l'onglet **Masques des noms de fichiers indésirables**, sélectionnez l'ensemble des masques à supprimer, puis cliquez sur le bouton **Supprimer**.

MODIFICATION DE L'ENSEMBLE DE MASQUES DES NOMS DE FICHIERS INDESIRABLES

Pour ajouter un masque des noms de fichiers indésirables dans l'ensemble, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats, sélectionnez **Masques des noms de fichiers indésirables** et dans le champ **Jeux de masque**, sélectionnez l'ensemble dont vous souhaitez ajouter un masque (cf. ill. ci-après).

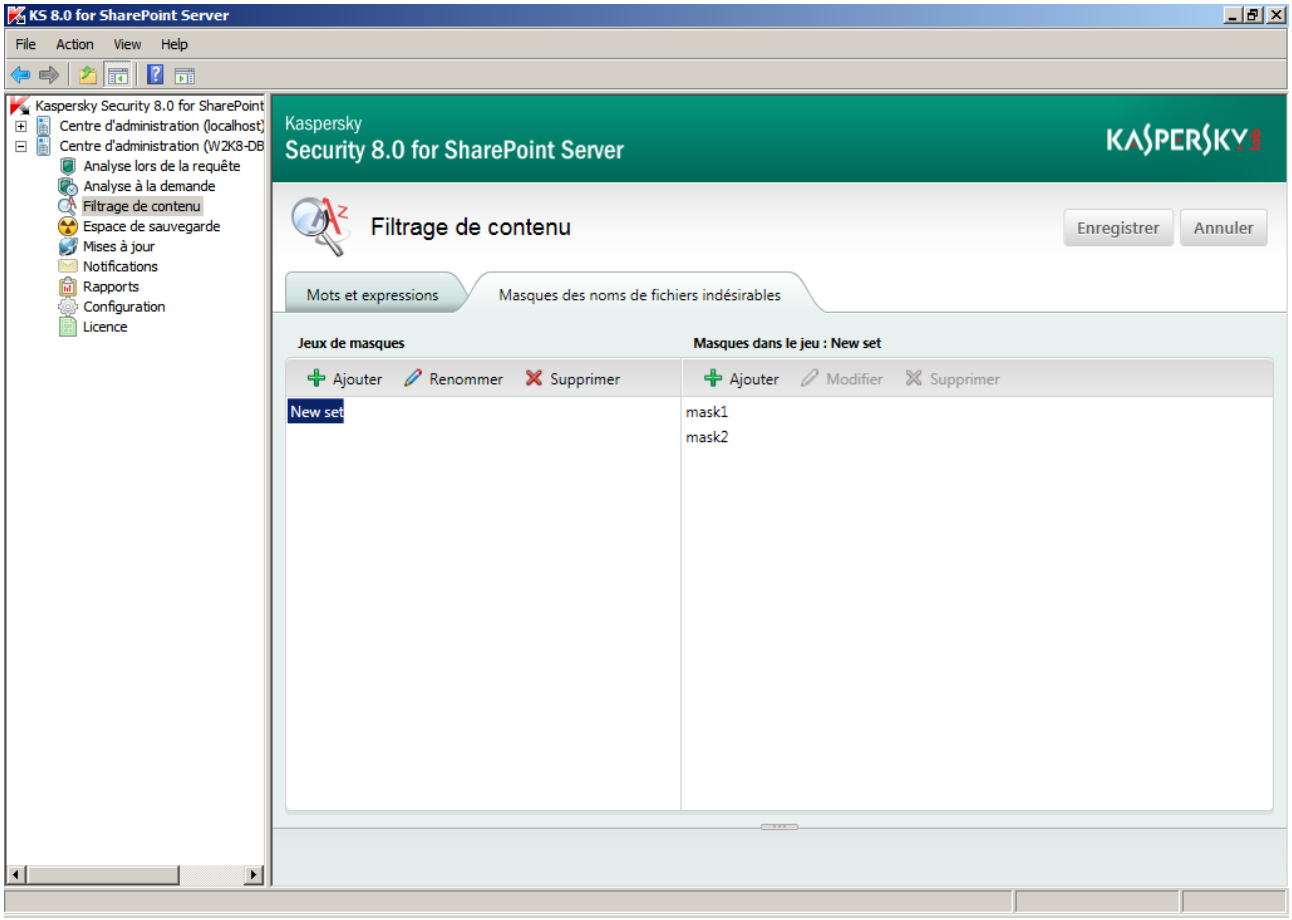

Figure 20. Masques des noms de fichiers indésirables

3. Dans le champ **Masques dans le jeu**, cliquez sur **Ajouter**. Dans la fenêtre qui apparaît, entrez dans le champ de saisie le masque des noms de fichiers indésirables.

Vous pouvez spécifier plusieurs masques. En les séparant par " ; ".

Pour modifier un masque de noms de fichiers indésirables, inclus dans l'ensemble sélectionné, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Puis, sélectionnez **Règles du filtrage de contenu**.

2. Dans le panneau de résultats, sélectionnez **Masques des noms indésirables de fichiers** et dans le champ **Jeux de masque**, sélectionnez l'ensemble dont vous souhaitez modifier le masque.

3. Dans le champ **Masques dans le jeu**, sélectionnez le masque que vous souhaitez modifier, puis cliquez sur **Modifier**.

4. Dans la fenêtre qui apparaît, modifiez le masque, puis cliquez sur **OK**.

Pour supprimer le masque de l'ensemble de masques des noms de fichiers indésirables, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Filtrage de contenu**.

2. Dans le panneau de résultats, sélectionnez **Masques des noms interdits de fichiers** et dans le champ **Jeux de masque**, sélectionnez l'ensemble dont vous souhaitez supprimer le masque.

   Vous pouvez sélectionner dans la liste plusieurs masques inclus dans l'ensemble en appuyant sur la touche **SHIFT** du clavier.

3. Dans le champ **Masques dans le jeu**, sélectionnez le masque que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Si vous avez sélectionné plusieurs masques inclus dans l'ensemble, alors vous pouvez supprimer uniquement ceux sélectionnés. D'autres actions applicables sur ces masques ne seront pas disponibles.

UTILISATION DES MASQUES DES NOMS DE FICHIERS INDESIRABLES

Lors de la création de masques, observez les recommandations suivantes :

- Utilisez les symboles suivants :
  - * : n'importe quelle séquence de caractères. Par exemple, le masque abc* signifie n'importe quel fichier dont le nom commence par la séquence abc : abc.exe, abc1.com, abc2.rar.
  - ? – n'importe quel symbole individuel. Par exemple, le masque abc?.exe signifie un fichier dont le nom commence par la séquence abc avec n'importe quel symbole après la lettre c, par exemple abc1.exe. Cependant, le fichier abc12345.exe ne sera pas défini par ce masque.
- Les limitations suivantes sont imposées aux masques des noms de fichiers :
  - Symboles interdits dans les masques : >, <, \, /, |, ", ;.
  - Nous déconseillons l'utilisation de masques désignant tous les fichiers avec les extensions contenant des fichiers auxiliaires SharePoint (par exemple, *.aspx, *.html et *.mht). En cas de suppression de fichiers de service SharePoint, son fonctionnement sera perturbé.

ESPACE DE SAUVEGARDE

Cette section contient des informations sur l'Espace de sauvegarde, ainsi que les instructions sur la gestion des copies des documents placées dans l'Espace de sauvegarde et sur la configuration des paramètres de l'Espace de sauvegarde.

DANS CETTE SECTION

A propos de l'Espace de sauvegarde 60

Actions sur les objets placés dans l'Espace de sauvegarde 61

A PROPOS DE L'ESPACE DE SAUVEGARDE

Kaspersky Security place des copies des fichiers à traiter dans l'Espace de sauvegarde. L'application place dans l'Espace de sauvegarde les copies de tous les fichiers classés malveillants par l'analyse à la demande ou la protection en temps réel. L'application place dans l'Espace de sauvegarde les copies de tous les fichiers malveillants qu'ils soient réparables ou irréparables.

Kaspersky Security place les fichiers dans l'Espace de sauvegarde en mode crypté ce qui assure :

- un risque zéro d'infection (les fichiers dans l'Espace de sauvegarde sont inaccessibles sans les déchiffrer) ;
- un gain de temps de fonctionnement de l'application antivirus (l'application antivirus ne considère pas les fichiers placés dans l'Espace de sauvegarde comme infectés et ne les analyse pas une deuxième fois).

Taille de l'Espace de sauvegarde

Le volume d'informations de l'Espace de sauvegarde est limité de la manière suivante :

- Le nombre total des fichiers dans l'Espace de sauvegarde ne doit pas dépasser 50 000. Cette restriction est une restriction système. Vous ne pouvez pas l'annuler.
- Vous pouvez imposer une restriction supplémentaire relative à la taille de l'Espace de sauvegarde dans les paramètres de l'Espace de sauvegarde.

Suppression des fichiers de l'Espace de sauvegarde

L'application vérifie périodiquement (chaque fois qu'elle place un nouveau fichier dans la sauvegarde) si les restrictions imposées relatives à la taille de l'Espace de sauvegarde sont respectées. Si les restrictions ne sont pas respectées, l'application supprime les fichiers de l'Espace de sauvegarde selon l'algorithme suivant :

- si le nombre limite des fichiers dans la sauvegarde est dépassé, aucun fichier ne sera plus placé dans l'Espace de sauvegarde ;
- si une restriction imposée relative à la taille de la sauvegarde est dépassée et un fichier de trop est copié, l'application supprime des fichiers les plus anciens pour acquérir ce fichier supplémentaire.

Vous pouvez également supprimer les fichiers de l'Espace de sauvegarde manuellement. Vous pouvez avoir besoin par exemple de supprimer les fichiers qui ont été restaurés, ou de supprimer tous les fichiers pour un nettoyage complet de l'Espace de sauvegarde.

ACTIONS SUR LES OBJETS PLACES DANS L'ESPACE DE SAUVEGARDE

Pour chacun des fichiers placés dans l'Espace de sauvegarde, vous pouvez effectuer les actions suivantes :

- **Consulter la liste des fichiers**. Vous pouvez consulter la liste des fichiers placés en quarantaine, sous forme d'une table.
- **Rechercher des fichiers requis dans la liste des fichiers**. Pour trouver les fichiers requis dans la liste des fichiers, vous pouvez utiliser la fonction de la recherche rapide ou le filtre avancé.
- **Consulter les propriétés des fichiers**. Vous pouvez consulter les informations détaillées sur les fichiers placés dans l'Espace de sauvegarde, notamment, le nom de l'utilisateur qui a modifié le fichier ou le nom de la menace que le fichier contient.
- **Restaurer les fichiers**. Vous pouvez restaurer le fichier dans son emplacement d'origine, si vous vous voulez, par exemple, le soumettre à une nouvelle analyse faite avec une version actualisée des bases.
- **Enregistrer les fichiers sur le disque**. Vous pouvez enregistrer le fichier sur le disque local de votre ordinateur pour avoir, par exemple, plus de détails sur ce fichier.
- **Supprimer les fichiers**. Vous pouvez supprimer de l'Espace de sauvegarde les fichiers que vous n'avez plus besoin de garder.
- **Nettoyer l'Espace de sauvegarde**. Vous pouvez nettoyer l'Espace de sauvegarde en supprimant tous les fichiers stockés.

DANS CETTE SECTION

Consultation de la liste des objets placés dans l'Espace de sauvegarde 61

Recherche des objets dans l'Espace de sauvegarde 64

Restauration des objets de l'Espace de sauvegarde 68

Enregistrement des objets placés dans l'Espace de sauvegarde sur le disque 70

Suppression des fichiers de l'Espace de sauvegarde 71

Nettoyage de l'Espace de sauvegarde 72

CONSULTATION DE LA LISTE DES OBJETS PLACES DANS L'ESPACE DE SAUVEGARDE

Vous pouvez consulter la liste des fichiers placés dans l'Espace de sauvegarde sous forme d'une table avec les en-têtes.

Pour consulter la liste des fichiers placés dans l'Espace de sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Sauvegarde**.

La fenêtre de résultats affichera les informations sur l'Espace de sauvegarde et la liste des fichiers placés dans l'Espace de sauvegarde (cf. ill. ci-après).

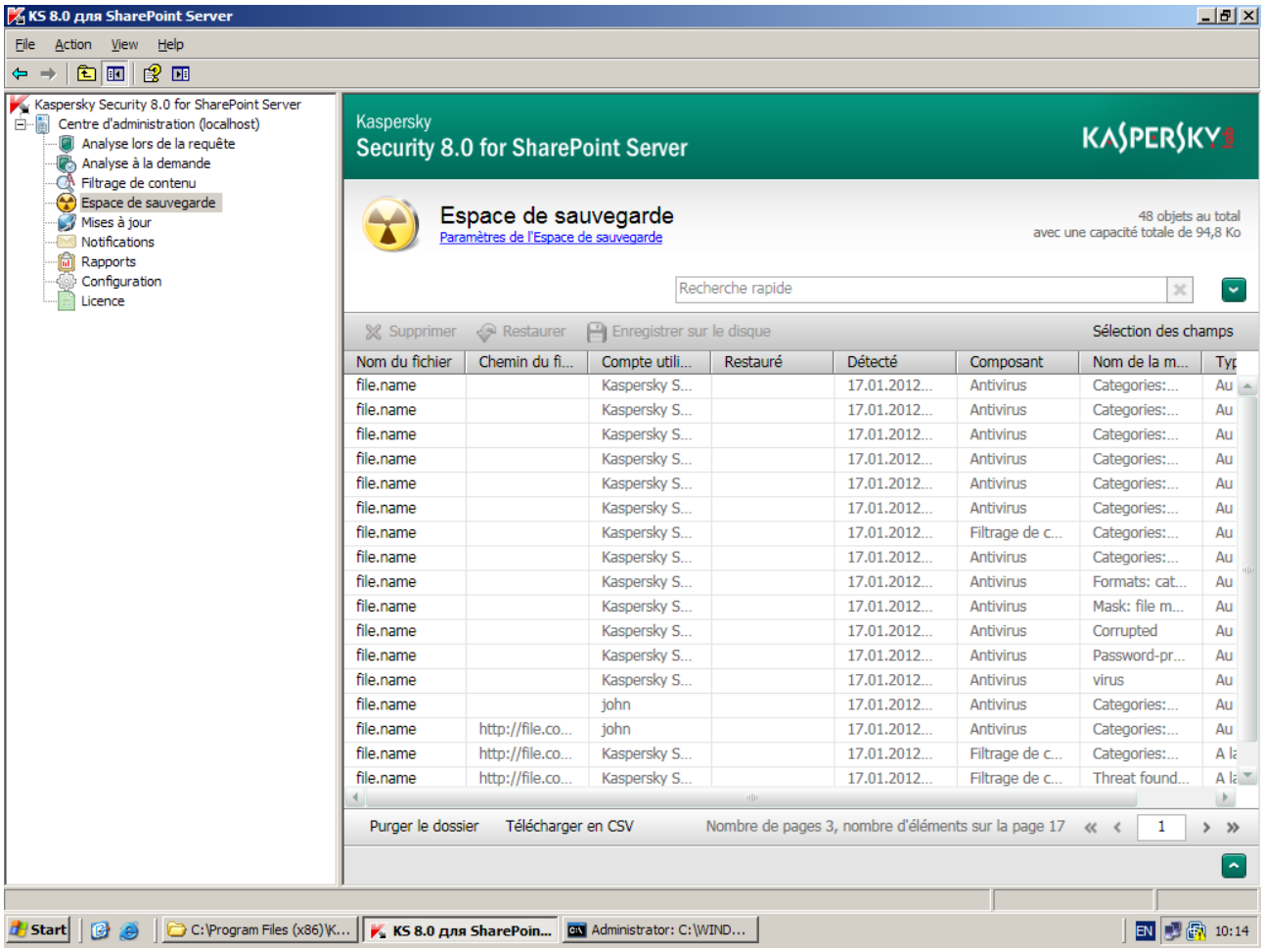

Figure 21. Sauvegarde

Dans le coin supérieur gauche du panneau des résultats, les informations suivantes sur l'Espace de sauvegarde sont affichées :

- le nombre de fichiers placés ;
- la capacité mémoire nécessaire au stockage des fichiers.

Dans le coin inférieur droit les informations suivantes sont affichées :

- La plage de lignes affichées dans la table avec la liste des fichiers.
- Le nombre de lignes dans la table avec la liste des fichiers.
- Le nombre de la page de la liste des fichiers.

Sur la liste des fichiers, vous pouvez consulter les informations sur les fichiers placés dans l'Espace de sauvegarde. En fonction des colonnes sélectionnées pour être affichées dans la table, la liste des fichiers peut s'afficher d'une manière différente. Par défaut, la liste affiche les informations suivantes sur les fichiers :

- **Nom du fichier**. Nom du fichier.
- **Chemin du fichier**. Chemin d'accès à l'emplacement du fichier.

- **Compte utilisateur**. Nom du compte de l'utilisateur qui a effectué l'action nécessitant le placement du fichier dans l'Espace de sauvegarde.
- **Restauré**. Date et heure de restauration du fichier sur le serveur.
- **Détecté**. Date et heure de détection d'une menace dans le fichier.
- **Composant**. Composant qui a marché lors de l'analyse du fichier : l'analyse antivirus ou le filtrage de contenu.
- **Nom de menace**. Nom de la menace identifiée dans le fichier.
- **Type d'analyse**. Type d'analyse lors de laquelle la menace a été détectée : à la demande ou lors d'une requête.

2. Vous pouvez configurer l'aperçu de la liste des fichiers en sélectionnant les colonnes à afficher dans la table. Pour sélectionner les colonnes, procédez comme suit :

   a. Cliquez sur le bouton **Choix des champs**.

   La fenêtre **Choix des champs pour l'affichage** s'ouvre (cf. ill. ci-après).

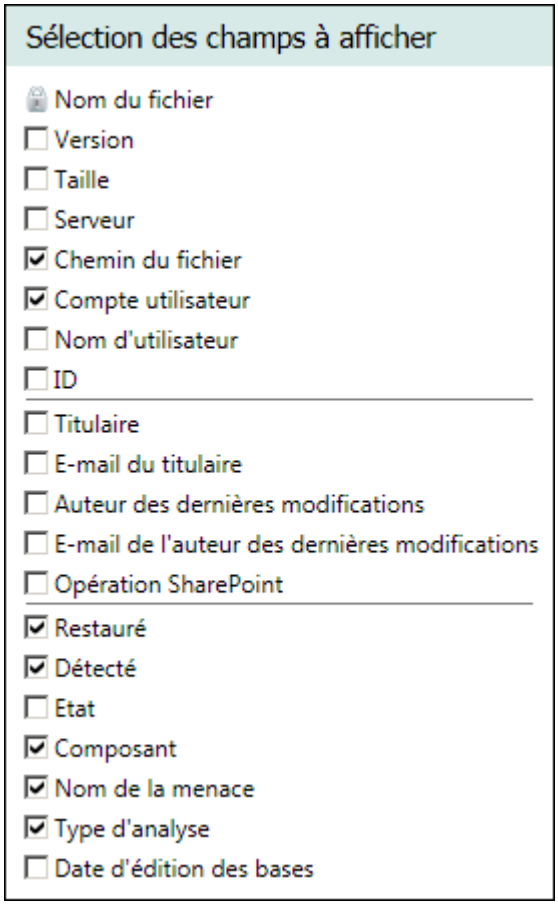

Figure 22. Sélection des champs pour afficher dans la Sauvegarde

   b. Cochez les cases des paramètres de fichiers que vous voulez afficher dans la fenêtre des résultats. Décochez les cases des paramètres de fichiers que vous ne voulez pas afficher dans la fenêtre des résultats.

   La colonne **Nom du fichier** est toujours affichée. Il est impossible de la masquer.

c. Cliquez sur le bouton **OK**, pour fermer la fenêtre.

La table avec la liste des fichiers affichera les colonnes sélectionnées.

Lorsque vous utilisez Microsoft SharePoint Server 2007, vous ne pouvez pas remplir les colonnes **Chemin du fichier**, **Détenteur**, **E-mail du détenteur**, **Auteur des modifications** et **E-mail de l'auteur des modifications** pendant l'analyse au moment de l'accès.

3. Vous pouvez trier la liste des fichiers dans la table par n'importe quelle colonne dans l'ordre croissant ou décroissant. Pour ce faire, cliquez sur l'en-tête de la colonne que vous souhaitez utiliser pour trier la liste des fichiers, par exemple **Nom du fichier**, **Chemin du fichier**, **Composant**. Pour inverser l'ordre du tri, cliquez encore une fois sur l'en-tête de la colonne.

4. La liste des fichiers sera triée par la colonne sélectionnée. L'en-tête de la colonne sélectionnée affichera le symbole du tri :

   - (*icône : flèche vers le bas*) : si un tri croissant a été effectué ;
   - (*icône : flèche vers le haut*) : si un tri croissant a été effectué.

Pour consulter les informations relatives à un fichier spécifique, vous pouvez le trouver dans la liste des fichiers en utilisant les boutons permettant de passer à la page suivante/précédente, à la première/à la dernière page de la liste des fichiers « ‹ 1 › ». Pour pouvoir trouver les fichiers requis dans la liste des fichiers, vous pouvez également utiliser la fonction de la recherche rapide et le filtre avancé.

RECHERCHE DES OBJETS DANS L'ESPACE DE SAUVEGARDE

Pour trouver les fichiers requis dans la liste des fichiers, vous pouvez utiliser les fonctions suivantes :

- **Recherche rapide**. La fonction de la recherche rapide vous permet de trouver les fichiers dont les paramètres (nom du fichier, compte utilisateur, etc.) contiennent une ligne modèle spécifique.
- **Filtre avancé**. Le filtre avancé vous permet de définir l'ensemble des conditions de filtrage relatives à plusieurs paramètres du fichier (nom du serveur SharePoint, type de menace, etc.) après avoir spécifié pour chacun des paramètres une ligne modèle spécifique et une règle de comparaison entre le paramètre et la ligne modèle. L'application du filtre avancé vous permet de trouver des fichiers dont les paramètres sont conformes à toutes les conditions de filtrage spécifiées.

RECHERCHE DES OBJETS DANS L'ESPACE DE SAUVEGARDE : RECHERCHE RAPIDE

Pour lancer la recherche des objets dans l'Espace de sauvegarde avec la fonction de la recherche rapide, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Sauvegarde**.

   Un panneau des résultats placés dans l'Espace de sauvegarde s'affichera dans la fenêtre des résultats.

2. Saisissez la ligne modèle pour rechercher des fichiers dans le champ **Recherche rapide**. Vous pouvez utiliser les masques dans la ligne modèle.

   Une fois la ligne modèle saisie, la fonction de la recherche rapide est activée.

   La table affiche uniquement les fichiers qui sont conformes à la condition de la recherche (cf. ill. ci-après). Le fichier est conforme à la condition de la recherche si la ligne modèle est présente au moins dans un des paramètres suivants du fichier :

- **Nom du fichier** ;
- **Nom du serveur SharePoint** ;
- **Chemin du fichier** ;
- **Compte utilisateur** ;
- **Nom d'utilisateur affiché** ;
- **Utilisateur qui a mis le fichier en version minimum** ;
- **Utilisateur qui a été le premier à modifier l'objet** ;
- **Nom de menace ;**
- **Numéro d'incident (ID)**.

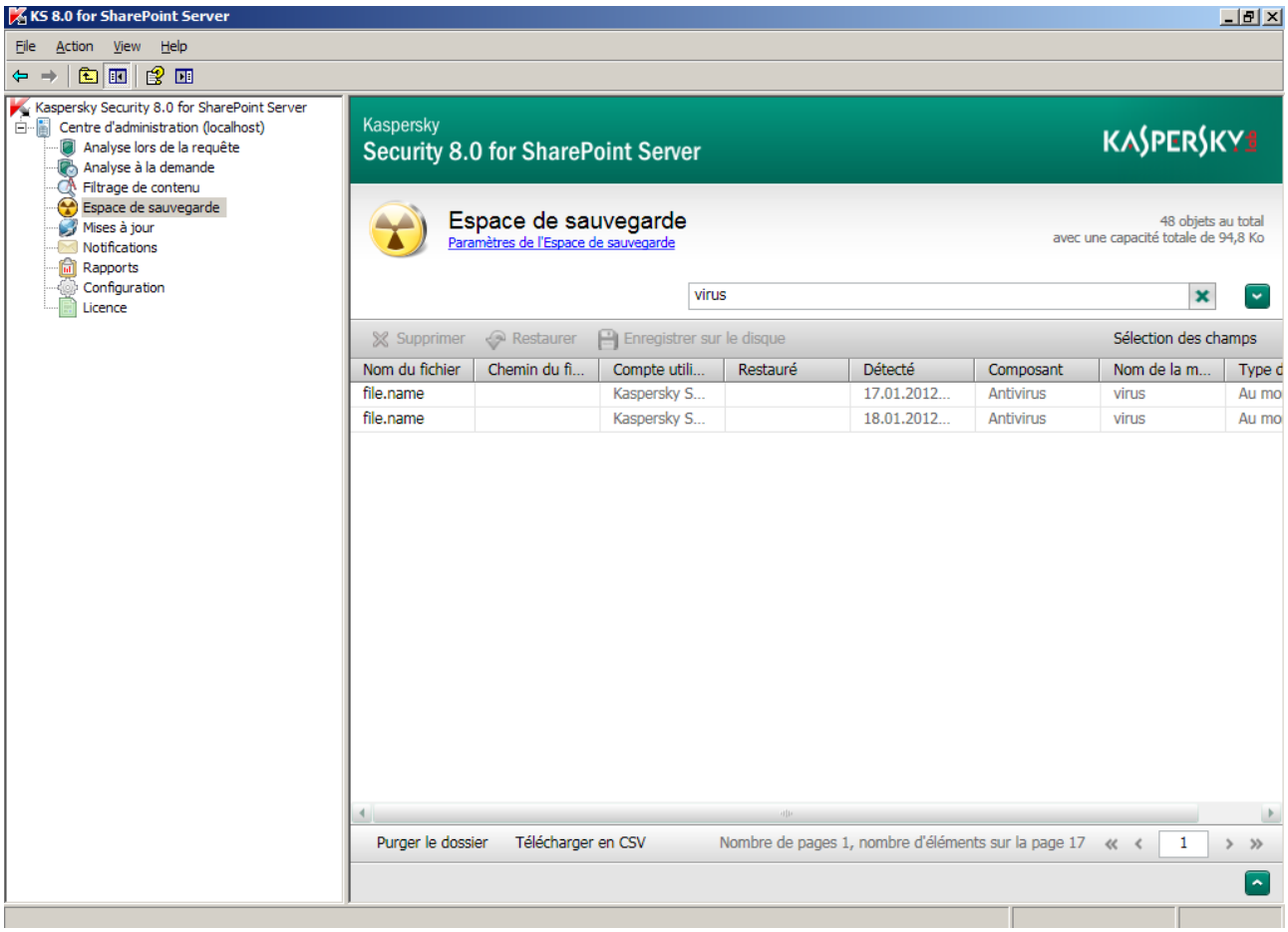

Figure 23. Recherche rapide dans la Espace de sauvegarde

Si vous souhaitez annuler la fonction de la recherche rapide, vous pouvez cliquer sur l'icône , qui se trouve à côté du champ **Recherche rapide**.

RECHERCHE DES OBJETS DANS L'ESPACE DE SAUVEGARDE : FILTRE AVANCE

Pour lancer la recherche des objets dans l'Espace de sauvegarde avec la fonction du filtre avancé, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Espace de sauvegarde**.

   Une liste des fichiers placés dans l'Espace de sauvegarde s'affichera dans la fenêtre des résultats.

2. Cliquez sur l'icône pour déployer le groupe du filtre avancé.

   Le groupe du filtre avancé s'affichera en grande taille. Le groupe reprendra la liste des conditions de filtrage. Par défaut, la liste des conditions de filtrage comprend trois lignes où vous pouvez spécifier les conditions de filtrage des copies de documents. Chacune des conditions de filtrage a trois parties : paramètre à vérifier, ligne modèle et règle de comparaison qui définit la comparaison entre le paramètre à vérifier et la ligne modèle.

3. Pour définir la condition de filtrage, procédez comme suit :

   a. Sélectionnez dans la liste déroulante dans la partie gauche de la ligne le paramètre à vérifier.

      Vous pouvez sélectionner en tant que paramètre à vérifier une des valeurs suivantes :

      - **Nom du fichier** ;
      - **Version du fichier** ;
      - **Taille du fichier** ;
      - **Nom du serveur SharePoint** ;
      - **Chemin du fichier** ;
      - **Compte utilisateur** ;
      - **Nom d'utilisateur** ;
      - **Numéro d'incident (ID)** ;
      - **Détenteur** ;
      - **E-mail du détenteur** ;
      - **Auteur des modifications** ;
      - **E-mail de l'auteur des modifications** ;
      - **Opération SharePoint** ;
      - **Date et heure de restauration** ;
      - **Date et heure de détection** ;
      - **Etat** ;
      - **Composant** ;
      - **Nom de menace** ;

- **Type d'analyse** ;
- **Date de sortie des bases**.

b. Sélectionnez dans la liste déroulante au centre de la ligne la règle de comparaison.

L'ensemble des valeurs de cette liste correspond à la valeur sélectionnée du paramètre à vérifier. Par exemple, pour le paramètre à vérifier **Nom du fichier** la liste contient les valeurs suivantes : **Contient**, **Ne contient pas**, **Champ non rempli**.

Si vous sélectionnez la valeur **Champ non rempli**, le champ **Saisissez le masque** devient inactif.

c. Dans le champ **Saisissez le masque** saisissez la ligne modèle. Vous pouvez utiliser les masques dans la ligne modèle.

La condition de filtrage est appliquée à la liste des fichiers placés dans la Sauvegarde, une fois que vous avez défini toutes les trois parties de la condition de filtrage. La liste des fichiers affiche uniquement les fichiers dont les paramètres sont conformes à toutes les conditions de filtrage spécifiées (cf. ill. ci-après).

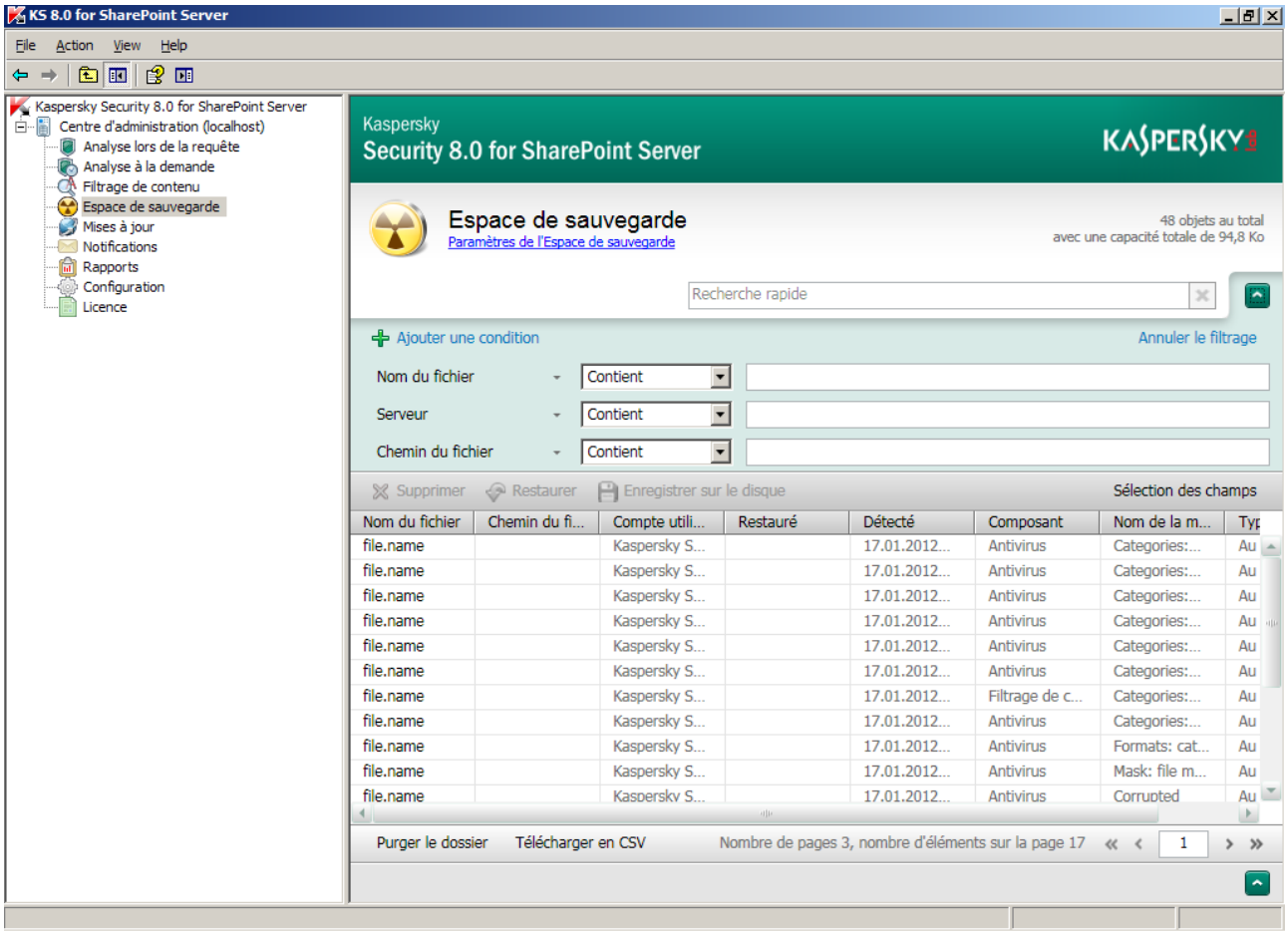

Figure 24. Application du filtre avancé

4. Si vous souhaitez définir plus de trois conditions de filtrage, vous pouvez ajouter des lignes supplémentaires à la liste des conditions de filtrage. Pour ce faire, cliquez sur le bouton **Ajouter une condition**.

Une nouvelle ligne s'affichera en bas de la liste des conditions de filtrage.

5. Si vous souhaitez supprimer une condition supplémentaire de filtrage, cliquez sur l'icône qui se trouve à la ligne avec la condition de filtrage.

La ligne sélectionnée sera supprimée de la liste des conditions de filtrage. La liste des fichiers sera actualisée conformément aux conditions de filtrages qui restent.

Pour votre confort, vous pouvez réduire le groupe du filtre avancé en cliquant sur l'icône . Le filtre avancé reste actif même si le groupe du filtre avancé est réduit. Si vous souhaitez annuler le filtre avancé, vous pouvez le faire en cliquant sur le lien **Annuler le filtrage**.

RESTAURATION DES OBJETS DE LA ESPACE DE SAUVEGARDE

Pour restaurer les fichiers de l'Espace de sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Sauvegarde**.

2. Un panneau des résultats placés dans l'Espace de sauvegarde s'affichera dans la fenêtre des résultats.

3. Sélectionnez les objets du tableau que vous souhaitez restaurer.

   Les fichiers restaurés peuvent être infectés.

4. Cliquez sur le bouton **Restaurer** (cf. ill. ci-après).

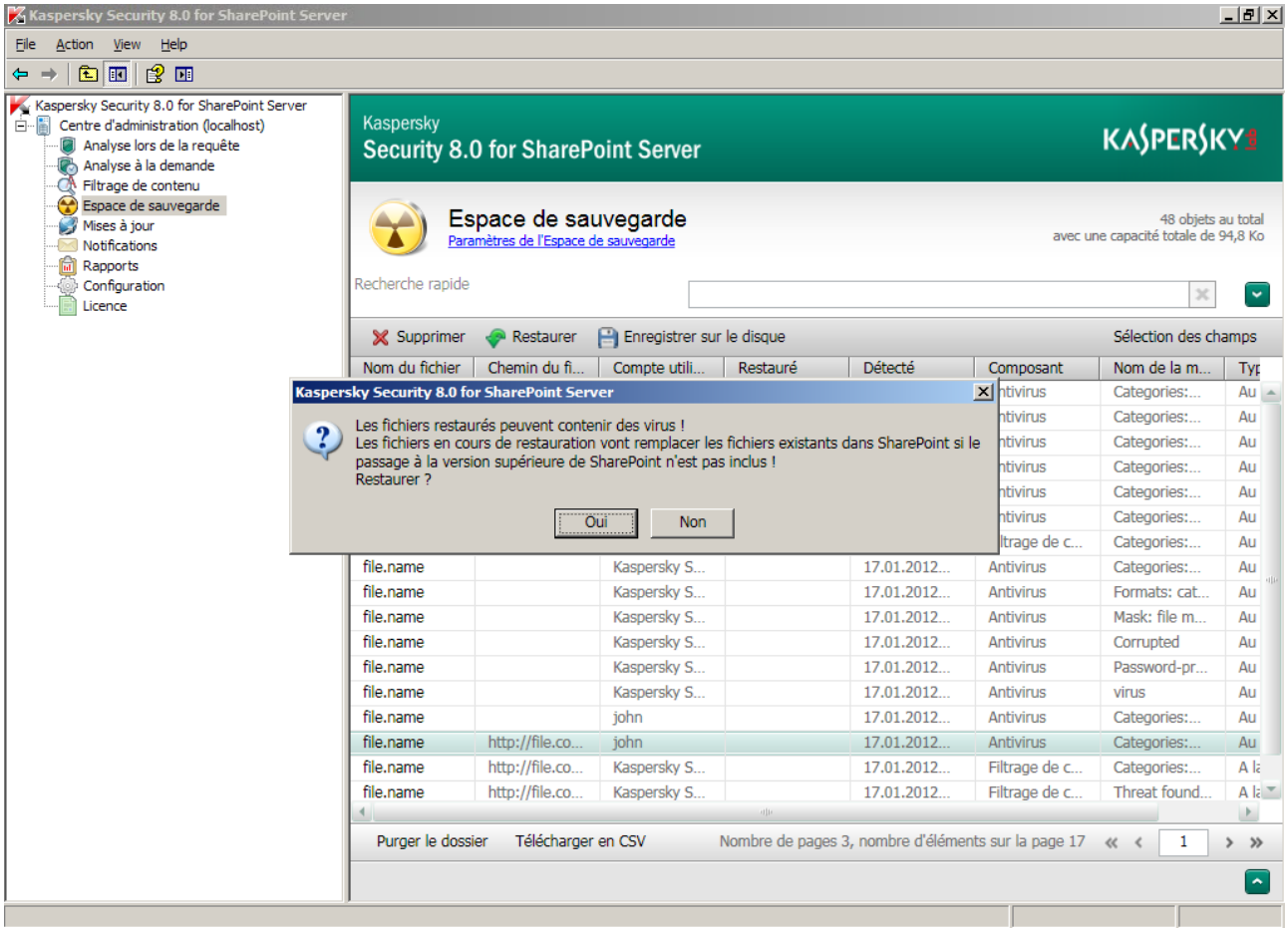

Figure 25. Restauration du fichier de l'Espace de sauvegarde

Les fichiers sélectionnés seront déchiffrés et restaurés sur le portail SharePoint dans leur emplacement d'origine. Les fichiers seront restaurés dans le même format et sous les mêmes noms qu'ils avaient lorsqu'ils ont été placés dans l'Espace de sauvegarde.

Lors de la restauration des objets, l'application actualise dans SharePoint les informations suivantes relatives à ces fichiers :

- **Utilisateur**. L'application consigne dans ce champ le nom du compte de l'Administrateur de l'application.
- **Commentaire**. L'application consigne dans ce champ le nom de l'application, la date de la mise dans l'Espace de sauvegarde et la version du fichier.
- **Version**. L'application met à jour la version du fichier.

Les copies et les informations relatives aux fichiers restaurés restent dans l'Espace de sauvegarde.

RESTAURATION DE FICHIERS DU MEME NOM

Lors de la restauration de fichiers de l'Espace de sauvegarde, un fichier peut être présent sur SharePoint sur le chemin indiqué avec le même nom et la même version ou une version supérieure (si la gestion des versions est activée sur SharePoint).

Gestion des versions désactivée sur SharePoint

Si la gestion des versions est désactivée sur SharePoint, lors de la restauration d'un fichier dans le cas où un fichier du même nom se trouve sur SharePoint, un avertissement apparaît pour annoncer un remplacement. Sélectionnez l'option nécessaire :

- Si vous souhaitez remplacer le fichier qui est restauré sur SharePoint, cliquez sur "Oui".
- Si vous n'avez pas besoin de le remplacer, cliquez sur "Non".

Lors de la restauration de plusieurs fichiers, si un fichier de nom identique à l'un d'entre eux se trouve sur SharePoint, un avertissement apparaît. Sélectionnez l'option nécessaire :

- "Oui, restaurer le fichier". Le fichier situé sur SharePoint est alors remplacé par le fichier restauré.
- "Non, ne pas restaurer le fichier". Le fichier n'est pas remplacé.
- "Oui, restaurer systématiquement le fichier". Les fichiers restaurés remplacent tous les fichiers du même nom.
- "Non, ne restaurer aucun fichier". Aucun fichier n'est restauré.

Gestion des versions activée sur SharePoint

Lorsqu'aucun fichier du même nom ne se trouve sur SharePoint, l'objet de l'Espace de sauvegarde est restauré comme fichier avec la première version mineure ou majeure, selon la version du fichier restauré.

Si la gestion des versions majeures est activée sur SharePoint, le fichier est restauré en tant que fichier avec la version majeure.

Si le fichier restauré n'est associé à aucune version, la restauration s'effectue selon les règles suivantes :

- comme fichier avec une nouvelle version mineure lors de la gestion des versions mineures et majeures sur SharePoint ;
- comme fichier avec une nouvelle version majeure lors de la gestion des versions majeures.

Si un fichier du même nom se trouve sur SharePoint, un avertissement annonce un remplacement. Sélectionnez l'option nécessaire :

- "Oui, restaurer le fichier" :

- une nouvelle version mineure est restaurée si la gestion des versions mineures et majeures est activée sur SharePoint et que la version du fichier de l'Espace de sauvegarde est mineure ;
- une nouvelle version majeure est restaurée dans les autres cas.

- "Non, ne pas restaurer le fichier". Le fichier de l'Espace de sauvegarde n'est pas restauré.

ENREGISTREMENT DES OBJETS PLACES DANS L'ESPACE DE SAUVEGARDE SUR LE DISQUE

Pour enregistrer sur le disque les fichiers placés dans la sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Sauvegarde**.

   Une liste des fichiers placés dans l'Espace de sauvegarde s'affichera dans la fenêtre des résultats.

2. Si vous souhaitez enregistrer un seul fichier sur le disque, procédez comme suit :

   a. Cochez dans la liste le fichier que vous souhaitez enregistrer sur le disque. Vous pouvez lancer la recherche du fichier avec les fonctions de la recherche rapide ou le filtre avancé.

   b. Cliquez sur le bouton **Enregistrer**.

      Une boîte de dialogue standard pour enregistrer le fichier sur le disque s'ouvre.

   c. Sélectionnez le dossier de destination où vous voulez enregistrer le fichier.

   d. Si vous souhaitez enregistrer le fichier sous un autre nom, modifiez le nom du fichier dans le champ **Nom du fichier**,

   e. Cliquez sur le bouton **Enregistrer**.

      Le fichier sélectionné sera enregistré dans le dossier de destination.

3. Si vous souhaitez enregistrer plusieurs fichiers sur le disque, procédez comme suit :

   a. Cochez dans la liste les fichiers que vous souhaitez enregistrer sur le disque. Vous pouvez lancer la recherche des fichiers avec les fonctions de la recherche rapide ou le filtre avancé.

   b. Cliquez sur le bouton **Enregistrer**.

      Une boîte de dialogue standard pour sélectionner le dossier de destination s'ouvre.

c. Sélectionnez le dossier de destination où vous voulez enregistrer les fichiers et cliquez sur le bouton **OK**.

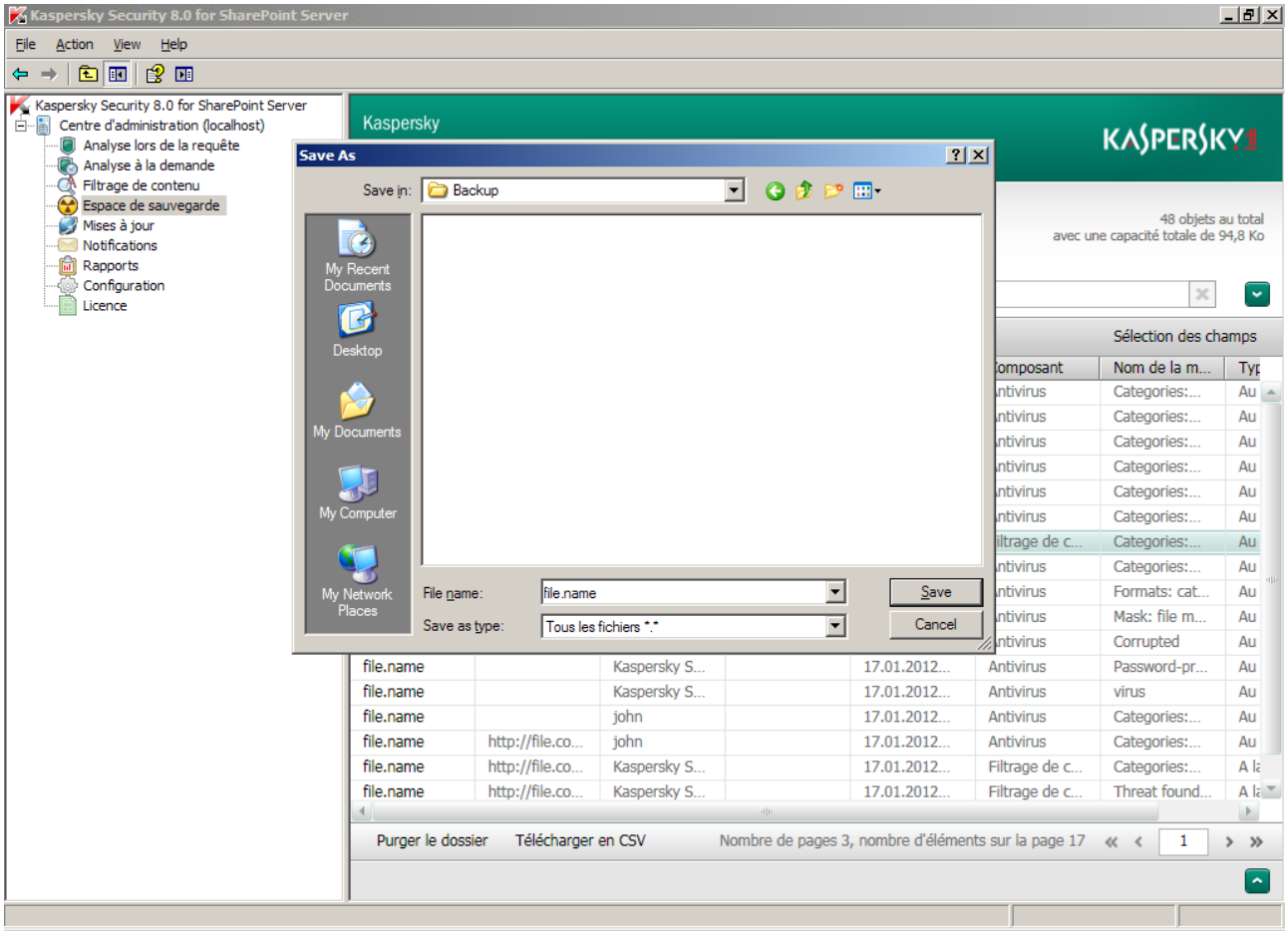

Figure 26. Enregistrement du fichier de l'Espace de sauvegarde

Les fichiers sélectionnés seront enregistrés dans le dossier de destination.

SUPPRESSION DES FICHIERS DE LA ESPACE DE SAUVEGARDE

Pour supprimer les fichiers de l'Espace de sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœudqui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Sauvegarde**.

   Une liste des fichiers placés dans l'Espace de sauvegarde s'affichera dans la fenêtre des résultats.

2. Cochez dans la liste les fichiers que vous souhaitez supprimer. Vous pouvez lancer la recherche des fichiers avec les fonctions de la recherche rapide ou le filtre avancé.

Les fichiers seront définitivement supprimés de l'Espace de sauvegarde. Il ne sera plus possible de les restaurer.

3. Cliquez sur le bouton **Supprimer** (cf. ill. ci-après).

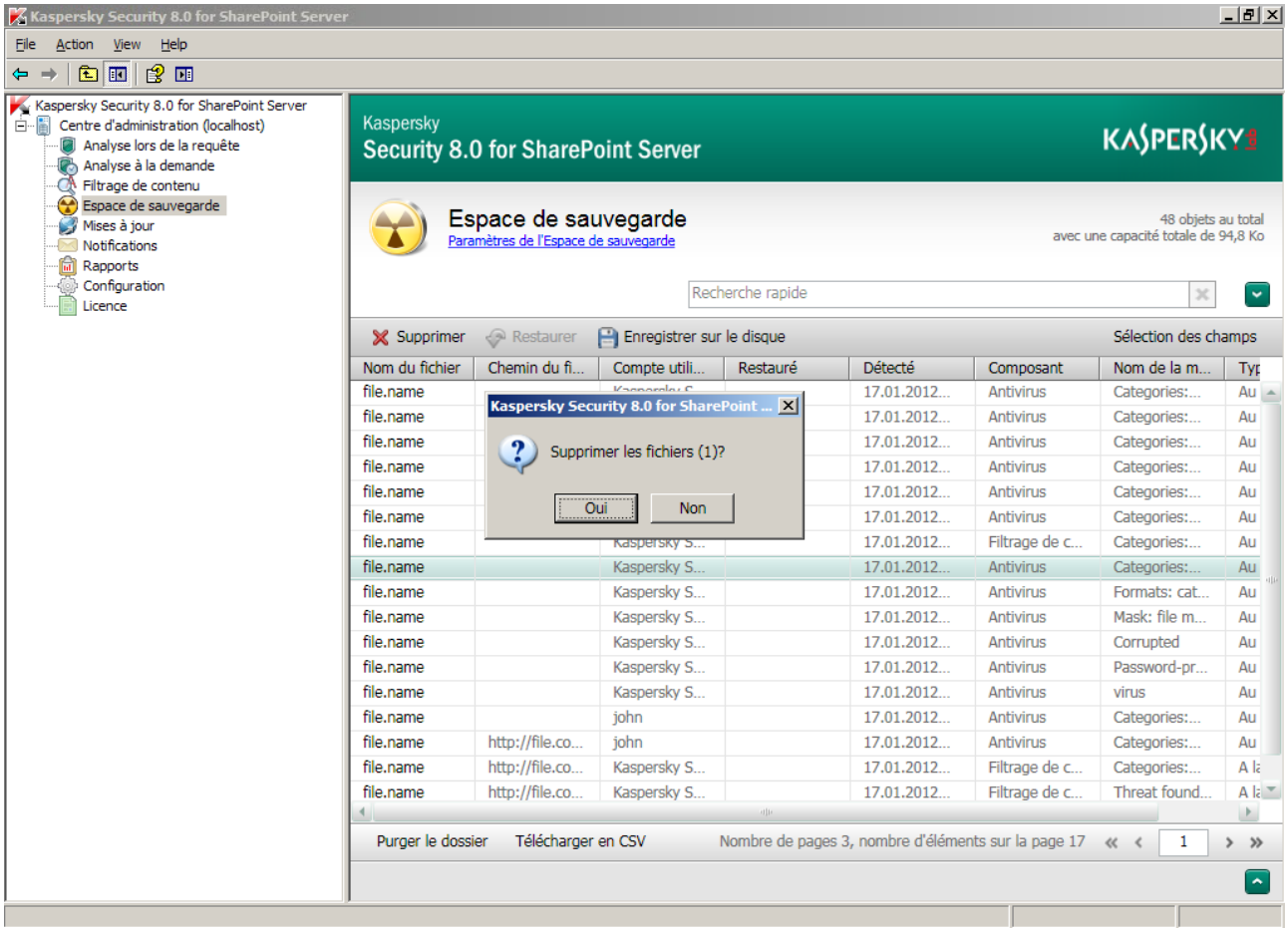

Figure 27. Suppression de fichier de l'Espace de sauvegarde

Une fenêtre avec un message d'avertissement s'ouvre.

4. Cliquez sur le bouton **Oui**.

Les fichiers sélectionnés seront supprimés de l'Espace de sauvegarde.

NETTOYAGE DE L'ESPACE DE SAUVEGARDE

Vous pouvez nettoyer l'Espace de sauvegarde en supprimant tous les objets stockés.

Pour nettoyer l'Espace de sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Espace de sauvegarde**.

2. Dans le panneau de résultats, cliquez sur le bouton **Purger le dossier**, situé sous la liste d'objets placés dans l'Espace de sauvegarde.

NOTIFICATIONS

Cette section contient des informations sur les notifications de l'application et sur la configuration de l'envoi de ces notifications aux adresses électroniques.

DANS CETTE SECTION

A propos des notifications 73

Paramètres des notifications sur les événements liés aux clés 73

Paramètres des notifications sur les infractions aux stratégies de protection 74

Paramètres de notifications des événements système 74

A PROPOS DES NOTIFICATIONS

Kaspersky Security permet de créer et d'envoyer des notifications par courrier électronique sur les événements suivants dans l'application :

- sur les évènements relatifs à l'attribution de la licence de l'application et aux clés ;
- sur les infractions aux stratégies de protection antivirus et de filtrage de contenu : détection des fichiers ou des documents infectés, corrompus ou protégés par mot de passe qui perturbent la stratégie du filtrage de contenu lors de l'analyse à la demande ou lors de la requête ;
- sur les évènements système : événements liés aux bases de Kaspersky Security, exécution de la tâche d'analyse à la demande.

PARAMETRES DES NOTIFICATIONS SUR LES EVENEMENTS LIES AUX CLES

Pour configurer l'envoi des notifications sur les événements liés aux clés à plusieurs adresses électroniques, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Notifications**.
2. Dans le bloc de paramètres **Licence**, indiquez les adresses électroniques des destinataires des notifications :
   - **Informer l'administrateur des événements liés aux clés**. Les notifications sont envoyées à l'adresse électronique de l'administrateur figurant dans la fenêtre **Configuration** (cf. la rubrique "**Configuration des paramètres du fonctionnement de l'application**" à la page 80).
   - **Adresses supplémentaires**. Les notifications sont envoyées aux adresses électroniques indiquées dans le champ de saisie à droite.
3. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre.

PARAMETRES DES NOTIFICATIONS SUR LES INFRACTIONS AUX STRATEGIES DE PROTECTION

Pour configurer l'envoi de notifications sur les infractions aux stratégies de sécurité à plusieurs adresses électroniques, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Notifications**.

2. Dans le groupe de paramètres **Infractions aux stratégies de sécurité**, cochez les cases suivant les adresses des destinataires de notifications :

   - **Administrateur**. Les notifications sont envoyées à l'adresse électronique de l'administrateur figurant dans la fenêtre **Configuration** (cf. la rubrique "**Configuration des paramètres du fonctionnement de l'application**" à la page 80).

   - **Auteur**. Les notifications sont envoyées à l'adresse électronique de l'auteur du document pendant l'analyse duquel une infraction aux règles de protection s'est produite.

   - **Utilisateur**. Les notifications seront envoyées à l'adresse électronique de l'auteur des modifications et à l'adresse électronique de l'utilisateur qui télécharge/envoie le document. L'adresse de l'utilisateur se trouve dans les paramètres du serveur SharePoint.

     Lors du travail avec Microsoft SharePoint Server 2007, suite aux particularités techniques, les notifications ne peuvent pas être envoyées à l'auteur du document, à l'auteur des modifications ni à l'utilisateur qui télécharge/envoie le document.

   - **Avancé**. Les notifications sont envoyées aux adresses électroniques indiquées dans le champ de saisie **Adresses supplémentaires**.

3. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre.

PARAMETRES DE NOTIFICATIONS DES EVENEMENTS SYSTEME

Pour configurer l'envoi de notifications des événements système aux clés à plusieurs adresses électroniques, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Notifications**.

2. Dans le bloc de paramètres **Evénements système**, cochez les cases correspondant aux événements sur lesquels des notifications doivent être envoyées :

   - **Evénements liés aux bases**. Des notifications sont envoyées sur les erreurs liées aux bases de Kaspersky Security.

   - **Rapports des tâches d'analyse à la demande**. Des rapports sur l'exécution des tâches d'analyse à la demande sont envoyés aux adresses indiquées.

3. Indiquez les adresses des destinataires de notifications :

   - **Administrateur**. Les notifications sont envoyées à l'adresse électronique de l'administrateur figurant dans la fenêtre **Configuration** (cf. la rubrique "**Configuration des paramètres du fonctionnement de l'application**" à la page 80).

- **Avancé**. Les notifications sont envoyées aux adresses électroniques indiquées dans le champ de saisie **Adresses supplémentaires**. Séparez plusieurs adresses avec un point-virgule.

RAPPORTS

Cette section contient les informations sur les rapports de fonctionnement de l'application, les instructions sur la configuration de la planification de la création des rapports, ainsi que les informations s'y afférant.

DANS CETTE SECTION

Présentation des rapports 76

Tâches de composition des rapports 76

Consultation des rapports prêts 78

Création de rapports rapides 78

Envoi des rapports par courrier électronique 79

PRESENTATION DES RAPPORTS

Kaspersky Security offre la possibilité de créer et de visualiser les rapports sur la protection antivirus, le filtrage du contenu et le fonctionnement de l'application.

Les rapports peuvent être créés automatiquement selon l'horaire défini ou manuellement. Le rapport peut être consulté dans l'application ou vous pouvez le recevoir par courrier électronique. Les rapports envoyés par courrier électronique sont présentés dans un fichier en pièce jointe.

De plus, vous pouvez créer des rapports rapides sur tous les événements survenus au cours de la période définie par l'utilisateur.

Lors d'une modification des paramètres des tâches de génération de rapports, vous pouvez créer un rapport test. L'exécution d'un rapport test permet de voir le résultat des modifications des paramètres de la tâche.

TACHES DE COMPOSITION DES RAPPORTS

Les tâches de composition des rapports servent à créer des rapports dans Kaspersky Security.

Vous pouvez créer de nouvelles tâches, supprimer des tâches existantes, modifier les paramètres des tâches déjà créées et lancer manuellement les tâches sélectionnées.

DANS CETTE SECTION

Lancement de la tâche sélectionnée de composition des rapports. 77

Configuration des paramètres de tâche de composition des rapports 77

Création d'une nouvelle tâche de composition des rapports. 78

Suppression d'une tâche de composition des rapports 78

LANCEMENT DE LA TACHE SELECTIONNEE DE COMPOSITION DES RAPPORTS.

Pour lancer manuellement la tâche de composition du rapport, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur. Sélectionnez ensuite le nœud **Rapports**.
2. Sélectionnez la tâche dans la liste du panneau des résultats.
3. Cliquez sur le bouton de **création du rapport**.

CONFIGURATION DES PARAMETRES DE TACHE DE COMPOSITION DES RAPPORTS

Pour configurer les paramètres de tâche de composition des rapports, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Rapports**.
2. Dans le panneau de résultats, sélectionnez la tâche dont vous souhaitez modifier les paramètres et, à l'aide du bouton **Modifier**, ouvrez la fenêtre **Paramètres de la tâche**.
3. Modifiez les paramètres requis :
   - Dans le champ **Nom de tâche**, modifiez le nom de la tâche.
   - Si vous souhaitez que le rapport soit composé à la demande, cochez la case **Lancer selon la planification**, et dans la liste qui apparaît, sélectionnez le serveur sur lequel la tâche va être lancée. Dans le groupe des paramètres **Programmation**, planifiez le lancement :
     - **Tous les N jours**. Le rapport sera généré grâce à un nombre de jours donné pour une période déterminée. Le rapport inclura les informations pour les N jours passés (de 0h00 du premier jour à 0h00 du jour de formation du rapport).
     - **Chaque semaine**. Le rapport sera généré un jour spécifique de la semaine pour une période déterminée. Le rapport inclura les informations pour les 7 jours passés (de 0h00 du dernier jour indiqué de la semaine à 0h00 du jour de formation du rapport, par exemple, du lundi à lundi).
     - **Chaque mois**. Le rapport sera généré un jour spécifique du mois pour une période déterminée. Le rapport inclura les informations pour le mois passé (de 0h00 du premier jour du mois passé à 0h00 du premier jour du mois de formation du rapport).

     Dans la planification de génération du rapport, l'heure du serveur est celle utilisée.
   - Si vous souhaitez que les rapports soient envoyés à l'adresse électronique de l'administrateur figurant dans la fenêtre **Notifications**, cochez la case **Envoyer à l'administrateur**.
   - Si vous souhaitez que les rapports soient envoyés à d'autres adresses électroniques, cochez la case **Envoyer aux destinataires** et indiquez les adresses électroniques dans le champ de saisie. Lors de la saisie de plusieurs adresses, utilisez le séparateur " ; ".
4. Pour enregistrer les modifications apportées et quitter la fenêtre, cliquez sur le bouton **OK**.

CREATION D'UNE NOUVELLE TACHE DE COMPOSITION DES RAPPORTS.

Pour créer une nouvelle tâche de composition des rapports, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Rapports**.
2. En cliquant sur le bouton **Créer** dans le panneau des résultats, ouvrez la fenêtre **Paramètres de la tâche**.
3. Définissez tous les paramètres requis de la tâche et cliquez sur le bouton **OK**. La tâche créée sera ajoutée sur la liste des tâches dans le panneau des résultats. Si nécessaire, vous pouvez modifier les paramètres de la tâche.

SUPPRESSION D'UNE TACHE DE COMPOSITION DES RAPPORTS

Pour supprimer une tâche de composition des rapports, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Rapports**.
2. Dans le panneau des résultats, sélectionnez sur la liste la tâche que vous souhaitez supprimer et cliquez sur le bouton **Supprimer**.

CONSULTATION DES RAPPORTS PRETS

Pour consulter un rapport prêt, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Rapports**.
2. Sous l'onglet **Rapports**, sélectionnez dans la liste le rapport à consulter et cliquez sur **Consulter**. Le rapport s'ouvre dans le navigateur, installé par défaut.

Les navigateurs suivants sont pris en charge dans l'application pour afficher les rapports :

- Windows Internet Explorer 7.x (32 bits) ;
- Windows Internet Explorer 7.x (64 bits) ;
- Windows Internet Explorer 8.x (32 bits) ;
- Windows Internet Explorer 8.x (64 bits) ;
- Windows Internet Explorer 9.x (32 bits) ;
- Windows Internet Explorer 9.x (64 bits) ;
- Mozilla Firefox 3,6 ;
- Google Chrome (dernière version).

CREATION DE RAPPORTS RAPIDES

Pour créer un rapport rapide, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Rapports**.

2. Dans le panneau de résultats, sous l'onglet **Rapports**, cliquez sur **Rapport rapide**.

3. Dans la fenêtre **Paramètres du rapport** qui apparaît, sélectionnez la période pour laquelle le rapport doit être créé :

   - **Pour la journée**. Le rapport sera créé pour les 24 heures définies dans le champ de données.

   - **Pour la période**. Le rapport sera créé pour la période définie.

4. Cliquez sur le bouton **OK**.

ENVOI DES RAPPORTS PAR COURRIER ELECTRONIQUE

Pour configurer l'envoi des rapports composés par courrier électronique, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Rapports**.

2. Dans le panneau de résultats, sous l'onglet **Tâches de composition des rapports**, sélectionnez la tâche dans la liste et cliquez sur **Modifier**.

3. Dans la fenêtre **Paramètres de la tâche** qui apparaît, cochez les cases correspondant aux destinataires concernés :

   - **Envoyer à l'administrateur**. Le rapport est envoyé à l'adresse électronique de l'administrateur figurant dans la fenêtre **Configuration** (cf. la rubrique "**Configuration des paramètres du fonctionnement de l'application**" à la page 80).

   - **Envoyer aux destinataires**. Le rapport est envoyé aux adresses électroniques indiquées dans le champ de saisie à droite. Utilisez le point-virgule en tant que séparateur lorsque vous indiquez plusieurs adresses.

CONFIGURATION DES PARAMETRES DU FONCTIONNEMENT DE L'APPLICATION

Cette section contient des informations sur la configuration des paramètres suivants du fonctionnement de l'application :

- paramètres d'envoi des messages électroniques ;
- paramètres de tenue du fichier de journal ;
- paramètres de nettoyage de l'Espace de sauvegarde.

DANS CETTE SECTION

Configuration des paramètres d'envoi des messages électroniques 80

Configuration des paramètres de diagnostic 81

Configuration des paramètres de l'Espace de sauvegarde 81

CONFIGURATION DES PARAMETRES D'ENVOI DES MESSAGES ELECTRONIQUES

Pour configurer les paramètres d'envoi des messages électroniques, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Ensuite, sélectionnez le nœud **Configuration.** Les paramètres d'envoi se trouvent dans le bloc de paramètres **Configuration du serveur SMTP pour l'envoi de notifications.**

2. Dans le champ **Adresse(s) de l'administrateur**, indiquez l'adresse électronique de l'administrateur du serveur SharePoint.

3. Dans le champ **Envoyer au nom de,** indiquez le nom de l'expéditeur des messages électroniques. La valeur du champ par défaut est celle définie dans les paramètres du serveur SharePoint. Si ce champ n'est pas rempli dans l'entrée **Configuration** et dans les paramètres SharePoint n'est pas rempli, alors les rapports ne seront pas envoyés.

4. Sélectionnez l'option d'utilisation des paramètres du serveur SMTP :

   - Si vous souhaitez utiliser les paramètres du serveur SMTP définis sur le serveur SharePoint, sélectionnez **Utiliser les paramètres du serveur SMTP définis sur SharePoint**.

   - Si vous souhaitez utiliser les autres paramètres du serveur SMTP, sélectionnez **Utiliser les paramètres spécifiques du serveur SMTP** et renseignez les champs **Adresse du serveur SMTP**, **Compte utilisateur** et **Mot de passe**. Si vous devez utiliser l'authentification NTLM, cochez la case **Utiliser l'authentification NTLM**.

5. Pour vérifier que les paramètres de configuration sont corrects, cliquez sur **Envoyer un message avec les paramètres définis**. Un message test est envoyé à l'adresse électronique indiquée de l'administrateur.

6. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre de l'application.

CONFIGURATION DES PARAMETRES DE DIAGNOSTIC

Pour limiter la taille du fichier du journal, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Configuration**.

2. Dans le groupe de paramètres **Diagnostic**, indiquez la taille limite du fichier du journal (en Mo) dans le champ de saisie **Taille limite du fichier du journal**. La valeur du champ par défaut est de 100 Mo.

Pour configurer le niveau de détail du fichier du journal, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Configuration.**

2. Dans la liste déroulante **Niveau de détail**, spécifiez le niveau de détail du fichier du journal :

   - **Minimum**. Le fichier du journal contient le minimum d'informations sur le fonctionnement de l'application : le résultat de l'analyse des objets, le résultat du téléchargement des mises à jour des bases et le résultat de l'ajout de la clé.

   - **Autre**. Le fichier du journal contient les informations sur le fonctionnement des composants spécifiés dans la fenêtre **Configuration des paramètres du diagnostic**. Pour ouvrir cette fenêtre, cliquez sur le bouton **Configuration** qui se trouve à droite de la liste déroulante.

3. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre.

CONFIGURATION DES PARAMETRES DE L'ESPACE DE SAUVEGARDE

Pour configurer les paramètres de l'Espace de sauvegarde, procédez comme suit :

1. Sélectionnez et déployez dans l'arborescence de la console d'administration le nœud qui correspond au serveur SharePoint. Sélectionnez ensuite le nœud **Configuration.**

2. Cochez la case **Nettoyer automatiquement le référentiel si sa taille dépasse :...Mo**.

3. Indiquez dans le champ de saisie la taille maximale de l'Espace de sauvegarde (en Mo). La valeur de ce paramètre peut être comprise entre 1 et 1 048 576 Mo. La valeur définie par défaut est de 3 686 Mo. Si lors de l'emplacement du fichier suivant, la limite établie de la taille du stockage sera dépassée, l'application va libérer le volume nécessaire grâce à la suppression des fichiers les plus anciens.

4. Pour enregistrer les modifications effectuées, cliquez sur le bouton **Enregistrer** dans la partie supérieure de la fenêtre de l'application.

CONTACTER LE SUPPORT TECHNIQUE

Cette section contient des informations sur les modes d'obtention d'une assistance technique et sur les conditions à remplir pour bénéficier de ce service.

DANS CETTE SECTION

Modes d'obtention d'une assistance technique 82

Assistance technique par téléphone 82

Obtention d'une assistance technique via votre espace personnel 82

Utilisation du fichier de trace et du script AVZ 83

MODES D'OBTENTION D'UNE ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé la solution à votre problème dans la documentation de l'application ou dans une des sources d'informations sur celle-ci (cf. la rubrique "Sources d'informations sur l'application" à la page 9), nous vous recommandons de vous adresser au service d'assistance technique de Kaspersky Lab. Les experts du Service d'assistance technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Avant de vous adresser au service d'assistance technique, prenez connaissance des règles pour l'octroi de l'assistance technique (http://www.kaspersky.com/fr/support).

Vous pouvez contacter les spécialistes du service d'assistance technique par l'un des moyens suivants :

- Téléphone. Vous pouvez consulter par téléphone les spécialistes du service d'assistance technique en russe ou dans d'autres langues.
- Envoi d'une demande de votre espace personnel sur le site Web du service d'assistance technique. Vous pouvez contacter via le formulaire de demande les spécialistes du service d'assistance technique.

L'assistance technique est fournie uniquement aux utilisateurs qui ont acquis une licence commerciale d'utilisation de l'application. Les détenteurs de licences d'essai n'y ont pas droit.

ASSISTANCE TECHNIQUE PAR TELEPHONE

En cas de problème urgent, vous pouvez téléphoner aux spécialistes de l'assistance technique russophone ou internationale (http://support.kaspersky.ru/support/support_local).

Avant de vous adresser au service d'assistance technique, prenez connaissance des règles applicables (http://support.kaspersky.fr/support/details). Nos experts pourront ainsi vous venir en aide plus rapidement.

OBTENTION D'UNE ASSISTANCE TECHNIQUE VIA VOTRE ESPACE PERSONNEL

L'espace personnel est la section qui vous est réservée (https://my.kaspersky.com/fr/) sur le site du service d'assistance technique.

Pour accéder à un espace personnel, vous devez vous enregistrer sur la page d'enregistrement (https://my.kaspersky.com/fr/registration). Vous devez indiquer votre adresse électronique et votre mot de passe.

Dans votre espace personnel, vous pouvez effectuer les actions suivantes :

- envoyer des demandes au service d'assistance technique et au laboratoire antivirus ;
- échanger des messages avec le service d'assistance technique sans utiliser le courrier électronique ;
- suivre l'état de vos demandes en temps réel ;
- consulter l'historique complet de vos demandes au service d'assistance technique ;
- obtenir une copie du fichier de licence si vous avez perdu ou supprimé l'original.

Envoi d'une demande au service d'assistance technique par voie électronique

Vous pouvez envoyer une demande par courrier électronique au service d'assistance technique en russe, en anglais, en allemand, en français et en espagnol.

Dans les champs du formulaire de demande, vous devez fournir les renseignements suivants :

- le type de requête ;
- le nom et le numéro de version de l'application ;
- le texte du message ;
- le numéro de client et mot de passe ;
- l'adresse électronique.

Un spécialiste du service d'assistance technique envoie la réponse à votre question dans votre espace personnel et à l'adresse électronique indiquée dans votre demande par voie électronique.

Demande par voie électronique au laboratoire antivirus

Certaines demandes ne doivent pas être envoyées au service d'assistance technique, mais au laboratoire antivirus.

Vous pouvez envoyer les types de demande suivants au laboratoire antivirus :

- *Programme malveillant inconnu* — vous soupçonnez qu'un fichier est infecté, mais Kaspersky Security ne le détecte pas comme tel.

  Les spécialistes du laboratoire antivirus analysent le code malveillant envoyé. S'ils détectent un virus inconnu jusqu'à présent, ils ajoutent la description de ce virus dans la base de données accessible lors de la mise à jour des applications antivirus.

- *Faux positif de l'application antivirus* — Kaspersky Security détecte qu'un fichier est infecté, mais vous êtes sûr que ce n'est pas le cas.

- *Demande de description d'un programme malveillant* — vous souhaitez obtenir une description d'un virus détecté par Kaspersky Security, grâce au nom de ce virus.

Vous pouvez également envoyer des demandes au laboratoire antivirus à partir de la page contenant le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous connecter à votre espace personnel.

UTILISATION DU FICHIER DE TRACE ET DU SCRIPT AVZ

Dès que vous informez les spécialistes du service d'assistance technique de l'apparition d'un problème, ils peuvent vous demander de créer et de leur envoyer un rapport avec des informations sur le système d'exploitation. Ils peuvent également vous demander de créer un *fichier de trace*. Ce fichier permet de suivre le processus d'exécution progressive des commandes de l'application et de détecter l'étape contenant l'erreur dans ce processus.

Suite à l'analyse des données que vous leur avez transmises, les spécialistes du service d'assistance technique peuvent créer et vous envoyer un script AVZ. L'exécution des scripts AVZ permet de rechercher le code malveillant dans les processus lancés et sur le système, de réparer/de supprimer les fichiers infectés et de créer des rapports sur les résultats de l'analyse du système.

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

GLOSSAIRE

A

Activation de l'application

Permutation de l'application en mode de pleine fonctionnalité. L'activation est exécutée par l'utilisateur pendant ou après l'installation de l'application. Pour activer l'application, l'utilisateur doit avoir le code d'activation ou le fichier clé.

Analyse a la demande

Mode de fonctionnement de l'application de Kaspersky Lab qui est initié par l'utilisateur et dirigé sur l'analyse de tous fichiers quelconques.

C

Cle complementaire

Clé confirmant les privilèges d'utilisation de l'application, mais non utilisée au moment actuel.

Cle d'activation

La clé utilisée au moment actuel pour travailler avec l'application.

D

Duree de validite de la licence

Durée de validité de la licence est une période de temps pendant laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. Le volume des fonctions disponibles et des services complémentaires dépend du type de licence.

I

Ignorer l'objet

Mode de traitement quand l'objet est retransmis à l'utilisateur sans aucune modification. Si l'enregistrement des événements de ce type est défini par les paramètres du rapport, les informations sur l'objet détecté sont inscrites dans le rapport.

L

Liste noire des fichiers cles

Base de donnes qui contient les informations sur les fichiers clés, bloqués par Kaspersky Lab. Le contenu du fichier avec la liste noire est actualisé en même temps que les bases.

M

Masque du fichier

Présentation du nom du fichier par des symboles généraux. Les symboles principaux, utilisés dans les masques des fichiers, sont * et ? (où * - n'importe quel nombre des symboles quelconques, et ? – un symbole quelconque).

MISE A JOUR DES BASES

Fonction de l'application de Kaspersky Lab qui permet de supporter la protection de l'ordinateur dans l'état actuel. Pendant la mise à jour, l'application copie les mises à jour des bases et des modules de l'application à partir des serveurs de mises à jour de Kaspersky Lab sur l'ordinateur et les installe et les applique automatiquement.

O

OBJET INFECTE

Objet dont une partie du code coïncide entièrement avec une partie du code d'une menace connue. Les experts de Kaspersky Lab ne vous conseillent pas de travailler avec de tels objets.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient le code modifié d'une menace connue, ou le code qui rappelle le code d'une menace par son comportement.

R

REPARATION DES OBJETS

Mode de traitement des objets infectés, en appliquant lequel une restauration complète ou partielle des données a lieu. Il n'est pas possible de réparer tous les objets infectés.

S

SAUVEGARDE

Stockage spécial, conçu pour enregistrer les copies de sauvegarde des objets créés avant leur première réparation ou suppression.

SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab, depuis lesquels l'application de Kaspersky Lab reçoit les mises à jour des bases et des modules de l'application.

SUPPRESSION DE L'OBJET

Mode de traitement de l'objet quand sa suppression physique depuis l'emplacement de sa détection par l'application a lieu (disque dur, dossier, ressource de réseau). Il est conseillé d'appliquer ce mode de traitement aux objets dangereux dont la réparation pour de telles ou telles raisons n'est pas possible.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement " IDC Worldwide Endpoint Security Revenue by Vendor "). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen-Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essais. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com
Laboratoire antivirus :	newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les questions aux experts de la lutte contre les virus)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.com

NOTIFICATIONS SUR LES MARQUES COMMERCIALES

Les marques commerciales et les marques de service enregistrées appartiennent à leurs propriétaires respectifs.

Microsoft, SharePoint, Windows, Windows Server et Windows Vista sont des marques commerciales de Microsoft Corporation enregistrées aux Etats-Unis et dans d'autres pays.

INDEX

A

Action
Analyse à la demande 46
Actions
analyse au moment de l'accès 33
Actions sur les objets 33, 46
Activation de l'application 14
activation/désactivation la protection en temps réel 23
Ajout du serveur 22
Analyse à la demande 40
Analyse à la demande
actions lors de la détection d'une menace 46
Analyse à la demande
actions lors de la détection d'une menace 46
Analyse au moment de l'accès 30
exclusions de l'analyse 35

C

Configuration logicielle 11
Configuration matérielle 11
Contrat de licence 13

E

Espace de sauvegarde 60
configuration des paramètres 81
restauration des objets 68
suppression de l'objet 71
Exclusions de l'analyse 35, 39, 49

F

Fenêtre principale 18
Arborescence de la console 18
Fenêtre principale de l'application 18
Filtrage de contenu 53
à la demande 51
au moment de l'accès 37
catégorie de mots et d'expressions indésirables 54
masques des noms de fichiers indésirables 57

I

Interface de l'application 18

K

KASPERSKY LAB 88
Kaspersky Lab ZAO 88

L

Lancement
Analyse à la demande 41
de la Console d'administration 22
la composition du rapport 77

Le fichier de licence 14
Les bases 24
mise à jour automatique 26
Mise à jour selon la planification 26
Licence 13
Contrat de licence 13
Le fichier de licence 14

M

Mise à jour
Lancement selon la planification 26
Mises à jour
source des mises à jour 28

N

Niveau de diagnostic 81
Notifications 73
des événements système 74
paramètres d'envoi 80
sur les événements liés aux clés 73
sur les infractions aux stratégies de protection 74

P

Planification
Analyse à la demande 43
la composition du rapport 77
Mise à jour 26
Protection 23
activation/désactivation 23

R

Rapports 76
création 76
rapports rapides 78
tâches de compositions 76
visualisation 78
Rapports
envoi automatique 79

S

Source des mises à jour 28

Z

Zone de l'analyse 47