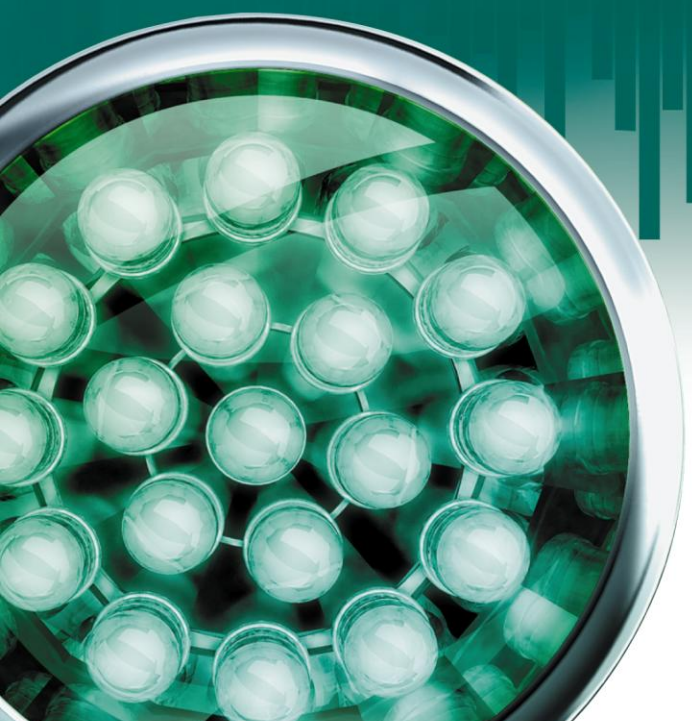
Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition

MANUEL DE L'ADMINISTRATEUR

VERSION DE L'APPLICATION : 8.0



KASPERSKY lab

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.

Date de rédaction du document : 02.11.2010

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

TABLE DES MATIERES

INTRODUCTION

Ce guide décrit l'utilisation de Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition (ci-après Kaspersky Anti-Virus).

Ce guide fournit des informations sur la manière d'administrer Kaspersky Anti-Virus via la console MMC installée sur le serveur protégé ou sur u un ordinateur distant (ci-après, la console de Kaspersky Anti-Virus).

Les commandes d'administration de Kaspersky Anti-Virus par la ligne de commande sont présentées dans la rubrique *Administration de Kaspersky Anti-Virus via la ligne de commande*.

La rubrique *Configuration et administration via Kaspersky Administration Kit* décrit l'administration centralisée de la protection des serveurs sur lesquels Kaspersky Anti-Virus est installée à l'aide de Kaspersky Administration Kit.

La rubrique *Compteurs de Kaspersky Anti-Virus* décrit les compteurs de Kaspersky Anti-Virus pour l'application "Moniteur système" ainsi que les compteurs et les pièges SNMP.

Si vous n'avez pas trouvé la réponse à votre question sur Kaspersky Anti-Virus dans ce document, vous pouvez utiliser d'autres sources d'informations sur Kaspersky Anti-Virus.

INFORMATIONS GENERALES SUR KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus protège les serveurs sous Microsoft Windows contre les menaces qui accompagnent l'échange de fichiers. Il a été développé pour les intranets des grandes et des moyennes entreprises. Les utilisateurs de Kaspersky Anti-Virus sont les administrateurs du réseau et les personnes chargées de la protection du réseau contre les virus.

Vous pouvez installer Kaspersky Anti-Virus sur des serveurs remplissant diverses fonctions : serveurs de terminaux et serveurs d'impression, serveurs d'applications et contrôleurs de domaines ainsi que des serveurs de fichiers. Ceux-ci sont plus exposés aux infections car ils échangent les fichiers avec les postes de travail de l'utilisateur.

Vous pouvez administrer la protection du serveur sur lequel est installé Kaspersky Anti-Virus des manières différentes : via la console de Kaspersky Anti-Virus ou à l'aide de la ligne de commande. Vous pouvez utiliser l'application Kaspersky Administration Kit pour l'administration centralisée de la protection de nombreux serveurs doté chacun de Kaspersky Anti-Virus. Il est possible de consulter les compteurs de performance de Kaspersky Anti-Virus pour l'application "Moniteur système" ainsi que les compteurs et les interruptions SNMP.

DANS CETTE SECTION DE L'AIDE

PROTECTION EN TEMPS REEL ET ANALYSE A LA DEMANDE

Pour protéger les serveurs, vous pouvez utiliser deux fonctions de Kaspersky Anti-Virus : la *protection en temps réel* et l'*analyse à la demande*. Ces fonctions peuvent être activées ou désactivées manuellement ou selon un programme défini.

Protection en temps réel des fichiers

La Protection en temps réel est lancée par défaut automatiquement au démarrage de Kaspersky Anti-Virus et elle fonctionne en continu.

Kaspersky Anti-Virus analyse les objets suivants sur le serveur protégé lorsqu'il est sollicité :

- Les fichiers ;
- Les flux alternatifs des systèmes de fichiers (flux NTFS) ;
- L'enregistrement principal de démarrage et les secteurs d'amorçage des disques durs locaux ou amovibles.

Lorsqu'un programme quelconque enregistre un fichier sur le serveur ou tente de le lire, Kaspersky Anti-Virus intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace, il exécute les actions définies : il tente de réparer le fichier ou il le supprime tout simplement. Kaspersky Anti-Virus rend le fichier au programme uniquement s'il est sain ou si sa réparation a réussi.

Kaspersky Anti-Virus recherche dans les objets non seulement la présence de virus mais également d'autres types de menaces comme les vers de réseau, les chevaux de Troie ou les logiciels publicitaires.

De plus, Kaspersky Anti-Virus surveille en permanence les tentatives d'exécution des scripts développés selon les technologies Microsoft Windows Script Technologies (ou Active Scripting), par exemple les scripts VBScript ou JScript sur le serveur protégé. Il analyse le code du script et interdit automatiquement l'exécution de tout script jugé dangereux.

La tâche de protection en temps réel du serveur consiste à offrir une sécurité maximale au serveur sans trop ralentir l'échange de fichiers.

Analyse à la demande

L'analyse à la demande consiste à analyser complètement ou de manière ponctuelle le serveur à la recherche de menaces dans les objets.

Kaspersky Anti-Virus analyse les fichiers, la mémoire vive du serveur ainsi que les objets de démarrage qui sont plus compliqués à restaurer en cas de corruption.

Par défaut, Kaspersky Anti-Virus procède une fois par semaine à l'analyse des secteurs critiques de l'ordinateur. Il est conseillé de lancer manuellement l'analyse des secteurs critiques de l'ordinateur après avoir désactivé la protection en temps réel des fichiers.

PRESENTATION DES OBJETS INFECTES ET SUSPECTS

Kaspersky Anti-Virus contient une sélection de bases. Les bases sont des fichiers contenant des enregistrements qui permettent de déceler la présence du code malveillant de centaines de milliers de menaces connues dans les objets analysés. Ces enregistrements sont composés d'informations sur les portions de contrôle du code des menaces ainsi que d'algorithmes de réparation des objets contenant les menaces.

Si Kaspersky Anti-Virus découvre, dans l'objet analyse, une portion de code qui correspond parfaitement au code de contrôle d'une menace connue quelconque selon les informations contenue dans les bases, il attribue l'état *infecté* à cet objet.

Kaspersky Anti-Virus attribue l'état *suspect* à l'objet découvert si ce dernier contient une partie du code d'une menace connue correspond au segment de contrôle (dans les conditions déterminées). Kaspersky Anti-Virus considère également comme suspects les objets découverts par l'*analyseur heuristique* (Heuristic Analyzer). L'analyseur heuristique découvre les objets suspects en étudiant leur comportement. Il est impossible de dire si le code d'un tel objet correspond totalement ou partiellement au code d'une menace connue mais il contient des instructions ou une suite d'instructions propres aux programmes malveillants.

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des question sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Anti-Virus, vous pourrez trouver les réponses en utilisant diverses sources d'informations. Vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION DE L'AIDE

SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDEPENDANTE

Pour la recherche indépendante, vous pouvez vous adresser aux sources d'informations suivantes :

- la page de l'application sur le site de Kaspersky Lab ;
- la page de l'application sur le site du support technique (dans la banque de solutions) ;
- système d'aide électronique ;
- documentation.

Page sur le site Web de Kaspersky Lab

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

Cette page vous propose des informations générales concernant Kaspersky Anti-Virus, ses possibilités et ses particularités. Vous pouvez acheter Kaspersky Anti-Virus ou prolonger la licence dans notre boutique en ligne.

www.kaspersky.com/anti-virus-for-storage

Cette page propose des informations générales sur la version de Kaspersky Anti-Virus compatible avec les systèmes de stockage de données en ligne EMC Celerra.

Page sur le site du Service d'assistance technique (dans la banque de solutions)

http://support.kaspersky.com/fr

Cette page regroupe des articles publiés par les experts du Service d'assistance technique.

Ces articles contiennent des informations utiles, des recommandations et les réponses aux questions les plus souvent posées sur l'achat, l'installation et l'utilisation de Kaspersky Anti-Virus. Ils sont regroupés par thèmes tels que "Manipulation des licences", "Mise à jour des bases" ou "Résolution de problèmes". Les articles peuvent répondre à des questions qui concernent non seulement Kaspersky Anti-Virus mais également d'autres logiciels de Kaspersky Lab. Ils peuvent contient des nouvelles du service d'assistance technique dans son ensemble.

Système d'aide électronique

La distribution de l'application contient un fichier d'aide complète.

L'aide contient des informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, recherche de virus dans divers secteurs de l'ordinateur, exécution d'autres tâches.

Pour ouvrir l'aide, sélectionnez l'élément **Ouverture de l'aide** dans le menu **Aide** de la console de Kaspersky Anti-Virus.

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

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

Documentation

Les documents livrés avec Kaspersky Anti-Virus contiennent les informations nécessaires à son utilisation.

Le Guide d'installation contient les configurations matérielle et logicielle requises pour l'installation de l'application les instructions pour l'installation du logiciel, la marche à suivre pour vérifier son fonctionnement et procéder à la configuration initiale.

Le Manuel de l'administrateur contient les informations concernant l'administration de l'application depuis la console de Kaspersky Anti-Virus, depuis la ligne de commande du serveur protégé et depuis Kaspersky Administration Kit, ainsi que les compteurs et les pièges SNMP de Kaspersky Anti-Virus.

Le Guide de déploiement décrit les schémas typiques de déploiement de l'application et les types d'objets protégés.

Les documents au format PDF sont livrés dans la distribution de Kaspersky Anti-Virus.

Après avoir installé la console de Kaspersky Anti-Virus, vous pouvez ouvrir le manuel de l'administrateur depuis le menu **Démarrer**.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection ou l'achat de Kaspersky Anti-Virus ou la prolongation de la licence, vous pouvez contacter le Service commercial (http://www.kaspersky.com/fr/contacts).

Contactez les collaborateurs du service commercial par courrier électronique à l'adresse sales@kaspersky.com.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez déjà acheté Kaspersky Anti-Virus, vous pouvez obtenir des informations sur cette application auprès des experts du service d'assistance technique par téléphone ou via Internet.

Les experts du Service d'assistance technique répondront à vos questions concernant l'installation et l'utilisation de l'application. Si votre ordinateur a déjà été infecté, ils vous aideront à réparer les dégâts causés par les programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

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

Vous pouvez poser des questions aux experts du service d'assistance technique via le formulaire en ligne du système de traitement des requêtes des clients Helpdesk (http://support.kaspersky.ru/helpdesk.html?LANG=fr).

Vous pouvez rédiger votre requête en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une requête électronique, saisissez votre **numéro de client**, reçu lors de l'enregistrement sur le site Web du Service d'assistance technique, ainsi que votre **mot de passe**.

Si vous n'êtes pas encore un utilisateur enregistré des applications de Kaspersky Lab, vous pouvez remplir un formulaire d'inscription (https://support.kaspersky.com/fr/personalcabinet/registration/form/). Lors de l'enregistrement, saisissez le *code d'activation* de l'application ou le *nom du fichier de licence*.

Les experts du service d'assistance technique répondront à la question dans votre Espace personnel (https://support.kaspersky.com/fr/PersonalCabinet) et à l'adresse électronique que vous aurez communiquée.

Décrivez le problème rencontré avec le plus de détails possible dans le formulaire en ligne. Dans les champs obligatoires, saisissez :

- **Le type de requête**. Sélectionnez la catégorie qui correspond le mieux à votre problème, par exemple "Installation/désinstallation de l'application" ou "Recherche/suppression de virus". Si vous ne trouvez pas le thème qui se rapporte à votre cas, choisissez "Question générale".
- **Le nom et le numéro de version de l'application**.
- **Le texte du message**. Décrivez le problème rencontré avec le plus de détails possibles.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement sur le site du service d'assistance technique de Kaspersky Lab.
- **Courrier électronique**. Les experts du service d'assistance technique enverront leurs réponses à cette adresse.

Assistance technique par téléphone

Si vous avez un problème urgent, vous pouvez contacter le Service d'assistance technique de votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.com/fr/support/support_local) ou internationale (http://support.kaspersky.com/fr/support/international) veuillez fournir l'information (http://support.kaspersky.com/fr/support/details Nos experts pourront ainsi répondre plus rapidement à vos questions.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM EN LIGNE

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.fr.

Dans le forum, vous pouvez y consulter les discussions antérieures, publier des commentaires, créer une nouvelle discussion ou lancer une recherche.

UTILISATION DE LA CONSOLE DE KASPERSKY ANTI-VIRUS ET ACCES AUX FONCTIONS DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

À PROPOS DE LA CONSOLE DE KASPERSKY ANTI-VIRUS

La console de Kaspersky Anti-Virus est un composant enfichable isolé qui est ajouté à la console MMC (Microsoft Management Console).

Une fois l'installation de la console de Kaspersky Anti-Virus terminée, le programme d'**Installation** conserve le fichier kavfs.msc dans le répertoire de Kaspersky Anti-Virus et ajoute le composant enfichable à la liste des composants isolés de Microsoft Windows.

Vous pouvez ouvrir la console d'administration de Kaspersky Anti-Virus sur le serveur protégé depuis le menu **Démarrer** ou depuis le menu contextuel de l'icône de Kaspersky Anti-Virus dans la zone de notification la barre des tâches.

En exécutant le fichier msc avec le composant enfichable ou en ajoutant le composant enfichable Kaspersky Anti-Virus dans la console existante en tant que nouvel élément de l'arborescence. Dans la version 64 bits de Microsoft Windows, vous pouvez ajouter le composant enfichable de Kaspersky Anti-Virus uniquement dans MCC de la version 32 bits (MMC32) : ouvrez MMC via la ligne de commande à l'aide de l'instruction mmc.exe /32.

Il est possible d'administrer Kaspersky Anti-Virus par la console installée sur le serveur protégé ou sur tout autre ordinateur du réseau. Une fois que la Console de Kaspersky Anti-Virus a été installée sur un autre ordinateur, vous devez réaliser la configuration avancée (cf. rubrique "Configuration avancée après l'installation de la console de Kaspersky Anti-Virus sur un autre ordinateur" à la page 20).

Dans une console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants enfichables Kaspersky Anti-Virus afin de pouvoir administrer ainsi la protection de plusieurs serveur sur lesquels Kaspersky Anti-Virus est installé.

CONFIGURATION AVANCEE APRES L'INSTALLATION DE LA CONSOLE DE KASPERSKY ANTI-VIRUS SUR UN AUTRE ORDINATEUR

Si vous avez installé la console de Kaspersky Anti-Virus sur un ordinateur autre que le serveur protégé, procédez comme suit pour pouvoir administrer Kaspersky Anti-Virus à distance sur le serveur protégé :

- sur le serveur protégé, ajoutez les utilisateurs de Kaspersky Anti-Virus au groupe KAVWSEE Administrators ;
- si le serveur protégé tourne sous Microsoft Windows Server 2008, autorisez les connexions de réseau pour le fichier du processus du service d'administration de Kaspersky Anti-Virus kavfsgt.exe ;
- si vous n'avez pas coché la case **Autoriser les connexions de réseau pour la console de Kaspersky Anti-Virus** lors de l'installation de la console, autorisez les connexions de réseau pour la console via le pare-feu sur l'ordinateur où la console est installée.

DANS CETTE SECTION DE L'AIDE

AJOUT D'UTILISATEURS DE KASPERSKY ANTI-VIRUS AU GROUPE KAVWSEE ADMINISTRATORS SUR LE SERVEUR PROTEGE

Pour administrer Kaspersky Anti-Virus via la console de Kaspersky Anti-Virus installée sur un autre ordinateur, les utilisateurs de Kaspersky Anti-Virus doivent avoir l'accès complet au service d'administration de Kaspersky Anti-Virus (Kaspersky Anti-Virus Management) sur le serveur protégé. Par défaut, le service est accessible aux utilisateurs qui appartiennent au groupe d'administrateurs sur le serveur protégé.

Pour connaître les services enregistrés par Kaspersky Anti-Virus, lisez le document Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition. Manuel d'installation".

Lors de l'installation, Kaspersky Anti-Virus enregistre le groupe KAVWSEE Administrators sur le serveur protégé. Les utilisateurs de ce groupe ont accès au service d'administration de Kaspersky Anti-Virus. Vous pouvez octroyer ou bloquer l'accès aux service d'administration de Kaspersky Anti-Virus en ajoutant des utilisateurs au groupe KAVWSEE Administrators ou en les supprimant.

Vous pouvez vous connecter à Kaspersky Anti-Virus sous un compte utilisateur local si un compte utilisateur avec le même nom et un mot de passe sont enregistrés sur le serveur protégé.

AUTORISATION DES CONNEXIONS DE RESEAU POUR LE SERVICE D'ADMINISTRATION DE KASPERSKY ANTI-VIRUS.

Pour établir la connexion entre la console et le service d'administration de Kaspersky Anti-Virus, vous devez autoriser les connexions de réseau via le pare-feu pour le service d'administration de Kaspersky Anti-Virus sur le serveur protégé.

Vous devez configurer les connexions réseau si Kaspersky Anti-Virus tourne sous Microsoft Windows Server 2003 ou Microsoft Windows Server 2008.

Pour autoriser les connexions de réseau pour le service d'administration de Kaspersky Anti-Virus, procédez comme suit :

1. Sur le serveur protégé tournant sous Microsoft Windows Server 2008, sélectionnez **Démarrer** → **Panneau de configuration** → **Sécurité** → **Pare-feu Windows**.
2. Dans la fenêtre **Paramètres du pare-feu Windows**, cliquez sur **Modifier les paramètres**.
3. Sur l'onglet **Exclusions** dans la liste des exclusions prédéfinies, cochez les cases **COM + Accès réseau**, **Windows Management Instrumentation (WMI)** et **Remote Administration**.
4. Cliquez sur **Ajouter programme**.
5. Dans la boîte de dialogue **Ajout de programme**, sélectionnez le fichier kavfsgt.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de la console de Kaspersky Anti-Virus.
6. Cliquez sur **OK**.
7. Cliquez sur le bouton **OK** dans la boîte de dialogue **Paramètres du pare-feu Windows**.

AUTORISATION DES CONNEXIONS DE RESEAU POUR LA CONSOLE DE KASPERSKY ANTI-VIRUS

La console de Kaspersky Anti-Virus sur l'ordinateur distant utilise le protocole DCOM pour obtenir les informations sur les événements de Kaspersky Anti-Virus (objets analysés, tâches terminées, etc.) fournies par le service d'administration de Kaspersky Anti-Virus sur le serveur protégé. Vous devrez autoriser les connexions de réseau via le pare-feu sur cet ordinateur afin d'établir des connexions entre la console et le service d'administration de Kaspersky Anti-Virus.

Exécutez les actions suivantes :

- assurez-vous que l'accès à distance anonyme aux applications COM est autorisé (mais pas le lancement à distance et l'activation des applications COM) ;
- dans le pare-feu Windows, ouvrez le port TCP 135 et autorisez les connexions de réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Anti-Virus kavfsrcn.exe.

L'ordinateur sur lequel la console de Kaspersky Anti-Virus est installée utilise le port TCP 135 pour échanger les informations avec le serveur protégé.

Pour appliquer les nouveaux paramètres de protection : si la console de Kaspersky Anti-Virus était ouverte lorsque vous configuriez la connexion entre le serveur protégé et l'ordinateur sur lequel la console est installée, fermez la console, attendez que le processus kavfsrcn.exe d'administration à distance de Kaspersky Anti-Virus s'arrête, puis relancez la console.

Pour autoriser l'accès à distance anonyme aux applications COM, procédez comme suit :

1. Sur l'ordinateur où la console de Kaspersky Anti-Virus est installée, ouvrez la console **Service des composants** : sélectionnez **Démarrer** ® **Exécuter**, saisissez la commande dcomcnfg, puis cliquez sur OK.
2. Dans la console Services des composants de l'ordinateur, déployez le nœud **Ordinateurs**, ouvrez le menu contextuel du nœud **Poste de travail** et sélectionnez **Propriétés**.
3. Dans l'onglet **Sécurité COM** de la boîte de dialogue **Propriétés**, cliquez sur le bouton **Modifier les restrictions** du groupe de paramètres **Privilèges d'accès**.

4. Dans la boîte de dialogue **Autorisation d'accès**, vérifiez que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur ANONYMOUS LOGON.

5. Cliquez sur **OK**.

Pour ouvrir le port TCP 135 du pare-feu Windows et autoriser les connexions de réseau pour le fichier exécutable du processus d'administration à distance de Kaspersky Anti-Virus, procédez comme suit :

1. Sur l'ordinateur distant, fermez la console de Kaspersky Anti-Virus.

2. Exécutez une des actions suivantes :

   - *Dans Microsoft Windows XP* ou *Microsoft Windows Vista* :

     a. Dans Microsoft Windows XP Service Pack 2 ou supérieur, sélectionnez **Démarrer → Pare-feu Windows**.

     Dans Microsoft Windows Vista, sélectionnez **Démarrer → Panneau de configuration → Pare-feu Windows**, et dans la fenêtre **Pare-feu Windows**, cliquez sur **Modifier les paramètres**.

     b. Sur l'onglet **Exclusions** de la fenêtre **Pare-feu Windows** (**Paramètres du pare-feu Windows**), cliquez sur le bouton **Ajouter port**.

     c. Dans le champ **Nom** , indiquez le nom du port RPC (TCP/135) ou définissez un autre nom, par exemple DCOM Kaspersky Anti-Virus et dans le champ **Numéro de port**, indiquez le numéro du port : 135.

     d. Sélectionnez le protocole **TCP**.

     e. Cliquez sur **OK**.

     f. Sur l'onglet **Exclusions**, cliquez sur le bouton **Ajouter programme**.

   - *Dans Microsoft Windows 7* :

     a. Sélectionnez **Démarrer → Panneau de configuration → Pare-feu Windows** dans la fenêtre **Pare-feu Windows** sélectionnez **Autoriser le lancement de l'application ou du composant depuis Pare-feu Windows**.

     b. Dans la boîte de dialogue **Autoriser un programme via le Pare-feu Windows**, cliquez sur le bouton **Autoriser un autre programme**.

3. Dans la boîte de dialogue **Ajout de programme**, désignez le fichier kavfsrcn.exe. Il se trouve dans le répertoire que vous avez indiqué en tant que répertoire d'installation de la console de Kaspersky Anti-Virus.

4. Cliquez sur **OK**.

5. Cliquez sur le bouton **OK** dans la boîte de dialogue **Pare-feu Windows** (**Paramètres du pare-feu Windows**).

LANCEMENT DE LA CONSOLE DE KASPERSKY ANTI-VIRUS DEPUIS LE MENU DEMARRER

Assurez-vous que la console de Kaspersky Anti-Virus est installée sur l'ordinateur.

Pour lancer la console de Kaspersky Anti-Virus depuis le menu Démarrer, procédez comme suit :

1. Choisissez l'option **Démarrer → Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Outils d'administration → Console de Kaspersky Anti-Virus**.

(Si vous avez l'intention d'ajouter d'autres composants enfichables à la console de Kaspersky Anti-Virus, ouvrez la console en mode édition : sélectionnez **Démarrer → Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Outils d'administration**. Ouvrez le menu contextuel de l'application **Console de Kaspersky Anti-Virus** et choisissez l'option **Auteur**).

Si vous avez lancé la console de Kaspersky Anti-Virus sur le serveur protégé, la fenêtre de la console s'ouvrira (cf. ill. ci-après).

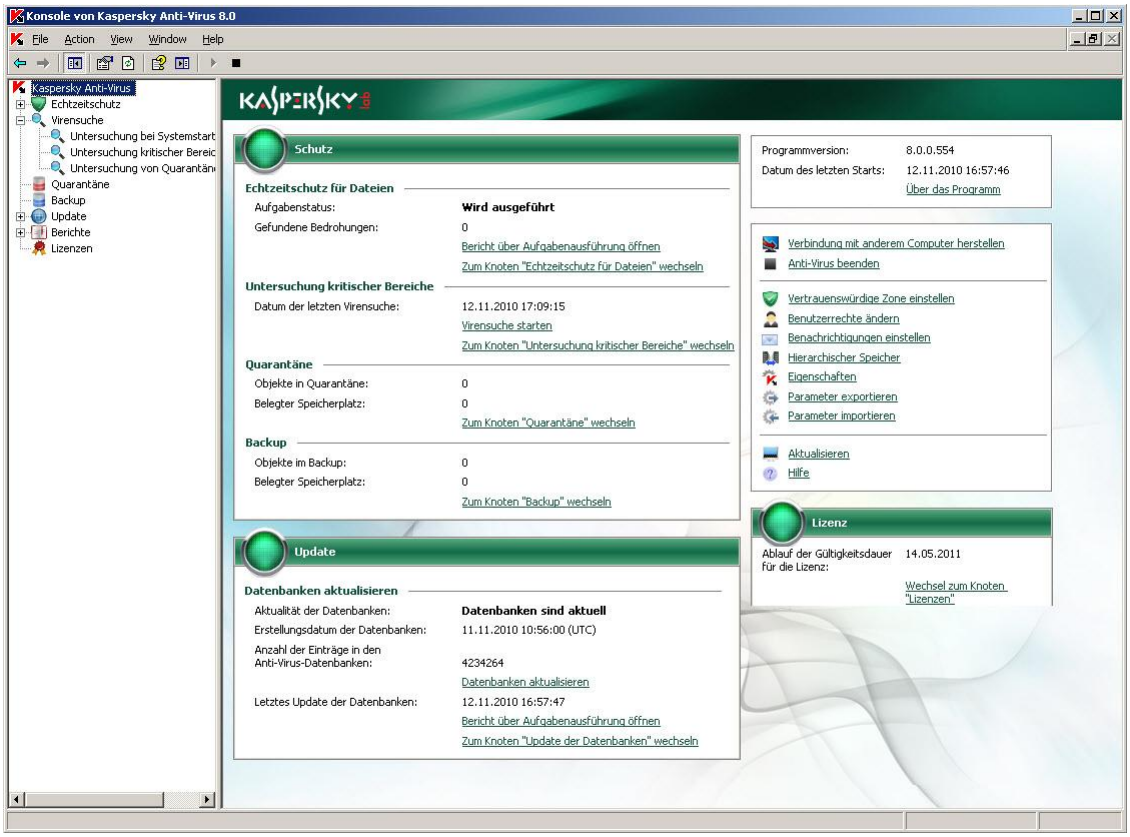


Illustration 1. Console de Kaspersky Anti-Virus

2. Si vous avez lancé la console de Kaspersky Anti-Virus non pas sur le serveur protégé, mais sur un autre ordinateur, connectez-vous au serveur à protéger : ouvrez le menu contextuel du nom du composant enfichable de Kaspersky Anti-Virus, sélectionnez la commande **Se connecter à un autre ordinateur**, puis dans la boîte de dialogue **Sélection de l'ordinateur**, sélectionnez **Autre ordinateur**, et dans le champ de saisie, indiquez le nom de réseau du serveur protégé.

   Si le compte utilisateur employé pour accéder à Microsoft Windows ne jouit pas des privilèges d'accès au service d'administration de Kaspersky Anti-Virus sur le serveur, indiquez un autre compte qui jouit de tels privilèges. Pour obtenir de plus amples informations sur les comptes utilisateurs qui peuvent jouir de l'accès au service d'administration de Kaspersky Anti-Virus, consultez le point "Ajout d'utilisateurs de Kaspersky Anti-Virus au groupe KAVWSEE Administrators sur le serveur protégé" (cf. page 20).

ICONE DE KASPERSKY ANTI-VIRUS DANS LA BARRE DES TACHES

Chaque fois que Kaspersky Anti-Virus se lance automatiquement après le redémarrage du serveur, son icône apparaît dans la zone de notification de la barre des tâches du serveur . L'icône de Kaspersky Anti-Virus est affichée par défaut si vous avez installé le composant **Application de la barre des tâches** lors de l'installation de Kaspersky Anti-Virus.

L'icône de Kaspersky Anti-Virus peut avoir un des états suivants :

- actif (en couleur) si une des tâches de protection en temps réel est en cours d'exécution : **Protection en temps réel des fichiers** ou **Analyse des scripts** (cf. page 87) ;

- inactif (noir et blanc) si les tâches **Protection en temps réel des fichiers** et **Analyse des scripts** ne sont pas en cours d'exécution.

Vous pouvez ouvrir le menu contextuel de l'icône de Kaspersky Anti-Virus avec un clic droit (cf. ill. ci-après).

Illustration 2. Menu contextuel de l'icône de Kaspersky Anti-Virus

Le menu contextuel contient plusieurs commandes d'affichage de boîtes de dialogue de l'application (cf. tableau ci-après).

Tableau 1. Commandes du menu contextuel de l'icône de Kaspersky Anti-Virus

INSTRUCTION	DESCRIPTION
Ouvrir la console de Kaspersky Anti-Virus	Ouvre la console de Kaspersky Anti-Virus (si celle-ci est installée).
À propos du logiciel	Ouvre la fenêtre **À propos du logiciel** qui contient des informations sur Kaspersky Anti-Virus. Si vous êtes un utilisateur enregistré de Kaspersky Anti-Virus, alors la fenêtre **À propos du logiciel** contient des informations sur les mises à jour urgentes installées.
Masquer	Cache l'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches. Pour afficher à nouveau l'icône de Kaspersky Anti-Virus, dans le menu **Démarrer**, choisissez l'option **Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Application** dans la barre des tâches.

Dans le cadre de la configuration des paramètres généraux de Kaspersky Anti-Virus, vous pouvez activer et désactiver l'affichage de l'icône de Kaspersky Anti-Virus au lancement automatique de Kaspersky Anti-Virus après le redémarrage du serveur (cf. rubrique "Procédure de configuration des paramètres de Kaspersky Anti-Virus dans MMC" à la page 38).

FENETRE DE LA CONSOLE DE KASPERSKY ANTI-VIRUS

La fenêtre de la console de Kaspersky Anti-Virus contient l'arborescence de la console et le panneau des résultats. L'arborescence reprend les nœuds des composants de Kaspersky Anti-Virus tandis que le panneau des résultats affiche les informations relatives au nœud sélectionné (cf. ill. ci-après).

La fenêtre de la console de Kaspersky Anti-Virus contient également le panneau d'accès rapide.

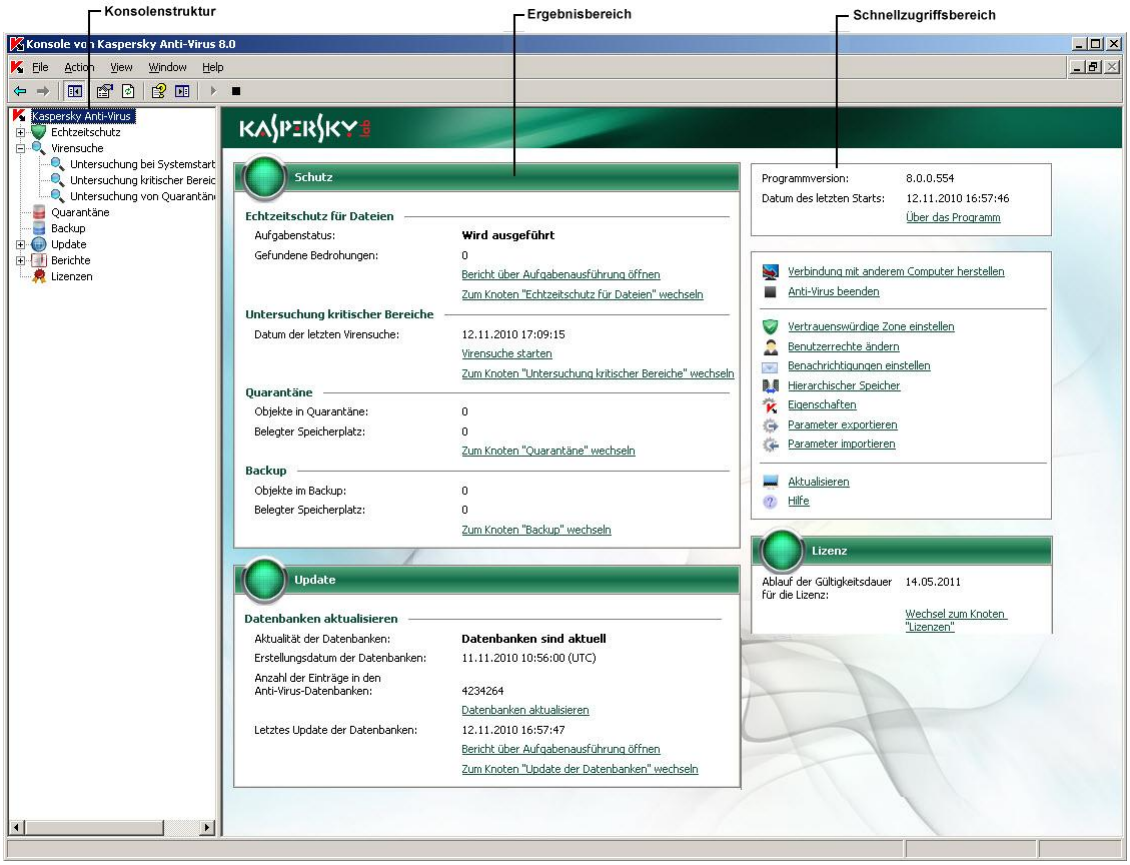


Illustration 3. Fenêtre de la console de Kaspersky Anti-Virus

RESTRICTION DES PRIVILEGES D'ACCES AUX FONCTIONS DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES PRIVILEGES D'ACCES AUX FONCTIONS DE KASPERSKY ANTI-VIRUS

Par défaut, l'accès à toutes les fonctions de Kaspersky Anti-Virus est octroyé aux utilisateurs du groupe Administrateurs et aux utilisateurs du groupe KAVWSEE Administrators créé sur le serveur protégé lors de l'installation de Kaspersky Anti-Virus.

Les utilisateurs qui ont accès à la fonction **Modification des privilèges** de Kaspersky Anti-Virus peuvent offrir l'accès aux fonctions de Kaspersky Anti-Virus aux autres utilisateurs enregistrés sur le serveur protégé ou repris dans le domaine.

Si l'utilisateur ne figure pas dans la liste des utilisateurs de Kaspersky Anti-Virus, il ne pourra pas consulter la Console.

Vous pouvez octroyer aux utilisateurs de Kaspersky Anti-Virus (groupe d'utilisateurs) les niveaux d'accès système suivants :

- **Contrôle complet** : accès à toutes les fonctions de Kaspersky Anti-Virus ;
- **Modification** : accès à toutes les fonctions de Kaspersky Anti-Virus, sauf l'administration des permissions des autres utilisateurs ;
- **Lecture** : uniquement la consultation des composants fonctionnels de Kaspersky Anti-Virus, des paramètres généraux de ses fonctions et de ses tâches, des statistiques et des permissions utilisateur.

Vous pouvez également réaliser une configuration étendue des droits d'accès : autoriser ou refuser l'accès à des fonctions particulières de Kaspersky Anti-Virus (cf. tableau ci-après).

Tableau 2. Restriction des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

FONCTION	DESCRIPTION
Consultation des statistiques	Consultation de l'état des composants fonctionnels de Kaspersky Anti-Virus et des statistiques sur les tâches en cours
Création et suppression de tâches	Lancement / arrêt/ suspension / rétablissement des tâches de Kaspersky Anti-Virus
Administration des tâches	Création et suppression de tâches d'analyse à la demande
Lire les paramètres	• Consultation des paramètres généraux de Kaspersky Anti-Virus et des paramètres des tâches • Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications • Exportation des paramètres de Kaspersky Anti-Virus
Modifier les paramètres	• Consultation et modification des paramètres généraux de Kaspersky Anti-Virus • Importation et exportation des paramètres de Kaspersky Anti-Virus • Consultation et modification des paramètres des tâches • Consultation et modification des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications
Gérer la quarantaine et les sauvegardes	• Placement des objets en quarantaine • Suppression des objets de la quarantaine et des fichiers de la sauvegarde • Récupération des objets de la sauvegarde et de la quarantaine
Lecture des journaux	Consultation des événements dans les journaux d'exécution des tâches et du journal d'audit système
Administration des journaux	Suppression des journaux d'exécution des tâches et purge du journal d'audit système
Administration des licences.	Installation et suppression des licences
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Anti-Virus
Modification des privilèges	• Ajout et suppression d'utilisateurs de Kaspersky Anti-Virus • Modification des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

•

CONFIGURATION DES PRIVILEGES D'ACCES AUX FONCTIONS DE KASPERSKY ANTI-VIRUS

Pour ajouter ou supprimer un utilisateur (groupe) ou modifier les droits d'accès d'un utilisateur (de groupe), procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du composant enfichable Kaspersky Anti-Virus et sélectionnez la commande **Modifier les permissions utilisateur**.

   La boîte de dialogue **Autorisations pour Kaspersky Anti-Virus** (cf. ill. ci-après) s'ouvrira.

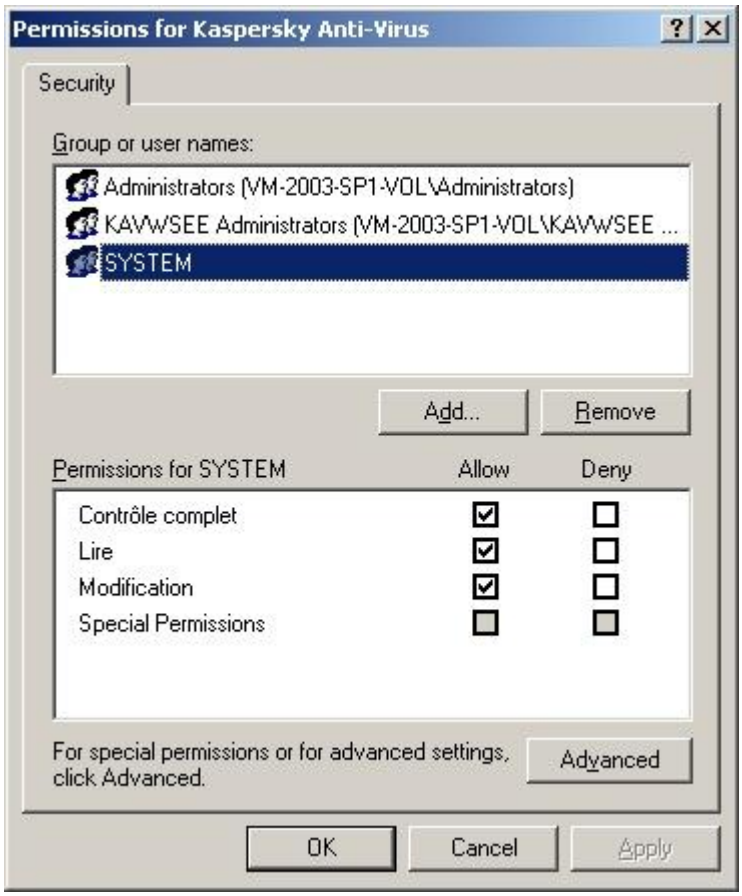


*Illustration 4. Boîte de dialogue **Autorisations***

2. Dans la boîte de dialogue **Autorisations pour Kaspersky Anti-Virus** exécutez les actions suivantes :

   - Pour ajouter un utilisateur (un groupe) à la liste des utilisateurs de Kaspersky Anti-Virus, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe que vous souhaitez ajouter.

   - Pour octroyer à l'utilisateur (groupe) ajouté des droits d'accès aux fonctions de Kaspersky Anti-Virus, sélectionnez l'utilisateur (du groupe) de la liste **Groupes ou utilisateurs** et sous le titre **Autorisations** pour **<Utilisateur (Groupe)>**, cochez la case **Autoriser** en regard des privilèges suivants :

     - **Contrôle complet** pour octroyer l'accès à toutes les fonctions de Kaspersky Anti-Virus ;

     - **Lecture** pour octroyer l'accès aux fonctions. **Lire les statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lecture des privilèges** ;

     - **Modification** pour octroyer l'accès à l'ensemble des fonctions de Kaspersky Anti-Virus, sauf **Modification des privilèges**.

- Pour réaliser une configuration élargie des privilèges (Autorisations spéciales), cliquez sur le bouton **Avancé**. Dans la boîte de dialogue **Paramètres de sécurité complémentaires**, sélectionnez l'utilisateur ou le groupe et cliquez sur **Modifier**, puis dans la boîte de dialogue **Elément d'autorisation pour Kaspersky Anti-Virus**, cochez la case **Autoriser** ou **Interdire** à côté des fonctions auxquelles vous souhaitez autoriser ou refuser l'accès (cf. ill. ci-après). La liste des fonctions avec leur brève description se trouve dans le tableau dans la section "Présentation des privilèges d'accès aux fonctions de Kaspersky Anti-Virus" (cf. page 25). Cliquez sur **OK**.

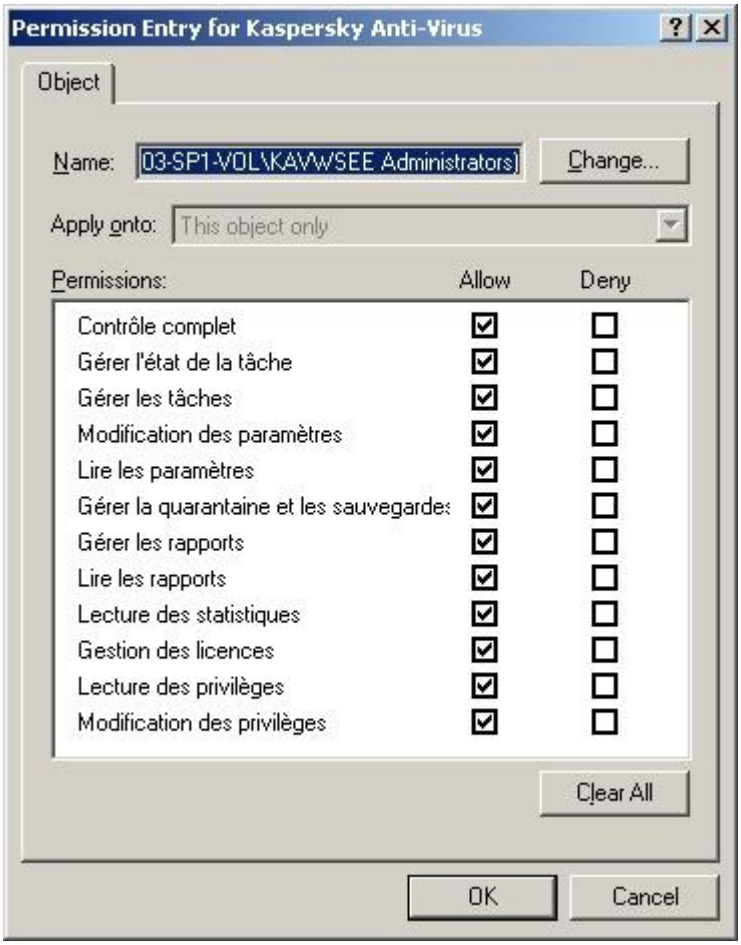


*Illustration 5. Boîte de dialogue **Elément d'autorisations pour Kaspersky Anti-Virus***

3. Cliquez sur **OK** dans la boîte de dialogue **Autorisations pour Kaspersky Anti-Virus**.

BOITES DE DIALOGUE : CONSOLE DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

FENETRE SELECTION D'ORDINATEUR

Dans la fenêtre **Sélection d'ordinateur**, spécifiez le serveur dont vous souhaitez administrer la protection par la console de Kaspersky Anti-Virus.

Vous avez le choix parmi les options suivants :

- **Ordinateur local** (sur lequel s'exécute la console), si vous avez lancé la console de Kaspersky Anti-Virus sur le serveur protégé.
- **Autre ordinateur** , si vous avez lancé la console de Kaspersky Anti-Virus sur un autre ordinateur que le serveur protégé. Spécifiez le nom de l'ordinateur dans la zone de saisie. Indiquez son nom manuellement ou sélectionnez le poste dans une liste avec le bouton **Parcourir**.

  Si le compte utilisateur utilisé pour ouvrir la session dans Microsoft Windows ne possède pas de privilèges d'accès suffisants au service d'administration du programme antivirus sur le serveur sélectionné, spécifiez un compte utilisateur avec les privilèges appropriés. Pour ce faire, sélectionnez **Se connecter sous le compte utilisateur**, saisissez manuellement le nom de l'utilisateur ou sélectionnez-le dans la liste ouverte avec **Parcourir**, puis spécifiez son mot de passe.

VOIR EGALEMENT

Lancement de la console de Kaspersky Anti-Virus depuis le menu Démarrer 22

KASPERSKY ANTI-VIRUS (ENTREE)

La console de Kaspersky Anti-Virus est affichée dans l'arborescence de la console MMC sous une entrée libellée **Kaspersky Anti-Virus**.

Après connexion au serveur, le nom de l'ordinateur et le compte utilisateur sont ajoutés au libellé de l'entrée **Kaspersky Anti-Virus <Nom de poste> en tant que <compte_utilisateur>**. Le nom de l'entrée ne change pas quand une connexion est faite sur un ordinateur local.

La fenêtre de la console de Kaspersky Anti-Virus contient l'arborescence de la console et le panneau des résultats. La fenêtre de la console de Kaspersky Anti-Virus contient également le panneau d'accès rapide.

Arborescence de la console

L'arborescence reprend les nœuds des composants de Kaspersky Anti-Virus.

Si la connexion se fait avec le serveur, l'entrée **Kaspersky Anti-Virus** affiche alors des sous-entrées qui permettent de gérer une caractéristique spécifique de l'antivirus :

- **Protection en temps réel des fichiers** : gestion de la protection en temps réel des fichiers et analyse des scripts. Une entrée séparée existe pour chacun des composants :
  - **Protection en temps réel des fichiers.**
  - **Analyse des scripts**.
- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Une entrée séparée existe pour chacune des tâches système :
  - **Analyse au démarrage du système**.
  - **Analyse des zones critiques**.
  - **Analyse des objets en quarantaine**.

Une entrée séparée existe pour chaque tâche personnalisée et pour chaque tâche de groupe créée et transmise au serveur par Kaspersky Administration Kit.

- **Quarantaine** contrôle les paramètres de la quarantaine et gère les objets en quarantaine. L'entrée contient une liste d'objets en quarantaine.
- **Sauvegardé** : contrôle les paramètres de sauvegardé et gère les objets sauvegardés. L'entrée contient une liste de copies de sauvegardé.
- **Mise à jour** : gère la mise à jour des bases de Kaspersky Anti-Virus et des modules de programmes ainsi que leur distribution vers un dossier local source de mises à jour. L'entrée contient des sous-entrées permettant d'administrer chacune des tâches de mise à jour ou d'annulation des mises à jour :
  - **Mise à jour des bases de l'application**.
  - **Mise à jour des modules de l'application**.
  - **Copie des mises à jour**.
  - **Annulation de la mise à jour**.

  Une entrée séparée existe pour chaque tâche créée et transmise au serveur par Kaspersky Administration Kit.
- **Journaux** : gère les journaux relatifs à la protection en temps réel, aux analyses à la demande et aux tâches de mise à jour; gère le journal d'audit de Kaspersky Anti-Virus.
- **Licences** : installation et suppression les licences de Kaspersky Anti-Virus, affichage des informations sur les licences installées.
- **EMC Celerra**: état de la prise en charge du système de stockage de données EMC Celerra.

Panneau de résultats

Le panneau des résultats affiche des informations sur l'état actuel de la protection du serveur, sur Kaspersky Anti-Virus ainsi que sur l'état de ses composants.

Panneau de tâches et menu contextuel de l'entrée Kaspersky Anti-Virus

À l'aide des commandes du menu contextuel de l'entrée **Kaspersky Anti-Virus** et des liens dans le panneau de tâches, vous pouvez effectuer les actions suivantes :

- **Se connecter à un autre ordinateur** : se connecte à un autre ordinateur pour gérer les composants de protection dont il est équipé.
- **Lancer Kaspersky Anti-Virus / Arrêter Kaspersky Anti-Virus** : lancer / arrêter l'application. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils.
- **Configurer la zone de confiance** : définit les exclusions de l'analyse.
- **Modifier les permissions utilisateur** : modifie les droits d'accès.
- **Configurer les notifications** : configure les paramètres de notification.
- **Sauvegarde hiérarchique** : configure les paramètres de la sauvegarde hiérarchique.
- **Exporter les paramètres** : enregistre les paramètres de l'application dans un fichier.
- **Importer les paramètres** : récupère les paramètres de l'application à partir d'un fichier.
- **A propos du programme** : affiche des informations générales sur l'application.

- **Propriétés**- affiche et configure les paramètres généraux de Kaspersky Anti-Virus.

VOIR EGALEMENT

Consultation de l'état de la protection et d'informations sur Kaspersky Anti-Virus 33

LANCEMENT ET ARRET DU SERVICE DE KASPERSKY ANTI-VIRUS

Le service de Kaspersky Anti-Virus est lancé automatiquement par défaut au démarrage du système d'exploitation. Il gère les processus actifs de la protection en temps réel, de l'analyse à la demande et de la mise à jour.

Le lancement du service de Kaspersky Anti-Virus s'accompagne par défaut de l'activation de la **Protection en temps réel des fichiers**, de l'**Analyse des scripts**, de l'**Analyse au démarrage du système** ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Si vous arrêtez le service de Kaspersky Anti-Virus, l'ensemble des tâches en cours d'exécution sera interrompu. Lorsque vous relancerez le service de Kaspersky Anti-Virus, sachez que les tâches interrompues ne seront pas automatiquement rétablies. Seules les tâches dont la fréquence d'exécution est définie par le paramètre **Au lancement de l'application** seront à nouveau exécutées.

Vous pouvez lancer et arrêter le service de Kaspersky Anti-Virus uniquement si vous faites partie du groupe d'administrateurs sur le serveur protégé.

Pour arrêter ou lancer le service de Kaspersky Anti-Virus, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nom du composant enfichable de Kaspersky Anti-Virus.
2. Choisissez une des commandes suivantes :
   - **Arrêter l'Anti-Virus** pour arrêter le service de Kaspersky Anti-Virus ;
   - **Lancer l'Anti-Virus** pour lancer le service de Kaspersky Anti-Virus.

Vous pouvez également lancer et arrêter le service de Kaspersky Anti-Virus via le composant enfichable **Services** de Microsoft Windows.

CONSULTATION DE L'ETAT DE LA PROTECTION ET D'INFORMATIONS SUR KASPERSKY ANTI-VIRUS

Vous pouvez consulter les informations relatives à l'état actuel de la protection du serveur ainsi que les informations sur Kaspersky Anti-Virus et l'état de ses composants fonctionnels.

- *Afin de consulter l'état de la protection et les informations sur Kaspersky Anti-Virus, procédez comme suit,*

  cliquez sur le nom du composant enfichable de Kaspersky Anti-Virus dans l'arborescence de la console (cf. ill. ci-après).

  Le nœud **Kaspersky Anti-Virus** s'ouvre.

Les informations présentées dans le nœud **Kaspersky Anti-Virus** sont actualisées par défaut toutes les minutes. Vous pouvez les actualiser en fonction de vos besoins.

- *Pour actualiser manuellement les informations du nœud **Kaspersky Anti-Virus**,*

  ouvrez le menu contextuel du composant logiciel enfichable de Kaspersky Anti-Virus et sélectionnez l'option **Mettre à jour**.

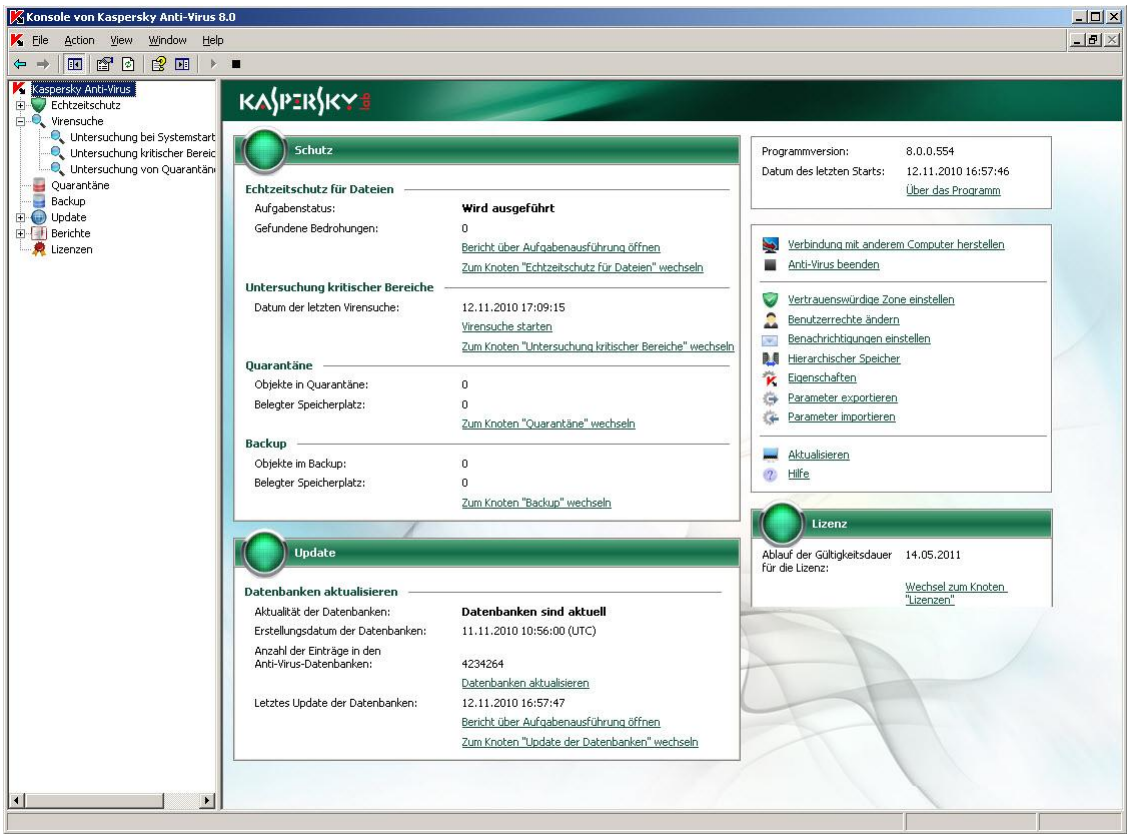


Illustration 6. Console de Kaspersky Anti-Virus

Le panneau des résultats reprend les informations suivantes sur Kaspersky Anti-Virus :

Tableau 3. Informations sur l'état de la protection

GROUPE "PROTECTION"	CONSEIL
Etat de la protection	Peut avoir une des valeurs suivantes :  – les tâches **Protection en temps réel des fichiers** et **Analyse des scripts** sont en cours, la tâche **Analyse des zones critiques** a été exécutée il y a moins de 14 jours (par défaut) ;  – une ou les deux tâches de protection en temps réel ont été arrêtées par l'utilisateur, ou l'événement *L'analyse des zones critiques n'a pas été réalisée depuis longtemps* s'est produit ;  – une des tâches de protection en temps réel s'est soldée sur un échec.
Protection en temps réel des fichiers	**Etat de la tâche** : l'état actuel de la tâche, par exemple *Exécutée*, *Arrêtée* ou *En pause*. **Statistiques de la tâche** : **Menaces découvertes** : nombre de menaces découvertes depuis le lancement de la tâche.
Analyse des scripts	**Etat de la tâche** : l'état actuel de la tâche, par exemple *Exécutée*, *Arrêtée* ou *En pause*. **Statistiques de la tâche** : **Scripts dangereux découverts** : nombre de scripts découvertes depuis le lancement de la tâche.
Analyse des zones critiques	**L'analyse des zones critiques n'a pas été réalisée depuis longtemps**. Ce statut s'affiche si la tâche **Analyse des zones critiques** n'a plus été réalisée depuis 30 jours (par défaut). Vous pouvez configurer la notification de l'administrateur sur cet événement ; vous pouvez modifier la durée avant le déclenchement de cet événement.
Quarantaine	**Etat de la quarantaine** : Si les paramètres **Taille maximale de la quarantaine** et **Seuil d'espace libre en quarantaine** de la quarantaine sont appliqués, alors une fois que le volume de données dans la quarantaine atteint les valeurs définies, les informations indiquent que : • Le seuil d'espace libre pour la quarantaine est atteint ; • La taille maximale de la quarantaine a été dépassée. Kaspersky Anti-Virus continue à isoler les objets suspects. Vous pouvez configurer les notifications de l'administrateur sur ces événements (cf. page 264). Vous pouvez modifier les paramètres de la quarantaine (cf. page 202). **Statistiques de quarantaine** : **Objets en quarantaine** : nombre d'objets qui se trouvent actuellement en quarantaine. **Taille** : volume d'espace occupé dans la quarantaine.

GROUPE "PROTECTION"	CONSEIL
Sauvegarde	**Etat de la sauvegarde** : Si les paramètres **Taille maximale de la sauvegarde** et **Seuil d'espace libre en sauvegarde** de la sauvegarde sont appliqués, alors une fois que le volume de données dans la sauvegarde atteint les valeurs définies, les informations indiquent que les événements suivants ont eu lieu : • Le seuil d'espace libre pour la sauvegarde est atteint ; • la taille maximale de la sauvegarde a été dépassée. Kaspersky Anti-Virus continue à placer les fichiers en sauvegarde. Vous pouvez configurer les notifications de l'administrateur sur ces événements (cf. page 264). Vous pouvez modifier les paramètres de la sauvegarde (cf. page 218). **Statistiques de sauvegarde** : **Nombre d'objets dans le dossier de sauvegarde** : nombre d'objets présents actuellement dans la sauvegarde. **Taille** : volume d'espace occupé dans la sauvegarde.

Tableau 4. Informations sur l'état des bases et des modules logiciels de Kaspersky Anti-Virus

LE BLOC "MISES A JOUR"	CONSEIL
Mises à jour des bases de l'application	Etat des bases que Kaspersky Anti-Virus utilise lors de l'analyse des objets dans la tâche **Protection en temps réel des fichiers** et dans les tâches d'analyse à la demande. État de la base de données. Peut avoir une des valeurs suivantes :  – les bases sont d'actualité, aucune mise à jour critique n'est disponible ;  – un des événements suivants s'est produit : *Les bases sont dépassées*; *Des mises à jour critiques sont disponibles*; *Les mise à jour critiques ont été rappelées*; *L'application des mises à jour requiert le redémarrage du serveur*; *Le rappel des mises à jour requiert le redémarrage du serveur;*  – l'événement *Les bases de données sont périmées* ou *Les bases sont corrompues*. **Date de publication des bases** – date et heure de la publication des dernières bases actualisées installées. Pour lancer la tâche **Mise à jour des bases de l'application**, cliquez sur le lien **Mettre les bases à jour**.
Mise à jour des modules	Quand des mises à jour critiques des modules de Kaspersky Anti-Virus sont diffusées (cf. rubrique "À propos de la mise à jour des modules de Kaspersky Anti-Virus" à la page 60), le nom de la mise à jour et le lien vers la page Web de Kaspersky Lab contenant les informations détaillées sur la mise à jour sont présentées ici. Le lien **Mettre à jour les modules** ouvre la tâche **Mise à jour des modules de l'application** si la tâche prévoit uniquement la réception d'informations sur la présence de mises à jour critiques et lance la tâche **Mise à jour des modules de l'application** si l'installation des mises à jour critique est configurée. Quand des mises à jour prévues des modules de Kaspersky Anti-Virus sont diffusées (cf. rubrique "À propos de la mise à jour des modules de Kaspersky Anti-Virus" à la page 60), le nom de la mise à jour et le lien vers la page Web de Kaspersky Lab contenant les informations détaillées sur la mise à jour sont présentées ici. Si l'application des mises à jour copiées requiert le redémarrage du serveur, le message **Redémarrez le serveur pour appliquer les mises à jour s'affiche**.

Tableau 5. Informations sur l'état de la licence

GROUPE "LICENCE"	CONSEIL
Etat de la licence	Peut avoir une des valeurs suivantes :  – licence active;  – il reste 14 jours ou moins avant expiration de la licence;  – la durée de validité de la licence est écoulée; la licence n'est pas installée; violation du contrat de licence (par exemple, le fichier de licence se trouve sur la liste noire). Vous pouvez configurer la notification de l'administrateur sur l'échéance prochaine de la licence (cf. page 264)
Licence	Le lien **Passer au nœud "Licences"** ouvre le nœud **Licences** de la console de Kaspersky Anti-Virus. Le lien **Installer** permet de lancer l'Assistant d'installation de la nouvelle clé de licence.

Tableau 6. Informations sur l'état de la prise en charge d'EMC Celerra

GROUPE " EMC CELERRA "	CONSEIL
État de la prise en charge d'EMC Celerra	Affiche l'état de la protection du système de conservation des données en réseau EMC Celerra. Peut prendre les valeurs suivantes : • **Agent antivirus Celerra introuvable** : l'application n'a pas trouvé le logiciel de la société EMC ou erreur s'est produite dans le code d'intégration. • **La protection est désactivée** : l'application a découvert l'application de la société EMC, mais le composant **Analyse à la demande** est désactivé dans Kaspersky Anti-Virus. • **La protection est activée** : l'application a découvert l'application de la société EMC, mais le composant **Analyse à la demande** est activé dans Kaspersky Anti-Virus.

•

CONFIGURATION DE PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS EN MMC

Les paramètres généraux de Kaspersky Anti-Virus définissent les conditions générales de fonctionnement de Kaspersky Anti-Virus. Ils déterminent le nombre de processus utilisés par Kaspersky Anti-Virus, ils permettent d'activer la restauration des tâches de Kaspersky Anti-Virus après un arrêt fautif de leur fonctionnement, de tenir un journal de traçage, d'activer le vidage de la mémoire des processus de Kaspersky Anti-Virus lorsqu'ils sont arrêtés en raison d'une erreur, d'activer ou de désactiver l'affichage de l'icône de Kaspersky Anti-Virus à l'ouverture automatique de l'application après le redémarrage du serveur et de configurer d'autres paramètres généraux.

DANS CETTE SECTION DE L'AIDE

CONFIGURATION DES PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS DANS MMC

Cette rubrique contient les informations relatives à la configuration des paramètres généraux de Kaspersky Anti-Virus.

Pour configurer les paramètres des journaux de Kaspersky Anti-Virus, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du composant logiciel enfichable Kaspersky Anti-Virus et sélectionnez le point **Propriétés** de l'application.

2. Sur les onglets suivants, modifiez la valeur des paramètres généraux de Kaspersky Anti-Virus en fonction de vos besoins :

   - L'onglet **Général** permet de définir les paramètres suivants (cf. ill. ci-après) :

     - Nombre maximum de processus de travail actifs que Kaspersky Anti-Virus peut lancer (cf. page 356) ;

     - Nombre fixe de processus pour les tâches de protection en temps réel (cf. page 357) ;

     - Nombre de processus de travail pour les tâches d'analyse à la demande en arrière-plan (cf. page 358) ;

- Nombre de tentatives de restauration des tâches après un arrêt sur un échec (cf. page 359).

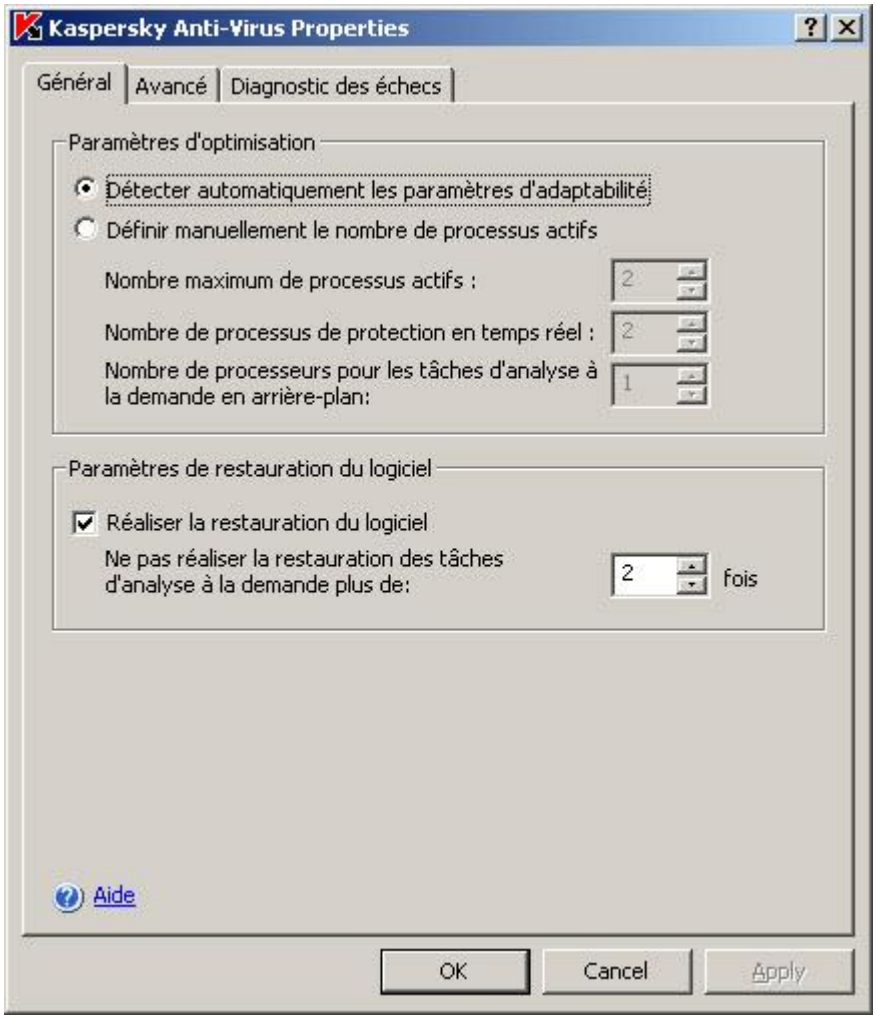


*Illustration 7. Boîte de dialogue **Propriétés : Kaspersky Anti-Virus**, onglet **Général***

- Sur l'onglet **Avancé**, exécutez les actions suivantes (cf. ill. ci-après) :
  - Précisez s'il faut afficher l'Icône de Kaspersky Anti-Virus dans la barre des tâches à chaque démarrage de Kaspersky Anti-Virus (cf. page 23).
  - Précisez les actions de Kaspersky Anti-Virus dans le fonctionnement sur la source d'alimentation de secours (cf. page 359) ;
  - indiquez le nombre de jours après lequel les événements *Les bases de données sont dépassées*, *Les bases de données sont périmées* et *L'analyse des zones critiques n'a pas été réalisée depuis longtemps seront déclenchés* (cf. page 360).

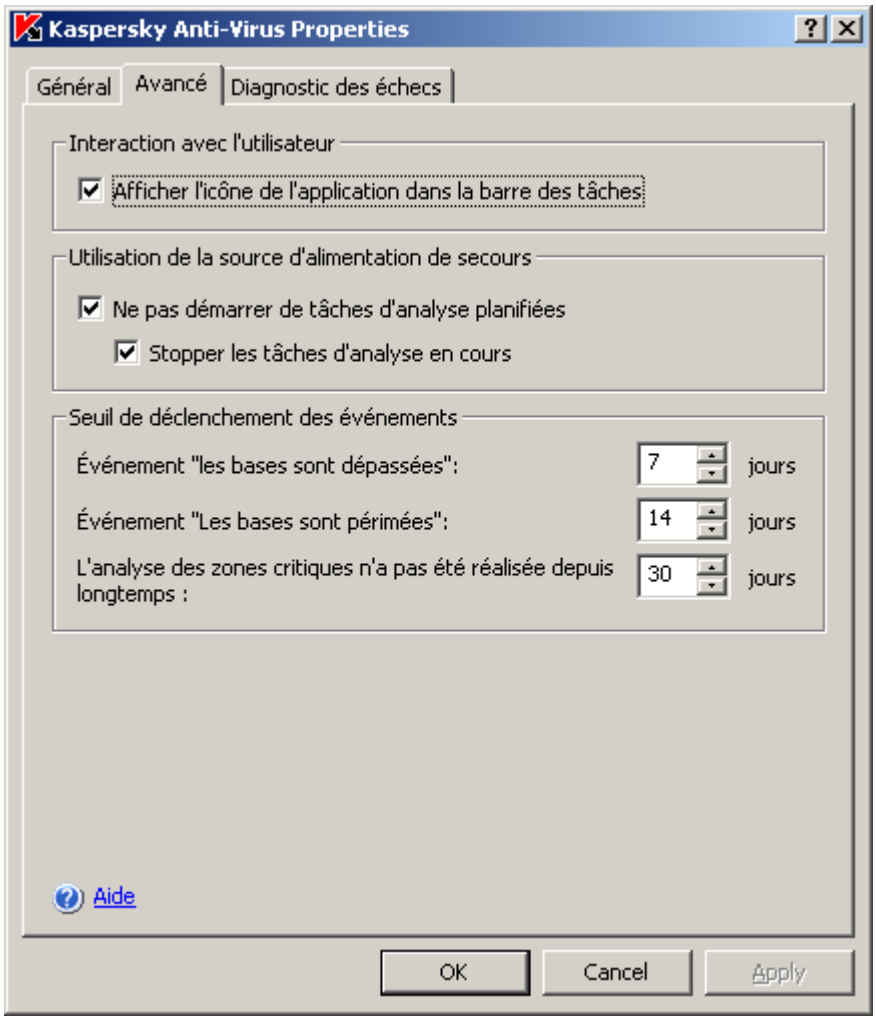


*Illustration 8. Boîte de dialogue **Propriétés : Kaspersky Anti-Virus**, onglet **Avancé***

- Sur l'onglet **Diagnostic des échecs**, exécutez les actions suivantes (cf. ill. ci-après) :
  - Activez ou désactivez la création d'un journal de traçage (cf. page 360) ; le cas échéant, configurez les paramètres du journal ;

- Activez ou désactivez la création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (cf. page 365).

*Illustration 9. Boîte de dialogue **Propriétés : Kaspersky Anti-Virus**, onglet **Diagnostic des échecs***

3. Une fois que les différents paramètres généraux de Kaspersky Anti-Virus ont été modifiés selon vos besoins, cliquez sur le bouton **OK** ou sur le bouton **Appliquer**.

BOITES DE DIALOGUE : CONFIGURATION DES PARAMETRES GENERAUX

DANS CETTE SECTION DE L'AIDE

PROPRIETES DE KASPERSKY ANTI-VIRUS : ONGLET GENERAL

Cet onglet affiche les paramètres permettant de définir les valeurs suivantes :

- Le nombre processus de travail utilisés par Kaspersky Anti-Virus ;
- La récupération automatique après un incident du processus de Kaspersky Anti-Virus.

Les valeurs par défaut sont les mêmes que pour une installation locale du programme. Vous pouvez les modifier si nécessaire.

La section **Paramètres d'optimisation** reprend les paramètres qui définissent le nombre de processus de travail utilisés par Kaspersky Anti-Virus.

Si vous souhaitez que Kaspersky Anti-Virus contrôle automatiquement le nombre de processus, cochez la case **Détecter automatiquement les paramètres d'optimisation**.

Pour indiquer le nombre maximum de processus que Kaspersky Anti-Virus peut utiliser, sélectionnez l'option **Définir manuellement le nombre de processus actifs** et définissez les valeurs suivantes :

- **Nombre maximum de processus actifs** : nombre maximum de processus de travail que Kaspersky Anti-Virus peut utiliser.
- **Nombre de processus pour la protection en temps réel** : nombre de processus utilisés uniquement par les tâches de protection en temps réel.
- **Nombre de processus pour les tâches d'analyse à la demande en arrière-plan** : nombre maximum de processus utilisés par les tâches d'analyse à la demande en arrière-plan.

Si vous réduisez le nombre processus, les processus en excès ne seront pas supprimés immédiatement. Ils seront supprimés graduellement à la fin de leur exécution pour éviter de forcer l'arrêt des tâches.

Les paramètres de la section **Paramètres de restauration du logiciel** permettent de contrôler la récupération de Kaspersky Anti-Virus si l'application complète ou des processus individuels se bloquent pendant leur fonctionnement. Cochez la case **Réaliser la restauration du logiciel** et spécifiez le nombre de tentatives à réaliser. Kaspersky Anti-Virus et tous les processus en exécution avant l'incident se récupéreront automatiquement. Dans ce cas, Kaspersky Anti-Virus rétablira les tâches de protection en temps réel tant qu'elles n'auront pas été lancées avec succès et les tâches d'analyse à la demande, autant de fois que ce paramètre l'indique. Par défaut, l'auto-récupération est activée, et le nombre de tentatives est fixé à 2. La valeur maximum possible est 10.

VOIR EGALEMENT

Nombre maximum de processus actifs 356

Nombre de processus pour la protection en temps réel 357

Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan 358

Récupération automatique 359

PROPRIETES DE KASPERSKY ANTI-VIRUS : ONGLET AVANCE

Cet onglet reprend les paramètres qui gèrent les processus suivants :

- L'affichage de l'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches ;
- Le mode de fonctionnement de Kaspersky Anti-Virus après activation d'un onduleur sur le serveur;

- Les événements suivants : **Les bases sont dépassées**, **Les bases sont périmées** et **L'analyse des zones critiques n'a pas été réalisée depuis longtemps**.

L'icône de Kaspersky Anti-Virus permet d'évaluer l'état de la protection en temps réel ainsi que de consulter les informations relatives à la version installée et de lancer la console de Kaspersky Anti-Virus. L'icône est activée (en couleurs) quand la tâche **Protection en temps réel des fichiers** ou **Analyse des scripts** est exécutée. Si les deux tâches sont arrêtées, l'icône est inactive (noir et blanc).

Cochez la case **Afficher l'icône de l'application dans la barre des tâches** afin d'afficher l'icône dans la zone de notification de la barre des tâches du serveur sécurisé. Désélectionnez la case s'il n'est pas nécessaire d'afficher l'icône. L'affichage de l'icône s'opère conformément à la valeur définie après la connexion suivante de l'utilisateur dans le système.

Dans la section **Utilisation de la source d'alimentation de secours**, spécifiez comment la charge du serveur créée par Kaspersky Anti-Virus doit être limitée en cas de passage à l'alimentation de secours. Cochez **Ne pas démarrer de tâches d'analyse planifiées**. L'analyse à la demande sera alors suspendue. Quand le mode d'alimentation normal est rétabli, la tâche reprendra son exécution planifiée. Afin que toutes les tâches en cours s'arrêtent, cochez la case **Stopper les tâches d'analyse en cours**. Vous pourrez toujours lancer manuellement les tâches d'analyse à la demande et elle ne seront pas arrêtées par Kaspersky Anti-Virus. Les deux cases sont cochées par défaut.

Dans la rubrique **Seuils de création d'événement**, sélectionnez une des valeurs suivantes :

- **"Les bases de données sont dépassées"** : nombre de jours écoulés depuis la publication de la base antivirus pour que l'événement **Les bases de données sont dépassées** soit consigné. La valeur par défaut est de 7 jours, avec une valeur maximum de 365 jours.

- **"Les bases de données sont périmées"** : nombre de jours écoulés depuis la publication de la base antivirus pour que l'événement **Les bases de données sont périmées** soit consigné. La valeur par défaut est de 14 jours, avec une valeur maximum de 365 jours. La valeur pour l'événement **La base de données n'est plus à jour** ne peut être supérieure à la valeur pour l'événement **La base de données est périmée**.

- **"L'analyse des zones critiques n'a pas été réalisée depuis longtemps"** : nombre de jours écoulés depuis la dernière exécution réussie de la tâche d'analyse des zones critiques pour que l'événement **L'analyse des zones critiques n'a pas été réalisée depuis longtemps** soit consigné. La valeur par défaut est de 30 jours, avec une valeur maximum de 365 jours.

En cas de dépassement, des événements sont enregistrés et une notification est générée conformément aux paramètres de notification pour ce type d'événement.

VOIR EGALEMENT

Icône de Kaspersky Anti-Virus dans la barre des tâches 23

Actions dans le fonctionnement sur la source d'alimentation de secours..... 359

Actions dans le fonctionnement sur la source d'alimentation de secours..... 360

PROPRIETES DE KASPERSKY ANTI-VIRUS : ONGLET DIAGNOSTIC DES ECHECS

Cet onglet configure l'enregistrement des informations de diagnostic en cas de défaillance de Kaspersky Anti-Virus.

Cochez la case **Consigner les informations de débogage dans le fichier** pour enregistrer les informations de mise au point dans un fichier et définissez les paramètres suivantes :

- Le dossier cible des fichiers de mise au point. Les informations de mise au point sont enregistrées dans un fichier séparé pour chaque projet. Vous pouvez entrer le chemin de l'objet manuellement au format UNC (Universal Naming Convention) ou sélectionner le dossier dans la fenêtre standard de sélection de fichiers avec **Parcourir**. Le dossier doit se trouver sur l'unité locale du serveur sécurisé. N'utilisez pas de dossiers situés sur

des unités virtuelles créées par une commande SUBST ou des unités réseau du serveur. Si vous spécifiez le chemin d'un dossier inexistant, les fichiers ne seront pas créés.

- Niveau de détail. Choisissez la valeur requise dans le menu déroulant : **Événements critiques**, **Erreurs**, **Événements importants**, **Événements d'information**, ou **Débogage**. Le niveau de détail le plus important est **Débogage**: tous les événements sont enregistrés. Les moins détaillé est celui des **Événements critiques** : seuls les événements critiques sont enregistrés. Le niveau par défaut est **Événements d'information**.

- Taille max. des fichiers de traçage. Dès que la taille du fichier de rapport atteint la valeur maximale, Kaspersky Anti-Virus consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé.

- Liste des sous-systèmes de Kaspersky Anti-Virus dont les informations sont enregistrées. Dans la fenêtre **Sous-systèmes à tracer**, saisissez les codes des sous-systèmes (cf. rubrique "Codes des sous-systèmes de Kaspersky Anti-Virus" à la page 44) dont l'arrêt pour cause d'erreur sera consigné. Les codes doivent être séparés par un point-virgule. Quand vous précisez un sous-système, utilisez son code. Les informations sur tous les sous-systèmes de Kaspersky Anti-Virus sont enregistrées par défaut.

Pour désactiver l'enregistrement des informations de mise au point, décochez la case **Consigner les informations de débogage dans le fichier**.

Cochez **Créer des fichiers de vidage sur incident** pour créer des fichiers de vidage lors d'un blocage des processus de Kaspersky Anti-Virus et spécifiez le dossier cible des fichiers de vidage. Vous pouvez entrer le chemin de l'objet manuellement au format UNC (Universal Naming Convention) ou sélectionner le dossier dans la fenêtre standard de sélection de fichiers avec Parcourir. Le dossier doit se trouver sur l'unité locale du serveur sécurisé. N'utilisez pas de dossiers situés sur des unités virtuelles créées par une commande SUBST ou des unités réseau du serveur. Si vous spécifiez le chemin d'un dossier inexistant, le fichier de vidage ne sera pas créé. Les fichiers de vidage ne sont pas créés par défaut.

Pour désactiver la création de fichiers de vidage, décochez **Créer des fichiers de vidage sur incident**.

VOIR EGALEMENT

Constitution d'un journal de traçage 361

Dossier contenant les fichiers du journal de traçage 362

Niveau de détail du journal de traçage. 362

Taille d'un fichier du journal de traçage. 363

Traçage de sous-systèmes individuels de Kaspersky Anti-Virus 363

CODES DU SOUS-SYSTEME DE KASPERSKY ANTI-VIRUS

Ce tableau répertorie les codes du sous-système de Kaspersky Anti-Virus utilisés dans les paramètres d'enregistrement des informations de mise au point dans le journal des traces. Quand vous précisez un sous-système, utilisez son code.

Tableau 7. Codes du sous-système de Kaspersky Anti-Virus

CODE DE SOUS-SYSTEME	NOM DU SOUS-SYSTEME
*	Tous les composants (défaut)
gui	Sous-système de l'interface utilisateur, complément de l'application antivirus dans MMC.
AK_conn	Sous-système d'intégration de NAgent et de Kaspersky Administration Kit.
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Anti-Virus.
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration distante de Kaspersky Anti-Virus.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de protection en temps réel des fichiers.
qb	Sous-système de la quarantaine et des sauvegardés.
scandll	Module auxiliaire d'analyse du programme antivirus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.
prague	Sous-système des fonctions de base.
scsrv	Sous-système d'affichage de messages sur les interceptions de scripts.
script	Intercepteur de scripts.
updater	Sous-système de mise à jour des bases et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant enfichable de Kaspersky Anti-Virus (gui) et du module externe d'administration de Kaspersky Anti-Virus pour Kaspersky Administration Kit (AK_conn) sont appliqués après le redémarrage de ces composants ; les paramètres de traçage du sous-système de prise en charge du protocole SNMP (snmp) sont appliqués après le redémarrage du service SNMP, le sous-système des compteurs de performances (perfcount) après le redémarrage de tous les processus qui utilisent des compteurs de performances. Les paramètres de traçage des autres sous-systèmes de Kaspersky Anti-Virus sont appliqués dès qu'ils ont été enregistrés.

ADMINISTRATION DES TACHES

DANS CETTE SECTION DE L'AIDE

CATEGORIES DE TACHE DANS KASPERSKY ANTI-VIRUS

Les fonctions **Protection en temps réel**, **Analyse à la demande**, **Mise à jour** et **Licences** de Kaspersky Anti-Virus se présentent sous la forme de tâches. Ces tâches peuvent être lancées et arrêtées manuellement ou selon un horaire.

Les tâches sont réparties entre les tâches *locales* et les tâches *de groupe* en fonction du lieu de création et d'exécution. Il existe deux catégories de tâches locales : *les tâches prédéfinies* et *les tâches définies par l'utilisateur*.

Tâches locales

Les tâches locales sont uniquement exécutées sur le serveur protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- Les **Tâches prédéfinies locales** sont créées automatiquement lors de l'installation de Kaspersky Anti-Virus. Vous pouvez modifier les paramètres de toutes les tâches prédéfinies à l'exception des tâches **Analyse des objets en quarantaine** et **Remise des bases de l'application à l'état antérieur**. Il est impossible de renommer ou de supprimer les tâches prédéfinies. Vous pouvez lancer les tâches d'analyse prédéfinies en même temps que les tâches définies par l'utilisateur.

- **Tâches locales définies par l'utilisateur**. La console de Kaspersky Anti-Virus vous permet d'ajouter de nouvelles tâches d'analyse à la demande. La console d'administration de Kaspersky Administration Kit vous permet de créer de nouvelles tâches d'analyse à la demande, de mise à jour des base, de remise à l'état antérieur à la mise à jour et de copie des mises à jour. C'est ce qu'on appelle les tâches définies par l'utilisateur. Vous pouvez renommer, configurer et supprimer les tâches définies par l'utilisateur. Vous pouvez exécuter simultanément plusieurs tâches définies par l'utilisateur.

Tâches de groupe

Les tâches de groupe et les tâches pour les sélections d'ordinateurs créées dans la console d'administration de Kaspersky Administration Kit sont affichées dans la console de Kaspersky Anti-Virus. Elles sont toutes désignées comme des tâches de groupe dans la console de Kaspersky Anti-Virus. Vous pouvez administrer les tâches de groupe et les configurer au départ de Kaspersky Administration Kit. La console de Kaspersky Anti-Virus vous permet uniquement de consulter l'état des tâches de groupe.

La console de Kaspersky Anti-Virus affiche les informations relatives aux tâches (cf. ill. ci-après).

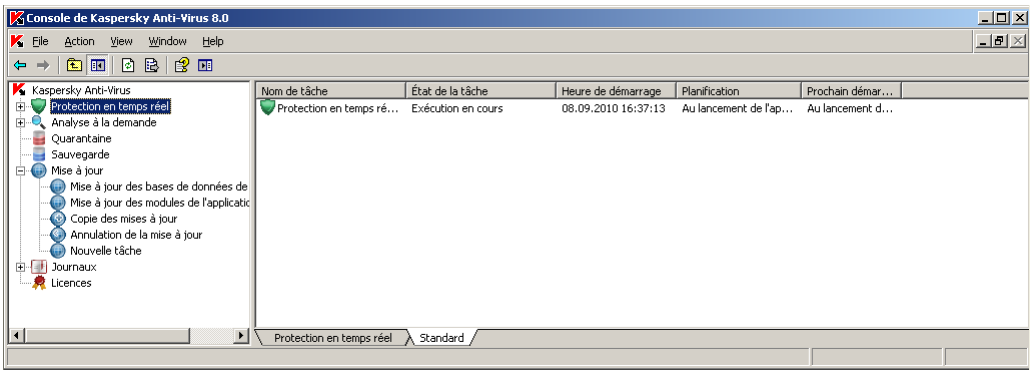


Illustration 10. Tâches de protection en temps réel dans la fenêtre de la console de Kaspersky Anti-Virus

Les commandes d'administration des tâches sont reprises dans le menu contextuel qui s'ouvre d'un clic droit de la souris sur le nom de la tâche.

Les opérations d'administration des tâches sont consignées dans le journal d'audit système (cf. page 226).

CREATION D'UNE TACHE D'ANALYSE A LA DEMANDE

Vous pouvez créer des tâches définies par l'utilisateur dans le nœud **Analyse à la demande**. Les autres composants de Kaspersky Anti-Virus ne prévoient pas la création de tâches définies par l'utilisateur.

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

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Analyse à la demande** et sélectionnez la commande **Ajouter tâche** (cf. ill. ci-après).

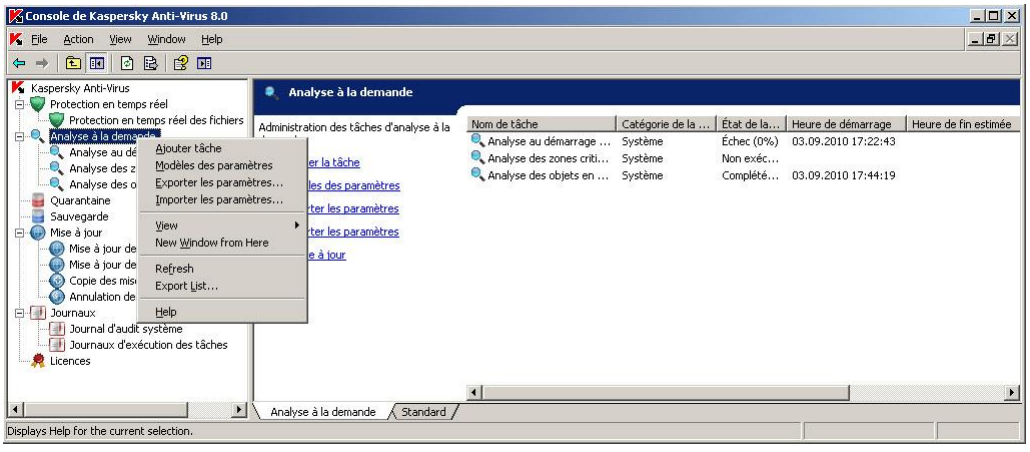


Illustration 11. Exemple de la nouvelle tâche

La boîte de dialogue **Nouvelle tâche** s'ouvrira (cf. ill. ci-après)**.**

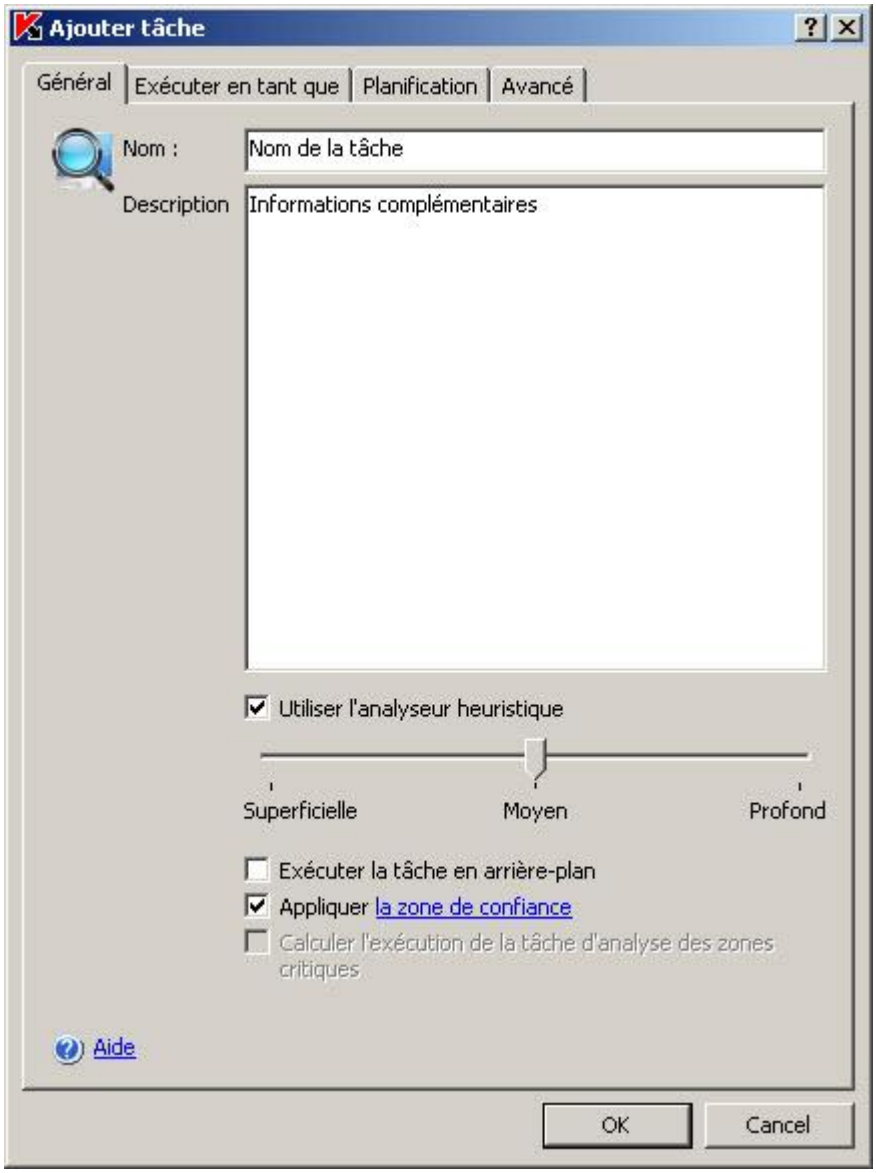


*Illustration 12. Boîte de dialogue **Nouvelle tâche***

2. Saisissez les informations suivantes relatives à la tâche :

   - **Nom** : nom de la tâche, 100 caractères maximum, peut contenir n'importe quel caractère sauf**% ? I \ | / : * < >.**

   - **Description** : toute information complémentaire relative à la tâche, 2 000 caractères maximum. Ces informations figurent dans la boîte de dialogue des propriétés de la tâche.

3. Le cas échéant, configurez les paramètres suivants de la tâche :

   - Utilisation de l'analyseur heuristique (cf. page 393). Par défaut, l'analyseur heuristique est activé pour toute nouvelle tâche d'analyse à la demande. Pour modifier le niveau d'analyse, vérifiez que la case **Utiliser l'analyseur heuristique** est cochée et déplacez le curseur à la position requise. Pour désactiver l'analyseur heuristique, décochez la case **Utiliser l'analyseur heuristique**.

   - Application de la zone de confiance (cf. page 178). La zone de confiance est appliquée par défaut dans les tâches d'analyse à la demande recréée. Pour désactiver l'application, désélectionnez la case **Appliquer la zone de confiance**.

- Exécution de la tâche en arrière-plan (cf. page 152). Pour exécuter la tâche dans un processus à priorité réduite, cochez la case **Exécuter la tâche en arrière-plan**.

4. Cliquez sur **OK**. La tâche est créée. Une ligne reprenant les informations qui la concernent apparaît dans la fenêtre de la console. L'opération sera consignée dans le journal d'audit système (cf. page 226).

ENREGISTREMENT D'UNE TACHE APRES MODIFICATION DE SES PARAMETRES

Vous pouvez modifier les paramètres d'une tâche, qu'elle soit en cours d'exécution ou arrêtée (suspendue). Les nouvelles valeurs des paramètres seront appliquées si les conditions suivantes sont remplies :

- si vous avez changé les paramètres tâche exécutée dans les tâches de protection en temps réel, les nouvelles valeurs des paramètres seront appliquées directement après leur enregistrement ; dans les autres tâches, ces valeurs entrent en vigueur au prochain lancement de la tâche ;

- si vous avez changé les paramètres de la tâche arrêtée : les nouvelles valeurs seront utilisées quand elles auront été enregistrées et que la tâche aura été lancée.

Pour enregistrer les modifications introduites dans les paramètres d'une tâche, ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche**.

Si, après la modification des paramètres de la tâche, vous sélectionnez un autre nœud dans l'arborescence de la console sans avoir sélectionné la commande **Enregistrer la tâche**, la boîte de dialogue d'enregistrement des paramètres s'ouvre. Cliquez sur le bouton **Oui** afin d'enregistrer les paramètres de la tâche ou sur **Non** afin de quitter le nœud sans enregistrement des modifications.

Vous pouvez également configurer les paramètres pour chacune des tâches suivantes : Protection en temps réel des fichiers (cf. rubrique "Configuration de la tâche Protection en temps réel des fichiers" à la page 87), Analyse à la demande ("Configuration des tâches d'analyse à la demande" à la page 132), Mise à jour (cf. page 65).

CHANGEMENT DE NOM D'UNE TACHE

Vous pouvez changer le nom uniquement des tâches définies par l'utilisateur dans la console de Kaspersky Anti-Virus. Vous ne pouvez pas renommer les tâches prédéfinies, ni les tâches de groupe.

Pour renommer une tâche, procédez comme suit :

1. Ouvrez le menu contextuel de la tâche et sélectionnez **Propriétés**.

2. Dans la boîte de dialogue **<Nom de la tâche> Propriétés**, saisissez le nouveau nom de la tâche dans le champ **Nom**, puis cliquez sur le bouton **OK** ou sur le bouton **Appliquer**.

   La tâche sera ainsi renommée. L'opération sera consignée dans le journal d'audit système (cf. page 226).

SUPPRESSION D'UNE TACHE

Vous pouvez supprimer uniquement des tâches définies par l'utilisateur dans la console de Kaspersky Anti-Virus ; vous ne pouvez pas supprimer les tâches prédéfinies, ni les tâches de groupe.

Pour supprimer une tâche, procédez comme suit :

1. Ouvrez le menu contextuel de la tâche et sélectionnez **Supprimer la tâche**.

2. Dans la boîte de dialogue **Supprimer tâche**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

La tâche sera supprimée et cette opération sera consignée dans le journal d'audit système (cf. page 226).

LANCEMENT / SUSPENSION / RETABLISSEMENT / ARRET MANUEL D'UNE TACHE

Vous pouvez suspendre et relancer toutes les tâches, à l'exception des tâches de mise à jour.

Pour lancer/suspendre/reprendre/arrêter une tâche,

ouvrez le menu contextuel de la tâche et sélectionnez la commande correspondante : **Démarrer la tâche**, **Suspendre la tâche**, **Continuer la tâche** ou **Arrêter la tâche**.

L'opération sera exécutée. L'état de la tâche change dans le panneau des résultats ; l'opération sera consignée dans le journal d'audit système (cf. page 226).

Quand vous suspendez puis relancez une tâche d'analyse à la demande, Kaspersky Anti-Virus reprend l'action à l'objet qui était analysé au moment de l'interruption.

PROGRAMMATION DES TACHES

DANS CETTE SECTION DE L'AIDE

ACTIVATION ET DESACTIVATION DE L'EXECUTION PROGRAMMEE

Une fois que la tâche a été programmée, vous pouvez l'activer ou la désactiver. Quand vous désactivez une tâche programmée, ses paramètres (fréquence, heure, etc.) ne sont pas perdus et vous pourrez à nouveau activer la programmation lorsque cela sera nécessaire.

Pour activer ou désactiver la planification, procédez comme suit :

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez programmer l'exécution et sélectionnez **Propriétés**.
2. Dans la boîte de dialogue **<Nom de la tâche> Propriétés**, sous l'onglet **Planification** exécutez une des actions suivantes :
   - pour activer la planification, cochez la case **Exécuter de manière planifiée**.
3. Cliquez sur le bouton **OK** ou sur le bouton **Appliquer**.

CONFIGURATION DE PLANIFICATION DES TACHES EN MMC

La console de Kaspersky Anti-Virus vous permet de programmer les tâches prédéfinies locales et les tâches définies par l'utilisateur (cf. page 46). Vous ne pouvez pas programmer l'exécution des tâches de groupe.

Lisez également la description des paramètres de planification des tâches (cf. page 369).

Pour configurer les paramètres de planification de la tâche, exécutez les actions suivantes *:*

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez programmer l'exécution et sélectionnez **Propriétés**.

2. Dans la boîte de dialogue **Propriétés : <Nom de tâche>** sous l'onglet **Planification**, activez le lancement programmé de la tâche : cochez la case **Exécuter de manière planifiée** (cf. ill. ci-après).

   Les champs des paramètres de programmation d'une tâche prédéfinie ne sont pas accessibles si l'exécution planifiée est interdite par une stratégie de Kaspersky Administration Kit (cf. rubrique "Désactivation de l'exécution programmée des tâches prédéfinies locales" à la page 339).

3. Configurez l'horaire en fonction de vos besoins. Pour ce faire, exécutez les actions suivantes *:*

   a. Spécifiez la fréquence d'exécution de la tâche (cf. page 370) : sélectionnez une des valeurs suivantes dans la liste **Fréquence d'exécution** : **Chaque heure**, **Chaque jour**, **Chaque semaine**, **Au lancement de Kaspersky Anti-Virus**, **A la mise à jour des bases** .Spécifiez les paramètres suivants :

      - si vous avez sélectionné **Chaque heure**, indiquez le nombre d'heures dans le champ **Tous les <chiffres> heure(s)** du groupe de paramètres **Configuration du démarrage des tâches** ;

      - si vous avez sélectionné **Chaque jour**, indiquez le nombre de jours dans le champ **Tous les <chiffres> jour(s)** du groupe de paramètres **Configuration du démarrage des tâches** ;

- si vous avez sélectionné **Chaque semaine**, indiquez le nombre de semaines dans le champ **Tous les <chiffres> semaine(s)** du groupe de paramètres **Configuration du démarrage des tâches**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi).

*Illustration 13. Exemple de l'onglet **Programmation** avec la fréquence d'exécution **Chaque semaine***

b. B Indiquez, dans le champ **Heure d'exécution**, l'heure de la première exécution de la tâche (cf. ill. ci-après 371).

c. Indiquez, dans le champ **A partir du**, la date d'entrée en vigueur de la programmation (cf. ill. 371).

Après avoir indiqué la fréquence d'exécution de la tâche, l'heure de la première exécution et la date d'entrée en vigueur de la planification, dans la partie supérieure dans la boîte de dialogue, le champ **Prochain démarrage** affiche des informations relatives au temps restant avant la nouvelle exécution de la tâche. Des informations actualisées sur le temps restant seront proposées à chaque ouverture de la boîte de dialogue **<Nom de la tâche> Propriétés** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** du champ **Prochain démarrage** s'affiche si le lancement programmé des tâches prédéfinies est interdit par la stratégie en vigueur de l'application Kaspersky Administration Kit (cf. rubrique "Désactivation de l'exécution programmée des tâches prédéfinies locales" à la page. 339).

4. Sous l'onglet **Avancé**, configurez le reste des paramètres en fonction de vos besoins (cf. ill. ci-après).

*Illustration 14. Boîte de dialogue **Propriétés : <nom de la tâche>**, onglet **Avancé***

a. Pour définir la durée maximale de l'exécution d'une tâche (cf. page 372), dans le groupe **Informations sur l'arrêt de la tâche**, champ **Durée**, saisissez le nombre d'heures et de minutes.

b. Pour désigner l'intervalle de temps au cours d'une journée pendant lequel l'exécution de la tâche sera suspendue (cf. page 373), saisissez, dans le groupe **Informations sur l'arrêt de la tâche** les valeurs de début et de fin de l'intervalle dans le champ **Pause à partir de... jusqu'à**.

c. Pour définir la date à partir de laquelle la programmation ne sera plus active (cf. page 372), cochez la case **Suspendre la planification à** partir du et à l'aide de la boîte de dialogue **Calendrier**, sélectionnez la date à partir de laquelle la planification ne sera plus en vigueur.

d. Pour activer le lancement des tâches ignorées (cf. page 373), cochez la case **Lancer les tâches non exécutées**.

e. Pour activer le paramètre "répartition des lancements dans l'intervalle, min" (cf. page 374), cochez la case **Répartir l'exécution dans un intervalle de** et définissez le paramètre en minutes.

5. Cliquez sur le bouton **OK** ou sur le bouton **Appliquer**, afin d'enregistrer les modifications introduites dans la boîte de dialogue **<Nom de la tâche> Propriétés**.

UTILISATION DES COMPTES UTILISATEUR POUR L'EXECUTION DES TACHES

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE L'UTILISATION DES COMPTES UTILISATEUR POUR L'EXECUTION DES TACHES

Vous pouvez indiquer un compte utilisateur sous les privilèges duquel la tâche sélectionnée de n'importe quel composant de Kaspersky Anti-Virus, à l'exception de la **Protection en temps réel, sera exécutée**.

Par défaut, toutes les tâches, à l'exception des tâches de protection en temps réel, sont exécutées sous le compte **Système local** (**SYSTEM**). Dans les tâches de protection en temps réel, Kaspersky Anti-Virus intercepte l'objet à analyser lorsqu'il est sollicité par une application quelconque et il utilise pour ce faire les privilèges de cette application.

Il faudra définir un autre compte avec les privilèges suffisants dans les cas suivants :

- Pour la tâche de mise à jour, si la source de mise à jour est un répertoire de réseau partagé sur un autre ordinateur du réseau ;
- Pour la mise à jour, si l'accès à la source des mises à jour s'opère via un serveur proxy doté de la vérification intégrée de l'authenticité Microsoft Windows (authentification NTLM) ;
- dans les tâches d'analyse à la demande, si le compte **Système local** (**SYSTEM**) ne jouit pas des privilèges d'accès à un des objets à analyser (par exemple, aux fichiers d'un répertoire partagé sur le réseau).

Vous pouvez lancer la tâche de mise à jour et l'analyse à la demande dans lesquelles Kaspersky Anti-Virus s'adresse à des répertoires de réseau partagé sur un autre ordinateur sous le compte utilisateur **Système local** (**SYSTEM**) si cet ordinateur est enregistré dans le même domaine que le serveur protégé. Dans ce cas, le compte utilisateur **Système local** (**SYSTEM**) doit jouir des privilèges d'accès à ces répertoires. Kaspersky Anti-Virus contactera cet ordinateur avec les privilèges du compte **Nom_de_domaine\nom_d'ordinateur$**.

DEFINITION DU COMPTE UTILISATEUR POUR L'EXECUTION DE LA TACHE

Pour sélectionner le compte utilisateur sous lequel la tâche sera exécutée, procédez comme suit :

1. Ouvrez le menu contextuel de la tâche et sélectionnez **Propriétés**.

2. Dans la boîte de dialogue **Propriétés : <Nom de la tâche>**, ouvrez l'onglet **Exécuter en tant que** (cf. ill. ci-après).

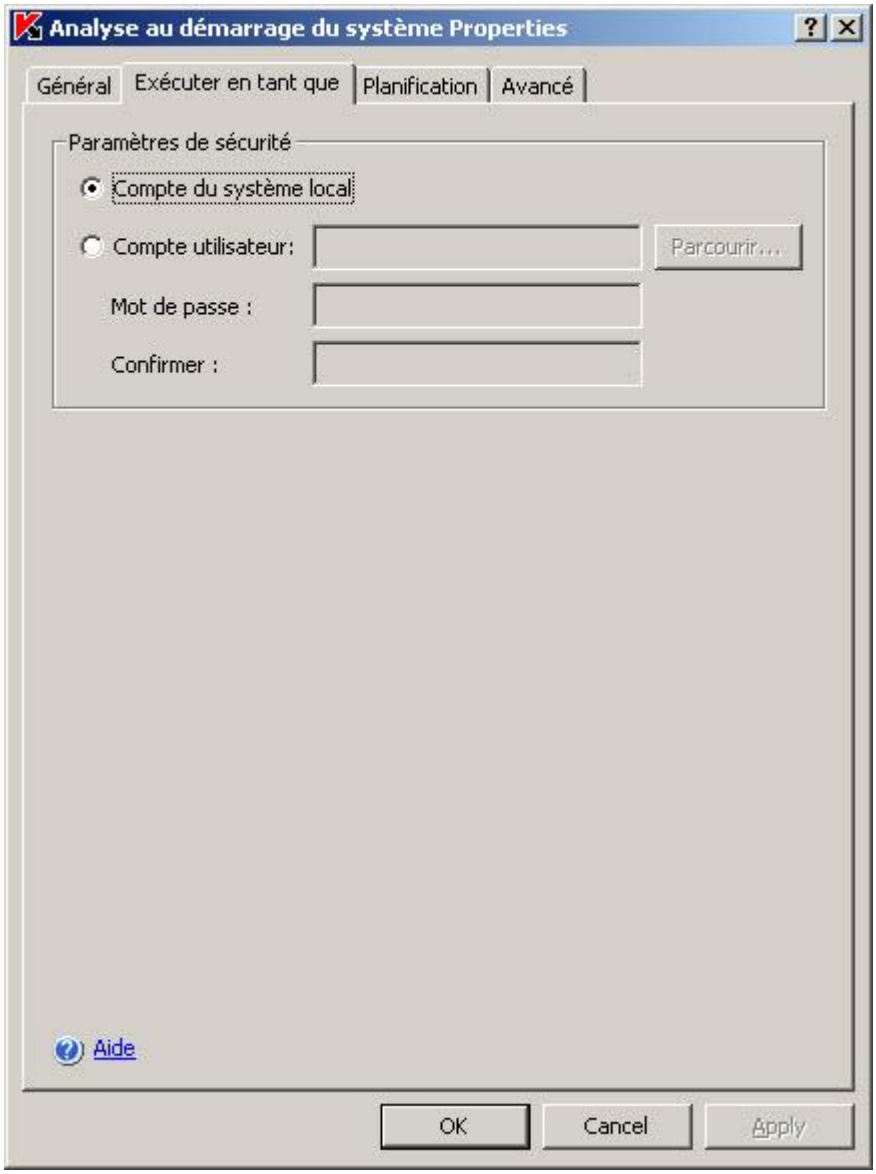


*Illustration 15. Boîte de dialogue **Propriétés :<Nom de tâche>**, onglet **Exécuter en tant que***

3. Exécutez les actions suivantes sur l'onglet **Exécuter en tant que** faire les actions :

   a. Sélectionnez l'élément **Compte utilisateur**.

   b. Saisissez le nom et le mot de passe de l'utilisateur dont vous souhaitez utiliser le compte.

L'utilisateur que vous sélectionnez doit être enregistré sur le serveur protégé ou dans le même domaine.

4. Cliquez sur **OK**.

BOITES DE DIALOGUE : GERER LES TACHES

DANS CETTE SECTION DE L'AIDE

PROPRIETES DE LA TACHE : ONGLET AVANCE

Cet onglet reprend les paramètres avancés pour le lancement planifié de tâches.

La partie supérieure de la fenêtre reprend l'heure de la prochaine exécution programmée de la tâche. L'heure du serveur protégé est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.

Vous pouvez configurer les paramètres suivants :

- **Durée** : durée maximum d'exécution d'une tâche. Après ce délai, la tâche sera interrompue.

  Cochez cette case pour limiter la durée d'exécution d'une tâche et spécifiez sa durée en heures et en minutes. Si la tâche doit être exécutée jusqu'à terme, décochez cette case. Ce paramètre ne concerne pas les tâches de mise à jour.

- **Pause à partir de... jusqu'à...** : période de la journée pendant laquelle la tâche sera suspendue.

  Cochez cette case pour réduire la charge du serveur pendant les heures de travail et spécifiez les heures de début et de fin correspondantes. Ce paramètre ne concerne pas les tâches de mise à jour. Les tâches de mise à jour et d'analyse à la demande continueront au point où elles auront été suspendues. Les tâches de protection en temps réel reprendront. Décochez la case si vous n'avez pas besoin de suspendre les tâches. La case est décochée par défaut.

- **Suspendre la planification à partir du** : date de la fin de la tâche automatique. Vous pouvez la lancer de nouveau manuellement.

  Cochez la case pour désactiver le lancement automatique de la tâche et spécifiez la date de fin de la planification. Décochez la case s'il n'est pas nécessaire de limiter la durée de la planification. La case est décochée par défaut.

- **Lancer les tâches non exécutées** : ce paramètre détermine l'ordre de lancement des tâches si le serveur protégé n'était pas disponible à l'heure planifiée (par exemple, s'il était éteint) ou si Kaspersky Anti-Virus était désactivé.

  Cochez la case pour que l'application exécute les tâches ignorées à la prochaine exécution de Kaspersky Anti-Virus sur l'ordinateur. Décochez la case si vous n'avez pas besoin d'exécuter les tâches ignorées. Les tâches seront exécutées conformément à la planification.

- **Répartir l'exécution dans un intervalle de** : délai maximum de l'exécution de la tâche par rapport à la date de départ planifiée. Cochez la case et spécifiez les heures de lancement de la tâche.

- Le paramètre n'est pas utilisé et la case est inaccessible lorsqu'une des fréquences d'exécution suivantes est sélectionnée : **Au lancement de l'application**, **Après réception des mises à jour par le serveur d'administration** et **A la mise à jour des bases antivirus**.

VOIR EGALEMENT

PROPRIETES DE LA TACHE : ONGLET EXECUTER EN TANT QUE

Sur cet onglet, vous pouvez définir un compte utilisateur sous lequel la tâche sera exécutée.

Sélectionnez un des types de compte utilisateur suivant :

- **Compte du système local** si aucun privilège supplémentaire n'est nécessaire pour exécuter la tâche.
- **Compte utilisateur** si des privilèges supplémentaires sont nécessaires pour exécuter la tâche avec succès. Dans le champ situé à droite saisissez **manuellement ou choisissez** dans la liste à l'aide du bouton le nom de l'utilisateur jouissant des privilèges suffisants et remplissez les champs Mots de passe et Confirmer.

VOIR EGALEMENT

PROPRIETES DE LA TACHE : ONGLET PLANIFICATION

Cet onglet affiche les paramètres de planification de la tâche. L'heure de la prochaine exécution programmée de la tâche apparaît dans la partie supérieure de la fenêtre. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.

Pour terminer une tâche planifiée, décochez la case **Exécuter de manière planifiée**. La tâche ne s'exécutera pas automatiquement, mais vous pourrez le faire manuellement.

Si vous souhaitez exécuter automatiquement une tâche, cochez la case **Exécuter de manière planifiée** et spécifiez les paramètres de planification. Choisissez dans la liste déroulante **Fréquence** une valeur qui corresponde au nombre de fois que vous souhaitez exécuter la tâche et spécifiez la période de temps entre deux exécutions de la tâche, ainsi que la date et l'heure exactes du premier lancement planifié :

- **Chaque heure** : l'intervalle entre les analyses est calculé en heures. Indiquez la durée entre deux lancements de la tâche dans la zone **Chaque N heure(s)**. Par exemple, si vous souhaitez exécuter la tâche toutes les heures : *Chaque 1 heure(s)*. Dans les zones **Heure de lancement** , spécifiez la date et l'heure de la première exécution planifiée.
- La tâche sera exécutée **tous les jours**. Entrez le nombre de jours entre deux lancements de la tâche dans la zone **Chaque N jour(s)**. Par exemple, si vous souhaitez exécuter la tâche tous les jours : *Chaque 1 jour(s)*. Dans les zones **Démarrer à** et **A partir du**, spécifiez la date et l'heure de la première exécution planifiée.
- La tâche sera exécutée **toutes les semaines**, certains jours de la semaine. Dans la zone **Chaque N semaine(s) sur**, définissez la durée entre les lancements de la tâche et cochez les cases des jours de la semaine où vous souhaitez lancer la tâche. Par exemple, pour exécuter la tâche toutes les deux semaines, le mardi et le vendredi : choisissez *Chaque 2 semaine(s)* et cochez les cases **Ma** et **Ve**. Dans les zones **Démarrer à** et **A partir du**, spécifiez la date et l'heure de la première exécution planifiée.

- **Au lancement de l'application** : la tâche est lancée à chaque démarrage de Kaspersky Anti-Virus.
- **À la mise à jour de la base antivirus** : la tâche est lancée après chaque mise à jour réussie de la base de Kaspersky Anti-Virus. Cette option n'est pas disponible pour les tâches de mise à jour.

VOIR EGALEMENT

Configuration de planification des tâches en MMC 50

Fréquence d'exécution 370

Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche 371

MISE A JOUR DES BASE ET DES MODULES LOGICIELS DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS

Les bases de Kaspersky Anti-Virus sur le serveur protégé sont très vite dépassées. Les experts en virus de Kaspersky Lab découvrent chaque jour des centaines de nouvelles menaces, créent les définitions qui permettent de les identifier et les intègrent aux mises à jour des bases. (Une Mise à jour des bases est un fichier ou un ensemble de fichiers contenant les définitions capables d'identifier les menaces qui ont fait leur apparition depuis la diffusion de la mise à jour précédente). Pour réduire le risque d'infection du serveur au minium, il est conseillé de réaliser une mise à jour régulière des bases.

Par défaut, si les bases de Kaspersky Anti-Virus ne sont pas actualisées dans la semaine qui suit la création des dernières mises à jour des bases installées, l'événement *Les bases sont dépassées* est déclenché et si les bases ne sont pas actualisées dans les deux semaines, l'événement *Les bases de données sont périmées* s'affiche. Les informations relatives à l'actualité des bases sont affichées dans le nœud **Kaspersky Anti-Virus** (cf. rubrique "**Consultation de l'état de la protection et d'informations sur Kaspersky Anti-Virus**" à la page 33). Vous pouvez indiquer un nombre de jours différent avant le déclenchement de ces événements grâce aux paramètres généraux de Kaspersky Anti-Virus (cf. page 38) et configurer la notification de l'administrateur sur ces événements (cf. page 264).

Vous pouvez mettre à jour les bases depuis les serveurs de mise à jour FTP ou HTTP de Kaspersky Lab ou à partir de toute autre source de mises à jour en utilisant la tâche de Kaspersky Anti-Virus **Mise à jour de la base de données de l'application** (cf. la rubrique "**Tâches de mise à jour**" à la page 64).

Vous pouvez télécharger les mises à jour sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les serveurs. Si vous utilisez Kaspersky Administration Kit pour l'administration centralisée de la protection des ordinateurs de l'entreprise, vous pouvez utiliser le serveur d'administration de Kaspersky Administration Kit en guise d'intermédiaire pour le chargement des mises à jour. Pour copier les bases sur l'ordinateur intermédiaire sans les appliquer, utilisez la tâches **Copie des mises à jour** (cf. rubrique "**Tâches de mise à jour**" à la page 64).

Vous pouvez lancer les tâches de mise à jour des bases manuellement ou selon une programmation (cf. page 50).

Si le chargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Anti-Virus reviendra automatiquement à l'utilisation des dernières mises à jour installées. Si les bases de Kaspersky Anti-Virus sont endommagées, vous pouvez revenir à l'état antérieur à la mise à jour des bases installées (cf. rubrique "Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus" à la page 74).

Si vous n'avez pas accès à Internet, vous pouvez recevoir les fichiers de mise à jour sur disquette ou sur cédérom ou chez l'un de nos partenaires. Vous pouvez consulter les informations relatives au partenaire chez qui vous avez acheté Kaspersky Anti-Virus dans la console de Kaspersky Anti-Virus et plus exactement, dans les propriétés de la licence installée. Si vous souhaitez connaître l'adresse de notre partenaire le plus proche, vous pouvez également contacter par téléphone notre siège principal à Moscou +7 (495) 797-87-07, +7 (495) 645-79-29 ou +7 (495) 956-87-08 (le service est offert en russe et en anglais).

PRESENTATION DE LA MISE A JOUR DES MODULES DE KASPERSKY ANTI-VIRUS

Kaspersky Lab peut diffuser des paquets de mise à jour des modules de l'application Kaspersky Anti-Virus. Les mises à jour sont réparties entre les *mises à jour urgentes* (ou *critiques*) et les *mises à jour prévues*. Les mises à jour urgentes suppriment des vulnérabilités et corrigent les erreurs tandis que les mises à jour prévues peuvent ajouter de nouvelles fonctions ou améliorer des fonctions existantes.

Les mises à jour urgentes sont publiées sur les serveurs de mise à jour de Kaspersky Lab. Vous pouvez configurer l'installation automatique grâce à la tâche **Mise à jour des modules de l'application**.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez obtenir des informations sur la diffusion des mises à jour prévues de Kaspersky Anti-Virus à l'aide des tâches **Mises à jour des modules de l'application**.

Vous pouvez télécharger les mises à jour urgentes depuis Internet sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez les mises à jour sans les installer avant de les diffuser sur les serveurs. Pour copier et enregistrer les mises à jour sans les installer, utilisez la tâche **Copie des mises à jour**.

Avant d'installer les mises à jour des modules logiciels, Kaspersky Anti-Virus crée une copie de sauvegarde des modules installés antérieurement. Si la mise à jour des modules logiciels est interrompue ou si elle se solde par un échec, Kaspersky Anti-Virus utilisera à nouveau automatiquement les modules logiciels installés précédemment. Vous pouvez aussi décider de revenir manuellement à l'état antérieur des modules logiciels correspondant à la mise à jour précédente.

Lors de l'installation des mises à jour récupérées, le service de Kaspersky Anti-Virus s'arrête puis redémarre automatiquement.

Si vous n'avez pas accès à Internet, vous pouvez recevoir les fichiers de mise à jour sur disquette ou sur cédérom ou chez l'un de nos partenaires. Vous pouvez consulter les informations relatives au partenaire chez qui vous avez acheté Kaspersky Anti-Virus dans la console de Kaspersky Anti-Virus et plus exactement, dans les propriétés de la licence installée. Si vous souhaitez connaître l'adresse de notre partenaire le plus proche, vous pouvez également contacter par téléphone notre siège principal à Moscou +7 (495) 797-87-07, +7 (495) 645-79-29 ou +7 (495) 956-87-08 (le service est offert en russe et en anglais).

SCHEMAS DE MISE A JOUR DES BASES ET DES MODULES LOGICIELS DES APPLICATIONS ANTIVIRUS DANS L'ENTREPRISE

Votre sélection de la source des mises à jour dans les tâches de mise à jour dépend du schéma de mise à jour des bases et des modules logiciels des applications antivirus que vous utilisez dans votre entreprise.

Vous pouvez actualiser les bases et les modules de Kaspersky Anti-Virus sur les serveurs protégés selon les schémas suivants :

- Télécharger les mises à jour directement depuis Internet sur chaque serveur protégé (schéma 1) ;
- Télécharger les mises à jour depuis Internet sur un ordinateur intermédiaire et organiser la diffusion sur les serveurs depuis cet ordinateur.

L'intermédiaire peut être n'importe quel ordinateur sur lequel une des applications suivantes est installée :

- Kaspersky Anti-Virus (un des serveurs protégés) (schéma 2).
- Serveur d'administration Kaspersky Administration Kit (schéma 3).

La mise à jour via un ordinateur intermédiaire permet non seulement de réduire le trafic Internet mais également d'offrir une sécurité supplémentaire aux serveurs de fichiers.

Les différents schémas de mise à jour sont décrits ci-après.

Schéma 1. Mise à jour directement depuis Internet

Sur chaque serveur protégé, configurez la tâche **Mise à jour des bases de l'application** (**Mise à jour des modules de l'application**). En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab. Programmez l'exécution de la tâche.

En guise de source, vous pouvez indiquer d'autres serveurs HTTP ou FTP qui contiennent un répertoire avec les fichiers des mises à jour.

Schéma 2. Mise à jour via un des serveurs protégés

Pour effectuer la mise à jour selon ce schéma, procédez comme suit :

1. **Copiez les mises à jour sur le serveur protégé sélectionné.**

   Sur le serveur protégé, configurez la tâche **Copie des mises à jour**. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab. Sélectionnez le répertoire où seront enregistrées les mises à jour : il doit s'agir d'un répertoire partagé.

   A l'aide de cette tâche, vous pouvez obtenir les mises à jour non seulement pour les serveurs protégés mais également pour les ordinateurs du réseau local sur lesquels sont installées d'autres applications de Kaspersky Lab version 6.0 et 8.0.

2. **Diffusez les mises à jour sur les autres serveurs protégés.**

Sur chaque serveur protégé, configurez la tâche **Mise à jour de la base de données de l'application** (**Mise à jour des modules de l'application**) (cf. ill. ci-après). En guise de source des mises à jour pour cette tâche, saisissez le répertoire de l'ordinateur intermédiaire dans lequel vous avez copié les mises à jour.

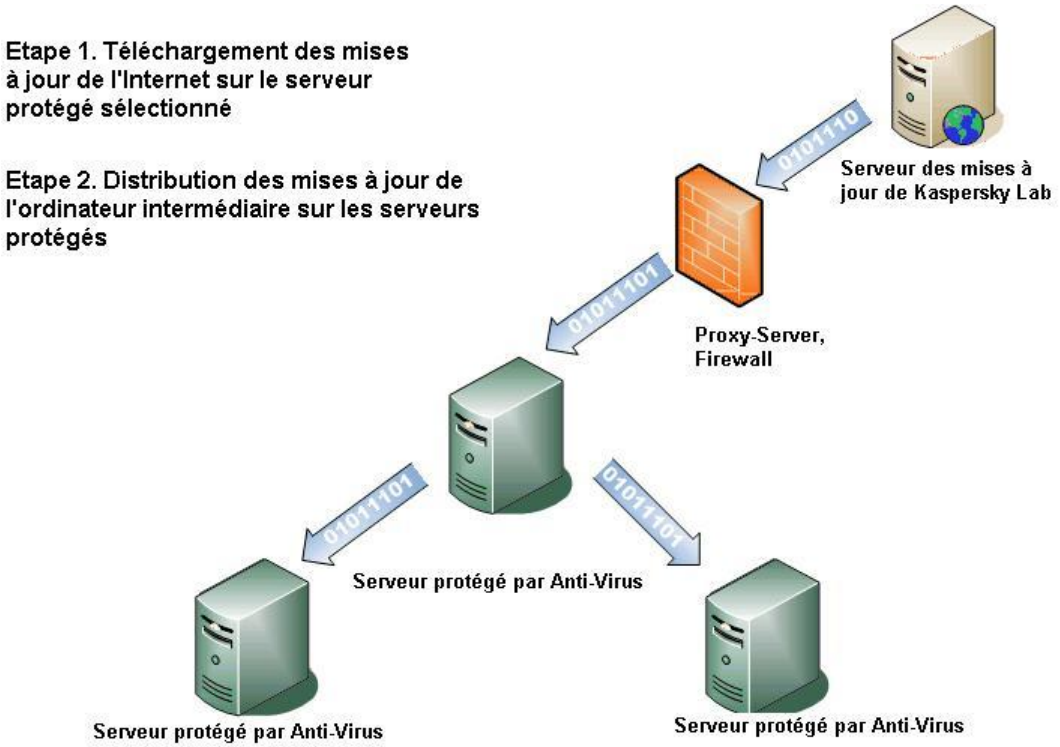


Illustration 16. Mise à jour via un des serveurs protégés

Schéma 3. Mise à jour via le serveur d'administration Kaspersky Administration Kit

Si vous utilisez l'application Kaspersky Administration Kit pour assurer l'administration centralisée de la protection de l'ordinateur, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Administration Kit (cf. ill. ci-après).

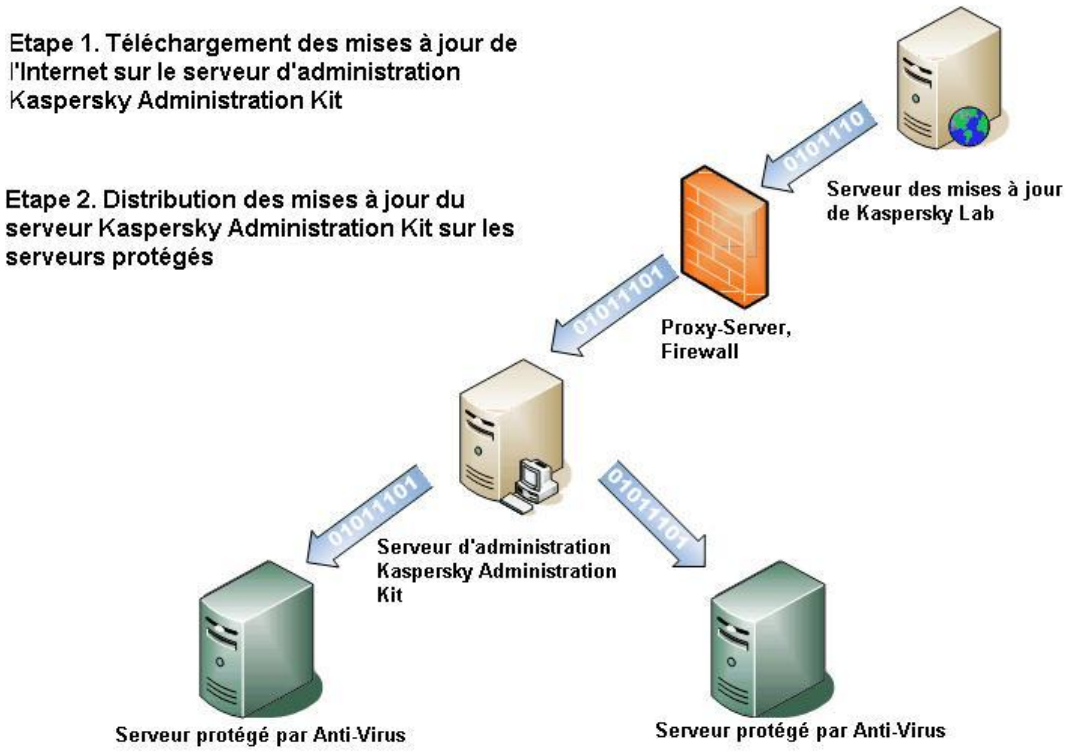


Illustration 17. Mise à jour par le serveur d'administration Kaspersky Administration Kit.

Pour effectuer la mise à jour selon ce schéma, procédez comme suit :

1. **Téléchargement des mises à jour depuis le serveur de mise à jour de Kaspersky Lab vers le serveur d'administration Kaspersky Administration Kit.**

   Configurez la tâche **Réception des mises à jour par le serveur d'administration** pour une sélection d'ordinateurs indiquée. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.

   Vous pouvez obtenir les mises à jour non seulement pour les serveurs protégés mais également pour les ordinateurs du réseau local sur lesquels sont installées d'autres applications de Kaspersky Lab version 6.0 et 8.0.

2. **Diffusez les mises à jour sur les serveurs protégés**

   Diffusez les mises à jour sur les serveurs protégés en adoptant une des méthodes suivantes :

   - Sur le serveur d'administration Kaspersky Administration Kit, configurez une tâche de groupe de mise à jour pour la copie des mises à jour sur les serveurs protégés.

     Dans la programmation de la tâche, choisissez la fréquence **Après réception des mises à jour par le serveur d'administration.**. Le serveur d'administration exécutera la tâche chaque fois qu'il reçoit les mises à jour (cette méthode est la méthode recommandée).

Vous ne pouvez pas sélectionner la fréquence d'exécution **Après réception des mises à jour par le serveur d'administration** dans la console de Kaspersky Anti-Virus.

- Configurez sur chacun des serveurs protégés la tâche **Mise à jour des bases de l'application** (**Mise à jour des modules de l'application**) où la source de mise à jour sera le serveur d'administration de Kaspersky Administration Kit. Programmez l'exécution de la tâche.

Si vous avez l'intention d'utiliser le serveur d'administration Kaspersky Administration Kit pour la diffusion des mises à jour, installez au préalable sur chaque serveur protégé le module logiciel Agent d'administration qui fait partie de l'application Kaspersky Administration Kit. Il assure l'interaction entre le serveur d'administration et Kaspersky Anti-Virus sur le serveur protégé. Pour obtenir de plus amples informations sur l'agent d'administration et sur sa configuration à l'aide de l'application Kaspersky Administration Kit, consultez le document *Kaspersky Administration Kit. Manuel de l'administrateur*.

TACHES DE MISE A JOUR

Kaspersky Anti-Virus prévoit quatre tâches prédéfinies pour la mise à jour : **Mise à jour de la base de données de l'application**, **Mise à jour des modules de l'application**, **Copie des mises à jour** et **Annulation de la mise à jour** (cf. ill. ci-après)**.**

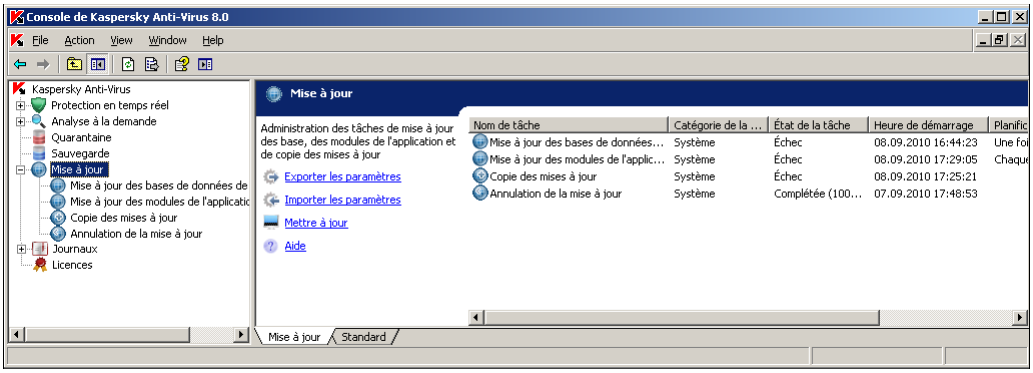


Illustration 18. Tâches de mise à jour dans la console de Kaspersky Anti-Virus

Par défaut Kaspersky Anti-Virus établit la connexion à la source des mises à jour, un des serveurs de mise à jour de Kaspersky Lab, en définissant automatiquement les paramètres du serveur proxy dans le réseau et sans recourir à la vérification de l'authenticité lors de l'accès au serveur proxy.

Vous pouvez configurer les tâches de mise à jour (cf. page 65). Une fois que les paramètres de la tâche ont été modifiés, Kaspersky Anti-Virus appliquera les nouvelles valeurs au prochain lancement de l'application.

Vous pouvez arrêter une mise à jour mais vous ne pouvez pas la suspendre.

Pour savoir comment administrer les tâches dans Kaspersky Anti-Virus, lisez la rubrique "Administration des tâches" (cf. page 46).

Mise à jour des bases de l'application

Kaspersky Anti-Virus copie les bases depuis la source des mises à jour sur le serveur protégé et les utilise directement dans les tâches de protection en temps réel et d'analyse à la demande en cours.

Kaspersky Anti-Virus lance la tâche **Mise à jour des bases de l'application** toutes les heures par défaut.

Mise à jour des modules de l'application

Kaspersky Anti-Virus copie les mises à jour de ses modules logiciels depuis la source des mises à jour sur le serveur protégé et les installe. L'application des modules logiciels installés peut impliquer le redémarrage de l'ordinateur et/ou de Kaspersky Anti-Virus.

Chaque semaine, le vendredi à 16:00 (l'heure correspond à celle définie dans les paramètres régionaux du serveur protégé), Kaspersky Anti-Virus lance la tâche **Mise à jour des modules de l'application** afin de vérifier seulement si des mises à jour critiques ou prévues des modules sont présentes, sans les copier.

Copie des mises à jour

Kaspersky Anti-Virus télécharge les fichiers des mises à jour des bases et des modules et les enregistre dans le répertoire de réseau ou local indiqué, sans les installer.

Retour à l'état antérieur à la mise à jour des bases

Kaspersky Anti-Virus utilise à nouveau les bases de la mise à jour antérieure.

CONFIGURATION DES TACHES LIEES A LA MISE A JOUR

DANS CETTE SECTION DE L'AIDE

SELECTION DE LA SOURCE DES MISES A JOUR, CONFIGURATION DE LA CONNEXION A LA SOURCE DES MISES A JOUR ET PARAMETRES REGIONAUX

Dans les tâches de mise à jour, vous pouvez indiquer une ou plusieurs sources de mise à jour, configurer les paramètres de connexion aux sources et préciser l'emplacement du serveur protégé afin d'optimiser la récupération des mises à jour (paramètres régionaux).

N'oubliez pas qu'après la modification des paramètres des tâches de mise à jour, les nouvelles valeurs seront appliquées uniquement lors du prochain lancement de la tâche.

➧ *Pour configurer les paramètres de la tâche de mise à jour, procédez comme suit :*

1. Dans l'arborescence de la console, déployez le nœud **Mise à jour** et sélectionnez une des tâches de mise à jour (cf. ill. ci-après).

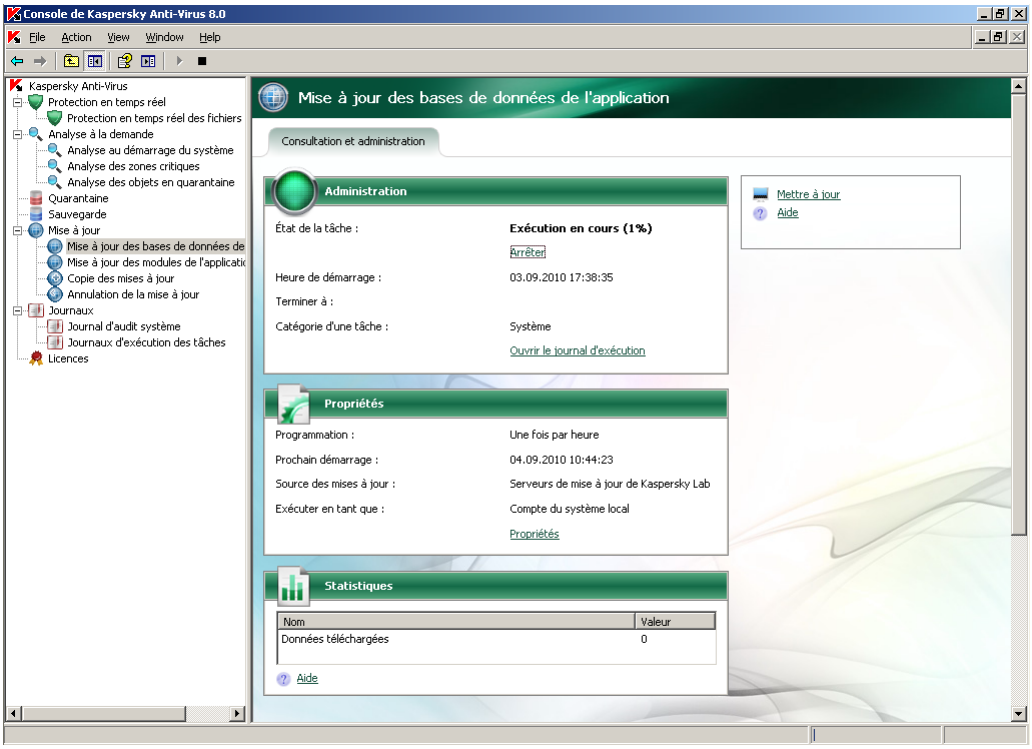


*Illustration 19. La tâche **Mise à jour de la base de données de l'application** est ouverte*

2. Dans le panneau de résultats, allez à la configuration de paramètres par le lien **Propriétés**.

   Sous les onglets de la boîte de dialogue **Propriétés : <Nom de tâche>**, configurez les paramètres de mise à jour conformément à vos exigences.

3. Sur l'onglet **Général**, sélectionnez la source où Kaspersky Anti-Virus récupérera la mise à jour (cf. page 396) (cf. ill. ci-après).

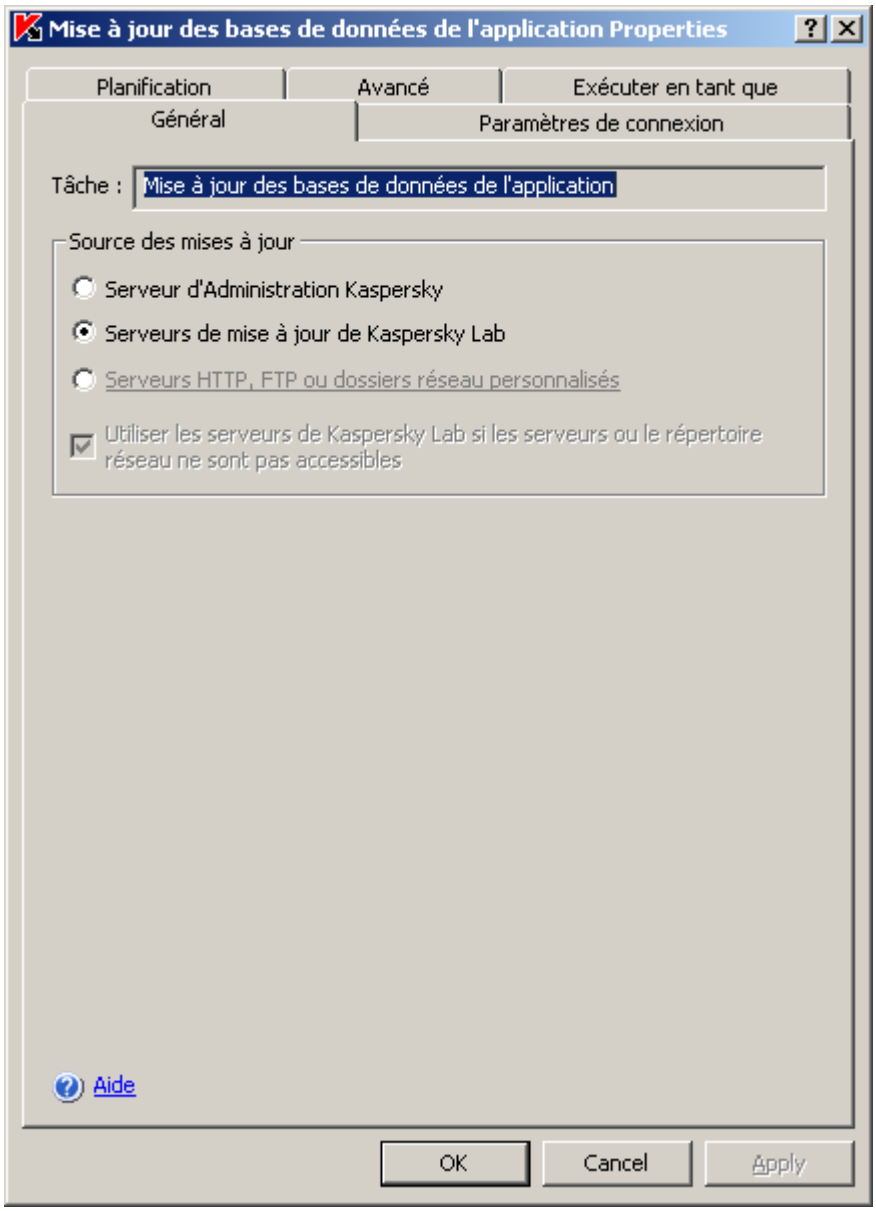


*Illustration 20. Boîte de dialogue **Propriétés : Mise à jour des bases de l'application**, onglet **Général***

4. Si vous avez sélectionné l'option **Serveurs HTTP, FTP ou dossiers réseau** personnalisés, ajoutez une ou plusieurs sources de mises à jour définies par l'utilisateur. Pour spécifier la source, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Serveurs de mise à jour**, cliquez sur le bouton **Ajouter** (cf. ill. ci-après). Dans la zone de saisie, saisissez l'adresse du répertoire contenant les fichiers de mise à jour sur le serveur FTP ou HTTP ; saisissez le répertoire local ou de réseau au format UNC (Universal Naming Convention). Cliquez sur **OK**.

   Vous pouvez inclure ou exclure les sources ajoutées par l'utilisateur : pour exclure une source ajoutée par l'utilisateur, désélectionnez la case en regard de celle-ci dans la liste ; pour inclure une source, cochez la case en regard de son nom dans la liste.

Pour modifier l'ordre de sollicitation des sources par Kaspersky Anti-Virus, déplacez la source sélectionnée vers le haut ou vers le bas de la liste (si vous voulez l'utiliser plus tôt ou plus tard) à l'aide des boutons **Monter** et **Descendre**.

Illustration 21. Ajout de sources de mise à jour définies par l'utilisateur

Pour modifier le chemin d'accès à une source, sélectionnez la source dans la liste et cliquez sur le bouton **Modifier**. Introduisez les modifications nécessaires dans le champ, puis appuyez sur la touche **ENTER**.

Pour supprimer une source, sélectionnez-la dans la liste et cliquez sur **Supprimer**. La source sera supprimée de la liste.

5. Pour récupérer les mises à jour depuis les serveurs de mises à jour de Kaspersky Lab si les sources définies par l'utilisateur ne sont pas accessibles, cochez la case **Utiliser les serveurs de Kaspersky Lab** si les serveurs ou le répertoire réseau ne sont pas accessibles.

6. Sur l'onglet **Paramètres de connexion** (cf. ill. ci-après), configurez la connexion à la source des mises à jour.

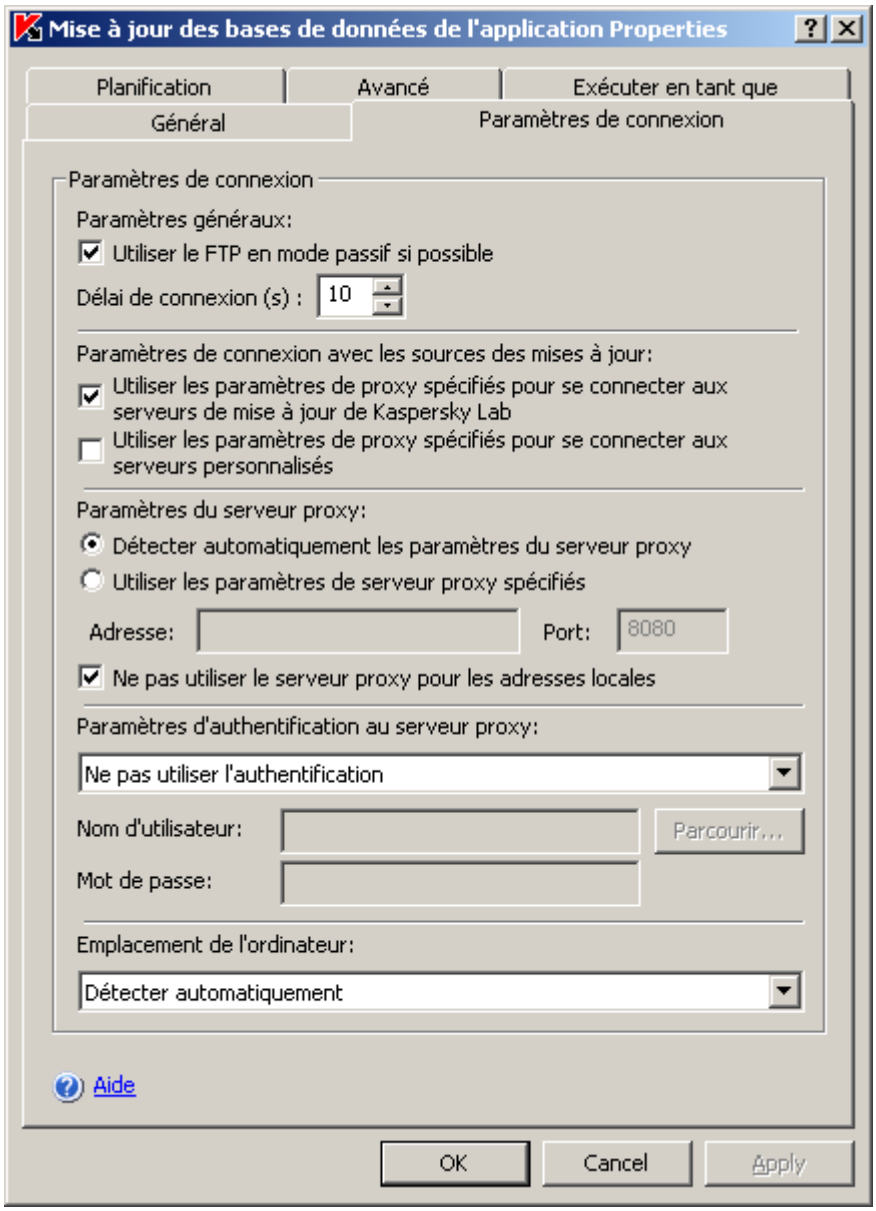


*Illustration 22. Boîte de dialogue **Propriétés : Mise à jour des bases de l'application**, onglet **Configuration de connexion***

Exécutez les actions suivantes :

- sélectez Mode du serveur FTP pour la connexion au serveur protégé (cf. page 397) ;
- Le cas échéant, modifiez la durée d'attente pour la connexion à la source de mise à jour (serveur FTP ou HTTP) (cf. page 397) ;
- si la réception des mises à jour depuis une des sources indiquées requiert l'accès au serveur proxy, précisez les paramètres d'accès à ce dernier :
  - requête adressée au serveur proxy différents lors de la connexion aux sources des mises à jour (cf. page 398) ;
  - paramètres du serveur proxy (cf. page 399) ;
  - méthode de vérification de l'authenticité lors de l'accès au serveur proxy (cf. page 400) ;
- sélectionnez le pays où se trouve le serveur protégé. (cf. page 401)

7. une fois que vous aurez configuré les paramètres requis, cliquez sur le bouton **OK** pour enregistrer les modifications.

CONFIGURATION DES PARAMETRES DE LA TACHE COPIE DES MISES A JOUR

*Pour configurer les paramètres de la tâche de **Copie des mises à jour**, procédez comme suit* :

1. Dans l'arborescence de la console, déployez le nœud **Mise à jour** et sélectionnez la tâche **Copie des mises à jour** (cf. ill. ci-après)**.**

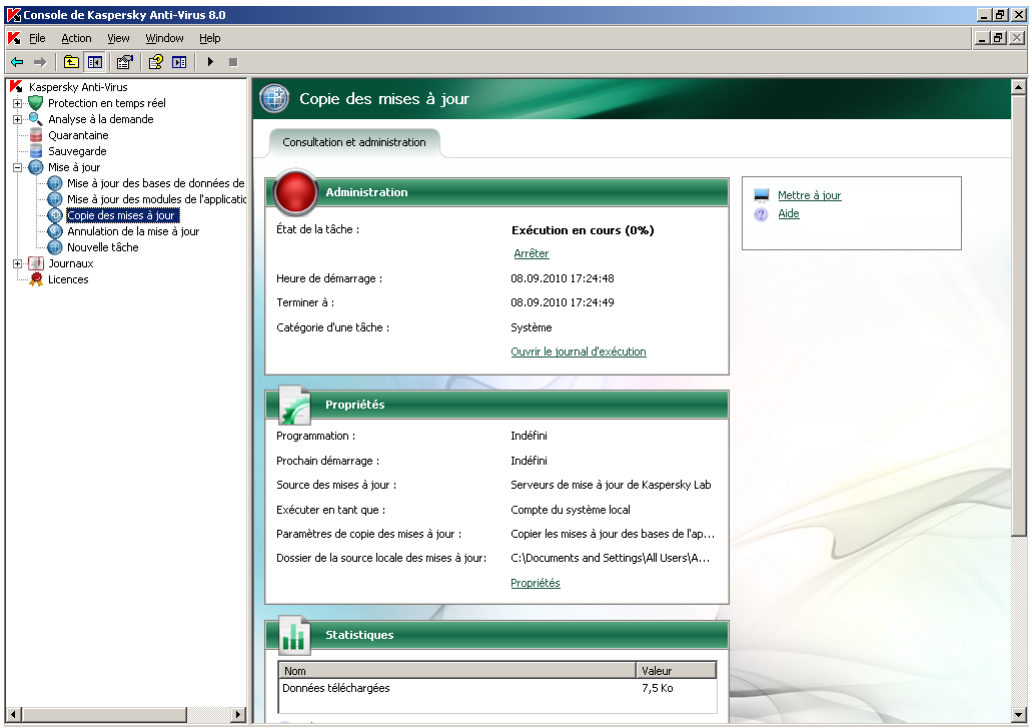


*Illustration 23. Tâche **Copie des mises à jour** ouverte*

2. Dans le panneau de résultats, passez au lien **Propriétés**.

3. Dans la boîte de dialogue **Copie des mises à jour Propriétés**, indiquez la source de la mise à jour et les paramètres de connexion à celle-ci. Lisez les instructions dans la rubrique "Sélection de la source des mise à jour, configuration de la connexion à la source des mises à jour" (cf. page 65).

4. Sous l'onglet **Général**, indiquez la composition des mises à jour (cf. page 404) (cf. ill. ci-après).

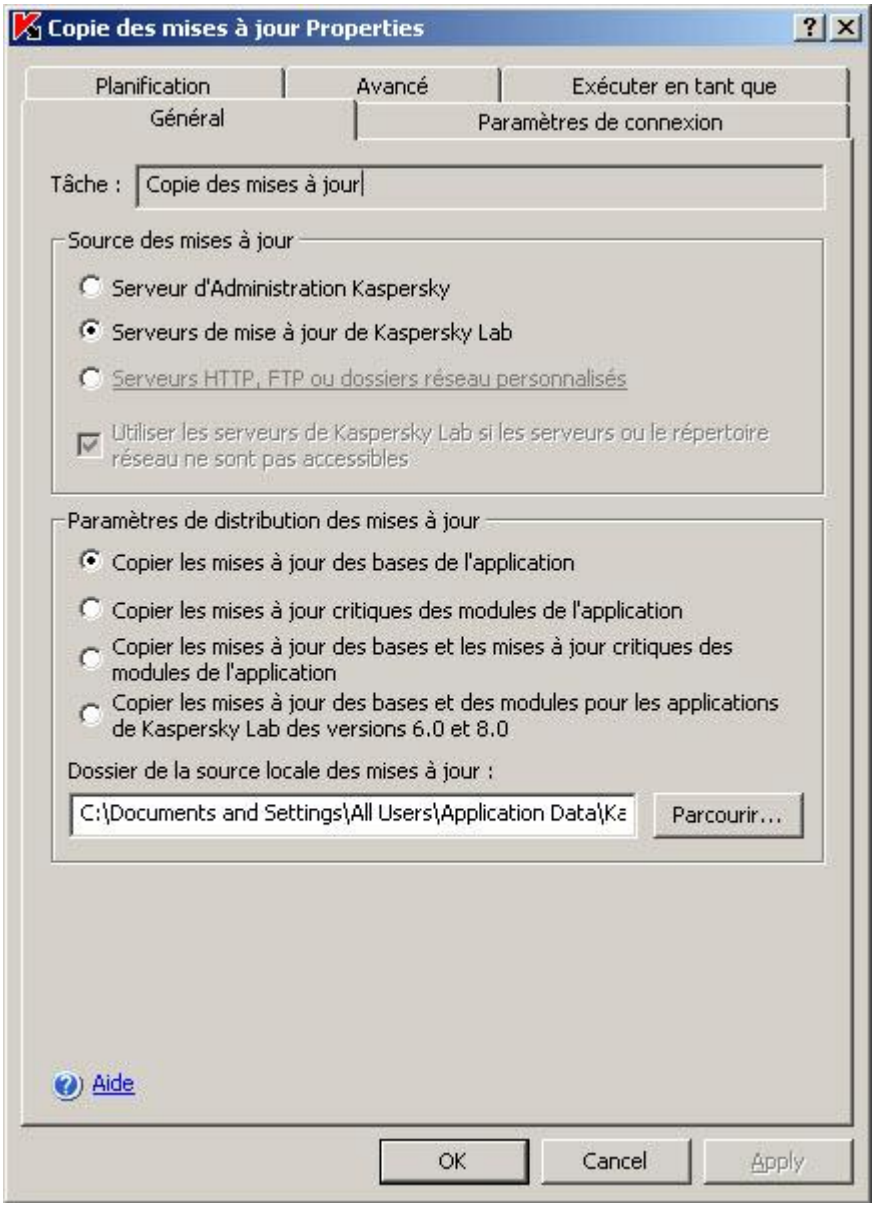


*Illustration 24. Boîte de dialogue **Propriétés : Copie des mises à jour**, onglet **Général***

5. Indiquez le répertoire local ou de réseau dans lequel Kaspersky Anti-Virus enregistrera les mises à jour reçues.

6. Cliquez sur **OK** pour enregistrer les modifications.

CONFIGURATION DES PARAMETRES DE LA TACHE MISE A JOUR DES MODULES

➧ *Pour configurer les paramètres de la tâche **Mise à jour des modules de l'application**, procédez comme suit* :

1. Dans l'arborescence de la console, déployez le nœud **Mise à jour** et sélectionnez la tâche **Mise à jour des modules de l'application** (cf. ill. ci-après)**.**

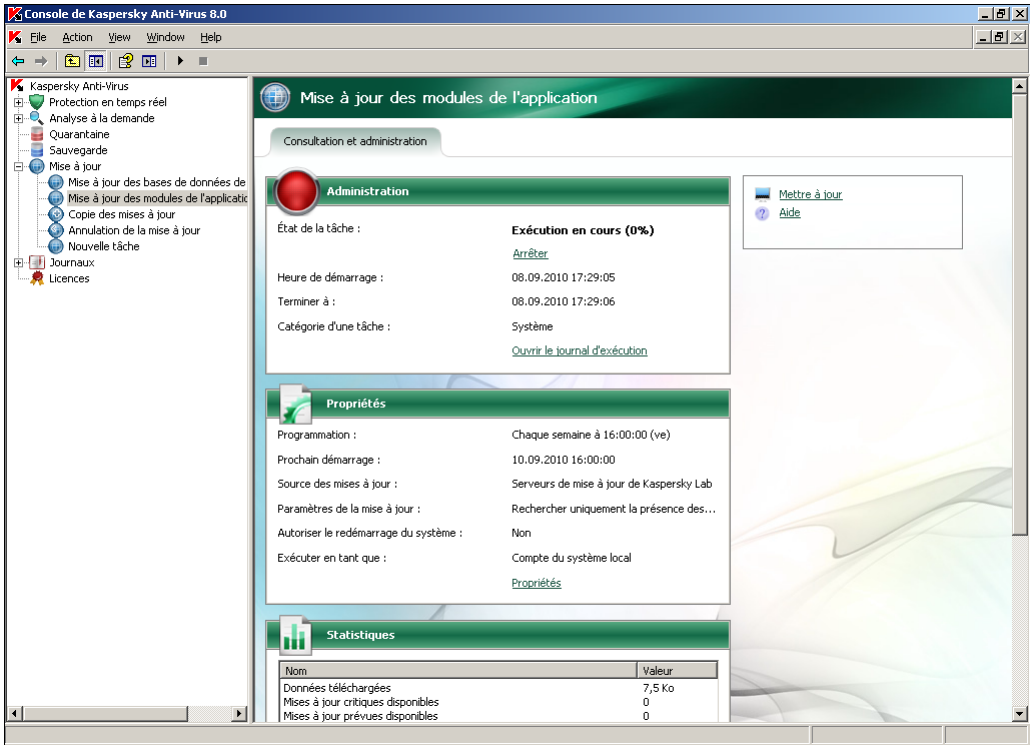


*Illustration 25. La tâche **Mise à jour des modules de l'application** est ouverte*

2. Dans le panneau de résultats, passez au lien **Propriétés**.

3. Dans la boîte de dialogue **Mise à jour des modules de l'application Propriétés**, indiquez la source de la mise à jour et les paramètres de connexion à celle-ci. Lisez les instructions dans la rubrique "Sélection de la source des mise à jour, configuration de la connexion à la source des mises à jour" (cf. page 65).

4. >Sous l'onglet **Général**, sélectionnez les actions à effectuer: copier et installer les mises à jour ou les rechercher uniquement (cf. page 402) (cf. ill. ci-après).

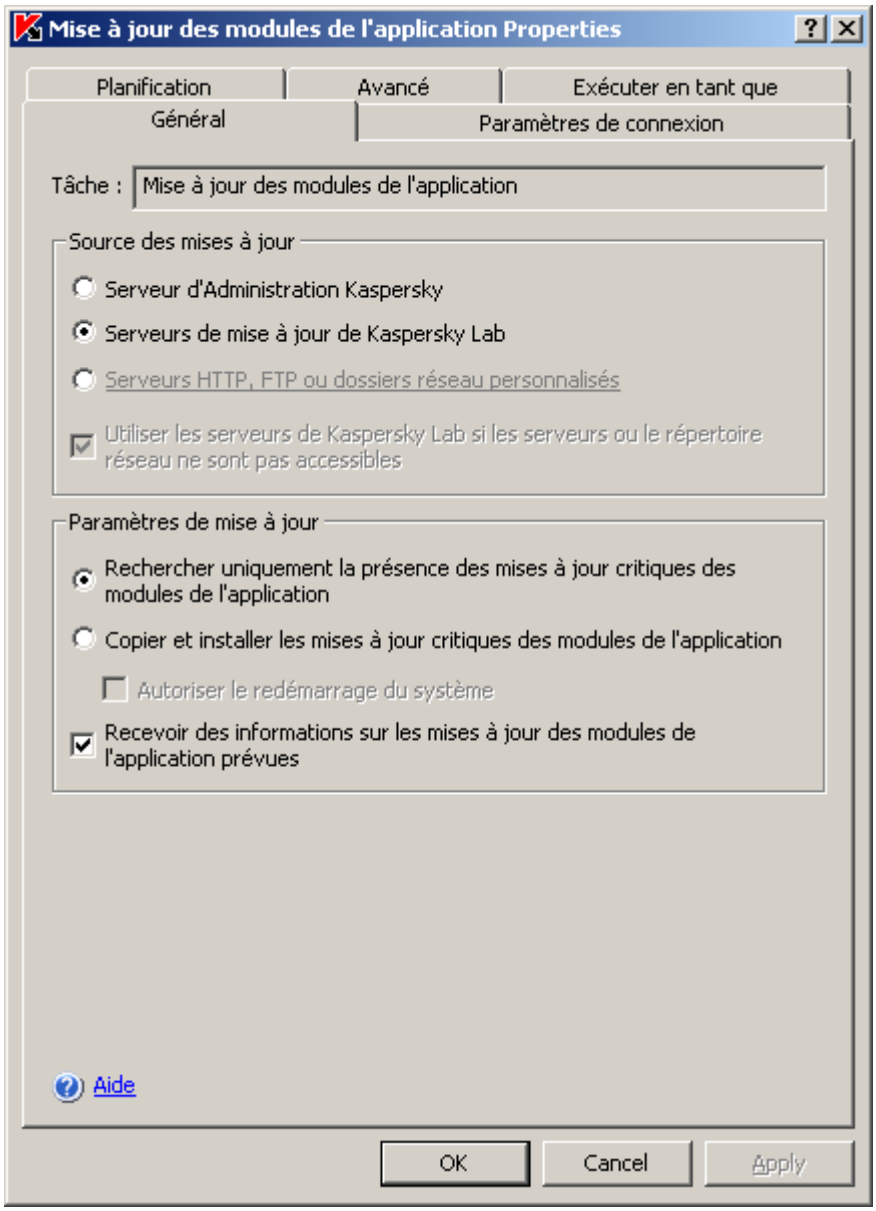


*Illustration 26. Boîte de dialogue **Propriétés : Mise à jour des modules de l'application**, onglet **Général***

5. Pour que Kaspersky Anti-Virus lance automatiquement le redémarrage du serveur à la fin de la tâche, si ce redémarrage est requis pour installer les modules logiciels, cochez la case **Autoriser le redémarrage du système**.

6. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

   Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement *Des mises à jour prévues des modules de Kaspersky Anti-Virus* sont disponibles. Celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées. Pour obtenir de plus amples informations, lisez la rubrique "Configuration des notification de l'administrateur et des utilisateurs" (cf. page 264).

7. Cliquez sur **OK** pour enregistrer les modifications.

PARAMETRES DES TACHES DE MISE A JOUR

Tandis que la tâche de mise à jour est exécutée, vous pouvez consulter les informations en temps réel relatives aux données reçues depuis le lancement de la tâche jusqu'à maintenant.

Après l'arrêt ou la suspension de la tâche, vous pouvez consulter les informations dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

Pour consulter les statistiques de la tâche de mise à jour, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Mise à jour**.
2. Sélectionnez la tâche dont vous souhaitez consulter les statistiques.

Le panneau des résultats du groupe **Statistiques** reprend les statistiques de la tâche.

Si vous consultez la tâche **Mise à jour des bases de l'application** ou la tâche **Copie des mises à jour**, dans le panneau des résultats, vous verrez le volume de données téléchargées par Kaspersky Anti-Virus en ce moment (**Données téléchargées**).

Si vous consultez la tâche **Mise à jour des modules de l'application**, vous verrez les informations décrites dans le tableau ci-dessous.

Tableau 8. Informations sur la tâche Mise à jour des modules de l'application

CHAMP	DESCRIPTION
Données téléchargées	Volume totale de données téléchargées
Mises à jour critiques disponibles	Nombre de mises à jour critiques prêtes pour l'installation.
Mises à jour prévues disponibles	Nombre de mises à jour prévues disponibles pour l'installation.
Erreur d'application des mises à jour	Si la valeur de ce champ est différente de zéro, la mise à jour n'a pas été appliquée. Vous pouvez consulter le nom de la mise à jour pendant laquelle l'erreur s'est produite dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234).

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS.

Kaspersky Anti-Virus, avant d'appliquer la mise à jour des bases, crée une copie de sauvegarde des bases utilisées jusqu'à présent. Si la mise à jour est interrompue ou se solde par un échec, Kaspersky Anti-Virus reviendra automatiquement à l'utilisation des mises à jour installées antérieurement.

Si vous rencontrez des problèmes après la mise à jour des bases, vous pouvez revenir à l'état antérieur des bases grâce à la tâche **Retour à l'état antérieur à la mise à jour des bases**.

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR DES MODULES LOGICIELS

Avant d'appliquer la mise à jour des modules logiciels, Kaspersky Anti-Virus crée une copie de sauvegarde des modules utilisés actuellement. Si la mise à jour des modules est interrompue ou se solde par un échec, Kaspersky Anti-Virus reviendra automatiquement à l'utilisation des derniers modules actualisés installés.

Pour revenir à l'état antérieur des modules logiciels, utilisez le composant **Ajout/suppression de programme** du panneau de configuration de Microsoft Windows.

Vous pouvez décider de revenir manuellement à l'état antérieur des modules logiciels correspondant à la mise à jour précédente.

BOITES DE DIALOGUE : MISE A JOUR

DANS CETTE SECTION DE L'AIDE

MISE A JOUR (ENTREE)

L'entrée **Mise à jour** est conçue pour contrôler les mises à jour des bases antivirus et des modules de Kaspersky Anti-Virus, la distribution des mises à jour dans un dossier local et l'annulation des mises à jour.

Elle comprend des sous-entrées pour la gestion des tâches système de mises à jour:**Mise à jour de la base de données de l'application**, **Mise à jour des modules de l'application**, **Copie des mises à jour**, **Annulation de la mise à jour**.

Une entrée séparée existe pour chaque tâche de groupe créée et transmise au serveur par Kaspersky Administration Kit.

Les tâches systèmes sont des caractéristiques intégrées de Kaspersky Anti-Virus qui prennent en charge les fonctions suivantes :

- **Mise à jour de la base de données de l'application** : mise à jour de la base de données de Kaspersky Anti-Virus.
- **Mise à jour des modules de l'application** : mise à jour des modules de Kaspersky Anti-Virus.
- **Copie des mises à jour** : enregistre les mises à jour des bases de données et des modules de programme dans un dossier local. Vous pouvez spécifier ce dossier en tant que source des mises à jour pour les programmes antivirus installés sur le réseau et pour les autres applications de Kaspersky Lab.

- **Annulation de la mise à jour** : rétablit les bases de données du programme à partir d'une copie de sauvegarde, pour l'utiliser en tant que version courante des bases de Kaspersky Anti-Virus.

Panneau de résultats

Le panneau de résultats affiche l'état actuel des tâches de mise à jour suivant :

- **Nom de tâche** : nom de la tâche de mise à jour.
- **Catégorie de tâche** :
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.
- **Etat de la tâche** : état actuel de la tâche, pourcentage de la tâche déjà accomplie.
- **Heure de démarrage** : **date et heure de démarrage de la tâche.** L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Planification** : conditions de lancement d'une tâche programmée.
- **Prochain démarrage** : heure prévue pour le prochain lancement de la tâche programmée.

Pour gérer une tâche, sélectionnez l'entrée appropriée dans l'explorateur de la console ou dans la liste affichée dans le panneau de résultats.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Exporter les paramètres** : enregistre toutes les tâches système ou personnalisées dans un fichier. Ce faisant, les paramètres de chaque tâche sont enregistrés.
- **Importer les paramètres** : restaure toutes les tâches de mise à jour depuis un fichier. Les tâches existantes ne sont pas supprimées. Les tâches importées sont ajoutées à la liste. Si une tâche existe avec le même nom, ses paramètres sont redéfinis avec les valeurs du fichier.

VOIR EGALEMENT

MISE A JOUR DES BASES DE L'APPLICATION (ENTREE)

La tâche système **Mise à jour de la base de données de l'application** permet de mettre à jour les bases de données utilisées par Kaspersky Anti-Virus.

Nous vous conseillons d'actualiser les bases antivirus directement après l'installation de l'application car les bases livrées avec la distribution ne sont déjà plus d'actualité au moment de l'installation.

L'entrée **Mise à jour de la base de données de l'application** permet de démarrer et d'arrêter les tâches de **Mise à jour de la base de données de l'application**, de configurer les paramètres de la tâche, de planifier ces tâches et d'afficher des statistiques de performances.

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours** ou **Complétée**).
- **Heure de démarrage** : date et heure de démarrage de la tâche.
- **Heure de fin** : date et heure prévues pour la fin de la tâche.
- **Catégorie de tâche** :
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Le bloc **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, à la source de mise à jour et à la configuration de la tâche.

Le lien **Modifier les paramètres de la tâche** ouvrir la fenêtre de dialogue **Propriétés : mise à jour de la base de données de l'application**.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

Menu contextuel

Le menu contextuel permet d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Propriétés** : affiche et configure les paramètres de la mise à jour des bases de l'application, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution.

VOIR EGALEMENT

MISE A JOUR DES MODULES DE L'APPLICATION (ENTREE)

Pour conserver le niveau de protection appropriée du serveur, nous vous recommandons d'installer régulièrement les mises à jour de Kaspersky Anti-Virus.

L'entrée **Mise à jour des modules de l'application** permet de démarrer et d'arrêter les tâches **Mise à jour des modules de l'application**, de planifier ces tâches et d'afficher des statistiques de performances.

Par défaut, la tâche de mise à jour des modules du programme est exécutée une fois par semaine. La mise à jour est effectuée depuis les serveurs de Kaspersky Lab. La tâche vérifie la présence de mises à jour de modules urgentes ou planifiées. Les mises à jour ne sont pas installées.

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours** ou **Complétée**).
- **Heure de démarrage** : date et heure de démarrage de la tâche.
- **Heure de fin** : date et heure prévues pour la fin de la tâche.
- **Catégorie de tâche** :
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Le bloc **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, à la source de mise à jour et à la configuration de la tâche.

Le lien **Propriétés** ouvre la boîte de dialogue **Propriétés : Mise à jour des modules de l'application**.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

Menu contextuel

Le menu contextuel permet d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Propriétés** : affiche et configure les paramètres de la mise à jour des modules de l'application, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution.

VOIR EGALEMENT

Présentation de la mise à jour des modules de Kaspersky Anti-Virus 60

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Configuration de planification des tâches en MMC 50

Affichage dans le journal d'informations relatives à la tâche 234

Paramètres des tâches de mise à jour 74

Configuration des paramètres de la tâche Mise à jour des modules 71

COPIE DES MISES A JOUR (ENTREE)

Kaspersky Anti-Virus prend en charge la distribution des mises à jour des bases et modules de programme, et leur enregistrement dans un dossier de mise à jour local. Vous pouvez spécifier ce dossier en tant que source des mises à jour pour les programmes antivirus installés sur le réseau et pour les autres applications de Kaspersky Lab. La tâche système **Copie des mises à jour** assure cette fonction.

L'entrée **Copie des mises à jour** permet **de démarrer et d'arrêter les tâches de** Copie des mises à jour, de planifier ces tâches et d'afficher des statistiques de performances.

La **Copie des mises à jour** est lancée manuellement par défaut. La mise à jour est effectuée depuis les serveurs de Kaspersky Lab. Les mises à jour de bases de données ne sont téléchargées que pour Kaspersky Anti-Virus 6.0 pour Windows Servers Enterprise Edition.

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours** ou **Complétée**).
- **Heure de démarrage** : date et heure de démarrage de la tâche.
- **Heure de fin** : date et heure prévues pour la fin de la tâche.
- **Catégorie de tâche** :

- **Système** : tâches intégrées dans l'application.
- **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Le bloc **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, à la source de mise à jour et à la configuration de la tâche.

Le lien **Propriétés** ouvre la boîte de dialogue **Propriétés : Copie des mises à jour**.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

Menu contextuel

Le menu contextuel permet d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Propriétés** : affiche et configure les paramètres de copie des mises à jour, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution.

VOIR EGALEMENT

Tâches de mise à jour 64

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Configuration de planification des tâches en MMC 50

Affichage dans le journal d'informations relatives à la tâche 234

Paramètres des tâches de mise à jour 74

Configuration des paramètres de la tâche Copie des mises à jour 70

ANNULATION DE LA MISE A JOUR (ENTREE)

Avant de mettre à jour les bases antivirus, Kaspersky Anti-Virus réalise une copie de sauvegarde. Si le téléchargement des mises à jour est interrompu ou produit une erreur, Kaspersky Anti-Virus reprend automatiquement la version précédente des bases antivirus. En outre, vous pouvez annuler la mise à jour de la base de données de l'application, qui peuvent être endommagées, par exemple.

Dans ce cas, la sauvegarde de la mise à jour est créée avant d'utiliser la dernière mise à jour.

La tâche système **Annulation de la mise à jour** permet de restaurer les bases de Kaspersky Anti-Virus à partir de leur copie de sauvegarde pour les utiliser en tant que version courante. Quand cette tâche est utilisée, la sauvegarde de la mise à jour est créée avant d'utiliser la dernière mise à jour. L'administrateur exécute la tâche manuellement.

L'entrée **Annulation de la mise à jour** permet de démarrer et d'arrêter les tâches **d'annulation de la mise à jour** et d'afficher des statistiques de performances.

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours** ou **Complétée**).
- **Heure de démarrage** : date et heure de démarrage de la tâche.
- **Heure de fin** : date et heure prévues pour la fin de la tâche.
- **Catégorie de tâche** :
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Le menu contextuel permet d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.

VOIR EGALEMENT

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

MISE A JOUR DES BASES : ONGLET GENERAL

Cet onglet permet de configurer les tâches de mise à jour de Kaspersky Anti-Virus. Le nom de la tâche est affiché dans la partie supérieure de l'onglet. Avec les champs disponibles dessous, vous pouvez sélectionner une source contenant l'ensemble des mises à jour les plus récentes.

Sélectionnez l'une des options suivantes dans le groupe **Source des mises à jour** :

- **Serveur d'Administration Kaspersky** : un dossier partagé sur le Serveur d'administration sera utilisé comme source de mises à jour. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

  Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'accès distant de Kaspersky Administration Kit et si L'Agent d'administration (composant de Kaspersky Administration Kit qui gère les connexions entre les ordinateurs et le serveur d'administration) est installé sur le serveur sécurisé. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

- **Les serveurs de mise à jour de Kaspersky Lab** : les sites Web de Kaspersky Lab seront utilisés comme sources de mises à jour. Ils hébergent les mises à jour des bases et des modules de programme de tous les produits de la société. Il s'agit de la source par défaut.

- **Serveurs HTTP, FTP ou dossiers réseau personnalisés**, des serveurs locaux ou des dossiers spécifiés par l'utilisateur sont utilisés comme source de mises à jour. Si vous sélectionnez cette option, vous devez créer une

liste de sources disposant d'ensembles actualisés de mises à jour. Pour ce faire, cliquez sur **Modifier**. Si plusieurs ressources sont définies en tant qu'origines de mises à jour, l'application tente de s'y connecter l'une après l'autre, en commençant par le début de liste et récupère les mises à jour de la première source disponible.

Si les ressources sélectionnées ne sont pas disponibles, les serveurs de mise à jour de Kaspersky Lab peuvent être utilisés comme sources. Pour activer cette fonction, cochez la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs spécifiés par l'utilisateur ne sont pas accessibles**.

VOIR EGALEMENT

Configuration des tâches liées à la mise à jour 65

MISE A JOUR DES MODULES DE L'APPLICATION : ONGLET GENERAL

Cet onglet permet de configurer les tâches de mise à jour des modules de Kaspersky Anti-Virus. Le nom de la tâche est affiché dans la partie supérieure de l'onglet. Grâce aux champs ci-dessous, vous pouvez définir les paramètres suivants de la tâche de mise à jour :

- Mises à jour : ressource hébergeant un ensemble actualisé de mises à jour ;
- Quelles mises à jour sont distribuées et installées
- L'action du système s'il est nécessaire de redémarrer Kaspersky Anti-Virus ou le système d'exploitation après une mise à jour.

Sélectionnez l'une des options suivantes dans le groupe **Source des mises à jour** :

- **Serveur d'Administration Kaspersky** : un dossier partagé sur le Serveur d'administration sera utilisé comme source de mises à jour. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

  Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'accès distant de Kaspersky Administration Kit et si L'Agent d'administration (composant de Kaspersky Administration Kit qui gère les connexions entre les ordinateurs et le serveur d'administration) est installé sur le serveur sécurisé. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

- **Les serveurs de mise à jour de Kaspersky Lab** : les sites Web de Kaspersky Lab seront utilisés comme sources de mises à jour. Ils hébergent les mises à jour des bases et des modules de programme de tous les produits de la société. Il s'agit de la source par défaut.

- **Serveurs HTTP, FTP ou dossiers réseau personnalisés**, des serveurs locaux ou des dossiers spécifiés par l'utilisateur sont utilisés comme source de mises à jour. Si vous sélectionnez cette option, vous devez créer une liste de sources disposant d'ensembles actualisés de mises à jour. Pour ce faire, cliquez sur **Modifier**. Si plusieurs ressources sont définies en tant qu'origines de mises à jour, l'application tente de s'y connecter l'une après l'autre, en commençant par le début de liste et récupère les mises à jour de la première source disponible.

Si les ressources sélectionnées ne sont pas disponibles, les serveurs de mise à jour de Kaspersky Lab peuvent être utilisés comme sources. Pour activer cette fonction, cochez la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs spécifiés par l'utilisateur ne sont pas accessibles**.

Dans le groupe de champs **Paramètres de la mise à jour**, choisissez les valeurs des paramètres qui définissent la manière dont Kaspersky Anti-Virus va copier et installer la mise à jour des modules.

Pour ce faire, sélectionnez l'une des options suivantes :

- **Rechercher uniquement la présence des mises à jour critiques des modules de l'application** pour recevoir des notifications sur les mises à jour de modules urgentes de l'application antivirus disponibles. Les

mises à jour ne seront pas téléchargées automatiquement. Vous ne recevrez une notification que si les notifications sont activée pour ce type d'événement. Il s'agit de l'option par défaut.

- **Copier et installer les mises à jour critiques de modules de l'application**, pour télécharger et installer les mises à jour urgentes des modules de l'application. Si vous sélectionnez cette option, sélectionnez les actions appliquées si l'ordinateur ou l'application doit être redémarré après l'installation :

  - Cochez la case **Autoriser le redémarrage du système**. Le redémarrage du système, si nécessaire pour compléter les mises à jour des modules du programme, sera alors effectué automatiquement, immédiatement après l'installation des mises à jour.

    Décochez la case si l'application exploitée sur le serveur sécurisé ne doit pas être interrompue.

  - Décochez la case **Autoriser le redémarrage du système**. Le redémarrage du système sera alors différé et vous pourrez le redémarrer vous-même.

Cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues pour recevoir des notifications sur toutes** les mises à jour pour les modules de Kaspersky Anti-Virus disponibles. Les mises à jour ne seront pas téléchargées automatiquement. Vous pouvez les télécharger manuellement à partir de l'adresse spécifiée dans le message que vous recevez. Vous ne recevrez une notification que si les notifications sont activées pour ce type d'événement. Cette case est cochée par défaut.

VOIR EGALEMENT

Configuration des paramètres de la tâche Mise à jour des modules 71

COPIE DES MISES A JOUR : ONGLET GENERAL

Cet onglet permet de configurer la tâche système **Copie des mises à jour**. Le nom de la tâche est affiché dans la partie supérieure de l'onglet.

La tâche de **Copie des mises à jour** recopie, depuis la source spécifiée, les mises à jour des bases de données et des modules de Kaspersky Anti-Virus dans un dossier local. Ce dossier peut être utilisé en tant que source des mises à jour des applications antivirus installées sur le réseau et des autres applications de Kaspersky Lab.

Sélectionnez l'une des options suivantes dans le groupe **Source des mises à jour** :

- **Serveur d'Administration Kaspersky** – un dossier partagé sur le Serveur d'administration sera utilisé comme source de mises à jour. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

  Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'accès distant de Kaspersky Administration Kit et si L'Agent d'administration (composant de Kaspersky Administration Kit qui gère les connexions entre les ordinateurs et le serveur d'administration) est installé sur le serveur sécurisé. Pour plus de détails, voir le document "Manuel de l'administrateur de Kaspersky Administration Kit 8.0".

- **Les serveurs de mise à jour de Kaspersky Lab** : les sites Web de Kaspersky Lab seront utilisés comme sources de mises à jour. Ils hébergent les mises à jour des bases et des modules de programme de tous les produits de la société. Il s'agit de la source par défaut.

- **Serveurs HTTP, FTP ou dossiers réseau personnalisés**, des serveurs locaux ou des dossiers spécifiés par l'utilisateur sont utilisés comme source de mises à jour. Si vous sélectionnez cette option, vous devez créer une liste de sources disposant d'ensembles actualisés de mises à jour. Pour ce faire, cliquez sur **Modifier**. Si plusieurs ressources sont définies en tant qu'origines de mises à jour, l'application tente de s'y connecter l'une après l'autre, en commençant par le début de liste et récupère les mises à jour de la première source disponible.

Si les ressources sélectionnées ne sont pas disponibles, les serveurs de mise à jour de Kaspersky Lab peuvent être utilisés comme sources. Pour activer cette fonction, cochez la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs spécifiés par l'utilisateur ne sont pas accessibles**.

Dans la section **Paramètres de copie des mises à jour**, spécifiez quelles mises à jour seront copiées et enregistrées dans le dossier local. Pour ce faire, sélectionnez l'une des options suivantes :

- **Copier les mises à jour des bases de l'application** : télécharge uniquement les mises à jour de la base antivirus (par défaut).
- **Copier les mises à jour critiques des modules de l'application** : télécharge uniquement les mises à jour des modules critiques de Kaspersky Anti-Virus.
- **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application** : télécharge les mises à jour de la base antivirus et des modules critiques de Kaspersky Anti-Virus.
- **Copier les mises à jour des bases et des modules pour les applications de Kaspersky Lab des versions 6.0 et 8.0** : télécharge les mises à jour des bases antivirus et tous les modules d'application disponibles sur la source des mises à jour pour les applications 6.0 et 8.0 de Kaspersky Lab (parmi les diverses solutions disponibles pour les entreprises), y compris Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition.

Dans la zone **Répertoire de la source locale des mises à jour**, spécifiez le chemin du dossier local ou réseau, dans lequel sont enregistrées les mises à jour de la base et des modules téléchargées. Vous pouvez entrer le chemin manuellement au format UNC (Universal Naming Convention) ou sélectionner le dossier avec **Parcourir**.

Ne choisissez pas d'unité virtuelle créée avec la commande SUBST ni d'unités réseau extérieures au serveur comme source de mises à jour. Précisez le chemin complet de la ressource.

VOIR EGALEMENT

Configuration des paramètres de la tâche Copie des mises à jour 70

SERVEURS DE MISE A JOUR (FENETRE)

La fenêtre **Serveurs de mise à jour** permet de créer une liste de sources de mises à jour, si vous avez sélectionné l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** dans les paramètres de Kaspersky Anti-Virus.

La liste peut inclure des adresses de serveurs HTTP et FTP ainsi que des adresses réseau ou des dossiers locaux. Si la case de l'adresse est cochée, la ressource est utilisée pour les mises à jour.

Pendant le processus de mise à jour, l'application consulte les sources dans l'ordre rigoureux de la liste et utilisera la première source disponible. Vous pouvez modifier l'ordre des sources dans la liste à l'aide des boutons **Monter** et **Descendre**.

Vous pouvez modifier la liste à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

VOIR EGALEMENT

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Source des mises à jour..... 396

ONGLET PARAMETRES DE CONNEXION

L'onglet **Paramètres de connexion** affiche les paramètres de connexion aux sources de mise à jour.

Spécifiez les paramètres de connexion dans la section **Paramètres généraux** :

- Cochez **Utiliser le FTP en mode passif si possible** si vous téléchargez les mises à jour depuis un serveur FTP utilisant le mode passif pour se connecter.

  Il est sous-entendu par défaut que le réseau local de la société utilise un pare-feu et que les connexions avec les serveurs FTP sont effectuées en mode passif. C'est pourquoi la case est cochée par défaut. Décochez la case si le mode actif FTP est utilisé.

- Spécifiez le délai de réponse du serveur de mise à jour dans le champ **Délai d'attente (sec.)**. Au delà du temps indiqué, une connexion est tentée avec le prochain serveur de mises à jour. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que tous les serveurs disponibles n'ont pas été sollicités. Le délai d'attente par défaut est de 10 seconds.

Si le programme se connecte aux ressources de mises à jour à travers un serveur proxy, cochez les cases suivantes dans la section **Paramètres de connexion avec la source des mises à jour** :

- **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab**, si vous choisissez de mettre à jour depuis les serveurs de Kaspersky Lab, ou si la case **Utiliser les serveurs de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles est cochée.**

- **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs personnalisés**, si vous avez sélectionné l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** en tant que sources de mises à jour.

Spécifiez la méthode de définition des paramètres de proxy dans la section **Paramètres du serveur proxy**. Pour ce faire, sélectionnez l'une des options suivantes :

- **Détecter automatiquement les paramètres du serveur proxy**, par exemple, si le protocole WPAD (Web Proxy Auto-Discovery) est utilisé sur le réseau local où se trouve le serveur sécurisé. Il s'agit de l'option par défaut.

- **Utiliser les paramètres de serveur proxy spécifiés** si vous préférez ne pas détecter automatiquement les paramètres. Dans le champ **Adresse**, indiquez l'adresse IP ou le nom symbolique du serveur proxy et spécifiez le numéro du port proxy utilisé pour mettre à jour l'application dans le champ **Port**.

Cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales** si vous prévoyez de télécharger les mises à jour depuis des serveurs locaux HTTP ou FTP.

Sélectionnez le mode d'authentification utilisé pour accéder au serveur proxy dans le groupe **Paramètres d'authentification au serveur proxy** : Pour ce faire, sélectionnez la valeur souhaitée dans la liste déroulante.

- **Aucune authentification requise** si le serveur proxy n'assure pas l'authentification des utilisateurs qui se connectent.

- **Utiliser l'authentification NTLM** si l'authentification NTLM est utilisée pour accéder au serveur proxy. Dans ce cas, c'est le compte utilisé pour exécuter la tâche de mise à jour qui est utilisé pour se connecter au serveur proxy.

- **Utiliser l'authentification NTLM avec utilisateur et mot de passe**, si le compte utilisateur de la tâche de mise à jour ne possède pas de privilèges suffisants pour accéder au serveur proxy. **Dans la zone Utilisateur**, sélectionnez un nom d'utilisateur avec des privilèges suffisants, manuellement ou dans la liste avec le bouton, et complétez la zone Mot de passe.

- **Utiliser le nom d'utilisateur et le mot de passe**, si l'authentification NTLM ne peut pas être utilisée. Complétez les zones **Utilisateur** et le **Mot de passe**.

Si vous sélectionnez l'option **Utiliser l'authentification NTLM avec utilisateur et mot de passe** ou **Utiliser le nom d'utilisateur et le mot de passe**, et l'authentification échoue, le programme tente de compléter l'authentification NTLM sous le compte utilisateur utilisé pour exécuter la tâche.

Spécifiez l'emplacement géographique du serveur sécurisé dans la section **Paramètres régionaux**. Pour ce faire, sélectionnez le pays souhaité dans la liste déroulante. Ces paramètres déterminent le serveur Kaspersky Lab le plus proche pour la récupération des mises à jour.

Les serveurs de mises à jour de Kaspersky Lab se trouvent dans divers pays. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mises à jour le plus proche.

L'option par défaut est **Détecter automatiquement** : le pays est déterminé à l'aide des paramètres régionaux de l'ordinateur équipé de Kaspersky Anti-Virus (**Démarrer → Configuration → Panneau de configuration → Options régionales et linguistiques → Paramètres régionaux → Emplacement**).

VOIR EGALEMENT

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour 398

Paramètres du serveur proxy 399

Méthode de vérification de l'authenticité lors de l'accès au serveur proxy 400

PARAMETRES REGIONAUX (ONGLET)

L'onglet **Paramètres régionaux** spécifie l'emplacement géographique du serveur sécurisé. Ces paramètres déterminent le serveur Kaspersky Lab le plus proche pour la récupération des mises à jour.

Les serveurs de mises à jour de Kaspersky Lab se trouvent dans divers pays. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mises à jour le plus proche.

L'option par défaut est **Détecter automatiquement** : le pays est déterminé à l'aide des paramètres régionaux de l'ordinateur équipé de Kaspersky Anti-Virus (**Démarrer → Configuration → Panneau de configuration → Options régionales et linguistiques → Paramètres régionaux → Emplacement**).

Pour configurer l'emplacement géographique du serveur, sélectionnez le pays dans la liste déroulante **Emplacement**.

VOIR EGALEMENT

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Paramètres régionaux pour l'optimalisation de la réception des mises à jour (Emplacement) 401

PROTECTION EN TEMPS REEL DES FICHIERS

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES TACHES DE LA PROTECTION EN TEMPS REEL

Kaspersky Anti-Virus prévoit deux tâches prédéfinies de protection en temps réel : **Protection en temps réel des fichiers** et **Analyse des scripts**. Pour obtenir de plus amples informations sur la fonction **Protection en temps réel**, lisez le point 13 "Protection en temps réel et analyse à la demande".

Par défaut, les tâches de protection en temps réel sont exécutées automatiquement au démarrage de Kaspersky Anti-Virus. Vous pouvez les arrêter et les relancer, de même que les programmer. Vous pouvez également suspendre et relancer la tâche de protection en temps réel, par exemple lorsqu'il est nécessaire d'interrompre l'analyse des objets pendant une brève période, telle que lors de la réplication des données.

Vous pouvez configurer la tâche **Protection en temps réel des fichiers** (cf. rubrique "**Configuration de la tâche Protection en temps réel des fichiers**" à la page 87) : composer la zone de protection et définir les paramètres de protection pour les nœuds sélectionnés, appliquer la zone de confiance et configurer l'application de l'analyseur heuristique.

Pendant l'exécution de la tâche **Analyse des scripts** Kaspersky Anti-Virus contrôle l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies (ou Active Scripting), par exemple les scripts VBScript ou JScript. Kaspersky Anti-Virus interdit l'exécution des scripts qu'il juge dangereux. Si Kaspersky Anti-Virus considère que le script est suspect, il exécute l'action que vous avez choisie : interdiction ou autorisation de l'exécution. Pour savoir comment autoriser ou interdire l'exécution de scripts suspects, lisez la rubrique "Configuration de la tâche **Analyse des scripts**" (cf. page 108).

CONFIGURATION DE LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Par défaut, la tâche prédéfinie **Protection en temps réel des fichiers** contient les paramètres décrits dans le tableau ci-après. Vous pouvez modifier les valeurs de ces paramètres et configurer la tâche.

Quand vous modifiez les paramètres de la tâche (par exemple, désignation d'une autre couverture d'analyse), Kaspersky Anti-Virus applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours. Il consigne la date et l'heure de la modification des paramètres dans le journal d'exécution de la tâche ainsi que les informations relatives aux paramètres de la tâche avant et après la modification.

*Pour configurer la tâche **Protection en temps réel des fichiers**, procédez comme suit* :

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection en temps réel des fichiers**.

   Le panneau des résultats sous l'onglet **Configuration de la zone de protection** (cf. ill. ci-après) affiche l'arborescence des ressources fichiers du serveur et la boîte de dialogue **Niveau de sécurité** (mode standard).

3. Configurez les paramètres de la tâche en fonction de vos besoins (cf. tableau ci-dessous).

4. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

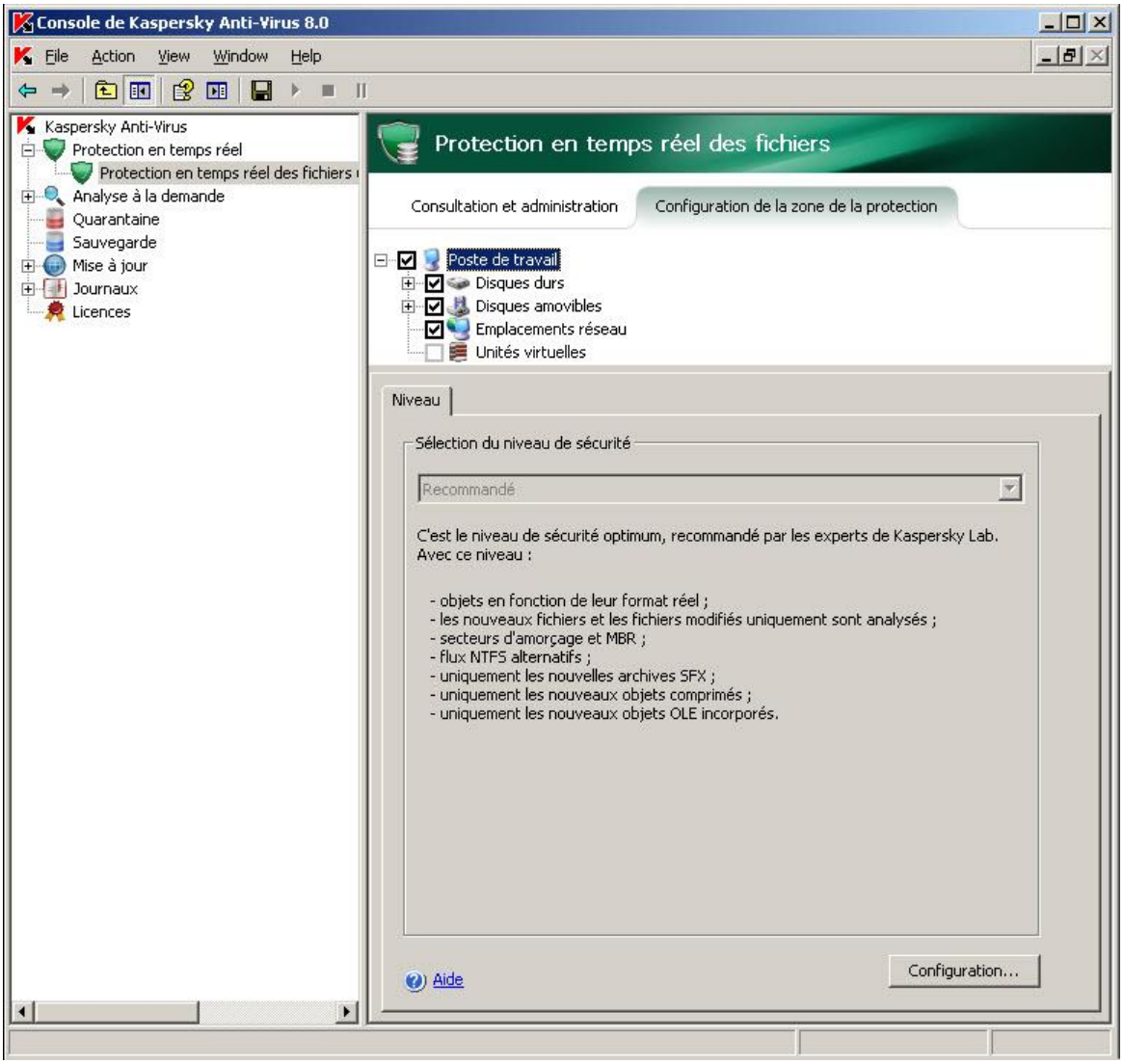


*Illustration 27. Tâche **Protection en temps réel des fichiers** ouverte*

*Tableau 9. Paramètres par défaut de la tâche **Protection en temps réel des fichiers***

PARAMETRE	VALEUR PAR DEFAUT	DESCRIPTION
Zone de protection	Tout le serveur	Vous pouvez limiter la couverture de protection (cf. page 90).
Paramètres de sécurité	Identiques pour toutes les couvertures de protection ; correspondent au niveau de protection **Recommandé** (cf. page 95).	Pour les nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur, *procédez comme suit* : • appliquer du niveau de sécurité prédéfini (cf. page 95) ; • modifier manuellement les paramètres de sécurité (cf. page 147) ; • enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud (cf. page 101).
Mode de protection	À l'accès et à la modification	Vous pouvez sélectionner le mode de protection des objets (cf. page 375) et indiquer, à savoir dans quel type d'accès aux objets Kaspersky Anti-virus les analyse-t-il.
Analyseur heuristique	Le niveau de protection **Moyen** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyseur heuristique (cf. page 393) et régler le niveau de l'analyse.
Zone de confiance	Appliquée Les programmes d'administration à distance **RemoteAdmin** sont exclus ainsi que les fichiers recommandés par Microsoft Corporation si, au moment de l'installation de Kaspersky Anti-Virus, vous avez sélectionné **Ajouter les menaces correspondant au masque not-a-virus:RemoteAdmin*** aux exclusions et **Ajouter les exclusions recommandées par Microsoft**.	Une liste unique d'exclusions que vous pouvez appliquer dans des tâches d'analyse à la demande sélectionnée et dans la tâche de **Protection en temps réel des fichiers**. Création et application de la zone de confiance (cf. page 178)

DANS CETTE SECTION DE L'AIDE

ZONE DE PROTECTION DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA CONSTITUTION D'UNE COUVERTURE DE PROTECTION DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Si la tâche **Protection en temps réel des fichiers** est exécutée selon les paramètres définis par défaut, Kaspersky Anti-Virus analyse tous les objets du système de fichiers du serveur. Si en raison des exigences de sécurité il n'est pas nécessaire d'analyser l'ensemble de ces fichiers, vous pouvez limiter la couverture de protection.

Dans la console de Kaspersky Anti-Virus, la zone de protection se présente sous forme d'une arborescence de ressources fichiers du serveur que Kaspersky Anti-Virus peut analyser (cf. ill. ci-après).

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrées de la manière suivante :

☑ Nœud repris dans la couverture de protection.

☐ Nœud exclu de la couverture de protection.

☑ Au moins un des nœuds intégrés à ce nœud est exclu de la couverture de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

Remarquez que le nœud parent sera indiqué par l'icône ☑ si vous sélectionnez tous les nœuds enfants et non le nœud parent. Dans ce cas, les fichiers et les répertoires qui se trouvent dans ce nœud ne seront pas automatiquement inclus dans la couverture de protection. Pour les inclure, il faudra inclure le nœud parent dans la couverture de protection. Vous pouvez également créer des "copies virtuelles" dans la console de Kaspersky Anti-Virus et les ajouter à la zone de protection.

Le nom des nœuds virtuels de la couverture d'analyse apparaît en lettres bleues.

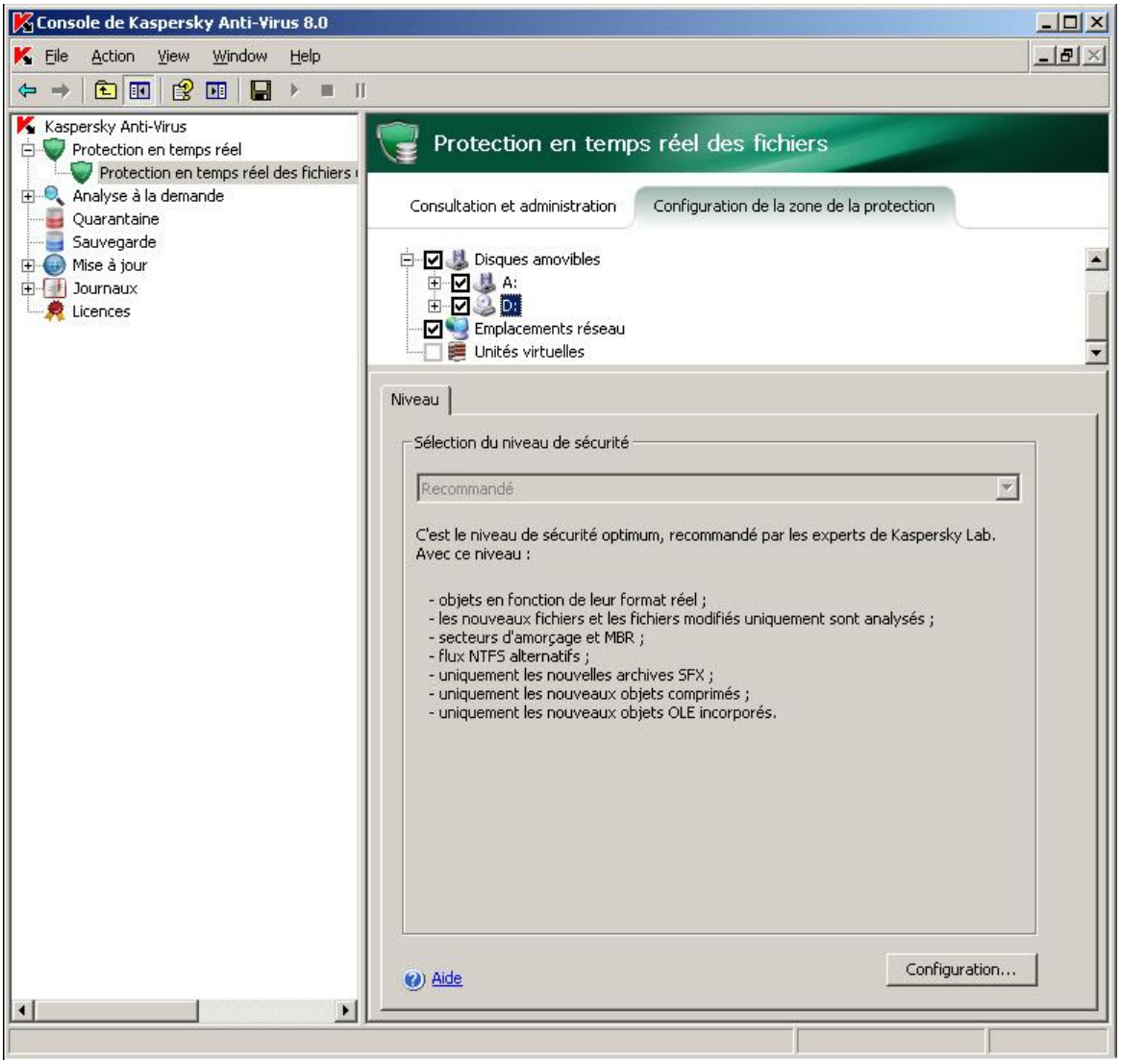


Illustration 28. Exemple d'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus.

COUVERTURES DE PROTECTION PREDEFINIES

Quand vous ouvrez la tâche **Protection en temps réel des fichiers**, l'arborescence des ressources fichier du serveur s'affiche dans le panneau des résultats sur l'onglet **Configuration de la zone de la protection** (cf. ill. ci-après).

L'arborescence des ressources fichiers représente les nœuds auxquels vous avez accès en lecture conformément aux paramètres de sécurité de Microsoft Windows.

L'arborescence des ressources fichiers du serveur contient les couvertures de protection prédéfinies suivantes :

- **Disques durs**. Kaspersky Anti-Virus analyse les fichiers du disque dur du serveur.
- **Disques amovibles**. Kaspersky Anti-Virus analyse les fichiers sur les disques amovibles tels que les disques compacts ou les clés USB.
- **Emplacements réseau**. Kaspersky Anti-Virus analyse les fichiers enregistrés dans les répertoires réseau ou lus par les applications exécutées sur le serveur. Kaspersky Anti-Virus n'analyse pas les fichiers dans les répertoires de réseau lorsqu'ils sont sollicités par des applications d'autres ordinateurs.

- **Unités virtuelles**. Vous pouvez inclure dans la couverture de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe (créer couverture de protection virtuelle).

Les pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus. Pour inclure les objets d'un pseudo-disque dans la couverture de protection, il faut inclure le répertoire du serveur auquel ce pseudo-disque est lié.

Les disques de réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. Pour inclure les objets d'un disque de réseau dans la couverture d'analyse, indiquez le chemin d'accès au répertoire correspondant à ce disque de réseau au format UNC (Universal Naming Convention).

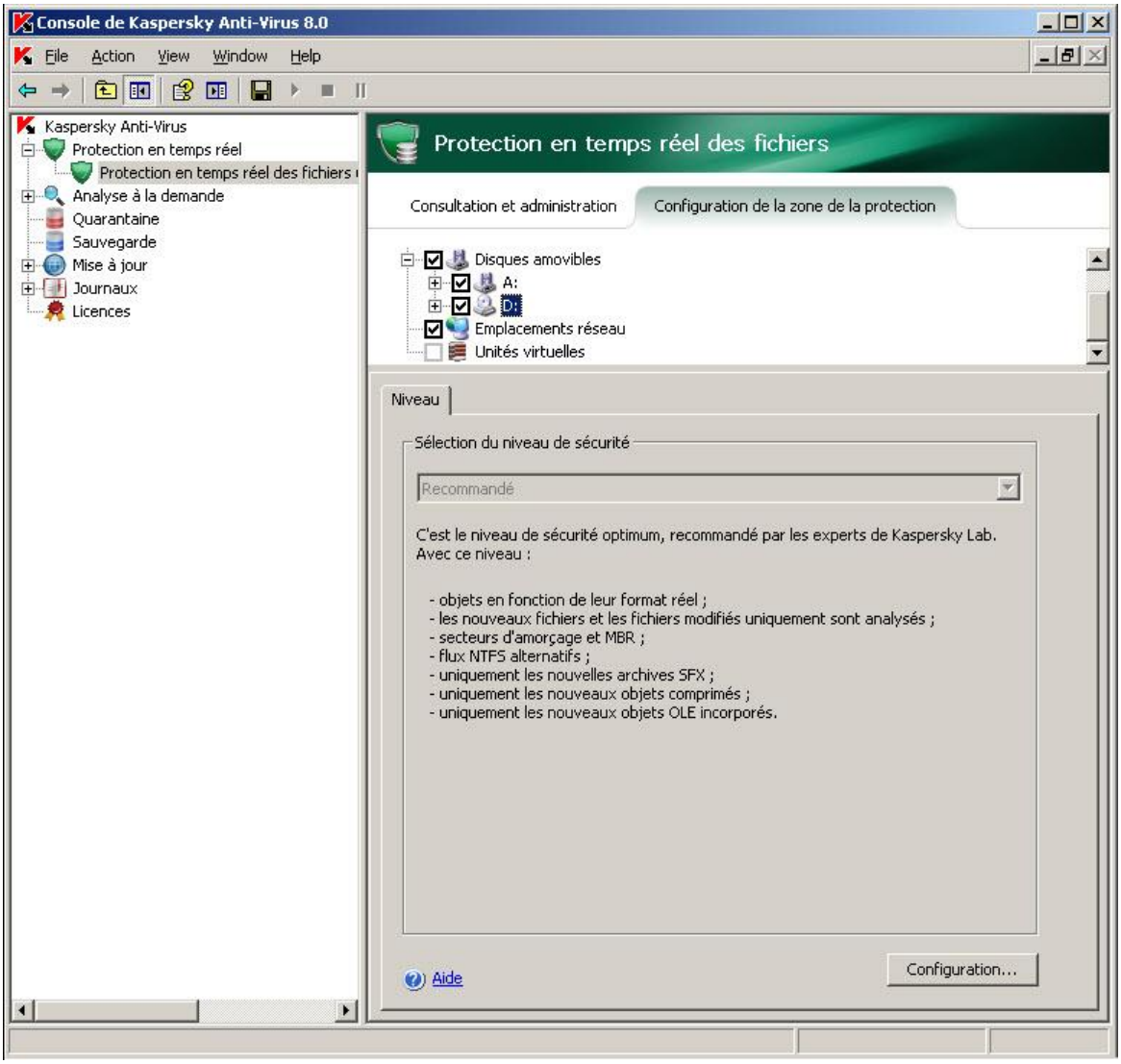


Illustration 29. Exemple d'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus.

CONSTITUTION DE LA COUVERTURE DE PROTECTION

➧ *Pour constituer la zone de protection, procédez comme suit :*

1. Ouvrez la tâche **Protection en temps réel des fichiers**.

2. Sous l'onglet **Configuration de la zone de la protection** dans le panneau des résultats, exécutez les actions suivantes dans l'arborescence des ressources fichier du serveur :

- Pour exclure un nœud particulier de la zone de protection, déployez l'arborescence des ressources fichiers pour afficher le nœud requis, puis désélectionnez la case contre de son nom.

- Pour sélectionner uniquement les nœuds que vous souhaitez inclure dans la zone de protection, désélectionnez la case **Poste de travail**, puis procédez d'une des manières suivantes :

  - si vous souhaitez inclure tous les disques d'un même type, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**) ;

  - Si vous souhaitez inclure un disque particulier du type requis, déployez le nœud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque. Par exemple, pour sélectionner le disque amovible **F:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:** ;

  - Si vous souhaitez inclure uniquement un répertoire particulier du disque, déployez l'arborescence des ressources du serveur afin d'afficher le répertoire que vous souhaitez inclure dans la couverture d'analyse puis, cochez la case en regard de son nom. Vous pouvez inclure des fichiers de la même manière.

3. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

Vous ne pourrez exécuter la tâche **Protection en temps réel des fichiers** que si au moins un nœud de l'arborescence des ressources fichiers du serveur est inclus dans la zone de protection.

Si vous définissez une couverture d'analyse complexe, par exemple en attribuant différentes valeurs aux paramètres de sécurité pour divers nœuds distincts de l'arborescence des ressources fichiers du serveur, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.

ZONE DE PROTECTION VIRTUELLE

Kaspersky Anti-Virus peut analyser non seulement les fichiers et les répertoires existants sur les disques durs et les disques amovibles mais également ceux présents sur les disques qui sont montés temporairement sur le serveur, par exemple les disques partagés de la grappe ou les fichiers et les répertoires qui sont créés dynamiquement sur le serveur par diverses applications et services.

Si vous avez inclus tous les objets du serveur dans la couverture de protection, ces nœuds dynamiques seront automatiquement repris dans la couverture de protection. Toutefois, si vous souhaitez attribuer des valeurs particulières aux paramètres de protection de ces nœuds dynamiques ou si vous avez sélectionné pour la protection en temps réel non pas tout le serveur, mais uniquement quelques secteurs, alors pour pouvoir inclure les disques, les fichiers ou les répertoires dans la couverture de protection, vous devrez d'abord les créer dans la console de Kaspersky Anti-Virus ; c'est ce que l'on appelle la création d'une couverture de protection virtuelle. Les disques, les fichiers ou les répertoires que vous créez existent uniquement dans la console de Kaspersky Anti-Virus et non pas dans la structure du système de fichiers du serveur protégé.

Si au moment de composer la couverture de protection, vous sélectionnez tous les fichiers ou les répertoires inclus sans choisir le répertoire parent, les répertoires ou les fichiers dynamiques qui s'y trouvent ne seront pas repris automatiquement dans la couverture de protection. Vous devez créer des "copies virtuelles" dans la console de Kaspersky Anti-Virus et les ajouter à la zone de protection.

Pour savoir comment créer une couverture de protection virtuelle dans la tâche "Protection en temps réel des fichiers" (cf. page 94)

Pour savoir comment créer une tâche de protection virtuelle dans les tâches d'analyse à la demande (cf. page 141)

CREATION D'UNE COUVERTURE DE PROTECTION VIRTUELLE : INCLUSION DES DISQUES, REPERTOIRES ET FICHIERS DYNAMIQUES DANS LA COUVERTURE DE PROTECTION

Pour ajouter à la zone de protection un disque virtuel, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

2. Sous l'onglet **Configuration de la zone de la protection** du panneau des résultats, dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud **Disques virtuelles** et sélectionnez le nom du disque virtuel créé dans la liste des noms disponibles (cf. ill. ci-après).

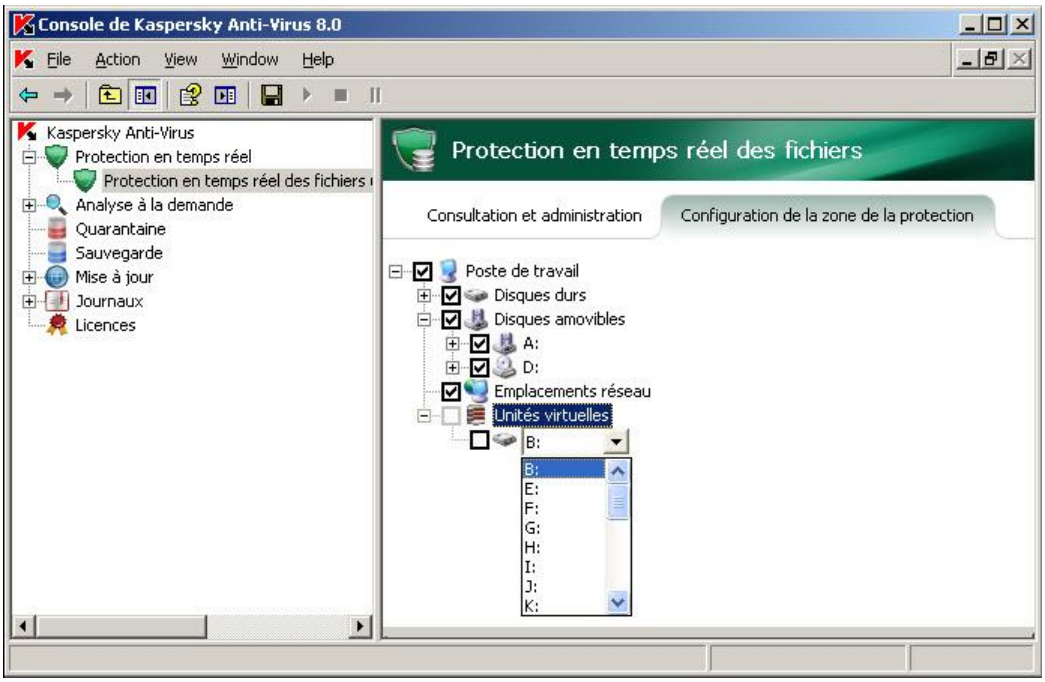


Illustration 30. Choix du nom du disque virtuel créé

3. Cochez la case à côté du disque ajouté afin de l'inclure dans la couverture de protection.

4. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

Pour ajouter un répertoire ou un fichier virtuel dans la zone de protection, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

2. Sous l'onglet **Configuration de la zone de la protection** du panneau des résultats, dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud auquel vous souhaitez ajouter le répertoire ou le fichier et sélectionnez **Ajouter un dossier virtuel** ou **Ajouter un fichier virtuel** (cf. ill. ci-après).

*Illustration 31. Sélection de l'élément du menu contextuel sous l'onglet **Configuration de la zone de la protection***

3. Dans le champ, saisissez le nom du répertoire (fichier). Vous pouvez définir un masque de nom de fichier en utilisant les caractères * et ?.

4. Dans la ligne contenant le nom du répertoire (fichier) créé, cochez la case afin de l'inclure dans la couverture de protection.

5. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

CONFIGURATION DES PARAMETRES DE SECURITE DU NŒUD SELECTIONNE

DANS CETTE SECTION DE L'AIDE

SELECTION DES NIVEAUX PREDEFINIS DE PROTECTION DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Pour les nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des niveaux de protection prédéfinis suivant : *vitesse maximale*, *recommandé et protection maximale. Chacun de ces niveaux possède sa propre sélection de paramètres de sécurité. Les valeurs des paramètres des niveaux prédéfinis sont reprises de le tableau de cette rubrique.*

Vitesse maximale

Vous pouvez sélectionner le niveau **Vitesse maximale** sur le serveur si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Anti-Virus sur les serveurs et les postes de travail ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** est sélectionné par défaut. Il est considéré par les experts de Kaspersky Lab comme suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux. Ce niveau offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés.

Protection maximum

Utilisez le niveau de protection **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau sont strictes.

Tableau 10. Niveaux de protection prédéfinis et valeurs des paramètres correspondants

PARAMETRES	NIVEAU DE SECURITE		
	VITESSE MAXIMALE	RECOMMANDE	PROTECTION MAXIMUM
Objets à analyser (cf. page 376)	Selon l'extension	En fonction du format	En fonction du format
Analyse uniquement des nouveaux fichiers et des fichiers modifiés (cf. page 382)	Activée	Activée	Désactivée
Actions à exécuter sur les objets infectés (cf. page 384)	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. page 386)	Quarantaine	Quarantaine	Quarantaine
Exclusion des objets (cf. page 379)	Non	Non	Non
Exclusion des menaces (cf. page 380)	Non	Non	Non
Durée maximale de l'analyse d'un objet (cf. page 388)	60 s	60 s	60 s
Taille maximale de l'objet composé analysé (cf. page 389)	à 8 Mo	8 Mo	Non défini
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. page 376)	Oui	Oui	Oui
Analyse des secteurs de démarrage (cf. page 376)	Oui	Oui	Oui
Analyse des objets composés (cf. page 383)	• Objets compactés* * uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* * uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* * Tous les objets

N'oubliez pas que les paramètres **Mode de protection**, **Application de la technologie iChecker**, **Application de la technologie iSwift**, **Application de l'analyseur heuristique** et **Vérification de la signature Microsoft des fichiers** ne font pas partie des paramètres des niveaux de protection prédéfinis. Si, après avoir choisi un des niveaux de protection prédéfinis, vous modifiez la valeur des paramètres **Mode de protection**, **Application de la technologie iChecker**, **Application de la technologie iSwift**, **Application de l'analyseur heuristique** ou **Vérification de la signature Microsoft des fichiers**, **le niveau de protection que vous avez défini sera conservé.**

Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

2. Sous l'onglet **Configuration de la zone de la protection** accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le nœud auquel vous souhaitez appliquer un des niveaux de protection prédéfini.

3. Assurez-vous que ce nœud est repris dans la zone d'analyse (cf. rubrique "Constitution de la couverture de protection" à la page 92).

4. Dans la boîte de dialogue **Niveau**, sélectionnez le niveau de protection que vous souhaitez appliquer dans la liste **Niveau de sécurité** (cf. ill. ci-après).

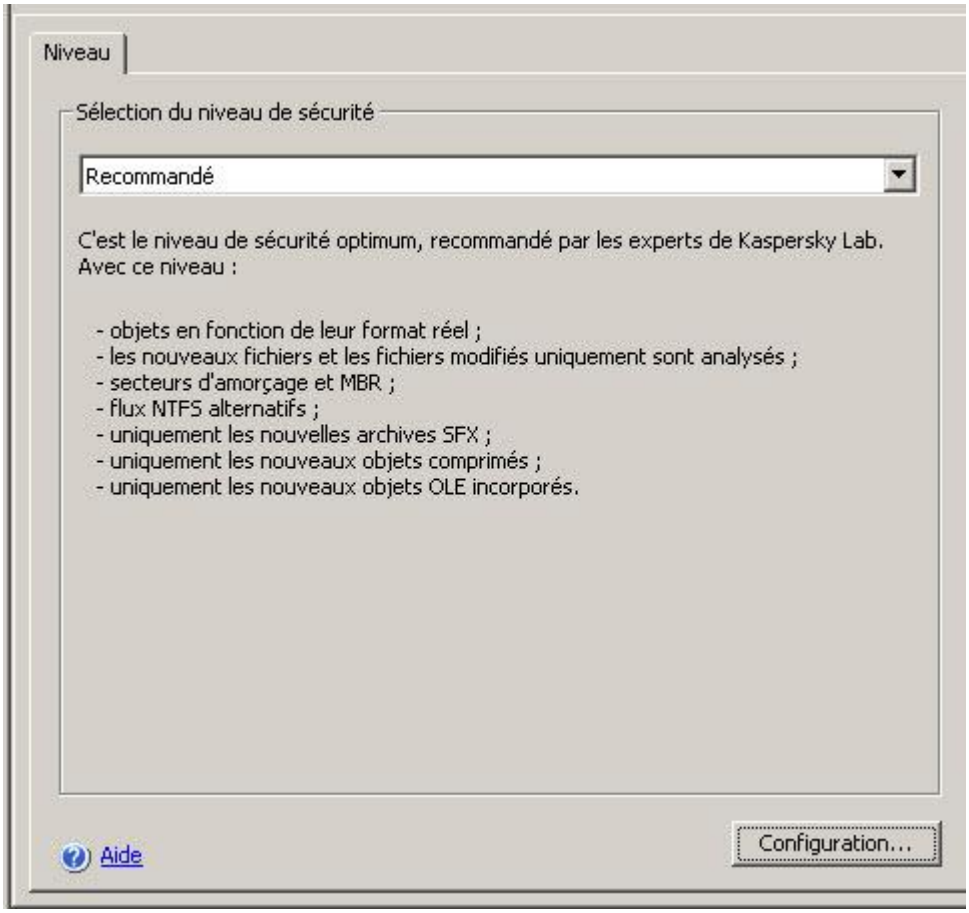


*Illustration 32. Boîte de dialogue **Niveau de sécurité***

5. La boîte de dialogue reprend la liste des valeurs des paramètres de sécurité correspondant au niveau que vous avez sélectionné.

6. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

CONFIGURATION DES PARAMETRES DE PROTECTION DE LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Par défaut, la tâche **Protection en temps réel des fichiers** applique les mêmes paramètres de sécurité à toutes les couvertures de protection. Les valeurs correspondent à celles du niveau prédéfini **Recommandé** (cf. page 95).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la couverture de protection ou avec des variations pour divers nœuds dans l'arborescence des ressources fichier du serveur.

Les paramètres de sécurité que vous définissez pour un nœud sélectionné seront automatiquement appliqués à tous les nœuds qu'il renferme. Toutefois, si vous configurez séparément les paramètres de sécurité du nœud enfant, les paramètres de sécurité du nœud parent ne seront pas appliqués à celui-là.

Pour configurer manuellement les paramètres de sécurité du nœud sélectionné, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

2. Sous l'onglet **Configuration de la zone de la protection** accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le nœud dont vous souhaitez configurer les paramètres de sécurité.

3. Cliquez sur le bouton **Paramètres** dans la partie inférieure de la boîte de dialogue.

   La boîte de dialogue **Paramètres de sécurité** s'ouvre.

   Pour le nœud sélectionné de la couverture de protection, vous pouvez appliquer un modèle contenant une combinaison de paramètres de sécurité (cf. page 101).

4. Configurez les paramètres de sécurité requis pour le nœud sélectionné en fonction de vos exigences. Pour ce faire, exécutez les actions suivantes :

   - Sur l'onglet **Général** (cf. ill. ci-après), réalisez les actions suivantes, le cas échéant :

     - sous le titre **Protection des objets**, indiquez si Kaspersky Anti-Virus analysera tous les objets de la couverture de protection ou uniquement les objets d'un format ou d'une extension déterminé, si Kaspersky Anti-Virus analysera les secteurs d'amorçage des disques et l'enregistrement principal d'amorçage ou les flux NTFS alternatifs – objets à analyser (cf. page 376) ;

     - Sous le titre **Optimisation**, indiquez si Kaspersky Anti-Virus analysera tous les objets dans la couverture sélectionnée ou uniquement les objets nouveaux ou modifiés (cf. page 382) ;

- Sous le titre **Analyse des objets composés**, indiquez les objets composés que Kaspersky Anti-Virus analysera (cf. page 383).

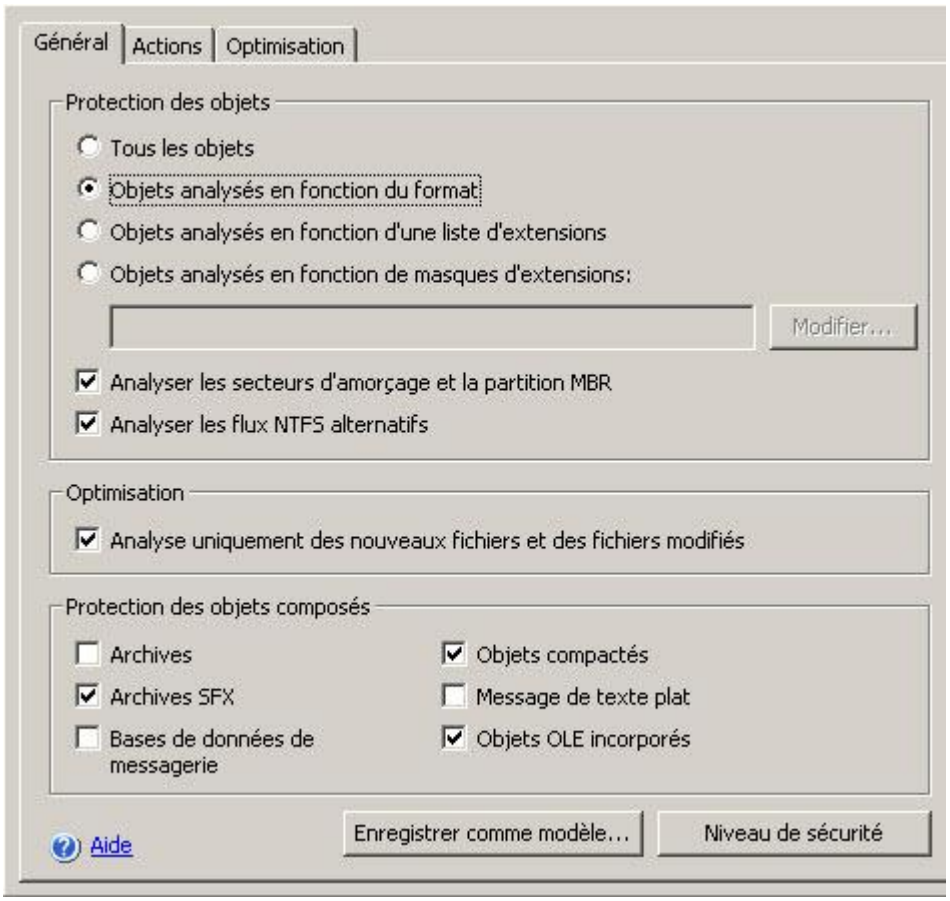


*Illustration 33. Fenêtre de configuration de paramètres de sécurité, onglet **Général***

- Sur l'onglet **Actions** (cf. ill. ci-après), réalisez les actions suivantes, le cas échéant :
  - Sélectionnez action à exécuter sur les objets infectés (cf. page 384) ;
  - Sélectionnez action à exécuter sur les objets suspects (cf. page 386) ;

- Configurez les actions à réaliser sur les objets en fonction du type de la menace découverte (cf. page 378).

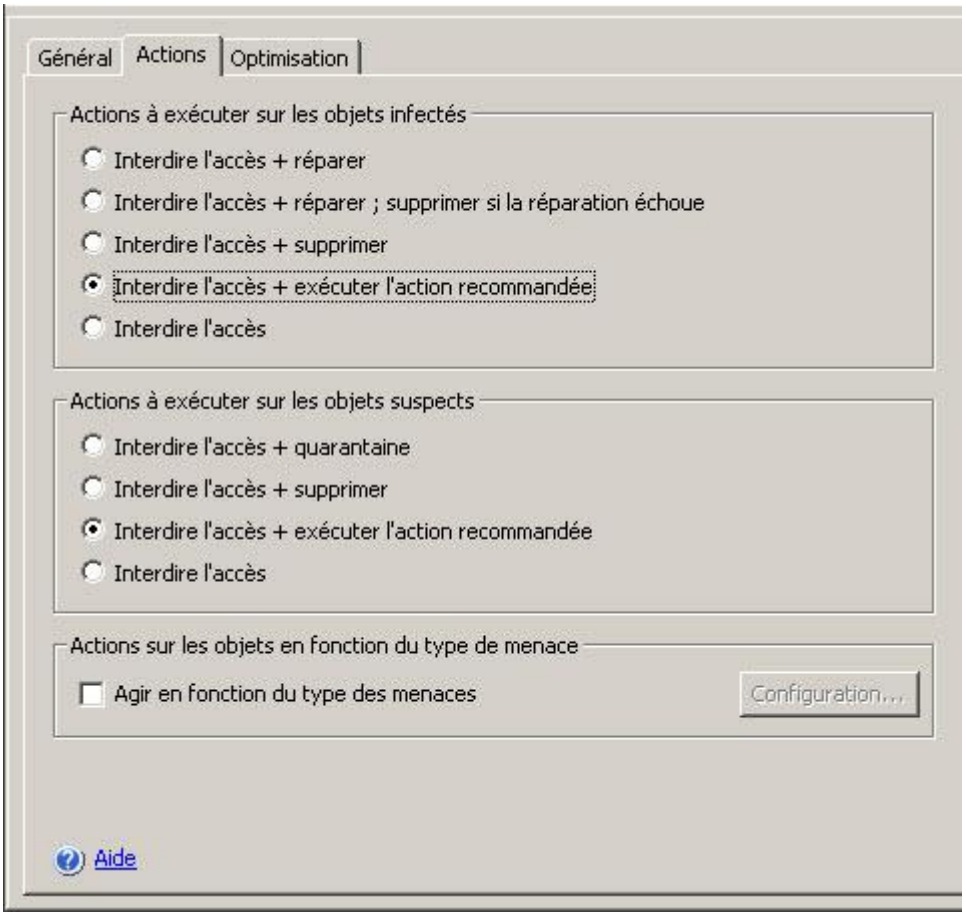


*Illustration 34. Fenêtre de configuration de paramètres de sécurité, onglet **Actions***

- Sur l'onglet **Optimisation** (cf. ill. ci-après), réalisez les actions suivantes, le cas échéant :
  - excluez du traitement les fichiers sur la base du nom ou du masque (cf. page 379) ;
  - excluez du traitement les menaces en fonction du nom ou du masque du nom (cf. rubrique 380) ;
  - indiquez la durée maximale de l'analyse de l'objet (cf. rubrique 388) ;
  - indiquez la Taille maximale de l'objet composé analysé (cf. page 389) ;
  - Activez ou désactivez l'application de la technologie iChecker (cf. page 389).
  - Activez ou désactivez l'application de la technologie iSwift (cf. page 390).

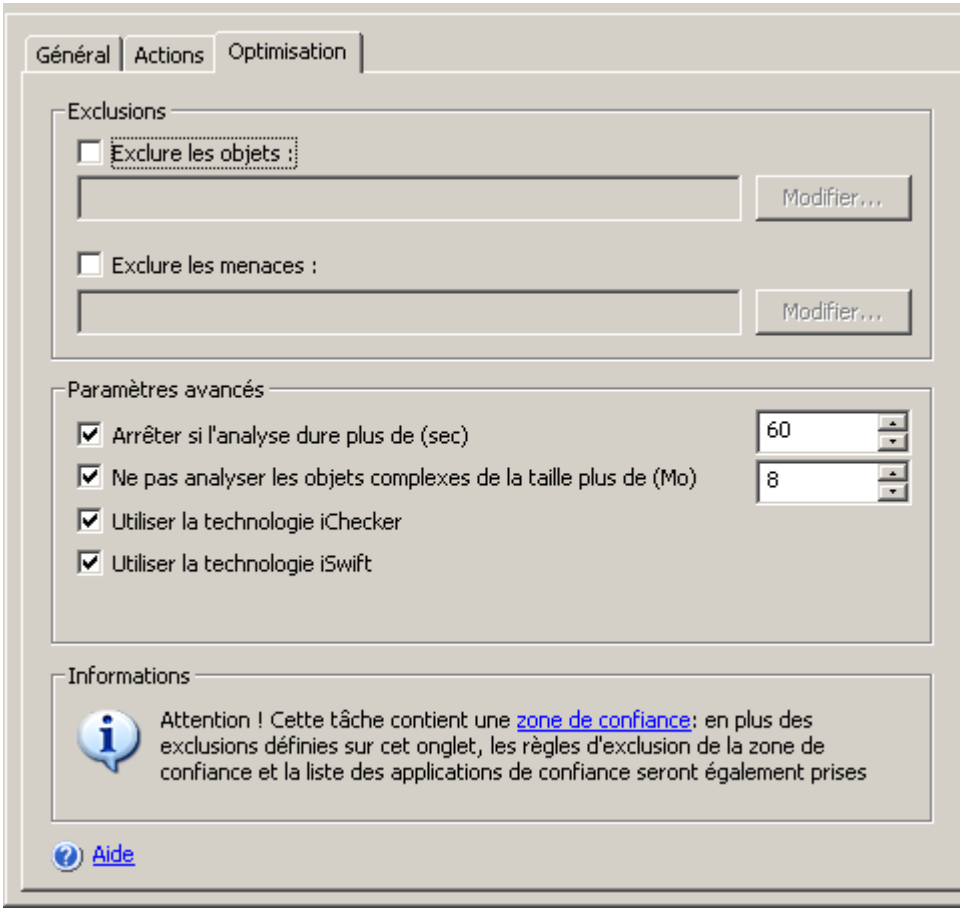


*Illustration 35. Fenêtre de configuration de paramètres de sécurité, onglet **Optimisation***

5. Une fois que vous aurez configuré les paramètres de sécurité requis, ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

UTILISATION DE MODELES DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

DANS CETTE SECTION DE L'AIDE

ENREGISTREMENT DES VALEURS DES PARAMETRES DE SECURITE DANS UN MODELE

Dans la tâche **Protection des fichiers en temps réel**, après avoir configuré les paramètres de sécurité d'un des nœuds de l'arborescence des ressources fichiers du serveur, vous pouvez enregistrer ces valeurs dans un modèle afin de pouvoir les appliquer par la suite à n'importe quel autre nœud.

Pour enregistrer les valeurs des paramètres de sécurité dans un modèle, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

2. Sur l'onglet **Configuration de la zone de la protection** accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le nœud dont vous souhaitez enregistrer les paramètres de sécurité.

3. Cliquez sur le bouton **Paramètres** dans la partie inférieure de la boîte de dialogue.

4. Dans la boîte de dialogue paramètres de la zone de protection, onglet **Général**, cliquez sur le bouton **Enregistrer comme modèle**.

5. Dans la boîte de dialogue **Propriétés du modèle** dans le champ **Nom du modèle**, saisissez le nom du modèle (cf. ill. ci-après).

6. Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.

*Illustration 36. Boîte de dialogue **Propriétés du modèle***

7. Cliquez sur **OK**. Le modèle avec la sélection de paramètres de sécurité sera conservé.

CONSULTATION DES PARAMETRES DE SECURITE DU MODELE

Pour consulter les valeurs des paramètres de sécurité dans le modèle créé, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.

2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez la commande **Modèles des paramètres** (cf. ill. ci-après).

*Illustration 37. Boîte de dialogue **Modèles***

3. Dans la boîte de dialogue **Modèles**, vous verrez la liste des modèles que vous pouvez appliquer à la tâche **Protection en temps réel des fichiers**.

4. Pour consulter les informations relatives au modèle et les valeurs des paramètres de sécurité, sélectionné le modèle requis dans la liste et cliquez sur le bouton **Voir**.

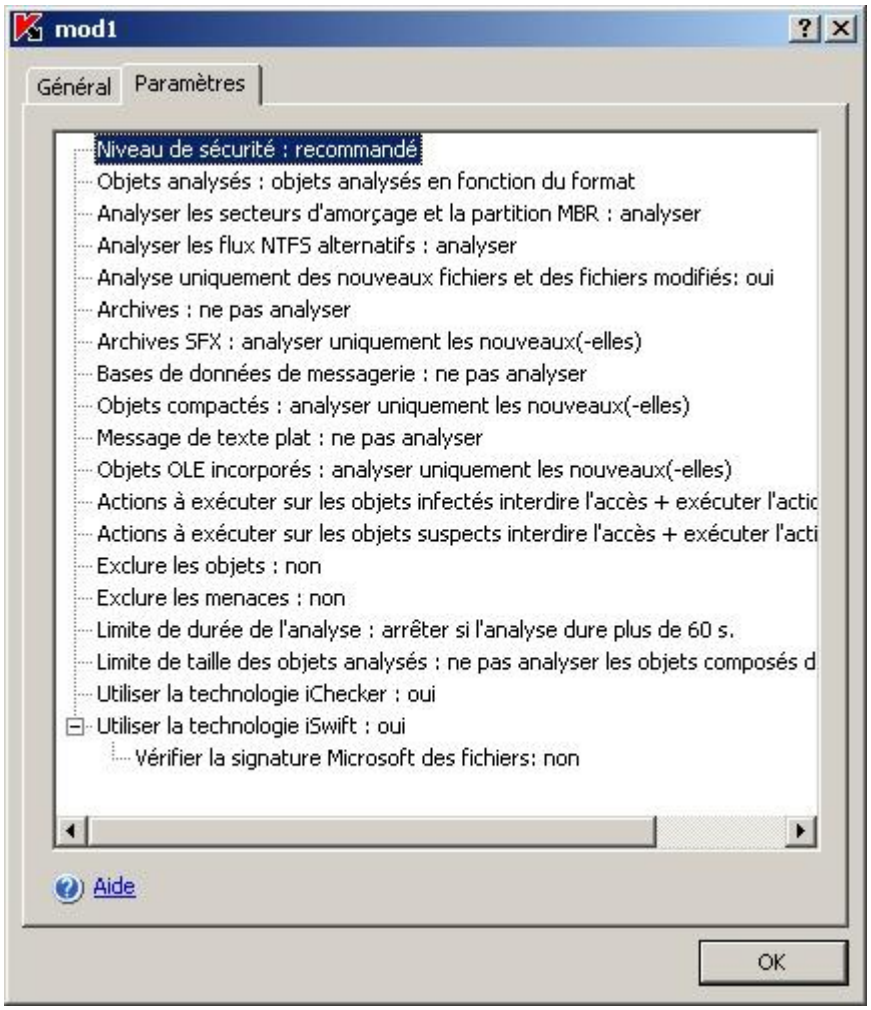


*Illustration 38. Boîte de dialogue **<Nom du modèle>**, onglet **Paramètres***

L'onglet **Général** reprend les noms des modèles et les informations complémentaires sur le modèle ; l'onglet **Paramètres** reprend la liste des valeurs des paramètres de sécurité enregistrés dans le modèle.

APPLICATION DU MODELE

Si vous appliquez le modèle au nœud parent, les paramètres de sécurité du modèle seront appliqués à tous les nœuds enfants, sauf pour les cas suivants :

- Le modèle ne sera pas appliqué aux nœuds pour lesquels vous avez configuré les paramètres de sécurité séparément. Pour définir les paramètres de sécurité du modèle pour tous les nœuds enfants, désélectionnez la case en regard du nœud parent dans l'arborescence des ressources fichier du serveur avant d'appliquer le modèle puis cochez-la à nouveau. Appliquez le modèle au nœud parent. Tous les nœuds enfants auront les mêmes paramètres de sécurité que le nœud parent.

- Le modèle ne sera pas appliqué aux nœuds enfants virtuels. Si vous souhaitez appliquer à un nœud enfant virtuel les paramètres du nœud parent, vous devrez sélectionner le nœud virtuel et appliquer le modèle séparément.

➧ *Pour appliquer le modèle avec la sélection de paramètres de sécurité au nœud sélectionné, procédez comme suit :*

1. Tout d'abord, enregistrez les valeurs des paramètres de sécurité dans un modèle (cf. page 137).

2. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez le nœud subalterne **Protection en temps réel des fichiers**.

3. Sur l'onglet **Configuration de la zone de la protection** accédez au panneau des résultats, dans l'arborescence des ressources fichier du serveur, ouvrez le menu contextuel du menu du nœud auquel vous souhaitez appliquer le modèle et sélectionnez **Appliquer un modèle**.

4. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez appliquer.

5. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

SUPPRESSION DU MODELE

Pour supprimer un modèle, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.

2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez la commande **Modèles des paramètres**.

3. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez supprimer dans la liste et cliquez sur **Supprimer**.

4. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**. Le modèle sélectionné sera supprimé.

CONFIGURATION DE LA TACHE ANALYSE DES SCRIPTS :

L'onglet **Protection en temps réel des fichiers** vous permet de sélectionner le mode de protection des objets (cf. page 375).

Pour sélectionner le mode de protection des objets, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.

2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez **Propriétés**.

3. Dans la boîte de dialogue **Propriétés : Protection en temps réel des fichiers** sous l'onglet **Général**, sélectionnez le mode de protection des objets que vous souhaitez activer et cliquez sur **OK** (cf. ill. ci-après).

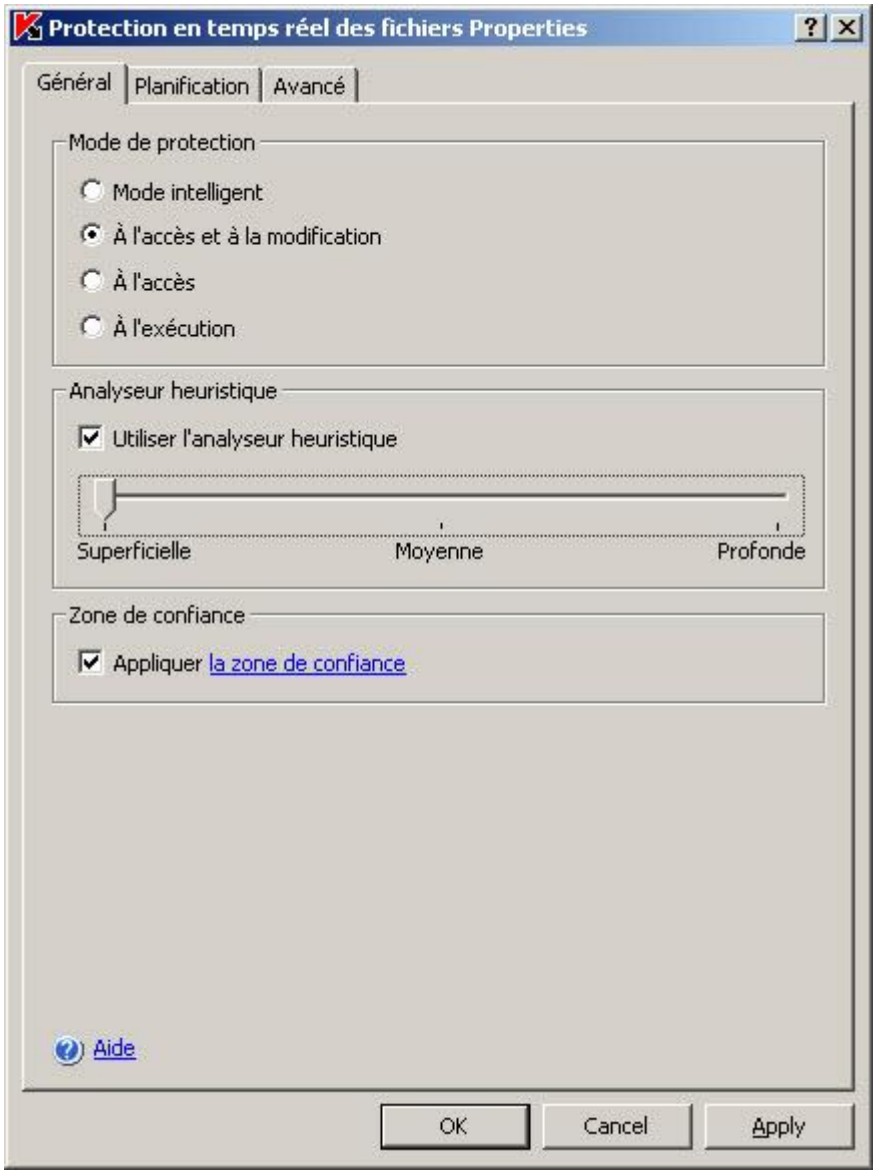


*Illustration 39. Boîte de dialogue **Propriétés Protection en temps réel des fichiers**, onglet **Général***

UTILISATION DE L'ANALYSEUR HEURISTIQUE DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS.

Vous pouvez, dans la tâche **Protection en temps réel des fichiers**, appliquer l'analyseur heuristique (cf. page 393) et configurer le niveau de l'analyse (cf. page 394).

Pour activer l'analyseur heuristique, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez **Propriétés**.
3. Dans l'onglet **Général** de la fenêtre **Protection en temps réel des fichiers Propriétés**, cochez la case **Utiliser l'analyseur heuristique** et ajuster le niveau d'analyse comme souhaité.

Pour désactiver l'analyseur heuristique, décochez la case **Utiliser l'analyseur heuristique**.

4. Cliquez sur **OK.**

STATISTIQUES DE LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Pendant que la tâche **Protection en temps réel des fichiers** est exécutée, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Anti-Virus depuis son lancement jusqu'à maintenant. Ces sont les statistiques de la tâche.

*Pour consulter les statistiques de la tâche **Protection en temps réel des fichiers**, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.
2. Ouvrez la tâche **Protection en temps réel des fichiers**.
3. Sous l'onglet **Consultation et administration** dans le panneau des résultats, cliquez sur le lien **Statistiques complètes** du groupe **Statistiques**.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Anti-Virus a traités depuis le lancement de la tâche jusqu'au moment actuel (cf. tableau ci-dessous).

*Tableau 11. Paramètres de la tâche **Protection en temps réel des fichiers**, **Statistiques complètes***

CHAMP	DESCRIPTION
Menaces détectées	Nombre de menaces détectées ; par exemple, si Kaspersky Anti-Virus a découvert un programme malveillant dans cinq objets, la valeur de ce champ augmentera d'une unité.
Objets infectés détectés	Total des objets infectés détectés
Objets suspects détectés	Nombre total d'objets suspects détectés
Objets non-réparés	Nombre d'objets que Kaspersky Anti-Virus n'a pas pu réparer pour les raisons suivantes : • le type de menace de l'objet ne peut pas être réparé ; • les objets de ce type ne peuvent pas être réparés ; • une erreur s'est produite lors de la réparation.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Anti-Virus aurait du mettre en quarantaine mais sans réussir à cause d'une erreur tel que le manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Anti-Virus a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone d'analyse que Kaspersky Anti-Virus n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre d'objets dont les copies auraient du être placées par Kaspersky Anti-Virus en sauvegarde mais qui n'ont pas pu l'être en raison d'une erreur.
Erreurs d'analyse	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets réparés	Nombre d'objets réparés par Kaspersky Anti-Virus.
Placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Anti-Virus.
Objets sauvegardés	Nombre d'objets dont une copie a été mise en sauvegarde par Kaspersky Anti-Virus.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Anti-Virus.
Objets protégés par mot de passe	Nombre d'objets (archives comprimées, par exemple) que Kaspersky Anti-Virus a ignorés en raison d'une protection par mot de mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Anti-Virus a ignorés à cause de leur format endommagé.
Objets analysés	Nombre total d'objets analysés par Kaspersky Anti-Virus.

CONFIGURATION DE LA TACHE ANALYSE DES SCRIPTS

La tâche prédéfinie **Analyse des scripts** possède par défaut les paramètres définis dans le tableau suivant. Vous pouvez modifier les valeurs de ces paramètres et configurer la tâche.

*Tableau 12. Paramètres par défaut de la tâche **Analyse des scripts***

PARAMETRE	VALEUR PAR DEFAUT	DESCRIPTION
Exécution des scripts infectés	Interdit	Kaspersky Anti-Virus interdit toujours l'exécution des scripts qu'il considère infectés.
Exécution des scripts suspects	Interdit	Vous pouvez préciser les actions que Kaspersky Anti-Virus exécutera sur les scripts qu'il considère suspect : autoriser ou interdire l'exécution.
Analyseur heuristique	Le niveau de protection **Moyen** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyseur heuristique (cf. page 393) et régler le niveau de l'analyse.
Zone de confiance	Appliquée La liste des exclusions est vide	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées. Création et application de la zone de confiance (cf. page 178)

*Pour configurer la tâche **Analyse des scripts**, procédez comme suit :*

1. Dans l'arborescence de la console, déployez le nœud **Protection en temps réel** et sélectionnez la tâche **Analyse des scripts** (cf. ill. ci-après)**.**

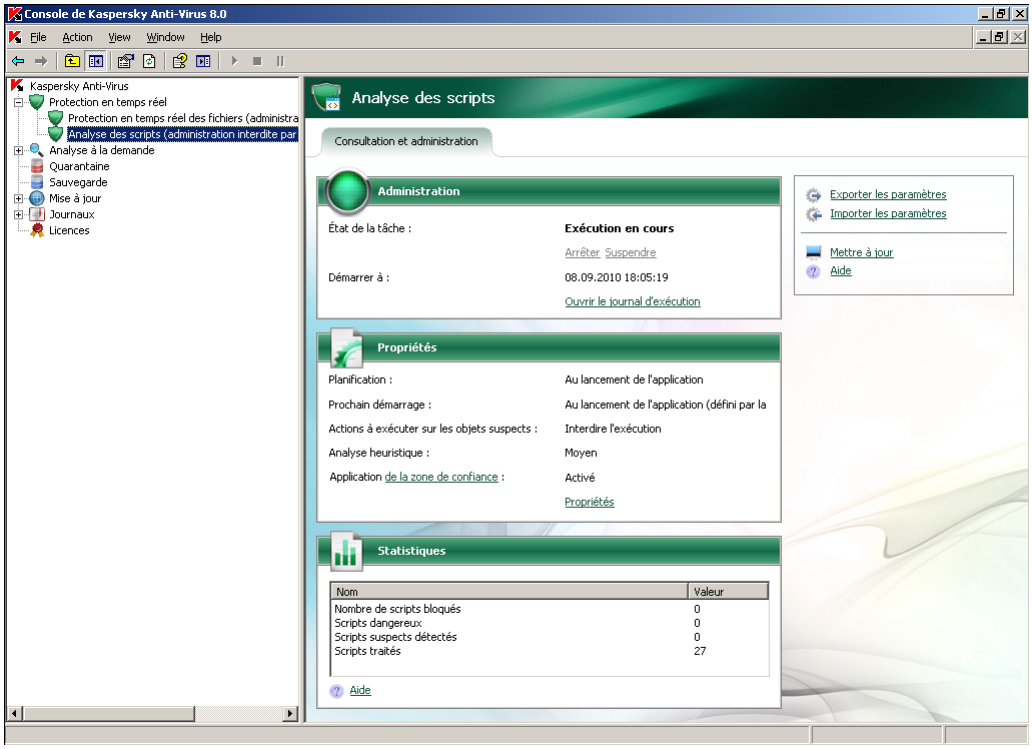


*Illustration 40. Tâche **Analyse des scripts***

Cliquez sur le lien **Propriétés** pour ouvrir la boîte de dialogue **Propriétés : Analyse des scripts** (cf. ill. ci-après)**.**

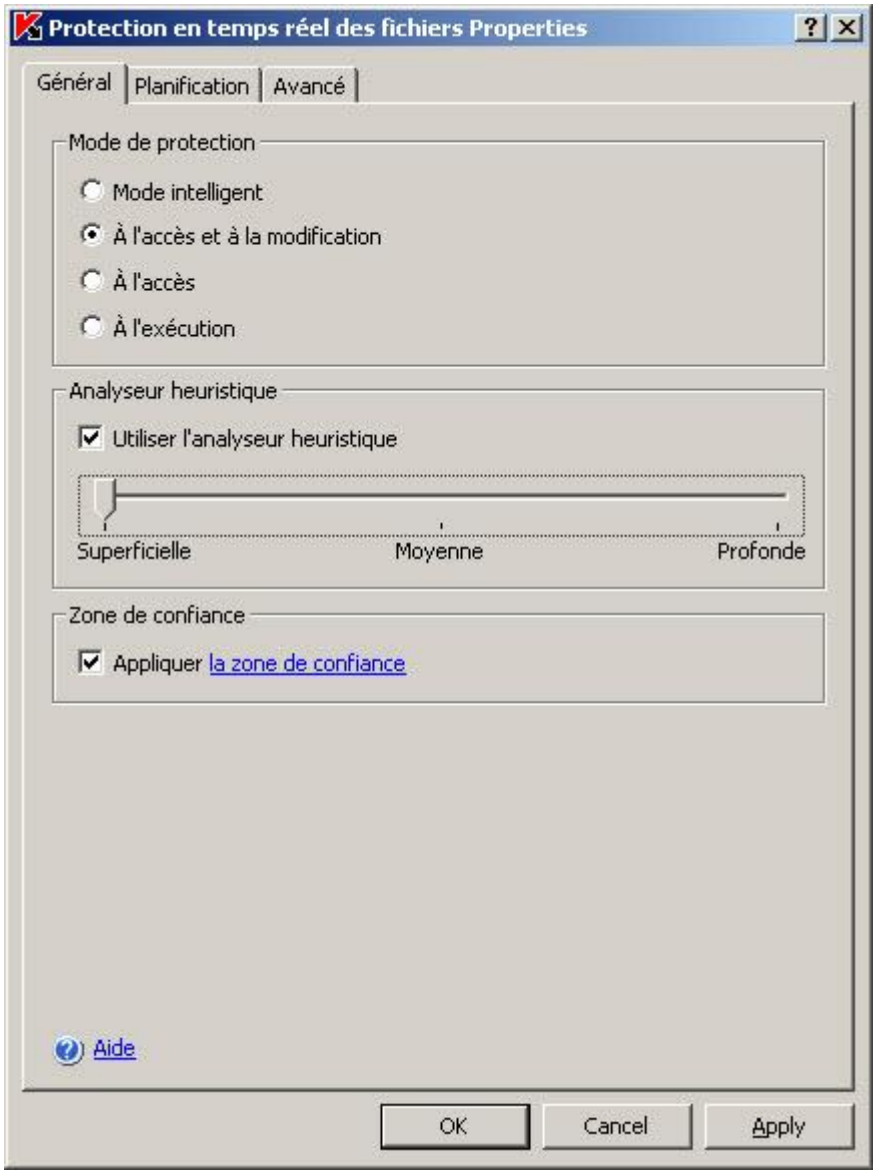


*Illustration 41. La boîte de dialogue **Propriétés : Analyse des scripts***

2. Dans le groupe de paramètres **Actions sur les scripts suspects**, autorisez ou interdisez l'exécution des scripts suspects : Pour ce faire, exécutez les actions suivantes :

   - pour autoriser l'exécution des scripts suspects, sélectionnez l'option **Autoriser l'exécution** ;
   - pour interdire l'exécution des scripts suspects, sélectionnez l'option **Interdire l'exécution**.

3. Dans le groupe de paramètres **Analyseur heuristique**, procédez aux configurations suivantes :

   - Pour activer l'utilisation de l'analyseur heuristique (cf. ill. 393), cochez la case **Utiliser l'analyseur heuristique**. Pour modifier le niveau d'analyse, déplacez le curseur à l'endroit souhaité.
   - Pour désactiver l'analyseur heuristique, décochez la case **Utiliser l'analyseur heuristique**.

4. Dans le groupe de paramètres **Zone de confiance**, activez ou désactivez l'application de la zone de confiance comme suit :

- pour activer l'application de la zone de confiance, cochez la case **Appliquer la zone de confiance** ;
- pour activer l'application de la zone de confiance, cochez la case **Appliquer la zone de confiance** ;

Pour savoir comment ajouter des scripts à la liste des exclusions de la zone de confiance (cf. page 182)

5. Dans la boîte de dialogue **Analyse des scripts Propriétés** cliquez sur **OK** afin de conserver les modifications.

STATISTIQUES DE LA TACHE ANALYSE DES SCRIPTS

Pendant que la tâche **Analyse des scripts** est exécutée, vous pouvez consulter en temps réel des informations détaillées sur le nombre de scripts traités par Kaspersky Anti-Virus depuis son lancement jusqu'à maintenant. Ces sont les statistiques de la tâche.

Pour consulter les statistiques de la tâche, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Protection en temps réel**.
2. Sélectionnez la tâche **Analyse des scripts**.

   Vous pouvez consulter les paramètres de la tâche **Analyse des scripts** (cf. tableau ci-dessous).

Tableau 13. Paramètres de la tâche Analyse des scripts, Statistiques complètes

CHAMP	DESCRIPTION
Scripts bloqués	Nombre de script dont l'exécution a été interdite par Kaspersky Anti-Virus
Scripts dangereux découverts	Nombre de scripts dangereux découverts
Scripts suspects découverts	Nombre de scripts suspects découverts
Scripts traités	Nombre total de scripts traités

BOITES DE DIALOGUE : PROTECTION EN TEMPS REEL

DANS CETTE SECTION DE L'AIDE

NŒUD PROTECTION EN TEMPS REEL

L'entrée **Protection en temps réel** permet de gérer la protection en temps réel des fichiers et l'analyse des scripts. Elle se compose des sous-entrées **Protection en temps réel des fichiers** et **Analyse des scripts**.

L'entrée **Protection en temps réel des fichiers** permet d'arrêter ou de démarrer des tâches de protection en temps réel des fichiers, de planifier ces tâches, d'afficher des statistiques de performances et de configurer des paramètres de protection.

L'entrée **Analyse des scripts** permet de stopper ou lancer la surveillance des tâches de script, de planifier ces tâches, d'afficher des statistiques et de configurer les paramètres de cette surveillance.

Pour travailler avec des tâches de **protection en temps réel des fichiers** ou **d'analyse des scripts**, sélectionnez l'onglet approprié dans l'arborescence de la console.

Panneau de résultats

Le panneau de résultats affiche l'état actuel des tâches de protection en temps réel :

- **Nom de tâche** : **Protection en temps réel des fichiers** et **Analyse des scripts**.
- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**).
- **Heure de démarrage** : **date et heure de démarrage de la tâche.** L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Planification** : conditions de lancement d'une tâche programmée
- **Prochain démarrage** : heure prévue pour le prochain lancement de la tâche programmée.

VOIR EGALEMENT

Présentation des tâches de la protection en temps réel 87

Configuration de planification des tâches en MMC 50

Configuration de la tâche Protection en temps réel des fichiers 87

Configuration de la tâche Analyse des scripts 108

NŒUD PROTECTION EN TEMPS REEL DES FICHIERS

La tâche **Protection en temps réel des fichiers** surveille les objets présents sur le serveur sécurisé, qui ont été ouverts par les applications des postes de travail.

L'entrée **Protection en temps réel des fichiers** permet d'arrêter ou de démarrer des tâches de protection en temps réel des fichiers, de planifier ces tâches, d'afficher des statistiques de performances et de configurer des paramètres de protection.

Le panneau de résultats contient deux onglets : **Consultation et administration** et **Configuration de la zone de protection**.

Onglet Consultation et administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**).
- **Heure de démarrage** – **date et heure de démarrage de la tâche.**

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Le bloc **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, au mode de protection des objets, à l'utilisation de l'analyseur heuristique et à l'application de la zone de confiance.

Le tableau contient la liste des couvertures ainsi que les niveaux de protection appliqués à chacune d'entre elles.

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

Configuration de la zone de protection (onglet)

L'onglet **Couverture d'analyse** présente l'arborescence des ressources fichiers du serveur. La partie inférieure de la fenêtre présente des informations relatives aux paramètres de protection du nœud sélectionné.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Enregistrer la tâche** : enregistre les modifications apportées aux valeurs des paramètres de la tâche.
- **Modèles de paramètres** : affiche la liste des modèles créés contenant des paramètres de protection.
- **Exporter les paramètres/Importer les paramètres** : exporte les paramètres de tâche dans un fichier ou les restaure à partir d'un fichier. Dans ce cas, l'enregistrement ou la restauration s'applique aux éléments suivants :
  - Couverture de protection et paramètres de chacune des zones de protection
  - Modèles de paramètres personnalisés
- **Propriétés** : sélectionne le régime de protection des objets et configurer les paramètres du lancement/de l'arrêt automatique de la tâche.

VOIR EGALEMENT

Configuration de la tâche Protection en temps réel des fichiers 87

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Statistiques de la tâche Protection en temps réel des fichiers 107

ONGLET CONSULTATION ET ADMINISTRATION. PROTECTION EN TEMPS REEL DES FICHIERS

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**).
- **Heure de démarrage – date et heure de démarrage de la tâche.**

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Le bloc **Propriétés** contient les informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche, à l'utilisation de l'analyseur heuristique, à l'application de la zone de confiance et à d'autres propriétés de la tâche.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

VOIR EGALEMENT

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Configuration de planification des tâches en MMC 50

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

Statistiques de la tâche Protection en temps réel des fichiers 107

Statistiques de la tâche Analyse des scripts 111

CONFIGURATION DE LA ZONE DE PROTECTION (ONGLET) PROTECTION EN TEMPS REEL DES FICHIERS

Sous l'onglet **Configuration de la zone de la protection**, la partie supérieure du panneau de résultats représente l'arborescence des ressources fichiers du serveur. La partie inférieure de la fenêtre présente des informations relatives aux paramètres de protection du nœud sélectionné.

Vous pouvez modifier la présentation de l'onglet **Configuration de la zone d'analyse**. Pour ce faire, dans le menu contextuel de la tâche de protection en temps réel, choisissez l'option **Apparence**, puis choisissez une des options proposées pour la présentation de cet onglet : **Hiérarchie horizontale**, **Hiérarchie verticale**, **Liste horizontale**, **Liste verticale**.

L'arborescence des ressources fichiers du serveur contient les nœuds suivants :

- **Poste de travail** : cette entrée contient tous les disques durs et les unités amovibles du serveur, avec leurs fichiers et leurs dossiers, ainsi que l'environnement réseau, les unités virtuelles et les couvertures de protection *virtuelles ajoutées par l'administrateur*.

En plus des dossiers, fichiers, unités fixes ou amovibles, Kaspersky Anti-Virus peut analyser les unités, fichiers et dossiers créés de manière dynamique sur le serveur par des applications ou des services, aussi bien que les unités connectées temporairement, comme les unités de cluster partagées. Ces objets peuvent être ajoutés à l'arborescence des fichiers du serveur en tant que couvertures de protection virtuelles : *unité virtuelle*, *dossier virtuel*, *fichier virtuel*.

- **Disques durs** : cette entrée contient tous les disques durs avec leurs dossiers et fichiers, ainsi que dossiers et fichiers virtuels ajoutés par l'administrateur.

- **Disques amovibles** : cette entrée contient tous les supports amovibles connectés au serveur sécurisé, y compris les disquettes, les CD-ROM et les unités flash USB, avec leurs fichiers et dossiers, ainsi que dossiers et fichiers virtuels ajoutés par l'administrateur.

- **Emplacements réseau** : cette entrée permet d'analyser tous les objets placés sur des ressources réseau auxquelles peuvent accéder les applications installées sur le serveur sécurisé. Kaspersky Anti-Virus n'analysera

pas les objets des ressources réseau consultés par des applications d'autres postes de travail. Le nœud peut inclure des dossiers et des fichiers de réseau ajoutés par l'administrateur. La configuration de leur protection peut se faire individuellement.

- **Unités virtuelles** : cette entrée contient les unités virtuelles, avec leurs dossiers et fichiers, ajoutées par l'administrateur.

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrées de la manière suivante :

☑ Nœud repris dans la couverture de protection.

☐ Nœud exclu de la couverture de protection.

☑ Au moins un des nœuds intégrés à ce nœud est exclu de la couverture de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

N'oubliez pas que le nœud parent sera indiqué par l'icône ☑ si vous sélectionnez tous les nœuds et non pas le nœud parent. Dans ce cas, les fichiers et les répertoires qui se trouvent dans ce nœud ne seront pas automatiquement inclus dans la couverture de protection. Pour les inclure, il faudra inclure le nœud parent dans la couverture de protection. Ou vous pouvez également créer des "copies virtuelles" dans la console de Kaspersky Anti-Virus et les ajouter à la couverture de protection.

"Niveau de sécurité" (fenêtre)

Dans la fenêtre **Niveau de sécurité**, vous pouvez sélectionner l'un des niveaux de protection prédéfinis pour le nœud sélectionné ou ouvrir une fenêtre permettant de configurer les paramètres de protection avancés.

La protection des fichiers est fixée par défaut sur le niveau de sécurité **Recommandé**. Pour définir un autre niveau, choisissez une des valeurs suivantes de la liste déroulante **Niveau de protection** :

- La **vitesse maximum** ce niveau offre la vitesse la plus grande avec un niveau légèrement moindre de protection antivirus.

  Vous pouvez choisir de niveau de protection si votre réseau dispose, en plus de Kaspersky Anti-Virus, d'autres mécanismes de sécurité des pare-feu ou des stratégies de sécurité pou les utilisateurs, par exemple.

  Utilisez ce niveau de protection si vous devez garantir spécialement la vitesse d'échange des fichiers sur le serveur sécurisé.

- **Recommandé** : Kaspersky Lab considère ce niveau comme suffisant pour protéger les serveurs de fichiers sur la plupart des réseaux. Il combine de manière optimale la qualité de protection et la productivité du serveur.

- **Protection maximum** : le niveau le plus complet pour la surveillance des fichiers ouverts, modifiés ou exécutés. Ce niveau assure la protection antivirus la plus grande possible, avec une légère diminution de rendement du système.

Pour configurer manuellement la protection en temps réel, cliquez sur **Configuration**.

Si les paramètres de protection **en temps réel n'ont pas les valeurs par défaut, le niveau** Personnalisé sera automatiquement sélectionné dans la liste Niveau de sécurité.

Pour appliquer les modifications, cliquez sur le bouton **Enregistrer** dans la barre d'outils ou utilisez la même commande dans le menu contextuel de l'entrée **Protection en temps réel des fichiers**.

VOIR EGALEMENT

Sélection des niveaux prédéfinis de protection dans la tâche Protection en temps réel des fichiers 95

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

PROPRIETES DE LA TACHE : ONGLET GENERAL. ANALYSE DES SCRIPTS

Cet onglet vous permet de configurer les actions de Kaspersky Anti-Virus quand celui-ci détecte des scripts suspects, l'utilisation de l'analyseur heuristique et l'application de la zone de confiance.

Sélection des actions à exécuter sur les scripts suspects

Si la tâche **Analyse des scripts** est en exécution, Kaspersky Anti-Virus analyse le code VBScript et JScript avant son exécution par le module interpréteur du système d'exploitation, interdit les scripts dangereux et applique l'action spécifiée par les paramètres aux scripts suspects.

Les scripts suspects sont interdits par défaut.

Pour bloquer ou autoriser l'exécution de scripts suspects, sélectionnez une des options suivantes :

- **Autoriser l'exécution**.
- **Interdire l'exécution**.

Analyseur heuristique

L'option **Utiliser l'analyseur heuristique** permet d'activer/désactiver l'utilisation de l'analyseur heuristique. Le curseur placé sous l'option permet de modifier le niveau d'analyse mis en œuvre par l'analyseur heuristique.

Zone de confiance

La case **Appliquer la zone de confiance** cochée signifie que lors de l'exécution de la tâche, les objets qui répondent aux règles d'exclusion utilisées par le composant **Analyse des scripts** seront exclus. Pour afficher ou modifier les règles d'exclusion, cliquez le lien repris dans le nom de la case. Dans la fenêtre **Zone de confiance** qui s'ouvre, ouvrez l'onglet **Règles d'exclusion**. Cette case est cochée par défaut.

VOIR EGALEMENT

Utilisation de l'analyseur heuristique 393

Niveau d'analyse 394

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

PROPRIETES DE LA TACHE : ONGLET GENERAL. PROTECTION EN TEMPS REEL DES FICHIERS

Mode de protection

Pour ce faire, sélectionnez l'une des options de la section **Mode de protection** :

- **Mode intelligent** : Le programme antivirus analyse le fichier lors de sa première ouverture et de sa fermeture définitive, si le fichier a été modifié. Si le même processus ouvre et referme plusieurs fois un fichier dans la session, toutes les opérations transitoires sont ignorées par l'analyseur. Ce mode est destiné à accélérer le traitement des objets sans réduire la qualité de la protection sur le serveur.
- **Ouverture et modification** : Le fichier est analysé à l'ouverture ou lorsqu'il est exécuté et après enregistrement si le fichier a été modifié (sélection par défaut).

- **Ouverture** : Les fichiers sont analysés à l'ouverture ou à leur exécution uniquement.
- **Exécution** : Le fichier n'est analysé qu'au moment de son exécution.

Analyseur heuristique

L'option **Utiliser l'analyseur heuristique** permet d'activer/désactiver l'utilisation de l'analyseur heuristique. Le curseur placé sous l'option permet de modifier le niveau d'analyse mis en œuvre par l'analyseur heuristique.

Zone de confiance

Si la case **Appliquer la zone de confiance** est cochée dans la rubrique **Zone de confiance**, Kaspersky Anti-Virus exclura de l'analyse les opérations sur les fichiers des processus de confiance ainsi que les objets qui répondent aux règles d'exclusion utilisées par le composant **Protection en temps réel des fichiers**. Pour afficher ou modifier la liste des processus de confiance et des règles d'exclusion, cliquez le lien repris dans le nom de la case. Si la case **Appliquer la zone de confiance** n'est pas cochée, seuls les objets définis dans les paramètres de la tâche **Protection en temps réel des fichiers** à l'onglet **Optimisation** seront exclus de l'analyse. Cette case est cochée par défaut.

VOIR EGALEMENT

Mode de protection 375

Utilisation de l'analyseur heuristique 393

Niveau d'analyse 394

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET GENERAL. PROTECTION EN TEMPS REEL DES FICHIERS

L'onglet **Général** affiche les paramètres d'analyse à la demande qui déterminent quels fichiers seront explorés à la recherche de code malfaisant.

Sélectionnez l'une des options d'analyse suivantes dans la section **Protection des objets** :

- Analyser tous les **objets** : analyse tous les fichiers sans exception.
- **Objets analysés en fonction du format**- analyse tous les objets potentiellement infectés. La décision d'analyser dépend du format de fichier. Avant de rechercher des virus dans un objet, le format du fichier est identifié (fichier texte, archives de messagerie, etc.). Si ce format se trouve sur la liste des formats de fichiers potentiellement infectés, le fichier est transmis à Kaspersky Anti-Virus pour analyse.

  La liste de ces formats est élaborée par les experts de Kaspersky Lab. Elle fait partie de la base de Kaspersky Anti-Virus qui est mise à jour en même temps que celle-ci.

  Si vous sélectionnez cette option, les échanges de fichiers avec le serveur sécurisé seront plus lents qu'avec l'option d'analyse en fonction de l'extension, bien que la qualité de l'analyse soit meilleure.

  Un certain nombre de formats de fichiers ne présentent qu'un léger risque que du code malveillant ait été inséré et qu'il puisse être activé par la suite. Un fichier texte en est un exemple.

- **Objets analysés en fonction d'une liste d'extensions** : analyse uniquement les fichiers potentiellement infectés. La décision d'analyser dépend de l'extension de fichier. Si l'extension se trouve dans la liste des extensions de fichiers potentiellement infectés, le fichier sera transmis à Kaspersky Anti-Virus pour analyse.

La liste des extensions est élaborée par les experts de Kaspersky Lab. Elle fait partie de la base de Kaspersky Anti-Virus qui est mise à jour en même temps que celle-ci.

Cette option accélère la vitesse d'échange de fichiers entre l'application et le serveur sécurisé, mais Kaspersky Anti-Virus pourra ignorer un objet si son extension a été modifiée.

n'oubliez pas que quelqu'un peut transmettre à votre ordinateur un virus avec l'extension.txt, alors qu'il s'agit en fait d'un fichier exécutable renommé à fichier.txt. Si vous sélectionnez l'option **Objets analysés en fonction d'une liste d'extensions**, un tel fichier sera ignoré au cours du processus d'analyse. En revanche, si vous choisissez **Objets analysés en fonction du format**, alors quelle que soit l'extension, l'application détectera le format .exe et analysera le fichier.

- **Objets analysés en fonction de masques d'extensions**- analyse uniquement les objets qui répondent à la liste des extensions et des masques d'extensions créés par l'administrateur. Si cette option a été choisie, cliquez sur **Modifier** pour modifier la liste des extensions ou pour utiliser la liste prédéfinie (cf. page 172).

Cochez Analyser **les secteurs d'amorçage et la partition MBR** pour protéger les secteurs d'amorçage et l'enregistrement de démarrage (MBR). Si la case de la couverture d'analyse prédéfinie **Poste de travail** est cochée, les secteurs d'amorçage et la partition MBR des disques fixes ou amovibles seront analysés. Cette case n'est pas disponible pour les objets des Emplacements réseau.

Sélectionnez **Analyser les flux NTFS alternatifs** si vous souhaitez analyser les flux supplémentaires de fichiers et de dossiers sur les unités NTFS.

Dans la rubrique **Optimisation**, cochez la case **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** afin d'analyser uniquement les fichiers que Kaspersky Anti-Virus reconnaît comme neufs ou modifiés depuis la dernière analyse. Ce mode réduit considérablement la durée de l'analyse et augmente la vitesse de traitement de Kaspersky Anti-Virus. Si la case n'est pas cochée, tous les fichiers seront analysés. L'effet de ce paramètre touche aussi bien les objets simples que les objets composés.

Les fichiers composés peuvent contenir plusieurs objets et chacun de ceux-ci peut à son tour contenir plusieurs pièces jointes. archives, fichiers contenant des macros, des tableaux, des messages avec des pièces jointes, etc.

L'analyse des objets composés dure un certain temps. En ignorant ces objets au cours de l'analyse, vous augmenterez l'analyse des fichiers et la productivité du serveur de fichiers.

Dans la section **Protection des objets composés**, spécifiez les types d'objets composés qu'il faudra absolument soumettre à la recherche de virus. Par défaut, Kaspersky Anti-Virus analyse uniquement les fichiers composés qui appartiennent aux types les plus exposés aux infections et les plus dangereux pour les serveurs. Vous pouvez aussi configurer le traitement de nombreux types d'objets composés. Si la case **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** n'est pas cochée dans la rubrique **Optimisation**, il est possible de sélectionner un mode d'analyse pour chacun des types d'objets composés représentés dans la liste : analyser tous les fichiers ou uniquement ceux que Kaspersky Anti-Virus considère comme neufs ou modifiés depuis la dernière analyse. Pour ce faire, cliquez sur le lien situé en regard du nom du type. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si la case **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** est cochée, Kaspersky Anti-Virus analysera uniquement les nouveaux fichiers ainsi que les fichiers modifiés, y compris les fichiers composés, et la sélection du type d'analyse pour les objets composés n'est pas accessible.

Pour configurer le traitement d'objets composés, cochez les cases correspondantes :

- **Toutes les archives/uniquement les nouvelles archives** : analyse les archives au format ZIP, CAB, RAR, ARJ ou autres.

  Kaspersky Anti-Virus analyse la majorité des formats d'archivage existant dans l'actualité. Cependant, il ne neutralise les objets rencontrés que dans les archives au format .zip, .rar, .arj et .cab.

- **Tous les archives/les nouveaux archives SFX** : analyse les archives contenant un module d'auto-extraction. Ces archives se présentent sous l'aspect d'un fichier exécutable.

- **Toutes les/les nouvelles bases de données de messagerie**- analyse les bases de messagerie de Microsoft Outlook et de Microsoft Outlook Express.

- **Tous les/les nouveaux objets compactés** : analyse les fichiers exécutables comprimés par des utilitaires de compactage du code binaire, comme par exemple UPX ou ASPack. Ce type d'objet composé contient plus souvent des menaces que les autres.

- **Tous les/les nouveaux messages de texte plat** : analyse les fichiers de messagerie, tels que les courriers de Microsoft Outlook ou Microsoft Outlook Express.

- **Tous les/Les nouveaux objets OLE incorporés** : analyse les fichiers incorporés dans des objets (tableurs Excel, une macro Microsoft Word, pièces jointes, etc.). Les documents Microsoft Office contiennent souvent des objets exécutables qui peuvent renfermer des menaces.

Vous pouvez enregistrer les paramètres sélectionnés sous forme de modèle. Ce modèle pourra servir pour configurer les paramètres de protection des autres entrées. Cliquez sur **Enregistrer comme modèle**... pour enregistrer le modèle.

Pour configurer les paramètres en fonction des niveaux de sécurité prédéfinis de Kaspersky Lab, cliquez sur le bouton **Niveau de sécurité**.

Pour appliquer les modifications, cliquez sur le bouton **Enregistrer** dans la barre d'outils ou utilisez la même commande dans le menu contextuel de l'entrée **Protection en temps réel des fichiers**.

VOIR EGALEMENT

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET ACTIONS. PROTECTION EN TEMPS REEL DES FICHIERS

L'onglet **Actions** affiche les paramètres qui déterminent la réponse de Kaspersky Anti-Virus après une analyse. Les objets non infectés sont ignorés. Vous pouvez configurer le traitement des autres objets en fonction de leur état, attribué par l'analyse, ou du type de menace détecté.

Certains types de menaces sont plus dangereux que d'autres pour le serveur. Par exemple, un cheval de Troie peut causer plus de dommages qu'un logiciel publicitaire (adware).

Vous pouvez spécifier les différentes actions de Kaspersky Anti-Virus, en fonction du type de menace contenu dans l'objet.

Par défaut, Kaspersky Anti-Virus traite les objets en fonction de l'état attribué par l'analyse : les fichiers infectés sont réparés, les fichiers suspects sont envoyés en quarantaine. Avant traitement (réparé ou supprimé), l'exemplaire original est enregistré dans la zone de sauvegarde.

Vous pouvez modifier les valeurs attribuées ou configurer l'ordre de traitement de l'objet en fonction du type de menace détectée par Kaspersky Anti-Virus.

Pour analyser les objets en fonction de l'état attribué pendant l'analyse, sélectionnez l'une des options suivantes dans les sections **Actions à exécuter sur les objets infectés** et **Actions à exécuter sur les objets suspects** :

- **Interdire l'accès + réparer** (applicable uniquement aux objets infectés). Kaspersky Anti-Virus verrouille l'accès au fichier. Si c'est possible, l'objet est réparé et la version réparée est enregistrée sur disque, pour remplacer l'original. La version originale sera enregistrée dans la zone de sauvegarde. Si l'objet ne peut pas être réparé, il est laissé sur le disque dans son état d'origine. Une fois la procédure terminée, l'objet est de nouveau accessible. Nous vous recommandons de supprimer les objets qui ne peuvent pas être réparés.

- **Interdire l'accès + réparer ; supprimer si la réparation est impossible** (uniquement pour les objets infectés). Kaspersky Anti-Virus verrouille l'accès au fichier. Si c'est possible, l'objet est réparé et la version réparée est enregistrée sur disque, pour remplacer l'original. Une fois la procédure terminée, l'objet est de nouveau accessible. Si l'objet ne peut pas être réparé, Kaspersky Anti-Virus le supprime et en conserve une copie dans la zone de sauvegardé.

- **Interdire l'accès + supprimer**. Kaspersky Anti-Virus interdira l'accès au fichier, et le supprimera de l'unité du serveur sécurisé. La version originale sera enregistrée dans la zone de sauvegarde.

- **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus verrouille l'accès au fichier et prend une action déterminée automatiquement d'après les recommandations des experts de Kaspersky Lab. La version originale sera enregistrée dans la zone de sauvegarde. Une fois la procédure terminée, l'objet est de nouveau accessible.

- **Interdire l'accès**. Kaspersky Anti-Virus verrouille l'accès au fichier et enregistre des informations sur l'objet détecté dans le rapport, si l'enregistrement de ce type d'événement est activé. Une fois l'opération terminée, l'accès au fichier est restauré et le fichier enregistré sur disque dans son état d'origine.

- **Interdire l'accès + quarantaine** (uniquement pour les objets suspects). Kaspersky Anti-Virus verrouille l'accès au fichier et le déplace vers la quarantaine, où l'objet est enregistré sous un format chiffré, afin de neutraliser la menace d'infection. Les objets en quarantaine peuvent être analysés à l'aide d'une mise à jour de la base de Kaspersky Anti-Virus, par l'administrateur ou transmis à Kaspersky Lab.

Pour configurer le traitement d'un objet en fonction du type de menace détecté, cochez **Agir en fonction du type de menace** dans la section **Actions sur les objets en fonction du type de menace** et cliquez sur **Paramètres**.

Pour appliquer les modifications, cliquez sur le bouton **Enregistrer** dans la barre d'outils ou utilisez la même commande dans le menu contextuel de l'entrée **Protection en temps réel des fichiers**.

VOIR EGALEMENT

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET OPTIMISATION. PROTECTION EN TEMPS REEL DES FICHIERS

L'onglet **Optimisation** affiche les paramètres permettant d'exclure certains fichiers de l'analyse. Ces paramètres contrôlent la vitesse d'analyse et le rendement général du serveur.

Il est possible d'exclure de l'analyse les objets suivants :

- Fichiers en fonction du nom ou d'un masque de noms

- Objets en fonction du type de menace qu'ils contiennent ;

Cette option permet d'exclure des logiciels avec licence que Kaspersky Anti-Virus pourrait considérer comme malveillants ou potentiellement dangereux, comme par exemple des programmes d'administration à distance, des clients IRC, des serveurs FTP et tout utilitaire employé pour interrompre des processus.

Cochez **Exclure les objets** dans le groupe **Exclusions** pour exclure des objets de l'analyse en fonction du nom de fichier ou de l'extension ou d'un masque de fichier. Pour créer une liste d'exclusions, cliquez sur **Modifier**.

Cochez **Exclure les menaces** dans la zone **Exclusions** pour exclure de l'analyse les objets en fonction du type de menace détecté. Vous pouvez exclure des menaces en fonction du nom tel qu'il apparaît dans l'Encyclopédie des virus à l'adresse www.viruslist.com/fr/ ou en fonction d'un masque. L'usage de masques vous permet d'exclure une classe complète de menaces. Pour créer une liste d'exclusions, cliquez sur **Modifier**.

Dans le groupe de champs **Configuration complémentaire**, cochez une des cases suivantes :

- **Arrêter si l'analyse dure plus de** pour limiter le temps d'analyse d'un objet. Spécifiez la durée maximum d'analyse en secondes. La valeur par défaut est de 60 secondes.

- **Ne pas analyser les objets composés de plus de** pour ignorer les objets composés de taille supérieure à la taille spécifiée. Spécifier la taille maximum d'un objet composé, en mégaoctets. La valeur par défaut est de 8 Mo.

- **Utiliser la technologie iChecker** si vous souhaitez que Kaspersky Anti-Virus analyse uniquement les fichiers nouveaux ou modifiés depuis l'analyse précédente. L'utilisation de la technologie iChecker réduit la charge sur le processeur et sur le système disques et accélère l'analyse des objets.

  Kaspersky Anti-Virus n'ignore pas les objets s'ils ont été modifiés, si les paramètres de sécurité ont été renforcés après la dernière analyse, ou si la base antivirus a été mise à jour après la dernière analyse.

- **Utiliser la technologie iSwift** (pour des objets du système de fichiers NTFS) si vous souhaitez que Kaspersky Anti-Virus analyse uniquement les fichiers nouveaux ou modifiés depuis l'analyse précédente.

VOIR EGALEMENT

Exclusion des objets 379

Exclusion des menaces..... 380

Durée maximale de l'analyse d'un objet 388

Taille maximale de l'objet composé analysé 389

Application de la technologie iChecker..... 389

Application de la technologie iSwift 390

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Vérification de la signature Microsoft des fichiers 391

CHOISIR L'ACTION EN FONCTION DU TYPE DE MENACE (FENETRE). PROTECTION EN TEMPS REEL DES FICHIERS

Cette fenêtre permet de configurer l'ordre de traitement des objets par Kaspersky Anti-Virus, en fonction des types de menaces qu'ils contiennent.

Les actions définies en fonction des types de menaces détectées par Kaspersky Anti-Virus sont affichées dans le tableau **Actions actuelles**.

Certains types de menaces sont plus dangereux que d'autres pour le serveur. Par exemple, un cheval de Troie peut causer plus de dommages qu'un logiciel publicitaire (adware). Vous pouvez spécifier les différentes actions de Kaspersky Anti-Virus, en fonction du type de menace contenu dans l'objet.

Deux actions peuvent être définies pour chaque type de menace. Kaspersky Anti-Virus exécute la seconde action si la première échoue. Par exemple, si Kaspersky Anti-Virus ne parvient pas à réparer un objet ou à le supprimer en appliquant la première action, l'objet sera en quarantaine pour la seconde action.

Avant traitement (réparé ou supprimé), l'exemplaire original est enregistré dans la zone de sauvegarde.

Pour configurer le traitement d'objets en fonction du type de menace détecté, sélectionnez **Type de menace** dans la liste déroulante. Avec les menus **Première action** et **Deuxième action**, spécifiez ensuite les actions prises par Kaspersky Anti-Virus quand il détecte une menace de ce type.

La liste **Type de menace** affiche tous les types de menaces détectés par Kaspersky Anti-Virus. La liste des actions peut contenir les éléments suivants pour chacun des types de menaces :

- **Réparer** : réparer l'objet.
- **Supprimer** : supprimer l'objet.
- **Ignorer** : ignore l'objet. Si l'enregistrement de ce type d'événements est activé, les informations concernant l'objet détecté seront enregistrées dans le rapport.

  Si la première action sélectionnée est **Ignorer**, une seconde ne peut pas être configurée.

- **Quarantaine** : supprime l'objet de son emplacement d'origine et le déplace vers la Quarantaine.

Spécifiez les actions pour toutes les menaces de la liste.

VOIR EGALEMENT

Actions en fonction du type de menace 378

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

EXCLUSION DES OBJETS : FENETRE LISTE DES EXCLUSIONS PROTECTION EN TEMPS REEL DES FICHIERS

La fenêtre **Liste des exclusions** présente des noms et des extensions de fichiers que Kaspersky Anti-Virus n'analysera pas.

La partie supérieure de la fenêtre contient un champ pour ajouter un nouvel élément à la liste.

Pour ajouter un nouvel élément à la liste, entrez le nom ou l'extension de fichier ou le masque d'extension dans la zone de saisie supérieure et cliquez sur **Ajouter**.

Pour créer un masque, utilisez les caractères ***** et **?** (où ***** représente n'importe quel nombre de caractères et **?**, n'importe quel caractère).

Voici des exemples de masques autorisés utilisables pour créer des listes d'exclusion de fichiers :

- **eicar.*** : - tous les fichiers avec le nom **eicar** ;
- ***.exe** : tous les fichiers avec extension .exe ;
- ***.ex?** : tous les fichiers avec extension. ex?, où ? peut représenter tout caractère singulier. Par exemple : ex_, exe, ex1;
- **ex*** : tous les fichiers avec l'extension commençant par ex, où * représentent un nombre quelconque de caractères. Par exemple : ex, exe, exemple.

VOIR EGALEMENT

Exclusion des objets 379

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

EXCLUSION DES MENACES : FENETRE LISTE DES EXCLUSIONS. PROTECTION EN TEMPS REEL DES FICHIERS

La fenêtre **Liste des exclusions** permet de créer une liste de menaces exclues de l'analyse par Kaspersky Anti-Virus. La liste est vide par défaut.

Pour ajouter un nouvel élément à la liste, entrez le nom ou le masque de la menace dans la zone supérieure et cliquez sur **Ajouter**.

Vous pouvez spécifier le nom complet de la menace tel qu'il apparaît dans l'Encyclopédie des virus à l'adresse www.viruslist.com/fr/ ou encore, un masque du nom de la menace. L'usage de masques vous permet d'exclure une classe complète de menaces.

Le nom de la menace est défini lors de l'analyse de l'objet et peut contenir les informations suivantes : **<catégorie de menace>:<type de menace>.<nom abrégé de la plateforme>.<nom de la menace>.<code de modification de la menace>**.

Admettons que vous utilisez l'utilitaire Remote Administrator en guise d'outil d'administration à distance. La plupart des programmes antivirus classent le code de cet utilitaire dans la classe de menace "potentiellement dangereuses" (**Riskware**). Si vous ne souhaitez pas verrouiller Remote Administrator, ajoutez les informations suivantes à la liste des menaces exclues. Pour le nom, vous pouvez spécifier :

- **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus ignorera uniquement le programme Win32.RAdmin.20.
- Masque du nom complet de la menace : **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions de Remote Administrator.
- Masque du nom complet de la menace, avec uniquement le type de menace : **not-a-virus:***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions des objets contenant cette classe de menace.

Pour supprimer un élément de la liste,

sélectionnez-le dans la liste et cliquez sur **Supprimer**.

LISTE DES EXTENSIONS DE FICHIERS ANALYSES PAR DEFAUT. PROTECTION EN TEMPS REEL DES FICHIERS

Kaspersky Anti-Virus analyse par défaut les fichiers possédant les extensions suivantes :

386 : pilote du mode étendu ou fichier de Microsoft Windows ;

acm : fichier du répertoire système Windows ;

ade, *adp* : projet Microsoft Access ;

asp : script Active Server Pages ;

asx : script Cheyenne Backup ; fichier de réorientation (Redirector) pour Microsoft Advances Streaming Format ; fichier vidéo ;

ax : filtre DirectShow ;

bas : texte du programme BASIC ;

bat : fichier de paquet ;

bin : fichier binaire ;

chm : fichier HTML compilé ;

cla, *clas** : classe Java ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS) ;

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64Ko ;

cpl : module du panneau de configuration de Microsoft Windows :

crt : fichier Crontab dans Unix ou fichier de certificat ;

dll : bibliothèque dynamique ;

dpl : bibliothèque Borland Delphi compactée ;

drv : pilote d'un périphérique quelconque ;

dvb : pilote d'un périphérique DOS ;

dwg : base de données de dessins AutoCAD ;

efi : fichier Crontab ou fichier de certificat dans UNIX ;

emf : fichier au format Enhanced Metafile ;

eml : message électronique de Microsoft Outlook Express ;

exe : fichier exécutable ; archive autoextractibe ;

fon : fichier de police ;

fpm : programme de bases de données, fichier de démarrage de Microsoft Visual FoxPro ;

hlp : fichier d'aide au format Win Help ;

hta : programme hypertexte pour Microsoft Internet Explorer ;

htm, *html** : document hypertexte ;

htt : modèle de fichier hypertexte Microsoft Windows ;

ico : fichier d'icône d'objet ;

inf : fichier d'informations ;

ini : fichier d'initialisation ;

ins : script InstallShield (Installation Authoring Solution) ;

isp : fichier des paramètres Microsoft IIS du fournisseur (IIS Internet Service Provider Settings) ;

jpg, *jpeg :* fichier graphique de conservation de données compressées ;

js,*jse* : texte source JavaScript ;

lnk : fichier lien dans Microsoft Windows ;

mbx : base de Microsoft Outlook Express ;

msc : fichier de la console MMC ;

msg : message électronique de Microsoft Mail ;

msi : paquet Microsoft Windows Installer ;

msp : paquet de mise à jour Microsoft Windows Installer ;

mst : fichier de transformation de Microsoft Windows Installer ;

nws : nouveau message électronique de Microsoft Outlook Express ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

oft : modèle de message Microsoft Outlook ;

otm : projet VBA pour Microsoft Office Outlook ;

pcd : image Kodak Photo-CD ;

pdf : document Adobe Acrobat ;

php : script intégré dans les fichiers HTML ;

pht : fichier HTML avec scripts PHP intégrés ;

*phtm** : document hypertexte contenant des scripts PHP intégrés ;

pif : fichier contenant des informations sur un logiciel ;

plg : message électronique ;

png : image Portable Network Graphics ;

pot : modèle Microsoft PowerPoint ;

prf : fichier système Microsoft Windows ;

prg : texte du programme dBase, Clipper ou Microsoft Visual FoxPro, programme de la suite WAVmaker ;

reg : fichier d'enregistrement des clés de la base de registres système de Microsoft Windows ;

rsc : fichier Pegasus Mail Resource ;

rtf : document au format Rich Text Format ;

scf: fichier de commande Microsoft Windows Explorer ;

scr : fichier d'écran de veille de Microsoft Windows ;

sct : format Microsoft FoxPro ;

shb : présentation Corel Show ;

shs : fragment de Shell Scrap Object Handler ;

sht : document S-HTML ;

*shtm** est un document hypertexte contenant SSI : Server Side Includes d'ajout du serveur (certaines actions supplémentaires réalisées par le serveur) ;

swf : objet d'un paquet Shockwave Flash ;

sys : fichier système, par exemple fichier du pilote Microsoft Windows ;

the : modèle pour le bureaul Microsoft Windows 95 ;

*them** : thème pour le bureau Microsoft Windows ;

tsp : programme qui fonctionne en mode de partage du temps ;

url : lien Internet ;

vb : fichier Visual Basic ;

vbe : fichier VBScript Encoded Script ;

vbs : script Visual Basic ;

vxd : pilote d'un périphérique virtuel Microsoft Windows.

wma : fichier audio Microsoft Windows Media ;

wmf : métafichier Microsoft Windows Media ;

wmv : fichier vidéo Microsoft Windows Media ;

wsc : composant Windows Script ;

wsf : script Microsoft Windows ;

wsh : fichier de configuration de Windows Script Host ;

do? : – documents et fichiers de Microsoft Office Word tels que : *doc* – document Microsoft Office Word, *dot* – modèle de documents Microsoft Office Word, etc. ;

md? : – documents et fichiers de Microsoft Office Access tels que : *mda* – groupe de travail de Microsoft Office Access, *mdb* – base de données, etc.;

mp? fichier audio ou animation MPEG ;

ov?: fichiers exécutable MS DOS ;

pp? : – documents et fichiers de Microsoft Office PowerPoint tels que : *pps* – dia Microsoft Office PowerPoint ;

vs? : – documents et fichiers Visio tels que : *vss* – fichier de modèle Visio, *vsw* – espace de travail Vision, etc. ;

xl? : – documents et fichiers de Microsoft Office Excel tels que : *xla* – extension Microsoft Excel, *xlc* – schéma, *xlt* – modèle de document, etc.

ANALYSE SELON LA LISTE DES EXTENSIONS : FENETRE LISTE DES MASQUES D'EXTENSIONS PROTECTION EN TEMPS REEL DES FICHIERS

La fenêtre **Liste des masques d'extensions** permet de créer une liste d'extensions et des masques d'extensions de fichiers analysés par Kaspersky Anti-Virus.

Vous pouvez utiliser la liste par défaut (cf. page 172). Pour ce faire, cliquez sur **Par défaut**.

Pour ajouter un nouvel élément à la liste, entrez l'extension ou le masque d'extension du fichier dans la zone supérieure et cliquez sur **Ajouter**.

Pour créer les masques, utilisez les caractères génériques * et ? Notez que le point séparateur du nom et de l'extension du fichier n'est pas indiqué.

Voici des exemples de masques autorisés utilisables pour créer des listes d'exclusion de fichiers :

- **exe** : tous les fichiers avec l'extension .exe ;
- **ex?** - tous les fichiers avec extension. ex?, où ? peut représenter tout caractère singulier. Par exemple : ex, exe, ex1;
- **ex*** : tous les fichiers avec l'extension commençant par ex, où * représentent un nombre quelconque de caractères. Par exemple : ex, exe, exemple.

Pour supprimer un élément de la liste,

sélectionnez-le dans la liste et cliquez sur **Supprimer**.

MODELES (FENETRE). PROTECTION EN TEMPS REEL DES FICHIERS

Cette fenêtre affiche la liste des modèles créés contenant des paramètres d'analyse.

Vous pouvez examiner le paramètres contenus dans un modèle. Pour ce faire, sélectionnez le modèle dans la liste puis cliquez sur **Voir**.

Pour actualiser la liste des modèles,

Cliquez sur le bouton **Mettre à jour**.

Pour supprimer un modèle,

sélectionnez-le dans la liste et cliquez sur bouton **Supprimer**.

VOIR EGALEMENT

Utilisation de modèles dans la tâche Protection en temps réel des fichiers 101

Utilisation des modèles dans les tâches d'analyse à la demande 137

PROPRIETES DU MODELE (FENETRE). PROTECTION EN TEMPS REEL ET ANALYSE A LA DEMANDE

Dans les tâches **d'analyse à la demande** et de **Protection en temps réel des fichiers**, vous avez la possibilité d'enregistrer dans un modèle les paramètres d'analyse ou de protection configurés pour une certaine entrée.

Vous pouvez appliquer un modèle basé sur les paramètres de sécurité de n'importe quel nœud de manière à rapidement configurer les paramètres de sécurité d'un autre nœud.

Les modèles créés au sein d'une tâche **Protection en temps réel des fichiers** ne peuvent être appliqués qu'à une tâche **Protection en temps réel des fichiers**. Les modèles créés au sein d'une tâche d'analyse à la demande peuvent être appliqués dans toute autre tâche d'analyse à la demande. Ils ne peuvent pas être appliqués dans la tâche **Protection en temps réel des fichiers**.

Pour conserver les valeurs des paramètres de l'analyse (de la protection) dans le modèle, procédez comme suit :

saisissez le nom du modèle dans le champ **Nom du modèle**.

Dans la zone **Description**, entrez des informations supplémentaires pour décrire les paramètres enregistrés dans le modèle.

VOIR EGALEMENT

Utilisation de modèles dans la tâche Protection en temps réel des fichiers 101

Utilisation des modèles dans les tâches d'analyse à la demande 137

MODELES : GENERAL (ONGLET). PROTECTION EN TEMPS REEL DES FICHIERS

Cet onglet affiche des informations générales sur le modèle généré quand il a été créé :

- **Nom** : entrez le nom du modèle.
- **Description** : informations sur les paramètres enregistrés dans le modèle.

Ces zones ne sont pas modifiables.

VOIR EGALEMENT

Utilisation de modèles dans la tâche Protection en temps réel des fichiers 101

Utilisation des modèles dans les tâches d'analyse à la demande 137

PARAMETRES (ONGLET). PROTECTION EN TEMPS REEL DES FICHIERS

Cet onglet affiche la liste des paramètres enregistrés dans un modèle, avec leur configuration. Cette information est générée lors de la création du modèle et n'est pas modifiable.

VOIR EGALEMENT

Utilisation de modèles dans la tâche Protection en temps réel des fichiers 101

Utilisation des modèles dans les tâches d'analyse à la demande 137

NŒUD ANALYSE DES SCRIPTS

La tâche **Analyse des scripts** analyse les routines VBScript et JScript avant leur exécution. L'exécution de scripts dangereux est interdite et l'action spécifiée par les paramètres de tâche est appliquée aux scripts suspects (autoriser ou interdire l'exécution du script). Les scripts suspects sont interdits par défaut.

L'entrée **Analyse des scripts** est utilisée pour arrêter et démarrer les tâches **d'Analyse des scripts**, leur planification, l'examen des statistiques et la configuration de leur surveillance.

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche d'analyse des scripts :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**).
- **Heure de démarrage** – **date et heure de démarrage de la tâche.**

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Groupe **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, à l'utilisation de l'analyseur heuristique et à l'application de la zone de confiance.

Le lien **Propriétés** ouvre la fenêtre de configuration des paramètres de la tâche **Analyse des scripts**.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

Panneau de tâches et menu contextuel

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Exporter les paramètres/Importer les paramètres** : exporte les paramètres de tâche dans un fichier ou les restaure à partir d'un fichier.
- **Paramètres** : sélectionne l'action à exécuter sur les scripts suspects identifiés et configure les paramètres de lancement/d'arrêt automatique de la tâche.

VOIR EGALEMENT

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Configuration de planification des tâches en MMC 50

Utilisation de l'analyseur heuristique 393

ANALYSE A LA DEMANDE

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES TACHES D'ANALYSE A LA DEMANDE

Kaspersky Anti-Virus prévoit trois tâches prédéfinies d'analyse à la demande :

- La tâche **Analyse des zones critiques** est exécutée par défaut chaque jour selon la programmation. Kaspersky Anti-Virus analyse les objets situés dans les zones critiques du système d'exploitation : objets de démarrage, secteurs d'amorçage et entrées principales d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. Il analyse les fichiers qui se trouvent dans les répertoires système, par exemple dans le répertoire \system32. Kaspersky Anti-Virus applique les paramètres de sécurité dont les valeurs correspondent à celles du niveau **Recommandé** (cf. page 144). Vous pouvez modifier les paramètres la tâche **Analyse des zones critiques**.

- La tâche **Analyse des objets en quarantaine** est exécutée par défaut selon la programmation après chaque mise à jour des bases. Vous ne pouvez pas modifier les paramètres de la tâche **Analyse des objets en quarantaine** (cf. page 196).

- La tâche **Analyse au démarrage du système** est exécutée à chaque démarrage de Kaspersky Anti-Virus. Kaspersky Anti-Virus analyse ses propres modules logiciels, les secteurs d'amorçage et les principaux enregistrements d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. A chaque exécution de la tâche, Kaspersky Anti-Virus crée une copie des secteurs d'amorçage sains et si lors de l'exécution suivante de la tâche il découvre une menace, il remplace les secteurs d'amorçage infectés par les copies de sauvegarde saines.

Vous pouvez créer des tâches définies par l'utilisateur dans le nœud Analyse à la demande. Par exemple, vous pouvez créer une tâche d'analyse du répertoire partagé sur le serveur.

Kaspersky Anti-Virus peut exécuter simultanément plusieurs tâches d'analyse à la demande.

Catégories des tâches dans Kaspersky Anti-Virus en fonction de lieu de création et d'exécution (cf. page 46)

Présentation des fonctions "Protection en temps réel" et "Analyse à la demande" (cf. page 13)

A propos de la gestion des tâches via la console de Kaspersky Anti-Virus (cf. page 46)

CONFIGURATION DES TACHES D'ANALYSE A LA DEMANDE

Vous pouvez configurer la tâche système **Analyse des zones critiques**, ainsi que les tâches d'analyse à la demande définies par l'utilisateur (cf. tableau ci-dessous).

Pour savoir comment créer une tâche définie par l'utilisateur, lisez la rubrique "Création d'une tâche d'analyse à la demande" (cf. page 47).

Tableau 14. Paramètres par défaut d'une tâche d'analyse à la demande recréée

PARAMETRE	VALEUR	CONFIGURATION
Couverture de l'analyse	Tout le serveur	Vous pouvez modifier la zone d'analyse (cf. page 136).
Paramètres de sécurité	Identiques pour toutes les couvertures de protection ; correspondent au niveau de protection **Recommandé**.	Pour les nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur, procédez comme suit : • appliquer du niveau de sécurité prédéfini (cf. page 144) ; • modifier manuellement les paramètres de sécurité (cf. page 147). Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud (cf. page 137).
Analyseur heuristique	Appliqué au niveau d'analyse **Moyen**	Vous pouvez activer ou désactiver l'application de l'analyseur heuristique (cf. page 393) et régler le niveau de l'analyse.
Zone de confiance	Appliquée	Une liste unique d'exclusions que vous pouvez appliquer dans des tâches d'analyse à la demande sélectionnée et dans la tâche de **Protection en temps réel des fichiers**. Lisez également le chapitre consacré à la création et l'application de la zone de confiance (cf. page 178)

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

1. Dans l'arborescence de la console, déployez le nœud **Analyse à la demande** :
2. Sélectionnez la tâche que vous souhaitez configurer afin de l'ouvrir (cf. ill. ci-après).
3. Sous l'onglet **Configuration de la zone d'analyse** configurez les paramètres de la tâche : composez la zone d'analyse ; le cas échéant, modifiez les paramètres de sécurité de toute la zone d'analyse ou de certains de ces nœuds. Par défaut, les tâches définies par l'utilisateur qui sont recréées possèdent les paramètres décrits dans le tableau ci-dessous.
4. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

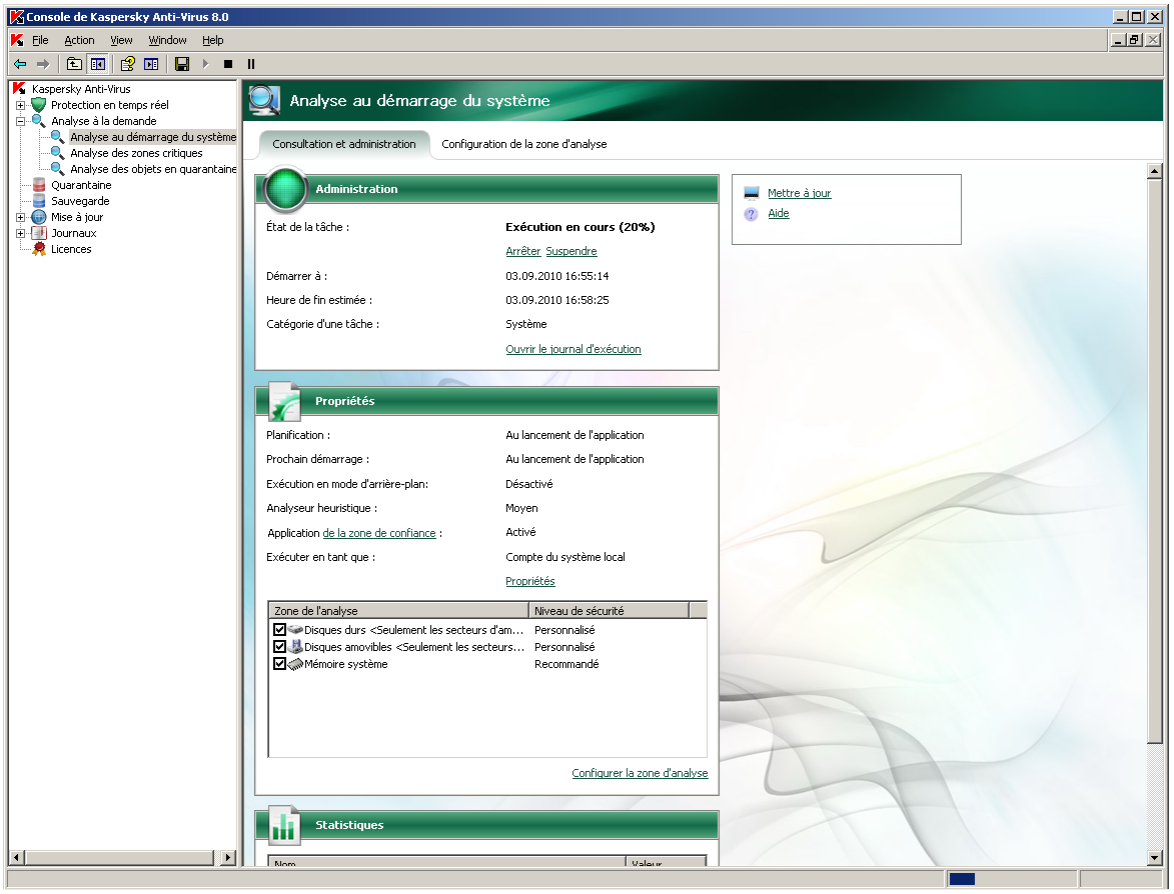


Illustration 42. Tâche d'analyse à la demande ouverte

DANS CETTE SECTION DE L'AIDE

COUVERTURE DE L'ANALYSE DANS LES TACHES D'ANALYSE A LA DEMANDE

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA CONSTITUTION D'UNE COUVERTURE D'ANALYSE DANS LES TACHES D'ANALYSE A LA DEMANDE

Dans les tâches d'analyse à la demande recréées, la couverture d'analyse reprend par défaut tout le serveur. Vous pouvez restreindre la couverture de l'analyse à certains secteurs du serveur uniquement si la politique de sécurité n'impose pas la nécessité de les analyser tous.

Dans la console de Kaspersky Anti-Virus, la couverture de l'analyse se présente sur la forme d'une arborescence des ressources fichiers du serveur que Kaspersky Anti-Virus peut analyser.

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrés de la manière suivante :

☑ Nœud repris dans la couverture de protection.

☐ Nœud exclu de la couverture de protection.

☑. Au moins un des nœuds intégrés à ce nœud est exclu de la couverture de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

Le nom des nœuds virtuels de la couverture d'analyse apparaît en lettres bleues.

COUVERTURES D'ANALYSE PREDEFINIES

➧ *Pour afficher l'arborescence des ressources fichiers du serveur, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter la couverture d'analyse afin d'ouvrir la tâche (cf. ill. ci-après).

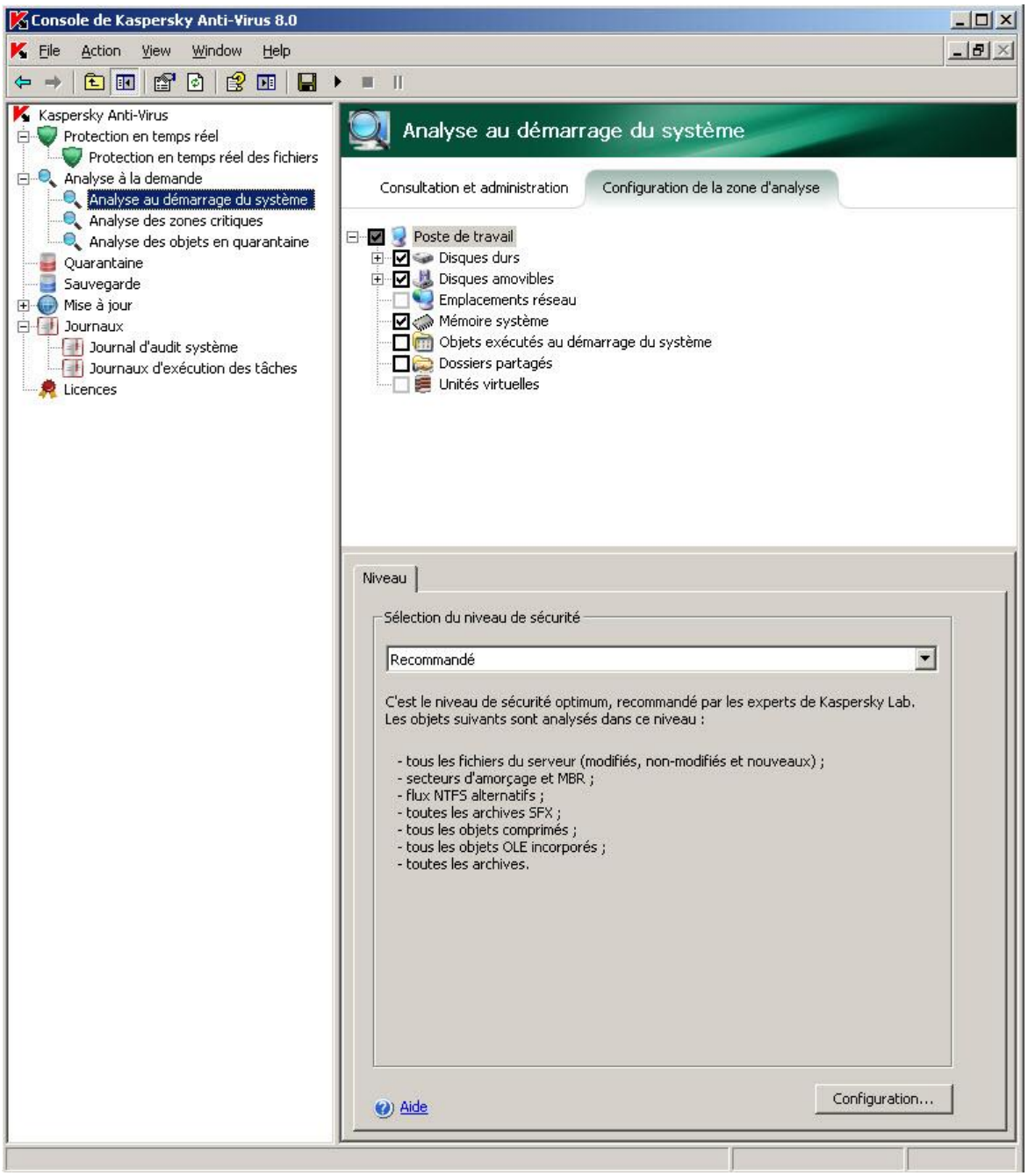


Illustration 43. Exemple d'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus.

Le panneau des résultats, sur l'onglet **Configuration de la zone d'analyse** affiche l'arborescence des ressources fichier du serveur dont les objets constitueront la couverture d'analyse.

L'arborescence des ressources fichiers du serveur contient les couvertures d'analyse prédéfinies suivantes :

- **Poste de travail**. Kaspersky Anti-Virus analyse tout le serveur.
- **Disques durs**. Kaspersky Anti-Virus analyse les objets du disque dur du serveur. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.

- **Disques amovibles**. Kaspersky Anti-Virus analyse les objets sur les disques amovibles tels que les disques compacts ou les clés USB. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.

- **Emplacements réseau**. Vous pouvez ajouter à la couverture d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux répertoires de réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte **Système local** (**SYSTEM**). Pour obtenir de plus amples informations, consultez le point "Inclusion des disques de réseau" (cf. page 141).

- **Mémoire système**. Kaspersky Anti-Virus analyse les fichiers exécutables et les modules des processus exécutés dans le système d'exploitation au moment de l'analyse.

- **Objets de démarrage**. Kaspersky Anti-Virus analyse les objets sur lesquels les clés de la base de registres et les fichiers de configuration, par exemple WIN.INI ou SYSTEM.INI, s'appuient ainsi que les modules logiciels des applications qui sont exécutées automatiquement au démarrage de l'ordinateur.

- **Dossiers partagés**. Kaspersky Anti-Virus analyse tous les dossiers partagés sur le serveur protégé.

- **Unités virtuelles**. Vous pouvez inclure dans la couverture de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe (créer couverture de protection virtuelle). Pour en savoir plus, lisez la rubrique "Création d'une couverture d'analyse virtuelle : inclusion des disques, répertoires et fichiers dynamiques dans la couverture d'analyse" (cf. page 141).

Les pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus. Pour analyser les objets d'un pseudo-disque, il faut inclure dans la couverture d'analyse le répertoire du serveur auquel ce pseudo-disque est lié.

Les disques de réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. Pour inclure les objets d'un disque de réseau dans la couverture d'analyse, indiquez le chemin d'accès au répertoire correspondant à ce disque de réseau au format UNC (Universal Naming Convention).

CONSTITUTION DE LA COUVERTURE D'ANALYSE

Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.

Si vous modifiez la zone d'analyse dans les tâches **Analyse au démarrage du système** et **Analyse des zones critiques**, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la restauration de Kaspersky Anti-Virus (**Démarrer ® Programmes ® Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition ® Modification ou suppression**). Dans l'Assistant cochez la case **Rétablir les paramètres recommandés de fonctionnement de l'application**.

Pour établir la zone d'analyse, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez constituer une couverture d'analyse.

3. Le panneau des résultats sous l'onglet **Configuration de la zone d'analyse** affiche l'arborescence des ressources fichiers du serveur. Dans les tâches d'analyse à la demande recréées, la zone d'analyse reprend par défaut le serveur.

4. Exécutez les actions suivantes :

   - Pour sélectionner les nœuds que vous souhaitez inclure dans la couverture d'analyse, désélectionnez la case **Poste de travail** puis réaliser les actions suivantes :

- Si vous souhaitez inclure tous les disques d'un même type dans la couverture d'analyse, cochez la case en regard du nom du type de disque requis ;

- Si vous souhaitez inclure un disque particulier dans la couverture d'analyse, déployez le nœud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque requis. Par exemple, pour sélectionner le disque amovible **F:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:** ;

- Si vous souhaitez inclure un répertoire particulier du disque dans la couverture d'analyse, déployez l'arborescence des ressources fichiers du serveur afin d'afficher le répertoire requis puis cochez la case en regard de son nom. Vous pouvez inclure des fichiers de la même manière ;

- pour exclure un nœud particulier de la couverture d'analyse, déployez l'arborescence des ressources de fichiers pour afficher le nœud requis et désélectionnez la case en regard de son nom.

5. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

Reportez-vous aux sections suivantes pour les informations concernant l'inclusion dans la zone d'analyse de :

- disque de réseau, dossier ou fichier (cf. page 141) ;

- disque dynamique, dossier ou fichier (cf. page 141).

UTILISATION DES MODELES DANS LES TACHES D'ANALYSE A LA DEMANDE

DANS CETTE SECTION DE L'AIDE

ENREGISTREMENT DES VALEURS DES PARAMETRES DE SECURITE DANS UN MODELE

Après avoir configuré les paramètres de sécurité d'un nœud quelconque dans l'arborescence des ressources fichiers du réseau dans la tâche d'analyse à la demande, vous pouvez enregistrer cet ensemble de paramètres dans un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres d'autres nœuds dans cette tâche ou dans d'autres tâches d'analyse à la demande.

Vous ne pouvez pas utiliser les modèles créés dans la tâche **Analyse à la demande** pour configurer les paramètres de la tâche **Protection en temps réel des fichiers**.

Pour enregistrer les valeurs des paramètres de sécurité dans un modèle, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Analyse à la demande** :

2. Sélectionnez la tâche d'analyse à la demande dont les paramètres doivent être enregistrés dans un modèle.

3. Sur l'onglet **Configuration de la zone d'analyse** dans l'arborescence des ressources fichier du réseau, sélectionnez le nœud dont vous souhaitez enregistrer les paramètres de sécurité.

4. Dans la boîte de dialogue **Paramètres de la couverture de protection**, onglet **Général**, cliquez sur le bouton **Enregistrer comme modèle**.

5. Dans la boîte de dialogue **Propriétés du modèle** dans le champ **Nom du modèle**, saisissez le nom du modèle (cf. ill. ci-après).

6. Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.

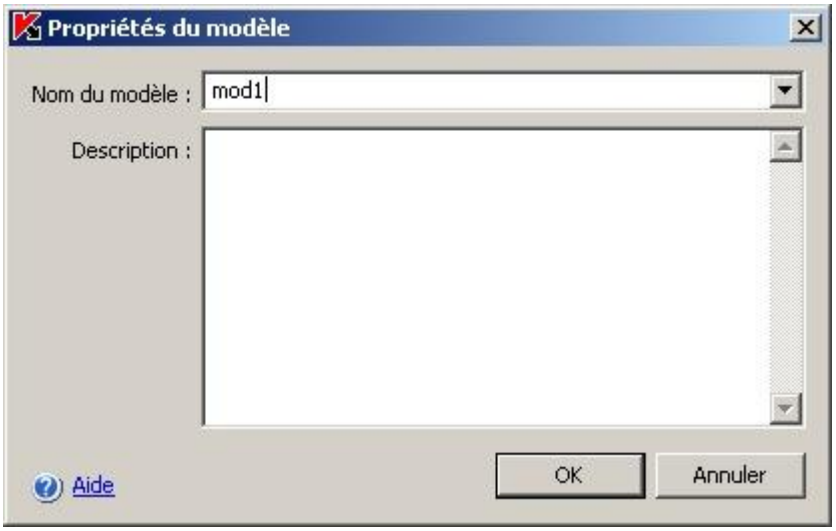


*Illustration 44. Boîte de dialogue **Propriétés du modèle***

7. Cliquez sur **OK**. Le modèle avec la sélection de paramètres sera conservé.

CONSULTATION DES PARAMETRES DE SECURITE DU MODELE

Pour consulter les valeurs des paramètres de sécurité dans le modèle créé, procédez comme suit :

1. **Dans l'arborescence de la console, ouvrez le menu contextuel du nœud Analyse à la demande** et sélectionnez l'option Modèles de paramètres.

Dans la boîte de dialogue **Modèles**, vous verrez la liste des modèles que vous pouvez appliquer aux tâches d'analyse à la demande (cf. ill. ci-après).

*Illustration 45. Boîte de dialogue **Modèles***

2. Pour consulter les informations relatives au modèle et les valeurs des paramètres de sécurité, sélectionné le modèle requis dans la liste et cliquez sur le bouton **Voir**.

L'onglet **Général** reprend le nom du modèle et des informations complémentaires sur celui-ci. L'onglet **Paramètres** affiche une liste des valeurs des paramètres de la sécurité enregistré dans le modèle (cf. ill. ci-après).

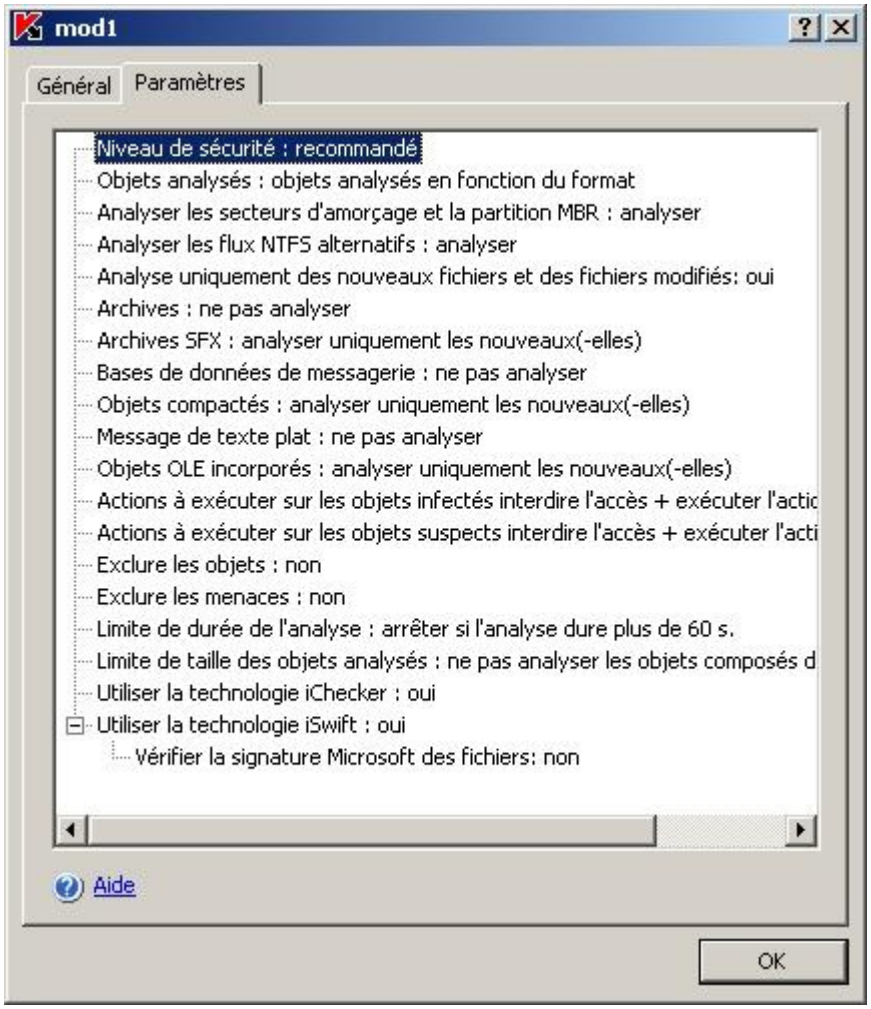


*Illustration 46. Boîte de dialogue **Nom du modèle**, onglet **Paramètres***

APPLICATION DU MODELE

Si vous appliquez le modèle au nœud parent, les paramètres de sécurité du modèle seront appliqués à tous les nœuds enfants, sauf dans les situations suivantes :

- Le modèle ne sera pas appliqué aux nœuds pour lesquels vous avez configuré les paramètres de sécurité séparément. Pour définir les paramètres de sécurité du modèle pour tous les nœuds enfants, désélectionnez la case en regard du nœud parent dans l'arborescence des ressources fichier du serveur avant d'appliquer le modèle puis cochez-la à nouveau. Appliquez le modèle au nœud parent. Tous les nœuds enfants auront les mêmes paramètres de sécurité que le nœud parent.

- Le modèle ne s'applique pas aux disques de réseau, aux dossiers et aux fichiers configurés.

Pour appliquer un modèle de paramètres de sécurité, procédez comme suit :

1. Tout d'abord, enregistrez la sélection de paramètres de sécurité dans un modèle (cf. page 101).

2. Dans l'arborescence de la console, sélectionnez le nœud **Analyse à la demande**.

3. Sélectionnez la tâche d'analyse à la demande à laquelle vous souhaitez appliquer les paramètres de sécurité repris dans le modèle.

4. **Sur l'onglet Configuration de la zone d'analyse** dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud auquel vous souhaitez appliquer le modèle et sélectionnez Appliquer un modèle.

5. Dans la liste des modèles, sélectionnez le modèle que vous souhaitez appliquer.

6. **Dans la boîte de dialogue Paramètres de sécurité**, cliquez sur OK afin de conserver les modifications.

SUPPRESSION DU MODELE

Pour supprimer un modèle, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Analyse à la demande** et choisissez l'option **Modèles de paramètres**.

2. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez supprimer dans la liste et cliquez sur **Supprimer**.

3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**. Le modèle sélectionné sera supprimé.

INCLUSION DES DISQUES DE RESEAU, DES REPERTOIRES OU DES FICHIERS DANS LA COUVERTURE D'ANALYSE

Vous pouvez inclure dans la couverture d'analyse des disques de réseau, des répertoires ou des fichiers en indiquant leur chemin d'accès de réseau au format UNC (Universal Naming Convention).

L'utilisateur n'a pas la possibilité d'analyser les dossiers réseau quand il est connecté sous le compte **Système local** (**Local System**).

Pour inclure un objet de réseau dans la zone d'analyse, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Analyse à la demande** :

2. Sélectionnez la tâche d'analyse à la demande dans la couverture d'analyse de laquelle vous souhaitez ajouter un chemin de réseau.

3. Sur l'onglet **Configuration de la zone d'analyse** ouvrez le menu contextuel au nœud **Emplacements réseau** et sélectionnez **Ajouter un répertoire de réseau** ou **Ajouter un fichier de réseau**.

4. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et appuyez sur la touche <**ENTER**>.

5. Cochez la case à côté de l'objet de réseau ajouté afin de l'inclure dans la couverture d'analyse.

6. Le cas échéant, modifiez les paramètres de protection de l'objet de réseau ajouté (cf. rubrique "Configuration des paramètres de protection dans les tâches d'analyse à la demande" à la page 143).

7. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

CREATION D'UNE COUVERTURE D'ANALYSE VIRTUELLE : INCLUSION DES DISQUES, REPERTOIRES ET FICHIERS DYNAMIQUES DANS LA COUVERTURE D'ANALYSE

Vous pouvez inclure dans la zone d'analyse les disques, les dossiers et les fichiers dynamiques, ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe – créer une zone d'analyse virtuelle (cf. page 141).

Pour inclure un disque virtuel dans la zone d'analyse, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Analyse à la demande** :

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez composer une couverture d'analyse virtuelle afin d'ouvrir la tâche.

3. Sous l'onglet **Configuration de la zone de l'analyse** du panneau des résultats, dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud **Disques virtuelles** et sélectionnez le nom du disque virtuel créé dans la liste des noms disponibles (cf. ill. ci-après).

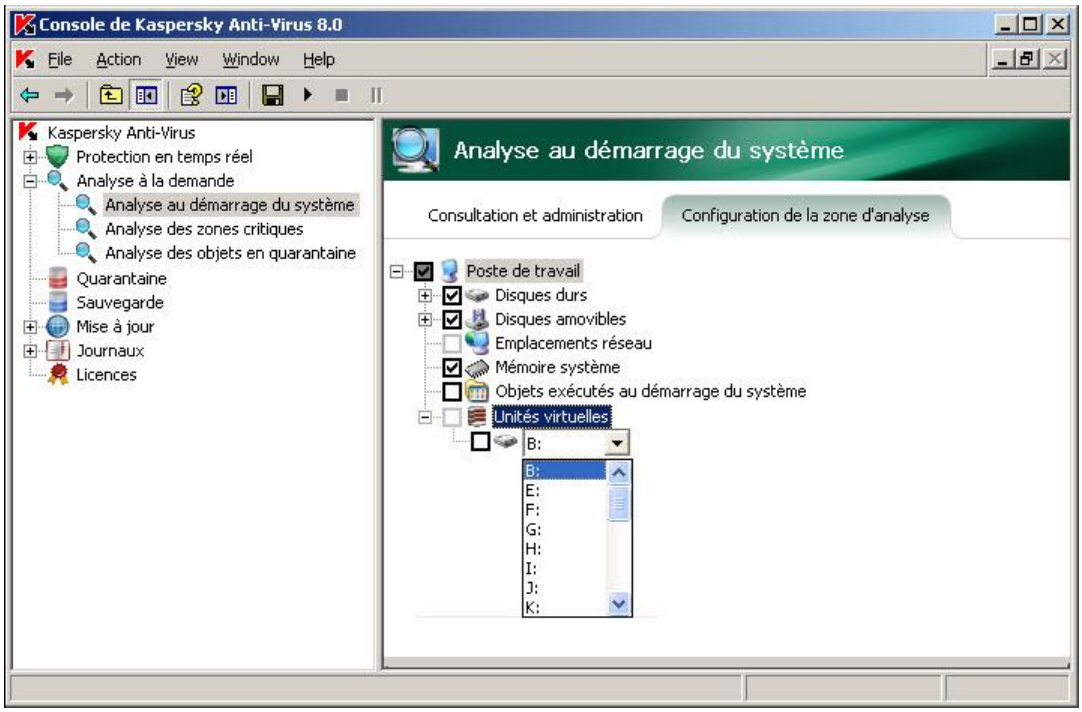


Illustration 47. Choix du nom du disque virtuel créé

4. Cochez la case à côté du disque ajouté afin de l'inclure dans la couverture d'analyse.

5. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

Pour ajouter un répertoire ou un fichier virtuel dans la zone d'analyse, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez composer une couverture d'analyse virtuelle afin d'ouvrir la tâche.

3. Sous l'onglet **Configuration de la zone d'analyse** du panneau des résultats, dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud auquel vous souhaitez ajouter le répertoire ou le fichier et sélectionnez la commande **Ajouter un dossier virtuel** ou **Ajouter un fichier virtuel** (cf. ill. ci-après).

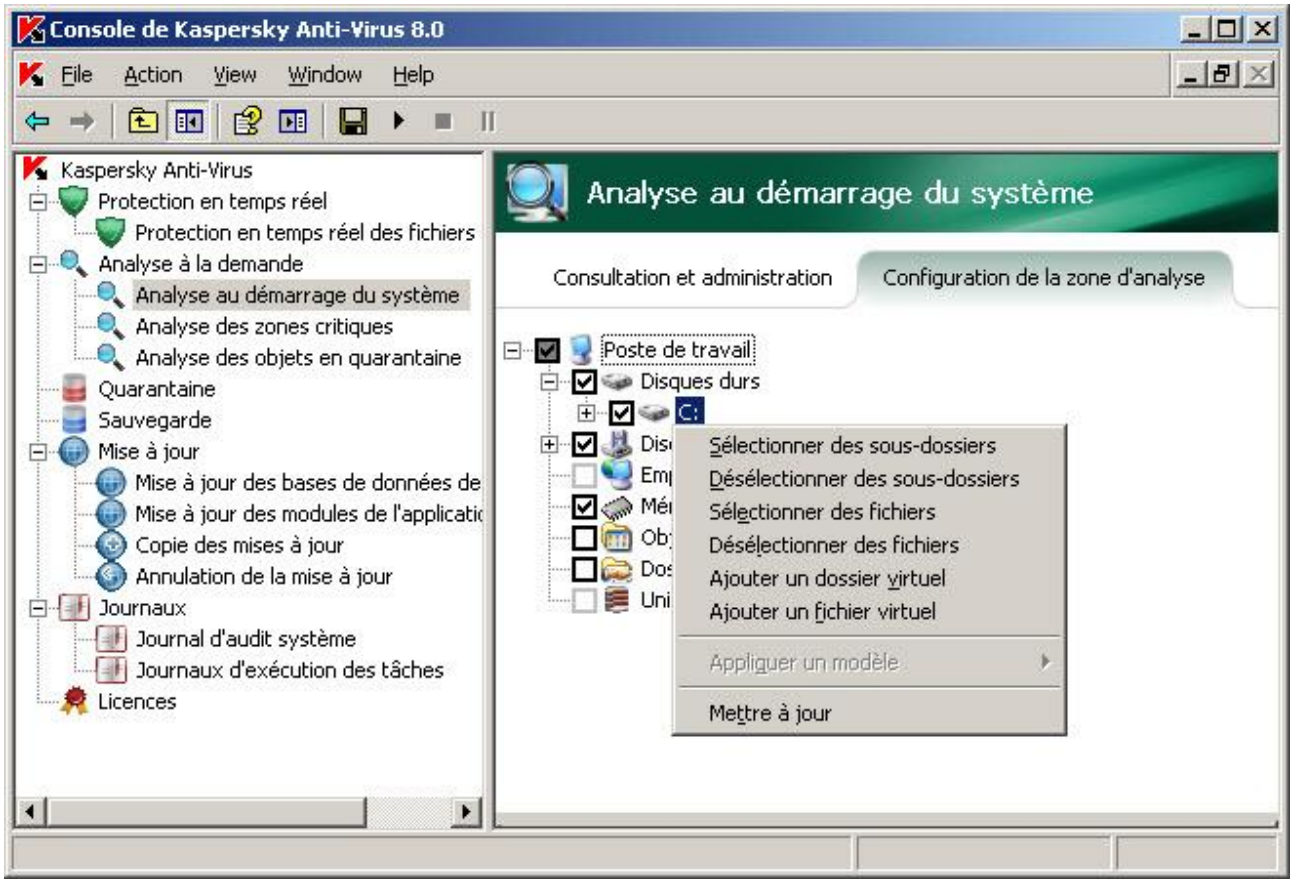


Illustration 48. Ajout d'un répertoire virtuel

4. Dans le champ, saisissez le nom du répertoire (fichier). Vous pouvez définir un masque de nom de répertoire (de fichier). Pour les masques, utilisez les caractères ***** et **?**.

5. Dans la ligne contenant le nom du répertoire (fichier) créé, cochez la case afin de l'inclure dans la couverture d'analyse.

6. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

CONFIGURATION DES PARAMETRES DE PROTECTION DANS LES TACHES D'ANALYSE A LA DEMANDE

Dans la tâche d'analyse à la demande sélectionnée, vous pouvez configurer les paramètres de sécurité en indiquant des valeurs communes pour toute la zone d'analyse ou des paramètres différents pour des nœuds différents dans l'arborescence des ressources fichiers du serveur. Les paramètres de sécurité que vous définissez pour un nœud sélectionné seront automatiquement appliqués à tous les nœuds qu'il renferme. Toutefois, si vous attribuez des valeurs distinctes aux paramètres de sécurité du nœud enfant, alors les paramètres de protection du nœud parent ne seront pas appliqués.

Vous pouvez configurer les paramètres de la couverture d'analyse sélectionnée de l'une des manières suivantes :

- Sélectionner un des trois niveaux de protection prédéfinis (vitesse maximale, recommandé ou protection maximale) ;

- Modifier manuellement les paramètres de protection des nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur.

Vous pouvez enregistrer la sélection de paramètres du nœud dans un modèle afin de l'appliquer à d'autres nœuds.

DANS CETTE SECTION DE L'AIDE

SELECTION DU NIVEAU DE SECURITE PREDEFINI DANS LES TACHES D'ANALYSE A LA DEMANDE

Pour le nœud sélectionné dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des trois niveaux de protection prédéfinis suivant : *vitesse maximale*, ***recommandé*** et *protection maximale*. Chacun de ces niveaux de sécurité prédéfinis possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Vitesse maximale

Vous pouvez sélectionner le niveau Vitesse maximale si votre réseau local prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Anti-Virus sur les serveurs et les postes de travail ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** est sélectionné par défaut. Il est considéré par les experts de Kaspersky Lab comme suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux. Ce niveau offre une combinaison idéale de qualité de l'analyse et de rapidité.

Protection maximum

Utilisez le niveau de sécurité **Protection maximale** si d'autres mesures de protection ne sont pas appliquées dans votre réseau.

Tableau 15. Niveaux de protection prédéfinis et valeurs des paramètres correspondants

PARAMETRES	NIVEAU DE SECURITE PREDEFINI		
	VITESSE MAXIMALE	RECOMMANDE	PROTECTION MAXIMUM
Objets à analyser (cf. page 376)	En fonction du format	Analyser tous les objets	Analyser tous les objets
Analyse uniquement des nouveaux fichiers et des fichiers modifiés (cf. page 382)	Activée	Désactivée	Désactivée
Actions à exécuter sur les objets infectés (cf. page 384)	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. page 386)	Quarantaine	Quarantaine	Quarantaine
Exclusion des objets (cf. page 379)	Non	Non	Non
Exclusion des menaces (cf. page 380)	Non	Non	Non
Durée maximale de l'analyse d'un objet (cf. page 388)	60 s	Non	Non
Taille maximale de l'objet composé analysé (cf. page 389)	à 8 Mo	Non	Non
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. page 376)	Oui	Oui	Oui
Analyse des secteurs de démarrage (cf. page 376)	Oui	Oui	Oui
Analyse des objets composés (cf. page 383)	• Archives SFX* • Objets compactés* • Objets OLE incorporés* * uniquement les objets nouveaux et modifiés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE incorporés* * Tous les objets	• Archives* • Archives SFX* • Bases de données de messagerie électronique* • Message de texte plat* • Objets compactés* • Objets OLE incorporés* * Tous les objets
Traitement des fichiers autonomes (cf. page 170)	Oui	Oui	Oui

N'oubliez pas que les paramètres de sécurité **Application de la technologie iChecker**, **Application de la technologie iSwift**, **Application de l'analyseur heuristique et Vérification de la signature Microsoft** des fichiers ne font pas partie des paramètres des niveaux de protection prédéfinis. Si vous modifiez la valeur des paramètres **Application de la technologie iChecker**, **Application de la technologie iSwift**, **Application de l'analyseur heuristique** ou **Vérification de la signature Microsoft des fichiers**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

➡ *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le nœud **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez configurer les paramètres de sécurité.

3. Dans le panneau des résultats, sur l'onglet **Configuration de la zone d'analyse** sélectionnez le nœud auquel vous souhaitez appliquer un des niveaux de protection prédéfini.

4. Assurez-vous que le nœud sélectionné se trouve dans la couverture d'analyse (cf. page 136).

5. Dans la boîte de dialogue **Niveau de sécurité**, sélectionnez le niveau que vous souhaitez appliquer (cf. ill. ci-après).

   La boîte de dialogue reprend la liste des valeurs des paramètres de sécurité correspondant au niveau que vous avez sélectionné.

6. **Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande** Enregistrer la tâche afin d'enregistrer les modifications dans la tâche.

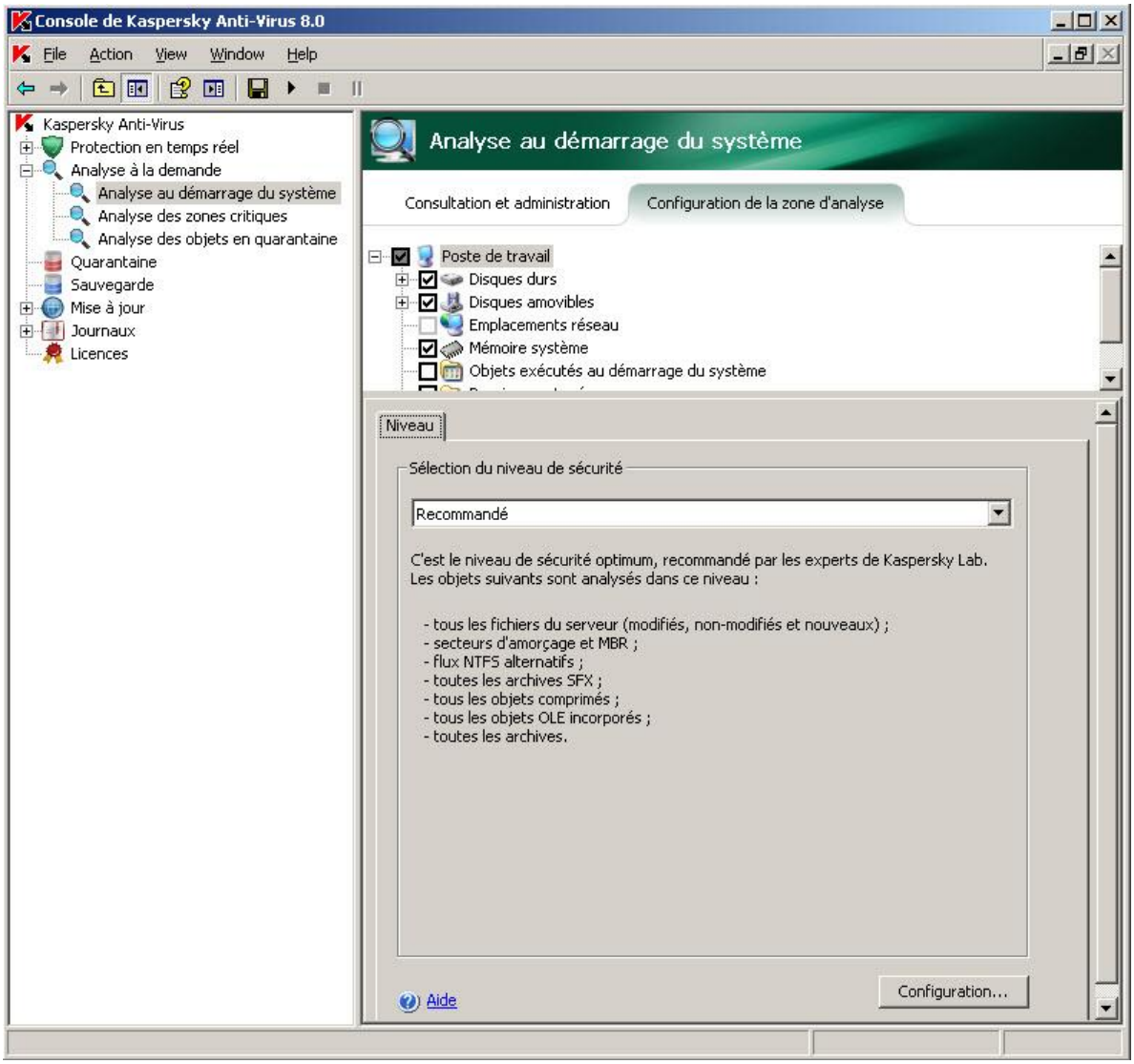


*Illustration 49. Boîte de dialogue **Niveau de sécurité***

CONFIGURATION MANUELLE DES PARAMETRES DE SECURITE DES TACHES D'ANALYSE A LA DEMANDE

Pour configurer les paramètres de sécurité manuellement, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Analyse à la demande** :

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez configurer les paramètres de sécurité.

3. Dans le panneau des résultats, sous l'onglet **Configuration de la zone de la protection**, sélectionnez le nœud dont vous souhaitez configurer les paramètres de sécurité. Assurez-vous que le nœud sélectionné se trouve dans la couverture d'analyse (cf. page 136).

4. La boîte de dialogue **Niveau** apparaît dans la partie inférieure du panneau des résultats (cf. ill. ci-après)**.**

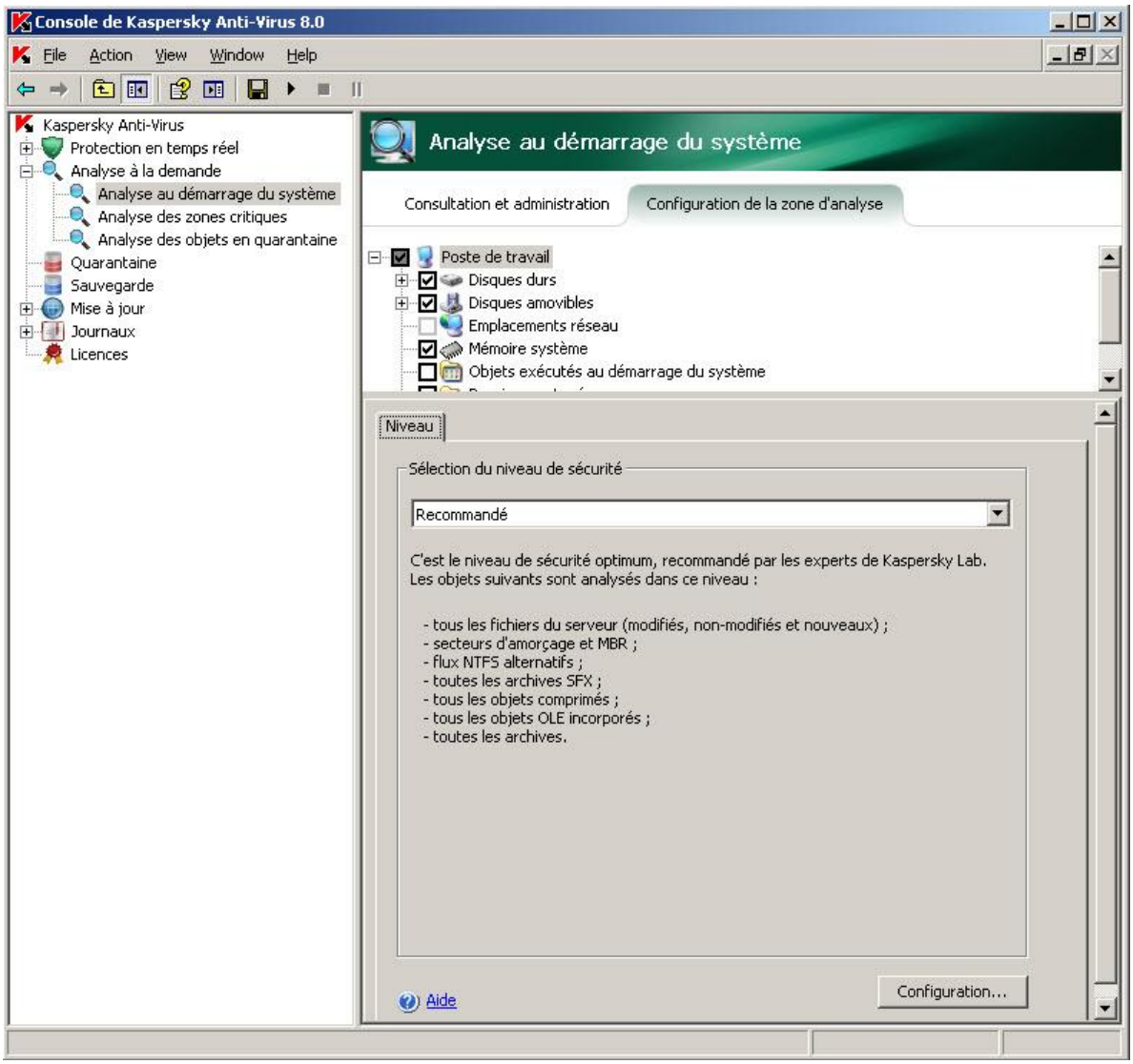


*Illustration 50. Boîte de dialogue **Niveau de sécurité***

5. Cliquez sur le bouton **Configuration** afin d'ouvrir la boîte de dialogue **Paramètres de sécurité**.

6. Dans la boîte de dialogue **Paramètres de sécurité**, configurez les paramètres requis pour le nœud sélectionné selon vos besoins. Pour ce faire, exécutez les actions suivantes :

- Sur l'onglet **Général**, exécutez les actions suivantes (cf. ill. ci-après) :
  - sous le titre **Étendue de la protection**, indiquez si Kaspersky Anti-Virus analysera tous les objets de la couverture de protection ou uniquement les objets d'un format ou d'une extension déterminé, si Kaspersky Anti-Virus analysera les secteurs d'amorçage des disques et l'enregistrement principal d'amorçage ou les flux NTFS alternatifs – objets à analyser (cf. page 376) ;
  - Sous le titre **Optimisation**, indiquez si Kaspersky Anti-Virus analysera tous les objets dans la couverture sélectionnée ou uniquement les objets nouveaux ou fichiers modifiés (cf. page 382) ;
  - Sous le titre **Protection des objets composés**, indiquez les objets composés que Kaspersky Anti-Virus analysera (cf. page 383).

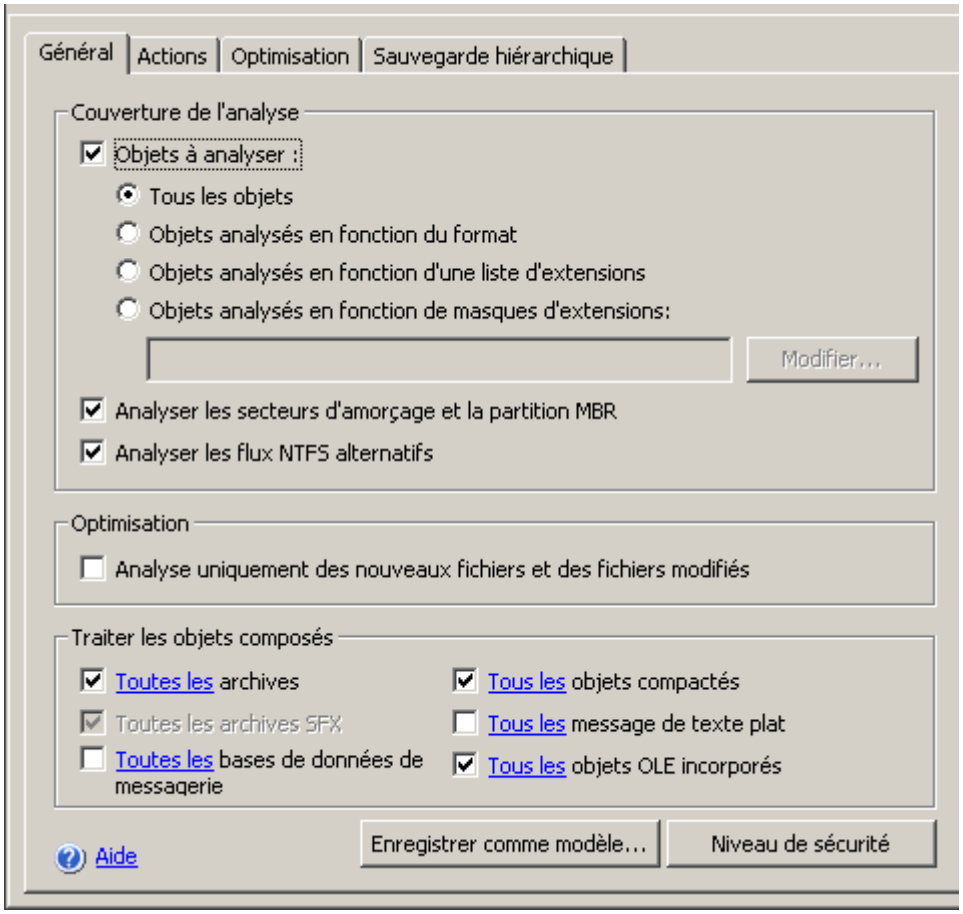


*Illustration 51. Fenêtre de configuration des paramètres de sécurité de la tâche d'analyse à la demande, onglet **Général***

- Le cas échéant, réalisez les opérations suivantes sous l'onglet **Actions** (cf. ill. ci-après) :
  - Sélectionnez action à exécuter sur les objets infectés (cf. page 384) ;
  - Sélectionnez action à exécuter sur les objets suspects (cf. page 386) ;
  - Le cas échéant, configurez les actions en fonction du type de menace découverte dans l'objet (cf. page 378).

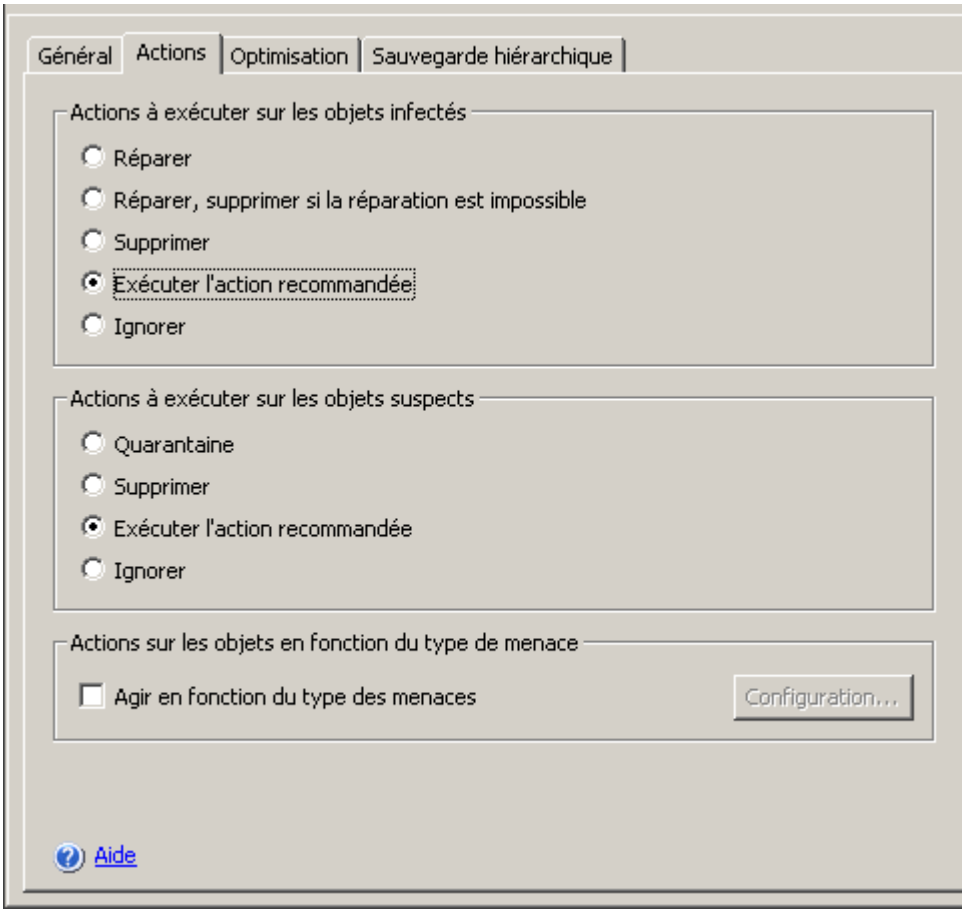


*Illustration 52. Fenêtre de configuration des paramètres de sécurité de la tâche d'analyse à la demande, onglet **Actions***

- Le cas échéant, réalisez les opérations suivantes sous l'onglet **Optimisation** (cf. ill. ci-après) :
  - excluez du traitement les fichiers sur la base du nom ou du masque (cf. page 379) ;
  - excluez du traitement les menaces en fonction du nom ou du masque du nom (cf. rubrique 380) ;
  - indiquez la durée maximale de l'analyse de l'objet (cf. rubrique 388) ;
  - indiquez la Taille maximale de l'objet composé analysé (cf. page 389) ;
  - activez ou désactivez l'application de la technologie iChecker (cf. page 389).
  - activez ou désactivez l'application de la technologie iSwift (cf. page 390) ;
  - indiquez si Kaspersky Anti-Virus vérifiera la présence de la signature de Microsoft dans les fichiers (cf. page 391).

*Illustration 53. Fenêtre de configuration des paramètres de sécurité de la tâche d'analyse à la demande, onglet **Optimisation***

- Sous l'onglet **Sauvegarde hiérarchique**, sélectionnez le mode de traitement des fichiers autonomes (cf. page 382) (cf. ill. ci-après).

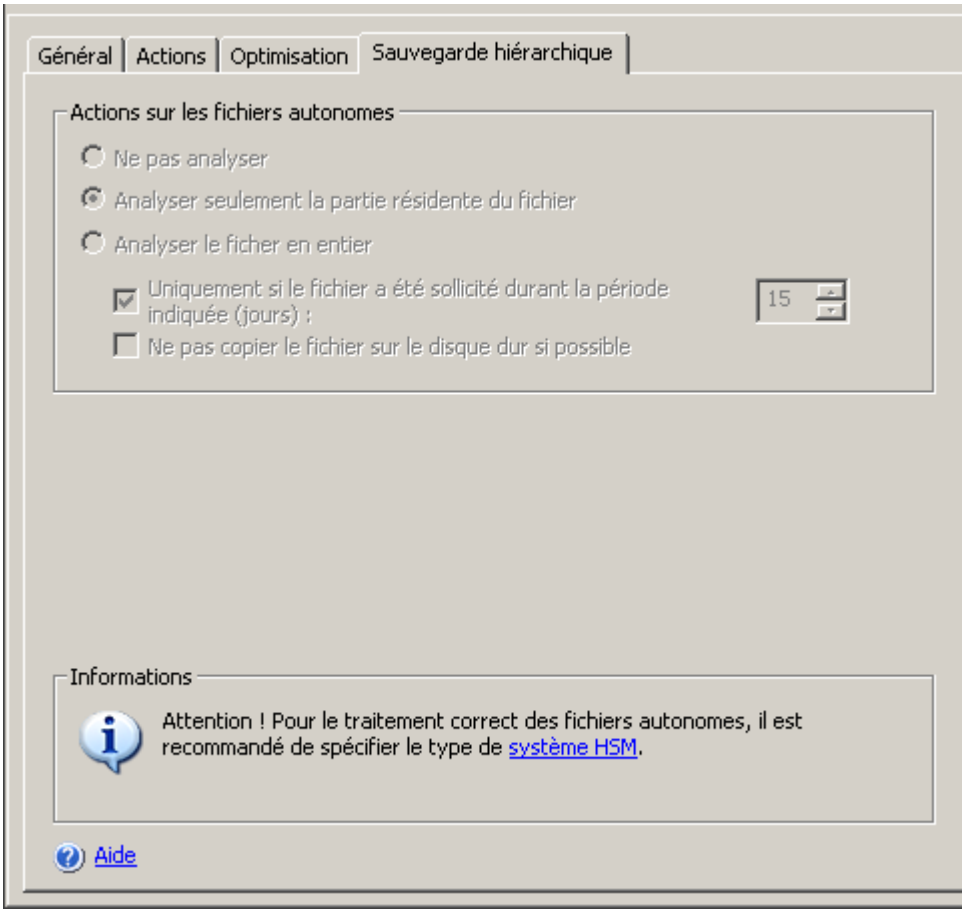


*Illustration 54. Fenêtre de configuration des paramètres de sécurité de la tâche d'analyse à la demande, onglet **Sauvegarde hiérarchique***

Vous pouvez désigner le mode de traitement des fichiers autonomes uniquement si vous aviez au préalable défini des paramètres d'accès à la sauvegarde hiérarchique différents des paramètres proposés par défaut.

7. Une fois que vous aurez configuré les paramètres de sécurité requis, ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

UTILISATION DE L'ANALYSEUR HEURISTIQUE DANS LA TACHE D'ANALYSE A LA DEMANDE

Vous pouvez, dans les tâches d'analyse à la demande, appliquer l'analyseur heuristique (cf. page 393) et configurer le niveau de l'analyse (cf. page 394).

Pour activer l'analyseur heuristique, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Analyse à la demande**.

2. Ouvrez le menu contextuel de la tâche d'analyse à la demande pour laquelle vous souhaitez activer l'analyse heuristique et sélectionnez **Propriétés**.

3. Dans l'onglet **Général** de la fenêtre **<Nom de la tâche> Propriétés**, cochez la case **Utiliser l'analyseur heuristique** et ajuster le niveau d'analyse comme souhaité.

Pour désactiver l'analyseur heuristique, décochez la case **Utiliser l'analyseur heuristique**.

4. Cliquez sur **OK**.

EXECUTION EN ARRIERE-PLAN DE LA TACHE D'ANALYSE A LA DEMANDE

Par défaut, les processus dans lesquels les tâches de Kaspersky Anti-Virus sont exécutées ont la priorité de base **Moyenne** (**Normal**).

Vous pouvez attribuer la priorité de base **Bas** (**Low**) au processus dans lequel la tâche d'analyse à la demande sera exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter quelques tâches en arrière-plan. Vous pouvez définir le nombre maximum de processus pour les tâches d'analyse à la demande en arrière plan (cf. page 358).

Vous pouvez définir la priorité de la tâche lors de sa création ou plus tard, dans la boîte de dialogue **<Nom de la tâche> Propriétés**.

Pour modifier la priorité de la tâche d'analyse à la demande, procédez comme suit :

1. Dans l'arborescence de la console, déployez le nœud **Analyse à la demande** :

2. Ouvrez le menu contextuel de la tâche d'analyse à la demande dont vous souhaitez modifier la priorité et sélectionnez la commande **Propriétés**.

3. La boîte de dialogue **Propriétés :<Nom de tâche>** s'ouvrira (cf. ill. ci-après).

*Illustration 55. Boîte de dialogue **Propriétés : <Nom de la tâche>***

4. Sur l'onglet **Général**, exécutez une des actions suivantes :

   - pour activer l'exécution en arrière-plan de la tâche, cochez la case **Exécuter la tâche en arrière-plan** ;

> Si vous activez ou désactivez l'exécution en arrière-plan de la tâche, la priorité de la tâche ne sera pas modifiée immédiatement mais uniquement au prochain lancement.

PARAMETRES DE PROTECTION DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS ET DANS LES TACHES D'ANALYSE A LA DEMANDE

Pendant que la tâche d'analyse à la demande est exécutée, vous pouvez consulter des informations détaillées sur le nombre d'objets traités par Kaspersky Anti-Virus depuis son lancement jusqu'à maintenant.

Ces informations seront accessibles si vous arrêtez la tâche. Vous pouvez consulter les statistiques de la tâche dans le journal d'exécution de la tâche (cf. rubrique " Consultation des informations relatives à la tâche dans le journal " à la page 234).

Pour consulter les statistiques de la tâche d'analyse à la demande, procédez comme suit :

1. Dans l'arborescence de la console, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.
3. Sous l'onglet **Consultation et administration** dans le panneau des résultats, cliquez sur le lien **Statistiques complètes** du groupe **Statistiques**.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Anti-Virus a traités depuis le lancement de la tâche jusqu'au moment actuel (cf. tableau ci-dessous).

Tableau 16. Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande

CHAMP	DESCRIPTION
Menaces détectées	Nombre de menaces détectées ; par exemple, si Kaspersky Anti-Virus a découvert un programme malveillant dans cinq objets, la valeur de ce champ augmentera d'une unité.
Objets infectés détectés	Total des objets infectés détectés
Objets suspects détectés	Nombre total d'objets suspects détectés
Objets non-réparés	Nombre d'objets que Kaspersky Anti-Virus n'a pas pu réparer pour les raisons suivantes : • le type de menace de l'objet ne peut pas être réparé ; • les objets de ce type ne peuvent pas être réparés ; • une erreur s'est produite lors de la réparation.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Anti-Virus aurait du mettre en quarantaine mais sans réussir à cause d'une erreur tel que le manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Anti-Virus a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone d'analyse que Kaspersky Anti-Virus n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre de fichiers dont les copies auraient du être placées par Kaspersky Anti-Virus en sauvegarde mais qui n'ont pas pu l'être en raison d'une erreur.
Erreurs d'analyse	Nombre d'objets dont le traitement a entraîné une erreur de Kaspersky Anti-Virus.
Objets réparés	Nombre d'objets réparés par Kaspersky Anti-Virus.
Placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Anti-Virus.
Objets sauvegardés	Nombre d'objets dont une copie a été mise en sauvegarde par Kaspersky Anti-Virus.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Anti-Virus.
Objets protégés par mot de passe	Nombre d'objets (archives comprimées, par exemple) que Kaspersky Anti-Virus a ignorés en raison d'une protection par mot de mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Anti-Virus a ignorés à cause de leur format endommagé.
Objets traités	Nombre total d'objets analysés par Kaspersky Anti-Virus.

BOITES DE DIALOGUE : ANALYSE A LA DEMANDE

DANS CETTE SECTION DE L'AIDE

ANALYSE A LA DEMANDE (ENTREE)

L'entrée **Analyse à la demande** permet de gérer les tâches d'analyse à la demande. Elle comprend des sous-entrées pour la gestion des tâches système : **Analyse au démarrage du système**, **Analyse complète de l'ordinateur** et **Analyse des objets en quarantaine**. Une sous-entrée séparée est créée pour chaque tâche créée par l'administrateur par la console de Kaspersky Anti-Virus et pour chaque tâche créée et transmise au serveur par Kaspersky Administration Kit.

Arborescence de la console

Les tâches systèmes sont des caractéristiques intégrées de Kaspersky Anti-Virus qui prennent en charge les fonctions suivantes :

- **Analyse au démarrage du système** : analyse à la recherche de virus la mémoire RAM, les secteurs d'amorçage et les programmes chargés au démarrage du système d'exploitation
- **Analyse complète de l'ordinateur** : analyse toutes les unités amovibles et fixes du serveur, les dossiers partagés, la mémoire du système et les objets de démarrage
- **Analyse des objets en quarantaine** : analyse les objets en quarantaine.

Les éléments d'administration repris dans le nœud **Analyse à la demande** permettent d'exécuter les opérations suivantes :

- Démarrer, stopper, suspendre et continuer des tâches
- Planifier le démarrage et l'arrêt automatiques des tâches
- Définir le compte utilisateur sous lequel la tâche sera exécutée
- Voir les statistiques d'activité de la tâche
- Ouvrir le dernier journal relatif à l'exécution de la tâche
- Créer et supprimer des tâches personnalisées d'analyse à la demande
- Configurer les paramètres des tâches prédéfinies et des tâches **Analyse au démarrage du système** et **Analyse complète de l'ordinateur**.

Panneau de résultats

Le panneau de résultats affiche l'état actuel des tâches d'analyse à la demande :

- **Nom de tâche** : nom de la tâche d'analyse à la demande
- **Catégorie de tâche** :
  - **Utilisateur** : la tâche a été créée sur le serveur sécurisé depuis une interface locale ou la ligne de commande, ou encore depuis la console d'administration, puis envoyée au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.
- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**) ; pourcentage de la tâche déjà terminé.
- **Heure de démarrage – date et heure de démarrage de la tâche.** L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Heure de fin estimée** : date et heure prévue pour la fin de la tâche. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Planification** : conditions de lancement d'une tâche programmée.

- **Prochain démarrage** : heure prévue pour le prochain lancement de la tâche programmée.

Panneau de tâches et menu contextuel

À l'aide des commandes du menu contextuel, vous pouvez effectuer les actions suivantes sur la tâche sélectionnée dans le panneau des résultats :

- **Ajouter tâche :** crée une tâche personnalisée d'analyse à la demande.
- **Modèles** : affiche la liste des modèles créés contenant des paramètres d'analyse.
- **Exporter les paramètres** : enregistre toutes les tâches système ou personnalisées d'analyse à la demande dans un fichier. Les données suivantes sont enregistrées :
  - Couverture de l'analyse
  - Couverture de protection et paramètres de chacune des zones d'analyse
  - Modèles de paramètres personnalisés
- **Importer les paramètres** : restaure les paramètres d'analyse à la demande depuis un fichier. Les tâches existantes ne sont pas supprimées. Les tâches importées sont ajoutées à la liste. Si une tâche existe avec le même nom, ses paramètres sont redéfinis avec les valeurs du fichier : la couverture d'analyse et les paramètres de chacune des zones d'analyse. Sont également ajoutés à la liste des modèles.

Pour gérer une tâche, sélectionnez l'entrée appropriée dans l'explorateur de la console ou dans la liste affichée dans le panneau de résultats.

VOIR EGALEMENT

Présentation des tâches d'analyse à la demande 131

Création d'une tâche d'analyse à la demande..... 47

Configuration de planification des tâches en MMC 50

Configuration des tâches d'analyse à la demande 132

ANALYSE AU DEMARRAGE DU SYSTEME (ENTREE)

La tâche prédéfinie **Analyse au démarrage du système** est lancée au démarrage de Kaspersky Anti-Virus sur le serveur. La mémoire vive, les secteurs d'amorçage et les principales entrées d'amorçage sur les disques durs et les disques amovibles du serveur sont analysés. Les objets qui ne peuvent être réparés sont supprimés et les objets suspects sont placés en quarantaine.

Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. La planification des tâches peut être modifiée.

L'entrée **Analyse au démarrage du système** permet de démarrer et d'arrêter les tâches **Analyse au démarrage du système**, de planifier ces tâches et d'afficher des statistiques de performances.

Onglet Consultation et administration

Le groupe **Administration** reprend les informations sur la catégorie de la tâche : **Prédéfinie**, tâche intégrée qui fait partie de l'application.

Configuration de la zone d'analyse (onglet)

L'onglet **Configuration de la zone d'analyse** représente l'arborescence des ressources fichiers du serveur. La partie inférieure de la fenêtre présente des informations relatives aux paramètres de protection du nœud sélectionné.

Si vous modifiez la zone d'analyse, vous pourrez rétablir la zone d'analyse par défaut en restaurant Kaspersky Anti-Virus (**Démarrer → Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Modification ou suppression**). Dans l'Assistant cochez la case **Rétablir** les paramètres recommandés de fonctionnement de l'application.

Menu contextuel

Le menu contextuel permet d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Enregistrer la tâche** : enregistre les modifications apportées aux valeurs des paramètres de la tâche.
- **Supprimer la tâche** : supprime la tâche personnalisée.
- **Paramètres** : affiche la description de la tâche, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution.

VOIR EGALEMENT

Configuration des tâches d'analyse à la demande 132

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande 154

Catégories de tâche dans Kaspersky Anti-Virus 46

NŒUD ANALYSE DES ZONES CRITIQUES

Le nœud **Analyse des zones critiques** sert à gérer la tâche système **Analyse des zones critiques**, à planifier son lancement et à afficher les statistiques de son exécution.

Par défaut, la tâche **Analyse des secteurs critiques** est exécutée une fois par semaine selon un horaire défini. Kaspersky Anti-Virus analyse les objets des secteurs critiques du système d'exploitation : objets de démarrage, secteurs d'amorçage et principales entrées d'amorçage des disques durs et amovibles et la mémoire système. Il analyse les fichiers qui se trouvent dans les répertoires système, par exemple dans le répertoire \system32.

Le panneau de résultats contient deux onglets : **Consultation et administration** et **Configuration de la zone d'analyse**.

Onglet Consultation et administration

Le groupe **Administration** reprend les informations sur la catégorie de la tâche : **Prédéfinie**, tâche intégrée qui fait partie de l'application.

Configuration de la zone d'analyse (onglet)

L'onglet **Configuration de la zone d'analyse** représente l'arborescence des ressources fichiers du serveur. La partie inférieure de la fenêtre présente des informations relatives aux paramètres de protection du nœud sélectionné.

Si vous modifiez la zone d'analyse, vous pourrez rétablir la zone d'analyse par défaut en restaurant Kaspersky Anti-Virus (**Démarrer → Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Modification ou suppression**). Dans l'Assistant cochez la case **Rétablir les paramètres recommandés de fonctionnement de l'application**.

Menu contextuel

Les commandes du menu contextuel permettent d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Enregistrer la tâche** : enregistre les modifications apportées aux valeurs des paramètres de la tâche.
- **Supprimer la tâche** : supprime la tâche personnalisée.
- **Paramètres** : affiche la description de la tâche, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution. Une liste détaillée des paramètres de la tâche sont affichés dans le journal d'exécution de la tâche, sur l'onglet **Paramètres**.

VOIR EGALEMENT

Configuration des tâches d'analyse à la demande 132

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande 154

ANALYSE DES OBJETS EN QUARANTAINE (ENTREE)

La tâche système **Analyse des objets en quarantaine** est utilisée pour l'analyse antivirus des objets se trouvant en quarantaine.

Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. La planification des tâches peut être modifiée.

Par défaut, la tâche est lancée après chaque mise à jour réussie de la base antivirus. Les fichiers infectés sont soumis à réparation et les fichiers qui ne peut être désinfecté sont envoyés en quarantaine. Avant d'être réparé ou supprimé, une

copie est enregistrée dans la zone de sauvegarde. Les objets classés comme suspects sont ignorés et restent alors en quarantaine.

L'entrée **Analyse des objets en quarantaine** permet de démarrer et d'arrêter les tâches **Analyse des objets en quarantaine**, de planifier ces tâches et d'afficher des statistiques de performances.

Onglet Consultation et administration

Le groupe **Administration** reprend les informations sur la catégorie de la tâche : **Prédéfinie**, tâche intégrée qui fait partie de l'application.

Menu contextuel

Les commandes du menu contextuel permettent d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Enregistrer la tâche** : enregistre les modifications apportées aux valeurs des paramètres de la tâche.
- **Supprimer (Supprimer la tâche)** : supprime la tâche personnalisée.
- **Paramètres** : affiche la description de la tâche, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution. Une liste détaillée des paramètres de la tâche sont affichés dans le journal d'exécution de la tâche, sur l'onglet **Paramètres**.

VOIR EGALEMENT

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande 154

Configuration de planification des tâches en MMC 50

NŒUD NOUVELLE TACHE D'ANALYSE A LA DEMANDE

Ce nœud est destiné à la configuration et à l'administration de la tâche d'analyse à la demande créée par l'utilisateur

Le panneau de résultats contient deux onglets : **Consultation et administration** et **Configuration de la zone d'analyse**.

Onglet Consultation et administration

Le groupe **Administration** reprend des informations sur la catégorie de la tâche : **Utilisateur** – la tâche a été créée pour un serveur protégé depuis l'interface locale ou la ligne de commande, ou encore depuis la console d'administration, puis envoyée au serveur à l'aide des outils d'administration à distance de Kaspersky Administration Kit.

Configuration de la zone d'analyse (onglet)

L'onglet **Configuration de la zone d'analyse** représente l'arborescence des ressources fichiers du serveur. La partie inférieure de la fenêtre présente des informations relatives aux paramètres de protection du nœud sélectionné.

Menu contextuel

Les commandes du menu contextuel permettent d'exécuter les opérations suivantes :

- **Démarrer** : démarre la tâche.
- **Suspendre** : suspend l'exécution de la tâche pour une période.
- **Relancer** : relance la tâche suspendue.
- **Arrêter** : arrête l'exécution de la tâche.
- **Ouvrir le journal d'exécution** : ouvre le dernier journal d'exécution de la tâche.
- **Enregistrer la tâche** : enregistre les modifications apportées aux valeurs des paramètres de la tâche.
- **Supprimer la tâche** : supprime la tâche personnalisée.
- **Paramètres** : affiche la description de la tâche, configure les paramètres de lancement/d'arrêt automatique et définit le compte utilisateur pour son exécution. Une liste détaillée des paramètres de la tâche sont affichés dans le journal d'exécution de la tâche, sur l'onglet **Paramètres**.

ONGLET CONSULTATION ET ADMINISTRATION. ANALYSE A LA DEMANDE

Administration

Le bloc **Administration** contient les informations suivantes relatives à la tâche :

- **Etat de la tâche** : état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée** ou **En pause**).
- **Heure de démarrage**.
- **Heure de fin.**
- **Catégorie de tâche** :
  - **Utilisateur** : la tâche a été créée sur le serveur sécurisé depuis une interface locale ou la ligne de commande, ou encore depuis la console d'administration, puis envoyée au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches créées pour le groupe administratif auquel le serveur sécurisé appartient, et envoyées au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.

Le lien **Ouvrir le journal d'exécution** ouvre le journal d'exécution de la tâche.

Propriétés

Le bloc **Propriétés** présente des informations relatives à la planification de la tâche, à l'heure prévue pour le prochain lancement de la tâche programmée, à la priorité de la tâche, à l'utilisation de l'analyseur heuristique et à l'application de la zone de confiance.

Le tableau contient la liste des couvertures d'analyse ainsi que les niveaux de protection appliqués à chacune d'entre elles.

Statistiques :

Le bloc **Statistiques** vous permet de visualiser les statistiques de la tâche.

VOIR EGALEMENT

Lancement / suspension / rétablissement / arrêt manuel d'une tâche 50

Affichage dans le journal d'informations relatives à la tâche 234

Configuration de planification des tâches en MMC 50

Utilisation de l'analyseur heuristique 393

Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande 154

Catégories de tâche dans Kaspersky Anti-Virus 46

CONFIGURATION DE LA ZONE D'ANALYSE (ONGLET) ANALYSE A LA DEMANDE

Cette entrée permet de démarrer ou de stopper les tâches d'analyse à la demande, de planifier ces tâches, d'afficher des statistiques et de configurer les paramètres d'analyse.

Vous pouvez modifier la présentation de l'onglet **Configuration de la zone d'analyse**. Pour ce faire, dans le menu contextuel de la tâche d'analyse à la demande, choisissez l'option **Apparence**, puis choisissez une des options proposées pour la présentation de cet onglet : **Hiérarchie horizontale**, **Hiérarchie verticale**, **Liste horizontale**, **Liste verticale**.

Par défaut, la tâche système **Analyse complète de l'ordinateur** est utilisée pour analyser toutes les unités amovibles et fixes du serveur, les dossiers partagés, la mémoire du système et les objets de démarrage.

Les tâches d'analyse d'utilisateur ou de groupe analysent la couverture spécifiée en fonction des paramètres associés.

La tâche prédéfinie **Analyse au démarrage du système** est lancée par défaut au démarrage de Kaspersky Anti-Virus sur le serveur. La mémoire vive, les secteurs d'amorçage et les principales entrées d'amorçage sur les disques durs et les disques amovibles du serveur sont analysés. Les objets qui ne peuvent être réparés sont supprimés et les objets suspects sont placés en quarantaine.

Si vous modifiez la zone d'analyse dans les tâches **Analyse au démarrage du système** et **Analyse des zones critiques**, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en restaurant Kaspersky Anti-Virus (**Démarrer → Programmes → Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition → Modification ou Suppression**).

La partie supérieure de l'onglet contient l'arborescence des ressources fichiers du serveur. Les éléments suivants sont affichés en tant qu'entrées :

- **Poste de travail**. Kaspersky Anti-Virus analyse tout le serveur.
- **Disques durs**. Kaspersky Anti-Virus analyse les objets du disque dur du serveur. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Disques amovibles**. Kaspersky Anti-Virus analyse les objets sur les disques amovibles tels que les disques compacts ou les clés USB. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Mémoire système**. Kaspersky Anti-Virus analyse la mémoire système et la mémoire des processus.
- **Objets de démarrage**. Kaspersky Anti-Virus analyse les objets auxquels renvoient les clés de la base de registres et les fichiers de configuration, par exemple WIN.INI ou SYSTEM.INI.
- **Dossiers partagés**. Kaspersky Anti-Virus analyse tous les dossiers partagés sur le serveur protégé.
- **Emplacements réseau**. Vous pouvez ajouter à la couverture d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux répertoires de réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte **Système local (SYSTEM)**.
- **Unités virtuelles**. Vous pouvez inclure dans la couverture de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe (créer couverture de protection virtuelle).

Les nœuds de l'arborescence des ressources fichiers du serveur sont illustrés de la manière suivante :

☑ Nœud repris dans la couverture de protection.

☐ Nœud exclu de la couverture de protection.

☑ Au moins un des nœuds intégrés à ce nœud est exclu de la couverture de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

Le nom des nœuds virtuels de la couverture d'analyse apparaît en lettres bleues.

"Niveau de sécurité" (fenêtre)

Dans la fenêtre **Niveau de sécurité**, vous pouvez sélectionner l'un des niveaux prédéfinis d'analyse à la demande ou ouvrir une fenêtre de configuration.

L'analyse est fixée par défaut sur le niveau de sécurité **Recommandé**. Pour modifier le niveau de protection, sélectionnez la valeur requise dans le menu déroulant **Niveau de sécurité** :

- La **vitesse maximum** ce niveau offre la vitesse la plus grande avec un niveau légèrement moindre de protection antivirus.

  Vous pouvez choisir de niveau de protection si votre réseau dispose, en plus de Kaspersky Anti-Virus, d'autres mécanismes de sécurité des pare-feu ou des stratégies de sécurité pou les utilisateurs, par exemple.

  Utilisez ce niveau de protection si vous devez garantir spécialement la vitesse d'échange des fichiers sur le serveur sécurisé.
- **Recommandé** : Kaspersky Lab considère ce niveau comme suffisant pour protéger les serveurs de fichiers sur la plupart des réseaux. Il combine de manière optimale la qualité de protection et la productivité du serveur.
- **Protection maximum** ce niveau assure la protection antivirus la plus grande possible, avec une légère diminution de rendement du système.

  Utilisez ce niveau si vous avez des besoins de sécurité plus grands sur le réseau.

Pour configurer manuellement la protection en temps réel, cliquez sur **Configuration**.

Si les paramètres de protection **en temps réel n'ont pas les valeurs par défaut, le niveau** Personnalisé sera automatiquement sélectionné dans la liste Niveau de sécurité.

Pour sauvegarder les modifications, cliquez sur **Enregistrer** dans la barre d'outils ou utilisez la même commande dans le menu contextuel de l'entrée de la tâche.

VOIR EGALEMENT

Sélection du niveau de sécurité prédéfini dans les tâches d'analyse à la demande 144

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

AJOUT D'UNE COUVERTURE D'ANALYSE (FENETRE)

Vous pouvez spécifier les objets qui seront ajoutés à la couverture d'analyse dans cette fenêtre. Sélectionnez une des options suivantes :

- **Couverture de l'analyse prédéfinie**, pour ajouter l'une des zones standard du système de fichiers du serveur. Choisissez la valeur requise dans le menu déroulant :
  - **Poste de travail** : la mémoire du système, les objets de démarrage, toutes les unités fixes et amovibles du serveur, ainsi que les dossiers partagés ne seront pas analysés
  - **Disques durs** : les disques durs du serveur seront tous analysés.
  - **Disques amovibles** : les supports amovibles connectés au serveur sécurisé, y compris les disquettes, les CD et les unités de mémoire flash USB, ne seront pas analysés.
  - **Mémoire système** : analyse tous les fichiers exécutables et les modules de processus exécutés par le système d'exploitation au moment de l'analyse.
  - **Dossiers partagés** : analyse tous les dossiers partagés situés sur le serveur.
  - **Objets de démarrage** : les objets chargés lors du démarrage du système d'exploitation seront analysés.
- **Unité ou dossier**, pour ajouter une unité ou un dossier complet à la couverture d'analyse. Indiquez le chemin complet et le nom de la ressource ou un masque utilisant les caractères génériques * et **?**, ou sélectionnez la ressource avec **Parcourir**. Vous pouvez indiquer plusieurs ressources séparées par un espace. Dans ce cas, chaque chemin doit figurer entre guillemets.
- **Fichier**, pour ajouter un fichier à la couverture d'analyse. Indiquez le chemin complet et le nom du fichier ou un masque utilisant les caractères génériques * et ?, ou sélectionnez le fichier avec Parcourir. Vous pouvez indiquer plusieurs fichiers séparés par un espace. Dans ce cas, chaque nom de fichier doit figurer entre guillemets. Pour sélectionner plusieurs fichiers dans la fenêtre Sélection du fichier, utilisez les touches **Ctrl** et **Maj**.

PROPRIETES DE LA TACHE : ONGLET GENERAL. ANALYSE A LA DEMANDE

Cette fenêtre affiche des informations générales à propos de la tâche :

- **Nom**- nom de la tâche. Cette zone peut contenir un maximum de 100 caractères.
- **Description**- informations supplémentaires sur la tâche, avec un maximum de 2000 caractères. Pour des tâches système, cette zone contient la description des fonctions réalisées et un résumé des principaux

paramètres. Pour des tâches personnalisées, la description est donnée par l'administrateur lorsqu'il crée la tâche.

Pour des tâches système, les informations de cette fenêtre ne sont pas modifiables. Les zones sont modifiables pour des tâches personnalisées.

Utiliser l'analyseur heuristique

Par défaut, l'analyseur heuristique est activé pour toute nouvelle tâche d'analyse à la demande. Pour modifier le niveau d'analyse, vérifiez que la case **Utiliser l'analyseur heuristique** est cochée et déplacez le curseur à la position requise. Pour désactiver l'analyseur heuristique, décochez la case **Utiliser l'analyseur heuristique**.

Appliquer la zone de confiance

La case cochée **Appliquer la zone de confiance** indique que lors de l'exécution de la tâche, outre les exclusions définies dans les paramètres de la tâche sur l'onglet **Optimisation**, seront également exclus les objets qui répondent aux conditions d'exclusion utilisées par le composant **Analyse à la demande**. Pour afficher ou modifier les règles d'exclusion, cliquez le lien repris dans le nom de la case. Dans la fenêtre **Zone de confiance** qui s'ouvre, ouvrez l'onglet **Règles d'exclusion**. Si la case **Appliquer la zone de confiance** n'est pas cochée, seuls les objets définis sur l'onglet **Performances** seront exclus de l'analyse. Cette case est cochée par défaut.

Exécuter la tâche en arrière-plan

La case **Exécuter la tâche en arrière-plan** permet de contrôler la priorité des tâches en exécution Respectez les règles suivantes lors de la définition de la priorité :

- Si la case est cochée, la tâche est exécutée avec une priorité inférieure aux autres tâches d'analyse à la demande et aux autres applications du serveur. De cette manière, le système d'exploitation accordera des ressources à la tâche en fonction de la charge de l'unité centrale et du système de fichier par les autres applications. L'activité de la tâche diminuera ou augmentera inversement à la charge du serveur.

- Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Anti-Virus et les autres applications. Dans ce cas, la charge du serveur sera plus grande, mais la tâche s'exécutera plus rapidement.

Par défaut, la case est décochée pour les tâches prédéfinies, de groupe et définies par l'utilisateur.

Si la case **Considérer comme une tâche d'analyse complète** est cochée, le serveur d'administration enregistrera l'événement **Analyse complète de l'ordinateur terminée** après l'exécution de cette tâche et mettra à jour l'état de protection du serveur. La case **Considérer l'exécution de la tâche d'analyse des zones critiques** est cochée pour la case prédéfinie **Analyse des secteurs critiques** et elle est désactivée pour toutes les autres tâches locales. Vous pouvez utiliser la console de Kaspersky Anti-Virus dans MMC afin de modifier l'état de la case pour les tâches de groupe.

VOIR EGALEMENT

Configuration des tâches d'analyse à la demande 132

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET GENERAL. ANALYSE A LA DEMANDE

L'onglet **Général** affiche les paramètres d'analyse à la demande qui déterminent les objets explorés à la recherche de code malfaisant.

Dans la section **Couverture de l'analyse**, définissez les objets qui seront soumis à la recherche de code malveillant.

Sélectionnez les **Types d'objets** et sélectionnez l'une des options d'analyse suivantes :

- Analyser tous les **objets**- analyse tous les fichiers sans exception.

- **Objets analysés en fonction du format**- analyse tous les objets potentiellement infectés. La décision d'analyser dépend du format de fichier. Avant de rechercher des virus dans un objet, le format du fichier est identifié (fichier texte, archives de messagerie, etc.). Si ce format se trouve sur la liste des formats de fichiers potentiellement infectés, le fichier est transmis à Kaspersky Anti-Virus pour analyse.

  La liste de ces formats est élaborée par les experts de Kaspersky Lab. Elle fait partie de la base de Kaspersky Anti-Virus qui est mise à jour en même temps que celle-ci.

  Si vous sélectionnez cette option, la tâche prendra plus de temps qu'avec l'option d'analyse en fonction de l'extension, bien que la qualité de l'analyse soit meilleure.

  Un certain nombre de formats de fichiers ne présentent qu'un léger risque que du code malveillant ait été inséré et qu'il puisse être activé par la suite. Un fichier texte en est un exemple. Par ailleurs, certains formats de fichiers contiennent ou peuvent contenir du code exécutable. Par exemple, les formats .exe, .dll, ou .doc. Le risque d'insertion et d'activation de code malveillant est nettement élevé pour ces fichiers.

- **Objets analysés en fonction d'une liste d'extensions** : analyse uniquement les fichiers potentiellement infectés. La décision d'analyser dépend de l'extension de fichier. Si l'extension se trouve dans la liste des extensions de fichiers potentiellement infectés, le fichier sera transmis à Kaspersky Anti-Virus pour analyse.

  La liste des extensions est élaborée par les experts de Kaspersky Lab. Elle fait partie de la base de Kaspersky Anti-Virus qui est mise à jour en même temps que celle-ci.

  Cette option accélère la vitesse d'échange de fichiers entre l'application et le serveur sécurisé, mais Kaspersky Anti-Virus pourra ignorer un objet si son extension a été modifiée.

  n'oubliez pas que quelqu'un peut transmettre à votre ordinateur un virus avec l'extension.txt, alors qu'il s'agit en fait d'un fichier exécutable renommé à fichier.txt. Si vous sélectionnez l'option **Objets analysés en fonction d'une liste d'extensions**, un tel fichier sera ignoré au cours du processus d'analyse. En revanche, si vous choisissez **Objets analysés en fonction du format**, alors quelle que soit l'extension, l'application détectera le format .exe et analysera le fichier.

Objets analysés en fonction de masques d'extensions- analyse uniquement les objets qui répondent à la liste des extensions et des masques d'extensions créés par l'administrateur. Si cette option a été choisie, cliquez sur **Modifier** pour modifier la liste des extensions ou pour utiliser la liste prédéfinie (cf. page 172).

VOIR EGALEMENT

Configuration des tâches d'analyse à la demande 132

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET ACTIONS. ANALYSE A LA DEMANDE

L'onglet **Actions** affiche les paramètres qui déterminent la réponse de Kaspersky Anti-Virus après une analyse. Les objets non infectés sont ignorés. Vous pouvez configurer le traitement des autres objets en fonction de leur état, attribué par l'analyse, ou du type de menace détecté.

Certains types de menaces sont plus dangereux que d'autres pour le serveur. Par exemple, un cheval de Troie peut causer plus de dommages qu'un logiciel publicitaire (adware). Vous pouvez spécifier les différentes actions de Kaspersky Anti-Virus, en fonction du type de menace contenu dans l'objet.

Par défaut, Kaspersky Anti-Virus traite les objets en fonction de l'état attribué par l'analyse : les fichiers infectés sont soumis à réparation. Si la réparation est impossible, ils sont supprimés. Avant traitement (réparé ou supprimé), l'exemplaire original est enregistré dans la zone de sauvegarde.

Vous pouvez modifier les valeurs attribuées ou configurer l'ordre de traitement de l'objet en fonction du type de menace détectée par Kaspersky Anti-Virus.

Pour analyser les objets en fonction de l'état attribué pendant l'analyse, sélectionnez l'une des options suivantes dans les sections **Actions à exécuter sur les objets infectés** et **Actions à exécuter sur les objets suspects** :

- **Réparer** (applicable uniquement aux objets infectés). Kaspersky Anti-Virus essaie de réparer l'objet infecté. Si c'est possible, l'objet est réparé et la version réparée est enregistrée sur disque. Il place l'exemplaire original de l'objet dans la zone de sauvegarde. Si l'objet ne peut pas être réparé, il est laissé sur le disque dans son état d'origine. Nous vous recommandons de supprimer les objets qui ne peuvent pas être réparés.

- **Réparer; supprimer si la réparation est impossible** (uniquement pour les objets infectés). Kaspersky Anti-Virus essaie de réparer l'objet infecté. Si c'est possible, l'objet est réparé et la version réparée est enregistrée sur disque, pour remplacer l'original. Si l'objet est impossible à réparer, Kaspersky Anti-Virus le supprime. La version originale sera enregistrée dans la zone de sauvegarde.

- **Supprimer**. Kaspersky Anti-Virus supprime l'objet infecté ou suspect. La version originale sera enregistrée dans la zone de sauvegarde.

- **Exécuter l'action recommandée**. Kaspersky Anti-Virus applique automatiquement l'action recommandée par les experts de Kaspersky Lab. La version originale sera enregistrée dans la zone de sauvegarde.

- **Ignorer.** Kaspersky Anti-Virus ignore l'objet. Si l'enregistrement de ce type d'événements est activé, les informations concernant l'objet infecté ou suspect détecté seront enregistrées dans le rapport. À l'issue de la procédure, l'objet est laissé sur disque dans son état d'origine.

- **Quarantaine** (uniquement pour les objets suspects). Kaspersky Anti-Virus déplace l'objet suspect vers la quarantaine, où l'objet est enregistré sous un format chiffré, afin de neutraliser la menace d'infection. Les fichiers en quarantaine peuvent être analysés à l'aide d'une mise à jour de la base de Kaspersky Anti-Virus, par l'administrateur ou transmis à Kaspersky Lab.

Pour configurer le traitement d'un objet en fonction du type de menace détecté, cochez **Agir en fonction du type de menace** dans la section **Actions sur les objets en fonction du type de menace** et cliquez sur **Paramètres**.

Pour sauvegarder les modifications, cliquez sur **Enregistrer** dans la barre d'outils ou utilisez la même commande dans le menu contextuel de l'entrée de la tâche.

VOIR EGALEMENT

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

CONFIGURATION DES PARAMETRES DE SECURITE : ONGLET OPTIMISATION. ANALYSE A LA DEMANDE

L'onglet **Optimisation** affiche les paramètres permettant d'exclure certains fichiers de l'analyse. Ces paramètres contrôlent la vitesse d'analyse et le rendement général du serveur.

Il est possible d'exclure de l'analyse les objets suivants :

- fichiers en fonction du nom ou d'un masque de noms ;

- objets en fonction du type de menace qu'ils contiennent ;

Cette option permet d'exclure des logiciels avec licence que Kaspersky Anti-Virus pourrait considérer comme malveillants ou potentiellement dangereux, comme par exemple des programmes d'administration à distance, des clients IRC, des serveurs FTP et tout utilitaire employé pour interrompre des processus.

- objets du système de fichier qui n'ont pas changé depuis la dernière analyse antivirus ;
- objets dont la durée d'analyse dépasse le délai défini
- objets composés de grande taille;
- les objets non infectés qui possèdent une signature numérique authentifiée et saine appartenant à la société Microsoft.

La liste des fichiers exclus de l'analyse est créée en fonction des caractéristiques spécifiques des objets présents sur le serveur, ainsi que des applications qui ont accès ou sont installées sur le serveur. La création d'une telle liste d'exclusion peut s'imposer, par exemple, si Kaspersky Anti-Virus bloque l'accès à un objet ou une application quelconque alors que vous êtes convaincu que cet objet ou cette application ne représente absolument aucun danger pour le serveur protégé. Cochez la case **Exclure les objets** dans le groupe de champs **Exclusions** afin d'exclure de l'analyse les objets en fonction du nom ou du masque de nom du fichier. Pour créer une liste d'exclusions, cliquez sur **Modifier**.

Cochez **Exclure les menaces** dans la zone **Exclusions** pour exclure de l'analyse les objets en fonction du type de menace détecté. Vous pouvez exclure des menaces en fonction du nom tel qu'il apparaît dans l'Encyclopédie des virus à l'adresse www.viruslist.com/fr/ ou en fonction d'un masque. L'usage de masques vous permet d'exclure une classe complète de menaces. Pour créer une liste d'exclusions, cliquez sur **Modifier**.

Dans le groupe de champs **Configuration complémentaire**, cochez une des cases suivantes :

- **Arrêter si l'analyse dure plus de** pour limiter le temps d'analyse d'un objet. Spécifiez la durée maximum d'analyse en secondes. La valeur par défaut est de 60 secondes.
- **Ne pas analyser les objets composés de plus de** pour ignorer les objets composés de taille supérieure à la taille spécifiée. Spécifier la taille maximum d'un objet composé, en mégaoctets. La valeur par défaut est de 8 Mo.
- **Utiliser la technologie iChecker** si vous souhaitez que Kaspersky Anti-Virus analyse uniquement les fichiers nouveaux ou modifiés depuis l'analyse précédente. L'utilisation de la technologie iChecker réduit la charge sur le processeur et sur le système disques et accélère l'analyse des objets.

  Kaspersky Anti-Virus n'ignore pas les objets s'ils ont été modifiés, si les paramètres de sécurité ont été renforcés après la dernière analyse, ou si la base antivirus a été mise à jour après la dernière analyse.

- **Utiliser la technologie iSwift** (pour des objets du système de fichiers NTFS) si vous souhaitez que Kaspersky Anti-Virus analyse uniquement les fichiers nouveaux ou modifiés depuis l'analyse précédente.
- **Vérifier la signature Microsoft des fichiers** si vous souhaitez exclure des analyses ultérieures les objets non infectés qui possèdent une signature numérique authentifiée et non altérée appartenant à la société Microsoft.

  Lorsque la case est cochée, Kaspersky Anti-Virus contrôlera, après l'analyse antivirus, la présence de signatures numériques Microsoft et leur authenticité pour tous les objets non infectés. Les fichiers non infectés et disposant d'une signature Microsoft non altérée et authentique ne seront plus analysés jusqu'à ce que le fichier soit modifié. Kaspersky Anti-Virus analysera à nouveau le fichier lorsque celui-ci sera modifié.

  La case **Vérifier la signature Microsoft des fichiers** est décochée et inaccessible si la case **Utiliser la technologie iSwift** est décochée.

  Lors de la modification de l'état de la case **Vérifier la signature Microsoft des fichiers** (cochée ou non), le niveau de protection sélectionné pour la zone ne change pas.

VOIR EGALEMENT

CONFIGURATION DES PARAMETRES DE SECURITE : L'ONGLET SAUVEGARDE HIERARCHIQUE. ANALYSE A LA DEMANDE

L'onglet **Sauvegarde hiérarchique** permet de définir les modes de traitement des fichiers qui se trouvent dans les stockages distants.

Vous pouvez attribuer les valeurs suivantes au paramètre :

- **Ne pas analyser**. Le système n'analyse pas le fichier autonome.
- **Analyser seulement la partie résidente du fichier**. Le système analyse la partie du fichier enregistrée sur le disque. La partie du fichier située sur le stockage distant n'est pas sollicitée.
- **Analyser le fichier en entier**. Vous pouvez définir les valeurs des paramètres complémentaires :
  - **Uniquement si le fichier a été sollicité durant la période indiquée (jours)**. Le système analyse uniquement les fichiers qui ont été sollicités durant la période indiquée.
  - **Ne pas copier le fichier sur le disque dur (si possible)**. Le système ne restaurera pas le fichier depuis le stockage HSM sur le disque dur mais l'analysera dans le stockage temporaire. Pour que cette option fonctionne correctement, assurez-vous que le système HSM installé prend en charge l'analyse de fichiers sans restauration sur le disque dur.

CHOISIR L'ACTION EN FONCTION DU TYPE DE MENACE (FENETRE). ANALYSE A LA DEMANDE

Cette fenêtre permet de configurer l'ordre de traitement des objets par Kaspersky Anti-Virus, en fonction des types de menaces qu'ils contiennent.

Les actions définies en fonction des types de menaces détectées par Kaspersky Anti-Virus sont affichées dans le tableau **Actions actuelles**.

Certains types de menaces sont plus dangereux que d'autres pour le serveur. Par exemple, un cheval de Troie peut causer plus de dommages qu'un logiciel publicitaire (adware). Vous pouvez spécifier les différentes actions de Kaspersky Anti-Virus, en fonction du type de menace contenu dans l'objet.

Deux actions peuvent être définies pour chaque type de menace. Kaspersky Anti-Virus exécute la seconde action si la première échoue. Par exemple, si Kaspersky Anti-Virus ne parvient pas à réparer un objet ou à le supprimer en appliquant la première action, l'objet sera en quarantaine pour la seconde action.

Avant traitement (réparé ou supprimé), l'exemplaire original est enregistré dans la zone de sauvegarde.

Pour configurer le traitement d'objets en fonction du type de menace détecté, sélectionnez **Type de menace** dans la liste déroulante. Avec les menus **Première action** et **Deuxième action**, spécifiez ensuite les actions prises par Kaspersky Anti-Virus quand il détecte une menace de ce type.

La liste **Type de menace** affiche tous les types de menaces détectés par Kaspersky Anti-Virus. La liste des actions peut contenir les éléments suivants pour chacun des types de menaces :

- **Ignorer, ne pas considérer comme une menace** : ignore l'objet en lui attribuant l'état *non infecté*. Si l'enregistrement de ce type d'événements est activé, les informations concernant l'objet non infecté détecté seront enregistrées dans le journal relatif à l'exécution de la tâche.
- **Réparer** : répare l'objet.
- **Supprimer** : supprime l'objet.
- **Ignorer** : ignore l'objet. Si l'enregistrement de ce type d'événements est activé, les informations concernant l'objet détecté seront enregistrées dans le rapport.

  Si la première action sélectionnée est **Ignorer, ne pas considérer comme une menace** ou **Ignorer**, il n'est pas possible de configurer une seconde action.

- **Quarantaine** : supprime l'objet de son emplacement d'origine et le déplace vers la Quarantaine.

Spécifiez les actions pour toutes les menaces de la liste.

Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

VOIR EGALEMENT

Actions en fonction du type de menace 378

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

EXCLUSION DES OBJETS : FENETRE LISTE DES EXCLUSIONS ANALYSE A LA DEMANDE

La fenêtre **Liste des exclusions** présente des noms et des extensions de fichiers que Kaspersky Anti-Virus n'analysera pas.

La partie supérieure de la fenêtre contient un champ pour ajouter un nouvel élément à la liste.

Pour ajouter un nouvel élément à la liste, entrez le nom ou l'extension de fichier ou le masque d'extension dans la zone de saisie supérieure et cliquez sur **Ajouter**.

Pour créer les masques, utilisez les caractères génériques * et ?

Voici des exemples de masques autorisés utilisables pour créer des listes d'exclusion de fichiers :

- **eicar.*** : tous les fichiers avec le nom **eicar** ;
- ***.exe** : tous les fichiers avec extension .exe ;

- ***.ex?** : tous les fichiers avec extension. Ex?, où ? peut représenter tout caractère singulier. Par exemple : ex, exe, ex1;

- **ex*** : tous les fichiers avec l'extension commençant par ex, où * représentent un nombre quelconque de caractères. Par exemple : ex, exe, exemple.

Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**.

EXCLUSION DES MENACES : FENETRE LISTE DES EXCLUSIONS. ANALYSE A LA DEMANDE

La fenêtre **Liste des exclusions** permet de créer une liste de menaces exclues de l'analyse par Kaspersky Anti-Virus. La liste est vide par défaut.

Pour ajouter un nouvel élément à la liste, entrez le nom ou le masque de la menace dans la zone supérieure et cliquez sur **Ajouter**.

Vous pouvez spécifier le nom complet de la menace tel qu'il apparaît dans l'Encyclopédie des virus à l'adresse www.viruslist.com/fr/ ou encore, un masque du nom de la menace. L'usage de masques vous permet d'exclure une classe complète de menaces.

Le nom de la menace est défini lors de l'analyse de l'objet et peut contenir les informations suivantes : **<catégorie de menace>:<type de menace>.<nom abrégé de la plateforme>.<nom de la menace>.<code de modification de la menace>**.

Admettons que vous utilisez l'utilitaire Remote Administrator en guise d'outil d'administration à distance. La plupart des programmes antivirus classent le code de cet utilitaire dans la classe de menace "potentiellement dangereuses" (**Riskware**). Si vous ne souhaitez pas verrouiller Remote Administrator, ajoutez les informations suivantes à la liste des menaces exclues. Pour le nom, vous pouvez spécifier :

- **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus ignorera uniquement le programme Win32.RAdmin.20.

- Masque du nom complet de la menace : **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions de Remote Administrator.

- Masque du nom complet de la menace, avec uniquement le type de menace :**not-a-virus:***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions des objets contenant cette classe de menace.

Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**.

LISTE DES EXTENSIONS DE FICHIERS ANALYSES PAR DEFAUT. ANALYSE A LA DEMANDE

Kaspersky Anti-Virus analyse par défaut les fichiers possédant les extensions suivantes :

386 : pilote du mode étendu ou fichier de Microsoft Windows ;

acm : fichier du répertoire système Windows ;

ade, *adp* : projet Microsoft Access ;

asp : script Active Server Pages ;

asx : script Cheyenne Backup ; fichier de réorientation (Redirector) pour Microsoft Advances Streaming Format ; fichier vidéo ;

ax : filtre DirectShow ;

bas : texte du programme BASIC ;

bat : fichier de paquet ;

bin : fichier binaire ;

chm : fichier HTML compilé ;

cla, *clas** : classe Java ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS) ;

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64Ko ;

cpl : module du panneau de configuration de Microsoft Windows :

crt : fichier Crontab dans Unix ou fichier de certificat ;

dll : bibliothèque dynamique ;

dpl : bibliothèque Borland Delphi compactée ;

drv : pilote d'un périphérique quelconque ;

dvb : pilote d'un périphérique DOS ;

dwg : base de données de dessins AutoCAD ;

efi : fichier Crontab ou fichier de certificat dans Unix ;

emf : fichier au format Enhanced Metafile ;

eml : message électronique de Microsoft Outlook Express ;

exe : fichier exécutable ; archive autoextractibe ;

fon : fichier de police ;

fpm : programme de bases de données, fichier de démarrage de Microsoft Visual FoxPro ;

hlp : fichier d'aide au format Win Help ;

hta : programme hypertexte pour Microsoft Internet Explorer ;

htm, *html** : document hypertexte ;

htt : modèle de fichier hypertexte Microsoft Windows ;

ico : fichier d'icône d'objet ;

inf : fichier d'informations ;

ini : fichier d'initialisation ;

ins : script InstallShield (Installation Authoring Solution) ;

isp : fichier des paramètres Microsoft IIS du fournisseur (IIS Internet Service Provider Settings) ;

jpg, *jpeg :* fichier graphique de conservation de données compressées ;

js,*jse* : texte source JavaScript ;

lnk : fichier lien dans Microsoft Windows ;

mbx : base de Microsoft Outlook Express ;

msc : fichier de la console MMC ;

msg : message électronique de Microsoft Mail ;

msi : paquet Microsoft Windows Installer ;

msp : paquet de mise à jour Microsoft Windows Installer ;

mst : fichier de transformation de Microsoft Windows Installer ;

nws : nouveau message électronique de Microsoft Outlook Express ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

oft : modèle de message Microsoft Outlook ;

otm : projet VBA pour Microsoft Office Outlook ;

pcd : image Kodak Photo-CD ;

pdf : document Adobe Acrobat ;

php : script intégré dans les fichiers HTML ;

pht : fichier HTML avec scripts PHP intégrés ;

*phtm** : document hypertexte contenant des scripts PHP intégrés ;

pif : fichier contenant des informations sur un logiciel ;

plg : message électronique ;

png : image Portable Network Graphics ;

pot : modèle Microsoft PowerPoint ;

prf : fichier système Microsoft Windows ;

prg : texte du programme dBase, Clipper ou Microsoft Visual FoxPro, programme de la suite WAVmaker ;

reg : fichier d'enregistrement des clés de la base de registres système de Microsoft Windows ;

rsc : fichier Pegasus Mail Resource ;

rtf : document au format Rich Text Format ;

scf: fichier de commande Microsoft Windows Explorer ;

scr : fichier d'écran de veille de Microsoft Windows ;

sct : format Microsoft FoxPro ;

shb : présentation Corel Show ;

shs : fragment de Shell Scrap Object Handler ;

sht : document S-HTML ;

*shtm** est un document hypertexte contenant SSI : Server Side Includes d'ajout du serveur (certaines actions supplémentaires réalisées par le serveur) ;

swf : objet d'un paquet Shockwave Flash ;

sys : fichier système, par exemple fichier du pilote Microsoft Windows ;

the : modèle pour le bureaul Microsoft Windows 95 ;

*them** : thème pour le bureau Microsoft Windows ;

tsp : programme qui fonctionne en mode de partage du temps ;

url : lien Internet ;

vb : fichier Visual Basic ;

vbe : fichier VBScript Encoded Script ;

vbs : script Visual Basic ;

vxd : pilote d'un périphérique virtuel Microsoft Windows.

wma : fichier audio Microsoft Windows Media ;

wmf : métafichier Microsoft Windows Media ;

wmv : fichier vidéo Microsoft Windows Media ;

wsc : composant Windows Script ;

wsf : script Microsoft Windows ;

wsh : fichier de configuration de Windows Script Host ;

do? : documents et fichiers de Microsoft Office Word tels que : *doc* – document Microsoft Office Word, *dot* – modèle de documents Microsoft Office Word, etc. ;

md? : documents et fichiers de Microsoft Office Access tels que : *mda* – groupe de travail de Microsoft Office Access, *mdb* – base de données, etc.;

mp? : fichier audio ou animation MPEG ;

ov?: fichiers exécutable MS DOS ;

pp? : documents et fichiers de Microsoft Office PowerPoint tels que : *pps* – dia Microsoft Office PowerPoint ;

vs? : documents et fichiers Visio tels que : *vss* – fichier de modèle Visio, *vsw* – espace de travail Vision, etc. ;

xl? : – documents et fichiers de Microsoft Office Excel tels que : *xla* – extension Microsoft Excel, *xlc* – schéma, *xlt* – modèle de document, etc.

ANALYSE SELON LA LISTE DES EXTENSIONS : FENETRE LISTE DES MASQUES D'EXTENSIONS ANALYSE A LA DEMANDE

La fenêtre **Liste des masques d'extensions** permet de créer une liste d'extensions et des masques d'extensions de fichiers analysés par Kaspersky Anti-Virus.

Vous pouvez utiliser la liste par défaut (cf. page 172). Pour ce faire, cliquez sur **Par défaut**.

Pour ajouter un nouvel élément à la liste, entrez l'extension ou le masque d'extension du fichier dans la zone supérieure et cliquez sur **Ajouter**.

Pour créer les masques, utilisez les caractères génériques * et ? Notez que le point séparateur du nom et de l'extension du fichier n'est pas indiqué.

Voici des exemples de masques autorisés utilisables pour créer des listes d'exclusion de fichiers :

- **exe** : tous les fichiers avec l'extension .exe ;
- **ex?** : tous les fichiers avec extension. Ex?, où ? peut représenter tout caractère singulier. Par exemple : ex, exe, ex1;
- **ex*** : tous les fichiers avec l'extension commençant par ex, où * représentent un nombre quelconque de caractères. Par exemple : ex, exe, exemple.

Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**.

MODELES (FENETRE). ANALYSE A LA DEMANDE

Cette fenêtre affiche la liste des modèles créés contenant des paramètres d'analyse.

Vous pouvez examiner le paramètres contenus dans un modèle. Pour ce faire, sélectionnez le modèle dans la liste puis cliquez sur **Voir**.

Pour actualiser la liste des modèles,

cliquez sur le bouton **Mettre à jour**.

Pour supprimer un modèle,

sélectionnez-le dans la liste et cliquez sur **Supprimer**.

PROPRIETES DU MODELE (FENETRE). ANALYSE A LA DEMANDE

Dans les tâches d'analyse à la demande et de **Protection en temps réel des fichiers**, vous avez la possibilité d'enregistrer dans un modèle les paramètres d'analyse ou de protection configurés pour une certaine entrée.

Vous pouvez appliquer un modèle basé sur les paramètres de sécurité de n'importe quel nœud de manière à rapidement configurer les paramètres de sécurité d'un autre nœud.

Les modèles créés au sein d'une tâche **Protection en temps réel des fichiers** ne peuvent être appliqués qu'à une tâche **Protection en temps réel des fichiers**. Les modèles créés au sein d'une tâche d'analyse à la demande peuvent être appliqués dans toute autre tâche d'analyse à la demande. Ils ne peuvent pas être appliqués dans la tâche **Protection en temps réel des fichiers**.

Pour conserver les valeurs des paramètres de l'analyse (de la protection) dans le modèle, procédez comme suit :

1. Saisissez le nom du modèle dans le champ **Nom du modèle**.
2. Dans la zone **Description**, entrez des informations supplémentaires pour décrire les paramètres enregistrés dans le modèle.

MODELES : GENERAL (ONGLET). ANALYSE A LA DEMANDE

Cet onglet affiche des informations générales sur le modèle généré quand il a été créé :

- **Nom** : entrez le nom du modèle.
- **Description** : informations sur les paramètres enregistrés dans le modèle.

Ces zones ne sont pas modifiables.

MODELES: ONGLET PARAMETRES ANALYSE A LA DEMANDE

Cet onglet affiche la liste des paramètres enregistrés dans un modèle, avec leur configuration. Cette information est générée lors de la création du modèle et n'est pas modifiable.

ZONE DE CONFIANCE

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA ZONE DE CONFIANCE DE KASPERSKY ANTI-VIRUS

Vous pouvez composer une liste unique d'exclusions de la zone de protection (d'analyse), et lorsque vous en aurez besoin, appliquer ces exclusions aux tâches sélectionnées **d'analyse à la demande** et à la tâche **Protection en temps réel des fichiers**. Cette liste d'exclusions s'appelle la *zone de confiance*.

La zone de confiance de Kaspersky Anti-Virus peut reprendre les objets suivants :

- les fichiers sollicités par les processus des applications et sensibles aux interceptions de fichiers (processus de confiance) ;
- les fichiers auxquels on accède durant les opérations de copie de sauvegarde (opérations de copie de sauvegarde) ;
- les fichiers et les scripts indiqués par l'utilisateur en fonction de leur emplacement et/ou de la menace (règles d'exclusion).

La zone de confiance est appliquée par défaut dans les tâches **Protection en temps réel des fichiers** et **Analyse des scripts**, dans les tâches d'analyse à la demande définies par l'utilisateur recréées et dans toutes les tâches prédéfinies d'analyse à la demande, sauf la tâche **Analyse des objets en quarantaine**.

Vous pouvez exporter la liste des exclusions de la zone de confiance dans le fichier de configuration afin de pouvoir l'importer par la suite dans une version de Kaspersky Anti-Virus installée sur un autre serveur.

Processus de confiance

Ces objets sont utilisés uniquement dans la tâche **Protection en temps réel des fichiers.**

Certaines applications du serveur peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par l'application antivirus. Les contrôleurs de domaine sont un exemple d'applications appartenant à cette catégorie.

Afin de ne pas perturber la stabilité de telles applications, vous pouvez désactiver la protection en temps réel des fichiers sollicités par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Microsoft Corporation recommande d'exclure de la protection en temps réel certains fichiers du système d'exploitation Microsoft Windows et les fichiers des applications de la société qui ne peuvent être infectés. Les noms de certains d'entre eux sont repris sur le site Web de Microsoft Corporationhttp://www.microsoft.com/rus/ (code de l'article : KB822158).

Vous pouvez appliquer une zone de confiance avec la fonction **Processus de confiance** ou sans celle-ci.

N'oubliez pas que si le fichier exécutable du processus change, par exemple s'il est actualisé, Kaspersky Anti-Virus l'exclura de la liste des applications de confiance.

Opérations de sauvegarde

Ces objets sont utilisés uniquement dans la tâche **Protection en temps réel des fichiers.**

Pendant la création d'une copie de sauvegarde des fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités durant les opérations de copie de sauvegarde. Kaspersky Anti-Virus n'analyse pas les fichiers que l'application de sauvegarde ouvre en lecture avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Règles d'exclusion

Ces objets sont utilisés uniquement dans les tâches **Protection en temps réel des fichiers** et **Analyse des scripts**, ainsi que dans les tâches d'analyse à la demande.

Vous pouvez exclure de l'analyse des objets dans les tâches sélectionnées sans utiliser la zone de confiance ou bien inclure la liste unique des exclusions dans la zone de confiance et, lorsque vous en aurez besoin, appliquer ces exclusions dans des tâches d'analyse à la demande, dans les tâches de la protection en temps réel des fichiers ou analyse des scripts.

Vous pouvez ajouter à la zone de confiance des objets en fonction de leur emplacement sur le serveur, en fonction du nom de la menace identifiée dans ceux-ci ou selon une combinaison de ces deux éléments.

Lorsque vous ajoutez une nouvelle exclusion à la zone de confiance, vous définissez une règle (les indices selon lesquels Kaspersky Anti-Virus ignorera les objets) et indiquez à quelles tâches (**Protection en temps réel des fichiers** et/ou Analyse à la demande) cette règle s'appliquera.

En fonction de la règle que vous aurez créée, Kaspersky Anti-Virus peut ignorer dans les tâches des composants sélectionnés des objets suspects de types suivants :

- Les menaces définies dans les secteurs indiqués du serveur ;
- Toutes les menaces dans les secteurs indiqués du serveur ;
- Les menaces définies dans toute la couverture d'analyse.

Si vous aviez choisi l'option **Ajouter les programmes d'administration à distance aux exclusions** et **Ajouter les fichiers recommandés par Microsoft aux exclusions**, ou **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions** lors de l'installation de Kaspersky Anti-Virus, ces règles d'exclusion seront appliquées dans la tâche **Protection en temps réel des fichiers**.

AJOUT D'EXCLUSIONS A LA ZONE DE CONFIANCE

DANS CETTE SECTION DE L'AIDE

AJOUT DE PROCESSUS A LA LISTE DES PROCESSUS DE CONFIANCE

Afin de ne pas perturber la stabilité des applications sensibles aux interceptions de fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Vous pouvez ajouter un processus à la liste des processus de confiance d'une des manières suivantes :

- Sélectionner ce processus dans la liste des processus exécutés actuellement sur le serveur protégé ;
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

Si le fichier exécutable du processus change, Kaspersky Anti-Virus l'exclut de la liste des processus de confiance.

Pour ajouter une application à la liste des applications de confiance, procédez comme suit :

1. Dans la console de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.

2. Dans la boîte de dialogue **Zone de confiance** sous l'onglet **Processus de confiance**, activez la fonction **Processus de confiance** : cochez la case **Ne pas surveiller l'activité sur fichiers des processus spécifiés** (cf. ill. ci-après).

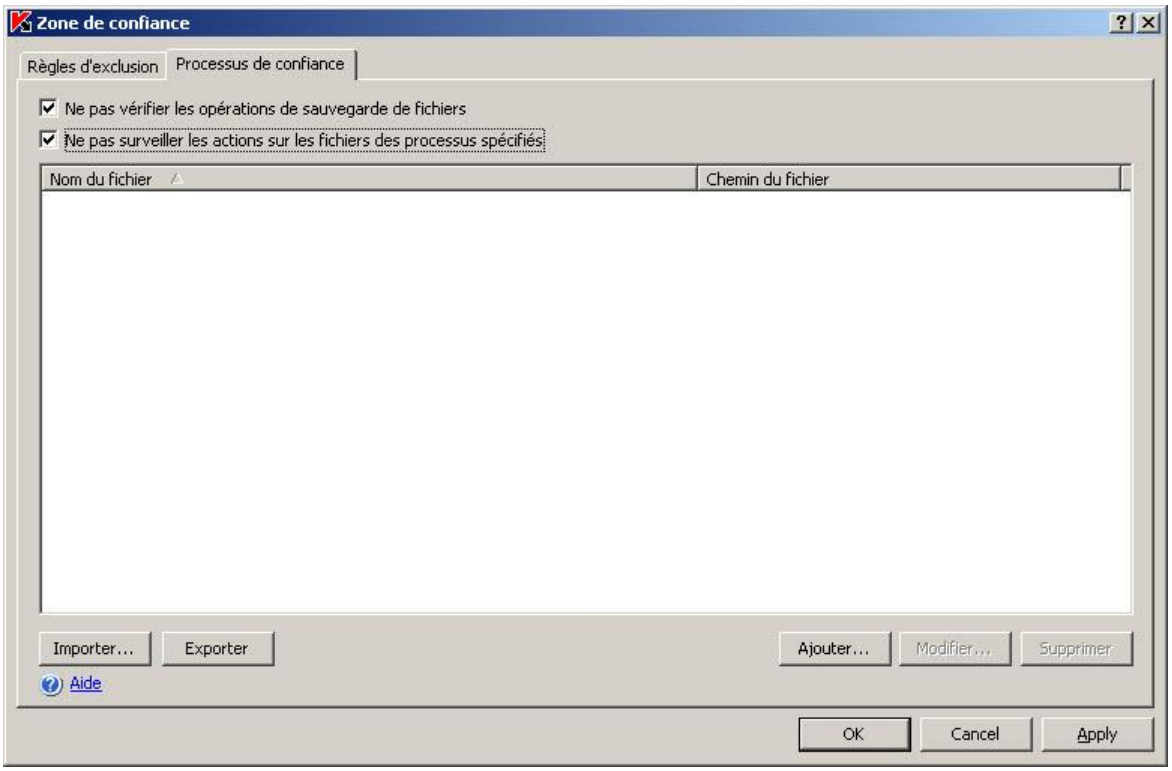


*Illustration 56. Boîte de dialogue **Zone de confiance**, onglet **Processus de confiance***

3. Ajoutez le processus de confiance de la liste des processus exécutés ou indiquez le fichier exécutable du processus.

   - Pour ajouter un processus de la liste des processus exécutés, procédez comme suit :

     a. Cliquez sur **Ajouter**.

     b. Dans la boîte de dialogue **Ajout d'un processus de confiance** cliquez sur le bouton **Processus**

(cf. ill. ci-après).

c. Dans la boîte de dialogue **Processus actifs**, sélectionnez le processus souhaité et cliquez sur **OK** (cf. ill. ci-après).

Pour trouver le processus souhaité dans la liste, vous pouvez trier les processus par nom, par PID ou par chemin d'accès au fichier exécutable du processus.

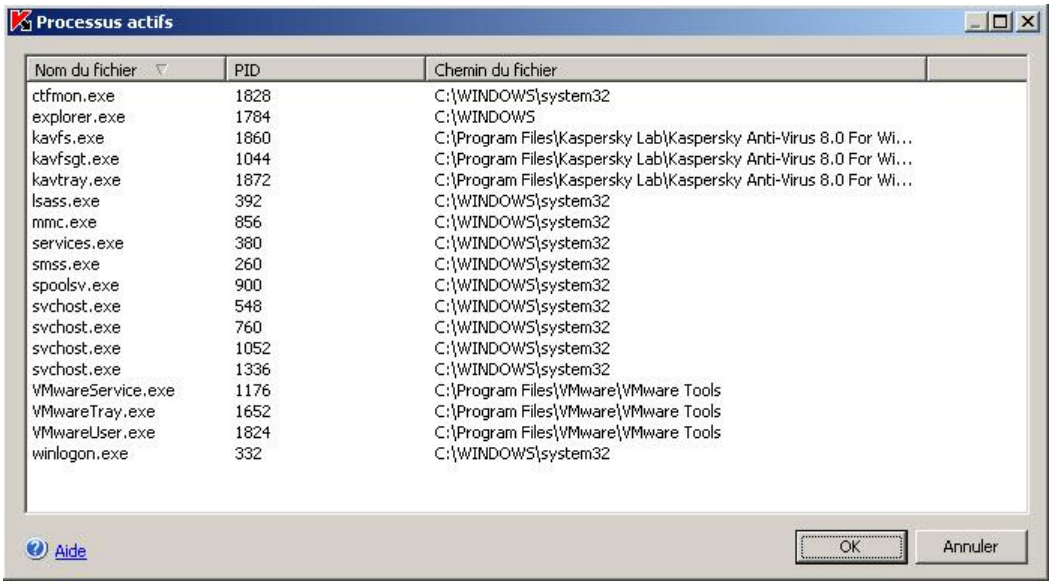


*Illustration 57. Boîte de dialogue **Processus actifs***

Vous devez faire partie du groupe des administrateurs sur le serveur protégé afin de consulter les processus actifs sur celui-ci.

Le processus sélectionné sera ajouté à la liste des processus de confiance dans la boîte de dialogue **Processus de confiance**.

- Pour sélectionner le fichier exécutable du processus sur le disque du serveur protégé, procédez de la manière suivante :

a. Sur l'onglet **Processus de confiance**, cliquez sur le bouton **Ajouter**.

b. Dans la boîte de dialogue **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du processus sur le disque local du serveur protégé. Cliquez sur **OK**.

Le nom du fichier et le chemin d'accès à celui-ci apparaît dans la boîte de dialogue **Ajout d'un processus de confiance**.

Pour désigner le chemin d'accès, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Kaspersky Anti-Virus ne considèrera pas un processus comme un processus de confiance si le chemin d'accès au fichier exécutable du processus est différent du chemin d'accès que vous avez saisi dans le champ **Chemin du fichier**. Si vous souhaitez que le processus exécuté depuis un fichier situé dans n'importe quel dossier soit considéré comme un processus de confiance, saisissez le caractère * dans le champ **Chemin du fichier**.

c. Cliquez sur **OK**.

Le nom du fichier exécutable du processus sélectionné apparaît dans la liste des processus de confiance de l'onglet **Processus de confiance**.

4. Cliquez sur **OK** pour enregistrer les modifications.

5. Assurez-vous que la zone de confiance est bien appliquée dans la tâche **Protection en temps réel des fichiers**.

DESACTIVATION DE LA PROTECTION EN TEMPS REEL DES FICHIERS PENDANT LA CREATION DE LA SAUVEGARDE

Pour désactiver la protection en temps réel des fichiers pendant la copie de sauvegarde, procédez comme suit :

1. Dans la console de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.

2. Dans la boîte de dialogue **Zone de confiance**, onglet **Processus de confiance**, cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.

3. Cliquez sur **OK** pour enregistrer les modifications.

4. Assurez-vous que la zone de confiance est bien appliquée dans la tâche **Protection en temps réel des fichiers**.

AJOUT DE REGLES D'EXCLUSION

Pour ajouter une règle d'exclusions, procédez comme suit :

1. Dans la console de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.

2. Sur l'onglet **Règles d'exclusion** de la fenêtre **Zone de confiance**, cliquez sur le bouton **Ajouter** (cf. ill. ci-après).

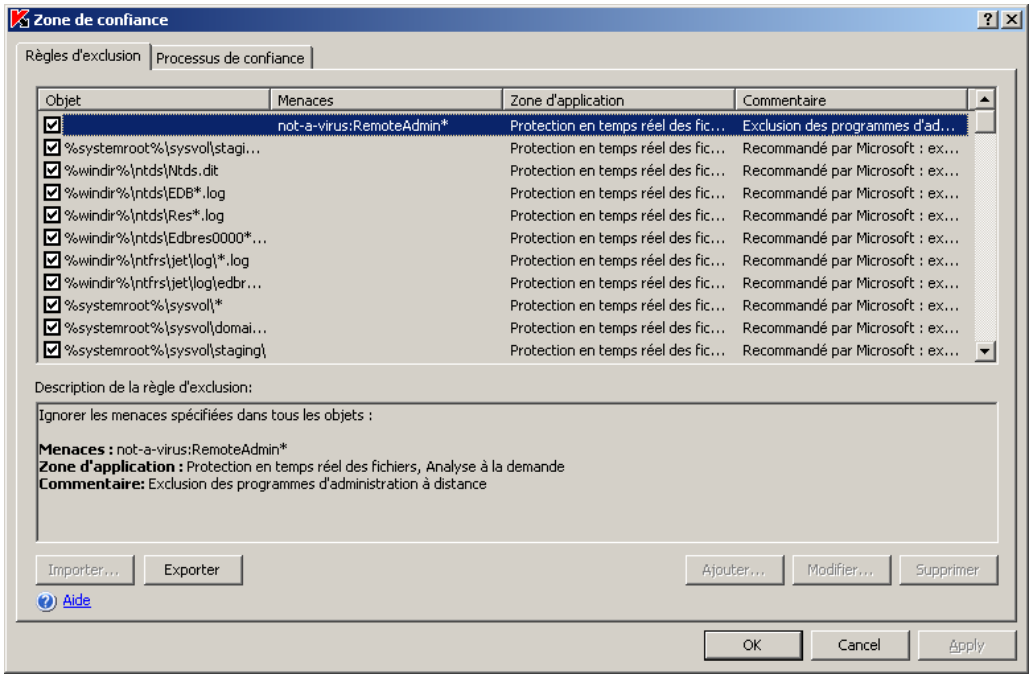


*Illustration 58. Boîte de dialogue **Zone de confiance**, onglet **Règles d'exclusion***

La boîte de dialogue **Règle d'exclusion** (cf. ill. ci-après) s'ouvre**.**

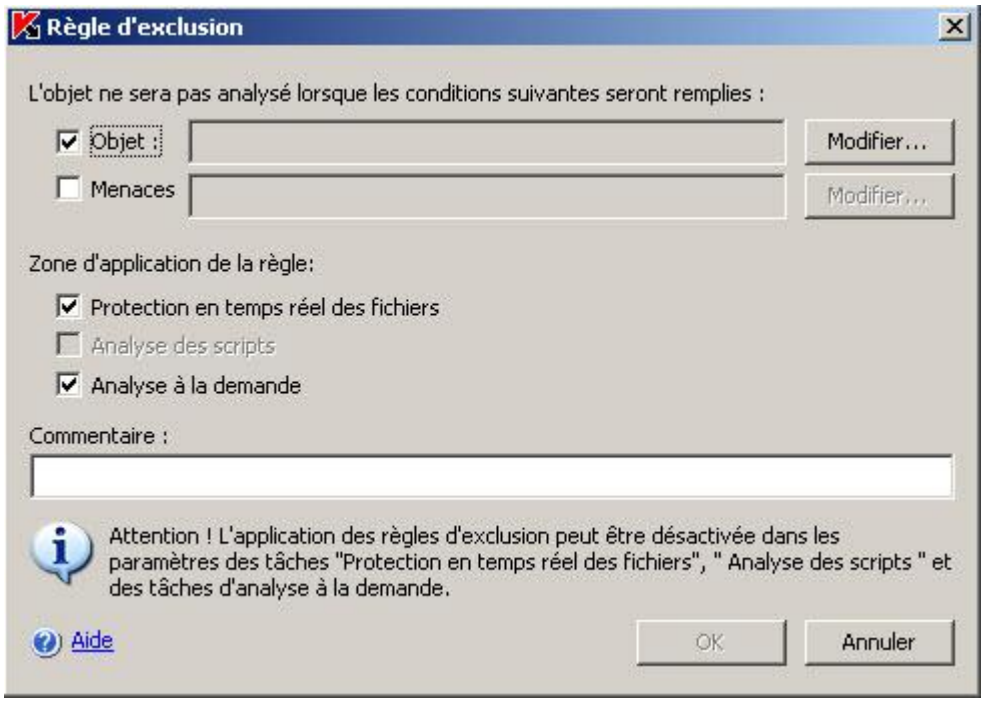


*Illustration 59. Boîte de dialogue **Règle d'exclusion**.*

3. Indiquez la règle selon laquelle Kaspersky Anti-Virus va exclure les objets. Utilisez les critères décrits ci-dessous.

   - Pour exclure toutes les menaces dans les secteurs indiqués, cochez la case **Objet** et désélectionnez la case **Menaces**.

   - Pour exclure toutes les menaces dans les secteurs indiqués, cochez la case **Objet** et désélectionnez la case **Menaces**.

- Pour exclure les menaces définies dans toute la couverture d'analyse, désélectionnez la case **Objet** et cochez la case **Menaces**.

Si vous souhaitez indiquer l'emplacement de l'objet, cochez la case **Objet**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Sélection de l'objet**, sélectionnez l'objet qui sera exclu de l'analyse, puis cliquez sur **OK** (cf. ill. ci-après). Vous pouvez exclure un des objets suivants :

- **Zone prédéfinie**. Sélectionnez une des zones d'analyse prédéfinie dans la liste.
- **Disque ou répertoire**. Indiquez le disque du serveur ou le répertoire sur le serveur ou dans le réseau local.
- **Fichier**. Indiquez le fichier sur le serveur ou dans le réseau local.
- **Fichier ou URL du script**. Désignez le script sur le serveur protégé, dans le réseau local ou sur Internet.

Au moment d'ajouter des règles d'exclusion, vous pouvez utiliser les caractères spéciaux ? et * afin de créer des masques de nom d'objet.

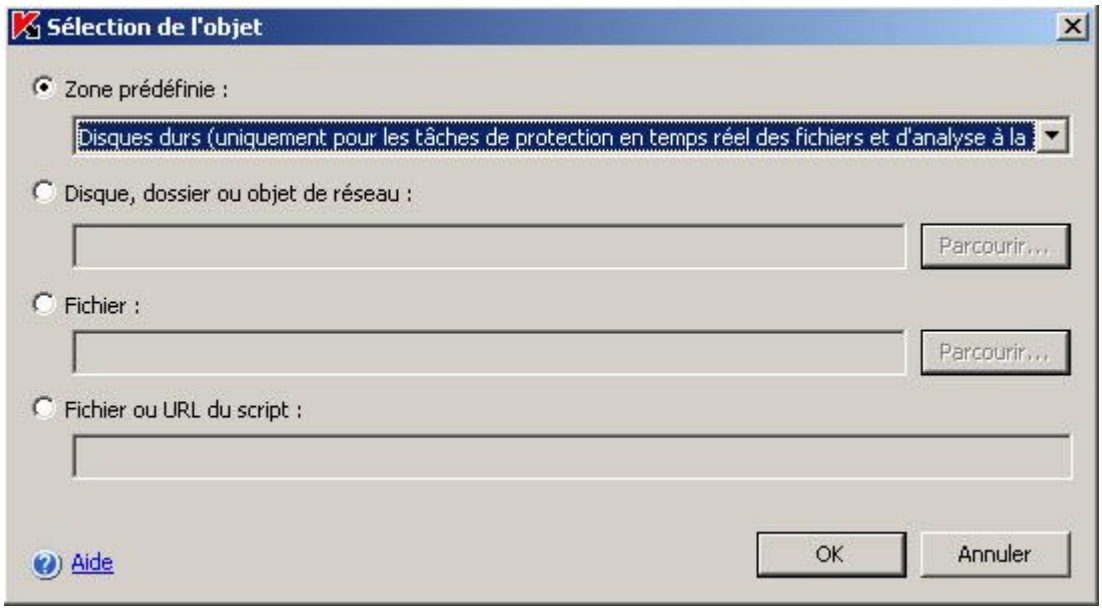


*Illustration 60. Boîte de dialogue **Sélection de l'objet***

- Si vous souhaitez préciser le nom de la menace, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Liste des exclusions**, ajoutez les noms des menaces. Pour en savoir plus sur le paramètre, lisez la rubrique "Exclusion des menaces" (cf. page 380) (cf. ill. ci-après)**.**

*Illustration 61. Boîte de dialogue **Liste des exclusions***

4. Dans la boîte de dialogue **Règle d'exclusion**, sous l'onglet **Zone d'application de la règle**, cochez la case en regard des composants fonctionnels dans les tâches desquels la règle d'exclusion sera appliquée.

5. Cliquez sur **OK**. Après cela, procédez comme suit :

   - Pour modifiez une règle, ouvrez la boîte de dialogue **Zone de confiance** et sur l'onglet **Règles d'exclusion**, sélectionnez la règle que vous souhaitez modifier, cliquez sur le bouton **Modifier** et introduisez les modifications dans la boîte de dialogue **Règle d'exclusion**.

   - Pour supprimer une règle, ouvrez la boîte de dialogue **Zone de confiance** et sur l'onglet **Règles d'exclusion**, sélectionnez la règle que vous souhaitez supprimer, cliquez sur le bouton **Supprimer** et confirmer l'opération.

6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Zone de confiance**.

APPLICATION DE LA ZONE DE CONFIANCE

Par défaut, la zone de confiance est appliquée dans les tâches du composant **Protection en temps réel**, dans les tâches d'analyse à la demande prédéfinies ou recréées.

Vous pouvez activer ou désactiver l'application de la zone de confiance dans des tâches distinctes dans les propriétés de la tâche.

Dès que la zone de confiance est activée/désactivée, les exclusions seront ou ne seront plus appliquées dans les tâches exécutées immédiatement.

Pour appliquer les exclusions de la zone de confiance à une tâche, procédez comme suit :

1. Dans la console de Kaspersky Anti-Virus, ouvrez le menu contextuel de la tâche et sélectionnez **Propriétés**.
2. Dans la boîte de dialogue **Propriétés : <Nom de tâche>**, sous l'onglet **Général**, cochez la case **Appliquer la zone de confiance**.
3. Cliquez sur **OK**.

BOITES DE DIALOGUE : ZONE DE CONFIANCE

DANS CETTE SECTION DE L'AIDE

PROCESSUS ACTIFS (FENETRE)

Cette fenêtre donne la liste des processus en exécution sur le serveur sécurisé. Les informations suivantes sont présentées pour chacun d'eux :

- **Nom du fichier** : nom utilisé pour exécuter le fichier du processus sur le serveur.
- **PID** : numéro d'identification du processus.
- **Chemin du fichier** : chemin au fichier du processus.

Sélectionnez le processus qui doit être ajouté à la liste des processus de confiance.

VOIR EGALEMENT

PROCESSUS DE CONFIANCE (ONGLET)

Cet onglet permet de créer une liste de processus de confiance dont l'activité sur les fichiers et sur le réseau n'est pas surveillée par Kaspersky Anti-Virus et qui détermine la réaction de Kaspersky Anti-Virus aux opérations de sauvegardé de sécurité exécutées sur le serveur.

Les opérations de fichiers des processus de confiance seront exclues de l'analyse uniquement si la case **Appliquer la zone de confiance** est cochée dans les propriétés de la tâche **Protection en temps réel des fichiers** dans l'onglet **Général**.

Le bouton **Exporter** vous permet de copier les paramètres de la zone de confiance dans un fichier de configuration. Le bouton **Importer** vous permet de rétablir les paramètres de la zone de confiance définis sur un autre serveur ou dans un fichier de configuration préalablement exporté. Lors de ces opérations, les paramètres des onglets **Processus de confiance** et **Règles d'exclusion** sont également exportés/importés.

VOIR EGALEMENT

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

Ajout de processus à la liste des processus de confiance 180

Désactivation de la protection en temps réel des fichiers pendant la création de la sauvegarde 182

AJOUT D'UN PROCESSUS DE CONFIANCE (FENETRE)

Utilisez cette fenêtre pour sélectionner le fichier exécutable dont l'activité fichier et réseau est à exclure par Kaspersky Anti-Virus. Vous pouvez sélectionner un processus de confiance parmi ceux en exécution sur le serveur, ou spécifier le chemin du fichier.

Seuls les processus lancés ou exécutés sur le serveur sécurisé peuvent être inclus en tant que processus de confiance.

Pour sélectionner un processus parmi ceux actuellement en exécution, cliquez sur **Processus**. La fenêtre ouverte présente la liste des processus actuellement en exécution sur le serveur. Sélectionnez le processus à ajouter à la liste des processus de confiance, puis cliquez sur **OK**.

Cliquez sur **Parcourir pour spécifier le fichier du processus.** Spécifiez le fichier exécutable du processus dans la fenêtre de sélection standard.

La zone **Nom du fichier exécutable** affichera le nom du fichier et la zone **Dossier contenant le fichier sur le serveur protégé** affichera le chemin du fichier sélectionné.

Les fichiers exécutables avec le même nom situés à des adresses différentes ne seront pas inclus parmi les processus de confiance. Entrez le chemin de la ressource au format UNC (Universal Naming Convention) ou avec un masque utilisant les caractères génériques ***** et **?**. Vous pouvez également utiliser des variables d'environnement (**%WINDIR%** par exemple).

VOIR EGALEMENT

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

Ajout de processus à la liste des processus de confiance 180

ONGLET REGLES D'EXCLUSIONS

Cet onglet reprend la liste des règles selon lesquelles les composants **Protection en temps réel des fichiers**, **Analyse des scripts** et **Analyse à la demande** excluent les objets de l'analyse. Les informations suivantes sont reprises pour les règles de la liste :

- **Objet** – nom du fichier, masque du nom de fichier, disque local ou disque amovible du serveur, répertoire local ou de réseau, secteur prédéfini, etc.

- **Menaces** : nom des menaces telles qu'elles figurent dans l'Encyclopédie des virus à l'adresse www.securelist.com/fr/ ou le masque du nom de la menace.

- **Zone d'application** – nom du composant de Kaspersky Anti-Virus associé dans lequel la règle est appliquée : **Protection en temps réel des fichiers**, **Analyse des scripts** ou **Analyse à la demande**. Si le champ indique **Analyse à la demande**, la règle sera utilisée par toutes les tâches prédéfinies, les tâches définies par l'utilisateur et les tâches de groupe de ce composant.

- **Commentaires** : informations complémentaires relatives à la règle.

Lorsque le composant indiqué dans la colonne **Zone d'application** fonctionne, et selon les conditions définies dans la règle, les actions suivantes seront exécutées :

- Si les champs **Objet** et **Menaces** sont remplis, les objets de la zone définie contenant les menaces indiquées seront ignorés. Si les paramètres du rapport prévoient l'enregistrement de ce type d'événements, les informations concernant les objets exclus de l'analyse seront reprises dans le rapport.

- Si seul le champ **Objet** est rempli, le secteur indiqué (objet) ne sera pas soumis à la recherche de code malveillant.

- Si seul le champ **Menaces** est rempli, les menaces indiquées seront ignorées. Si les paramètres du rapport prévoient l'enregistrement de ce type d'événements, les informations concernant les objets exclus de l'analyse seront reprises dans le rapport.

La case en regard des règles utilisées est cochée. Pour désactiver l'application des règles, désélectionnez la case ; pour activer la règle, cochez la case.

La partie inférieure de l'onglet reprend une description de la règle sélectionnée dans le tableau.

Vous pouvez modifier les conditions des règles ou ajouter ou supprimer des règles à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**. Dans le cadre de l'exécution des tâches **Protection en temps réel des fichiers**, **Analyse des scripts** et **Analyse à la demande**, les règles présentées sur cet onglet sont appliquées uniquement si la case **Appliquer la zone de confiance** a été cochée sous l'onglet **Général** dans les propriétés de la tâche. Dans ce cas, pour les tâches **Protection en temps réel des fichiers** et **Analyse à la demande**, les exclusions définies dans la stratégie ou dans les paramètres de la tâche sous l'onglet **Performance**s sont augmentées des règles utilisées par les composants de Kaspersky Anti-Virus. Si la case **Appliquer la zone de confiance** n'est pas cochée, seuls les objets définis dans les paramètres de la tâche à l'onglet **Performances** seront exclus de l'analyse.

Le bouton **Exporter** vous permet de copier les paramètres de la zone de confiance dans un fichier de configuration. Le bouton **Importer** vous permet de rétablir les paramètres de la zone de confiance définis sur un autre serveur ou dans un fichier de configuration préalablement exporté. Lors de ces opérations, les paramètres des onglets **Processus de confiance** et **Règles d'exclusion** sont également exportés/importés.

Après avoir composé la liste des règles, cliquez sur **OK** ou sur **Appliquer** pour enregistrer les modifications. Pour quitter la fenêtre sans enregistrer les modifications, cliquez sur **Annuler**.

FENETRE REGLE D'EXCLUSION

C'est dans cette fenêtre que vous pouvez composer la règle d'exclusion des objets de l'analyse. En fonction des conditions définies pour la règle, les objets suivants seront exclus de l'analyse :

- Les objets qui se trouvent dans le secteur défini et qui contiennent les menaces déterminées ;

- Tous les objets placés dans le secteur défini (ce secteur ne sera pas analysé par Kaspersky Anti-Virus) ;

- Les objets contenant les menaces définies, quel que soit l'endroit où ils se trouvent.

Pour exclure de l'analyse des objets situés dans un secteur défini et contenant des menaces déterminées, procédez comme suit :

1. Cochez la case **Objet** et indiquez le chemin d'accès complet à l'objet (fichier, répertoire, disque) ou sélectionnez l'objet à l'aide du bouton **Modifier**. En guise de chemin, saisissez le chemin d'accès complet au format UNC (Universal Naming Convention) ou à l'aide d'un masque utilisant les caractères génériques ***** et **?**. Vous pouvez également utiliser des variables d'environnement (**%WINDIR%** par exemple).

2. Cochez la case **Menaces** et indiquez le nom complet de la menace tel qu'il apparaît dans l'Encyclopédie des virus à l'adresse securelist.com/fr/ ou encore, un masque du nom de la menace. L'usage de masques vous permet d'exclure une classe complète de menaces. Pour créer une liste d'exclusions, cliquez sur **Modifier**.

   Le nom de la menace est défini lors de l'analyse de l'objet et peut contenir les informations suivantes : **<catégorie de menace>:<type de menace>.<nom abrégé de la plateforme>.<nom de la menace>.<code de modification de la menace>**.

   Admettons que vous utilisez l'utilitaire Remote Administrator en guise d'outil d'administration à distance. La plupart des programmes antivirus classent le code de cet utilitaire dans la classe de menace "potentiellement dangereuses" (**Riskware**). Si vous ne souhaitez pas verrouiller Remote Administrator, ajoutez les informations suivantes à la liste des menaces exclues. Pour le nom, vous pouvez spécifier :

   - **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus ignorera uniquement le programme Win32.RAdmin.20.
   - Masque du nom complet de la menace : **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions de Remote Administrator.
   - Masque du nom complet de la menace, avec uniquement la classe de menace :**not-a-virus:***. Kaspersky Anti-Virus n'appliquera aucune action sur les versions des objets contenant cette classe de menace.

3. Indiquez, pour chaque composant, si la règle sera appliquée. Pour ce faire, cochez les cases dans la rubrique **Zone d'application de la règle**:

   - **Protection en temps réel des fichiers**, dans ce cas, les objets définis dans les conditions seront ignorés pendant l'exécution de la tâche **Protection en temps réel des fichiers**.
   - **Analyse à la demande**, dans ce cas, les objets définis dans les conditions seront ignorés lors de l'exécution de toutes les tâches d'analyse à la demande prédéfinies, définies par l'utilisateur ou de groupe.
   - **Analyse des scripts**, dans ce cas les objets indiqués dans les conditions ne seront pas analysés lors de l'exécution de la tâche **Analyse des scripts**.

     Dans le champ **Commentaires**, le cas échéant, saisissez des informations complémentaires sur la règle :

Pour exclure de l'analyse des objets situés dans un secteur quelconque :

Cochez la case **Objet**, définissez le secteur exclu de l'analyse et indiquez le composant pour lequel la règle sera appliquée.

Pour exclure de l'analyse des objets contenant les menaces définies, quel que soit l'endroit où ils se trouvent :

Cochez la case **Menaces**, définissez les menaces à exclure de l'analyse et sélectionnez les composants pour lesquels la règle sera appliquée.

VOIR EGALEMENT

Ajout de règles d'exclusion..... 182

Présentation de la zone de confiance de Kaspersky Anti-Virus 178

SELECTION D'OBJETS (FENETRE)

Cette fenêtre permet de définir le secteur qui servir de condition dans les règles d'exclusion. Sélectionnez une des options suivantes :

- **Couverture de l'analyse prédéfinie**, pour ajouter l'une des zones standard du serveur. Choisissez la valeur requise dans le menu déroulant :
  - **Disques durs** – toutes les disques durs du serveur.
  - **Disques amovibles** : tous les supports amovibles connectés au serveur sécurisé seront analysés, y compris les disquettes, les CD et les unités de mémoire flash USB.
  - **Objets de démarrage (uniquement pour les tâches d'analyse à la demande)** : les objets qui sont exécutés au démarrage du système d'exploitation.
  - **Dossiers partagés (uniquement pour les tâches d'analyse à la demande)** : tous les dossiers partagés situés sur le serveur.
  - **Mémoire système (uniquement pour les tâches d'analyse à la demande)** : la mémoire système du serveur.
  - **Environnement réseau (uniquement pour les tâches d'analyse à la demande)** : objets situés sur les ressources de réseau sollicités par les applications installées sur le serveur. Kaspersky Anti-Virus n'analyse pas les fichiers si les applications y accèdent à partir d'autres postes du réseau.
- **Disque ou dossier**, si vous souhaitez définir un disque ou un dossier local ou de réseau. Indiquez le chemin complet à la ressource ou saisissez un masque utilisant les caractères génériques * et ?, ou sélectionnez la ressource à l'aide du bouton **Parcourir**. Vous pouvez également utiliser des variables d'environnement (**%WINDIR%** par exemple).
- **Fichier**, si vous souhaitez désigner un fichier local ou de réseau. Saisissez le nom du fichier, y compris le chemin, ou un masque utilisant les caractères génériques ***** et **?**, ou sélectionnez le fichier à l'aide du bouton **Parcourir**. Vous pouvez également utiliser des variables d'environnement (**%WINDIR%** par exemple).

Fichier ou URL du script : si vous souhaitez exclure un script de l'analyse. Indiquez le chemin d'accès au fichier de script local ou dans le réseau ou l'adresse du script dans Internet. Vous pouvez utiliser les masques, y compris les caractères ***** et **?**, ainsi que les variables d'environnement telles que **%WINDIR%**.

ISOLEMENT DES OBJETS SUSPECTS. UTILISATION DE LA QUARANTAINE

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE L'ISOLEMENT DES OBJETS SUSPECTS

Kaspersky Anti-Virus isole les objets qu'il considère suspects (cf. page 14). Il place ces objets en quarantaine, c'est à dire qu'il les déplace du lieu d'origine vers un dossier spécial où ils seront chiffrés par souci de sécurité.

CONSULTATION DES OBJETS EN QUARANTAINE

Vous pouvez consulter les objets en quarantaine dans le nœud **Quarantaine** de la console de Kaspersky Anti-Virus.

Pour consulter les objets en quarantaine, sélectionnez le nœud **Quarantaine** dans l'arborescence de la console (cf. ill. ci-après).

Pour trouver l'objet requis dans la liste des objets en quarantaine, vous pouvez les trier (cf. page 194) ou les filtrer (Filtrage des objets en quarantaine).

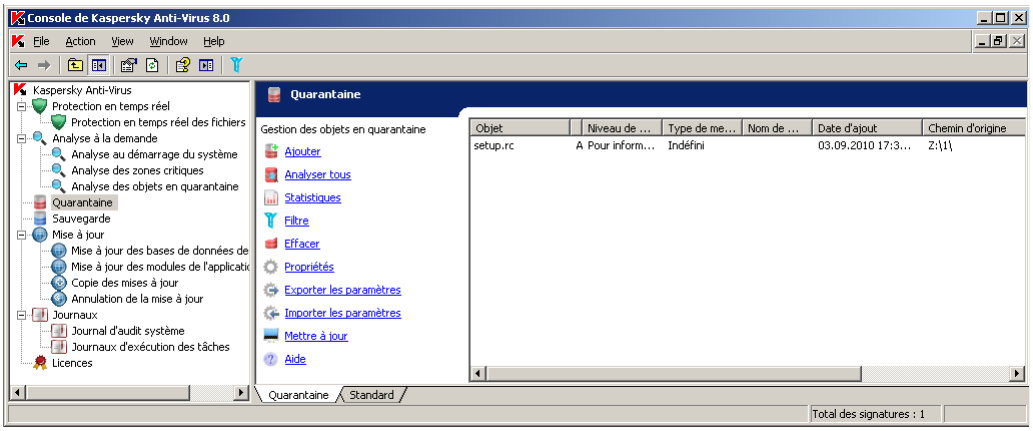


*Illustration 62. Informations relatives aux objets en quarantaine dans le nœud **Quarantaine***

Le panneau de résultats reprend l'information de chaque objet en quarantaine (cf. tableau ci-dessous).

Tableau 17. Information sur les objets en quarantaine

CHAMP	DESCRIPTION
Objet	Nom de l'objet placé en quarantaine.
Etat	Etat de l'objet en quarantaine ; peut prendre les valeurs suivantes : • **Suspect**. L'objet est suspect ; il existe une équivalence partielle entre une partie du code de l'objet et une partie du code d'une menace connue. • **Infecté**. L'objet est infecté ; il existe une équivalence parfaite entre une partie du code de l'objet et une partie du code d'une menace connue. • **Fausse alerte**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est sain. • **Réparé**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est infecté mais qu'il a pu être réparé. Vous pouvez restaurer l'objet sans craintes. • **Ajouté par l'utilisateur**. L'objet a été placé en quarantaine par l'utilisateur.
Niveau de danger	Le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace de l'objet. Le paramètre peut prendre les valeurs suivantes : • **Haut**. L'objet contient une menace de type vers de réseau, virus traditionnels, chevaux de Troie ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues). • **Moyen**. L'objet peut contenir une menace du type autres programmes malveillants, logiciels publicitaires ou programmes au contenu pornographique. • **Bas**. L'objet peut contenir une menace du type programmes présentant un risque potentiel. • **Événement d'information**. L'objet a été placé en quarantaine par l'utilisateur.
Type de menace	Type de menaces selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté.
Nom de menace	Nom de la menace selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez consulter le nom complet de la menace découverte dans l'objet dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234) (nœud **Journaux**).
Date de placement	Date de placement de l'objet en quarantaine.
Chemin d'origine	Chemin d'accès complet à l'emplacement d'origine de l'objet, par exemple au répertoire où se trouvait l'objet avant d'être placé en quarantaine, au fichier dans l'archive ou au fichier pst de la base de messagerie.
Taille	Taille de l'objet.
Nom d'utilisateur	Cette colonne reprend les informations suivantes : • Si l'objet a été isolé par Kaspersky Anti-Virus dans la tâche **Protection en temps réel des fichiers** – le nom du compte utilisateur sous les privilèges duquel l'application a sollicité l'objet au moment de l'interception. • Si l'objet a été isolé par Kaspersky Anti-Virus dans la tâche d'analyse à la demande – le nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée. • Si l'utilisateur a placé l'objet en quarantaine manuellement – le nom du compte de cet utilisateur.

•

DANS CETTE SECTION DE L'AIDE

TRI DES OBJETS EN QUARANTAINE

Par défaut, les objets dans la liste des objets en quarantaine sont triés par date de placement dans l'ordre chronologique inverse. Pour trouver l'objet souhaité, vous pouvez trier la liste selon le contenu des colonnes reprenant les informations sur les objets. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Quarantaine**, ou si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour trier les objets, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Quarantaine**.
2. Dans le panneau de résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les objets de la liste.

FILTRAGE DES OBJETS EN QUARANTAINE

Pour trouver l'objet souhaité en quarantaine, vous pouvez filtrer les objets de la liste et afficher uniquement ceux qui répondent aux critères de filtrage que vous avez définis. Les résultats du filtrage sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud Quarantaine, ou si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour définir un ou plusieurs filtres, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Quarantaine** et sélectionnez la commande **Filtre**.

La boîte de dialogue **Paramètres du filtre** s'ouvrira (cf. ill. ci-après).

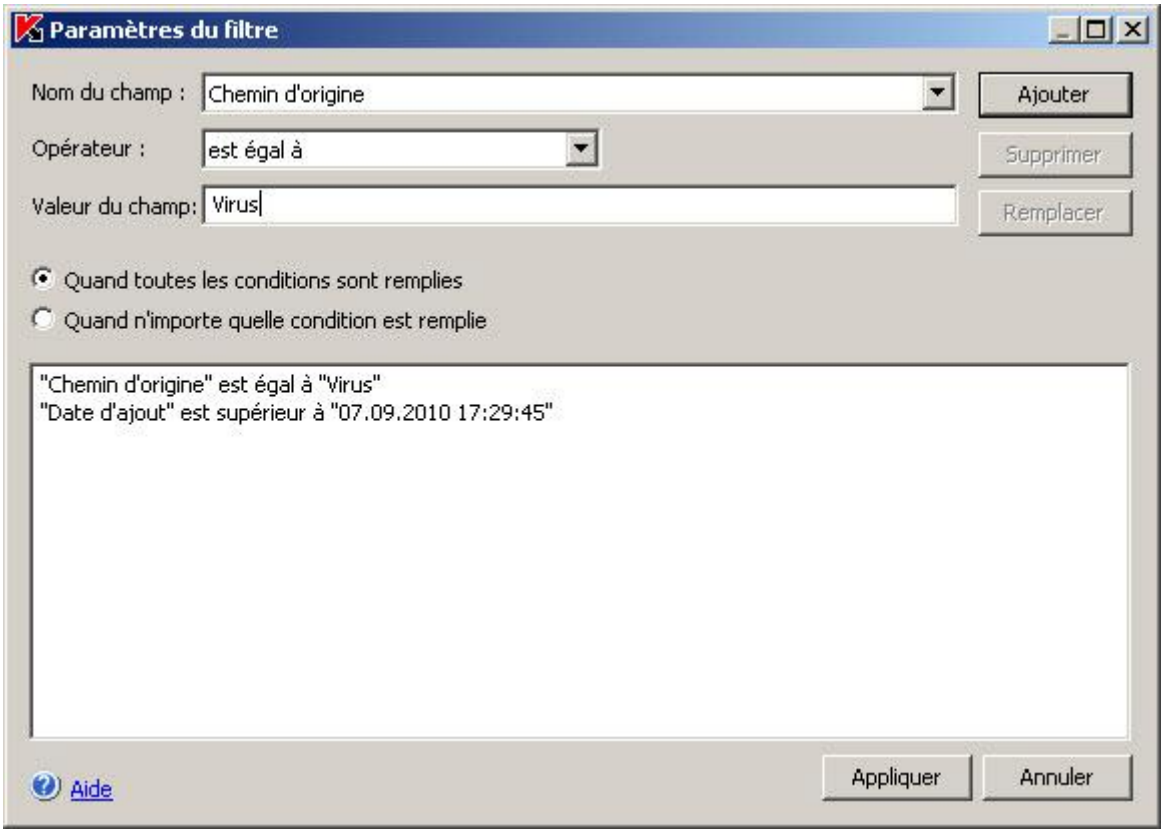


*Illustration 63. Boîte de dialogue **Paramètres du filtre***

2. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, observez les règles suivantes :

   - Afin de réunir quelques filtres selon le " ET " logique, sélectionnez l'option **En cas d'exécution de toutes les conditions**.
   - Afin de réunir quelques filtres selon le " OU " logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
   - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
   - Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**.

- *Pour afficher à nouveau tous les objets dans la liste des objets en quarantaine,*

  dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Quarantaine** et sélectionnez la commande **Supprimer le filtre**.

ANALYSE DES OBJETS EN QUARANTAINE PARAMETRES DE LA TACHE ANALYSE DES OBJETS EN QUARANTAINE

Par défaut, Kaspersky Anti-Virus exécute la tâche prédéfinie **Analyse des objets en quarantaine** après chaque mise à jour des bases. Les paramètres de la tâche sont présentés dans le tableau suivant. Vous ne pouvez pas les modifier.

Vous pouvez modifier la programmation de la tâche **Analyse des objets en quarantaine** ou la lancer manuellement.

Suite à l'analyse des objets en quarantaine après la mise à jour des bases, Kaspersky Anti-Virus peut décider que certains d'entre eux sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés par Kaspersky Anti-Virus, auquel cas il exécutera les actions définies dans les paramètres de la tâche d'analyse à la demande **Analyse des objets en quarantaine** : **Réparer, supprimer si la réparation est impossible**.

*Tableau 18. Paramètres de la tâche **Analyse des objets en quarantaine***

PARAMETRES DE LA TACHE "ANALYSE DES OBJETS EN QUARANTAINE"	VALEUR
Couverture de l'analyse	Répertoire de quarantaine
Paramètres de sécurité	Identiques pour toutes les couvertures de l'analyse ; les valeurs possibles sont reprises au tableau suivant.

*Tableau 19. Paramètres de sécurité de la tâche **Analyse des objets en quarantaine***

PARAMETRE DE SECURITE	VALEUR
Objets à analyser (cf. page 376)	Analyser tous les objets
Analyse uniquement des nouveaux fichiers et des fichiers modifiés (cf. page 382)	Désactivée
Actions à exécuter sur les objets infectés (cf. page 384)	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. page 386)	Rapport uniquement
Exclusion des objets (cf. page 379)	Non
Exclusion des menaces (cf. page 380)	Non
Durée maximale de l'analyse d'un objet (cf. page 388)	Non définie
Taille maximale de l'objet composé analysé (cf. page 389)	Non définie
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. page 376)	Activée
Analyse des secteurs de démarrage (cf. page 376)	Désactivée
Application de la technologie iChecker (cf. page 389)	Désactivée
Application de la technologie iSwift (cf. page 390)	Désactivée
Analyse des objets composés (cf. page 383)	• Archives* • Archives SFX* • Objets compactés* • Objets OLE incorporés* * L'analyse uniquement des nouveaux fichiers et des fichiers modifiés est désactivée.
Vérification de la signature Microsoft des fichiers (cf. page 391)	Non exécutée
Application de l'analyseur heuristique (cf. page 393).	Appliqué au niveau d'analyse **Profonde**
Zone de confiance (cf. page 178)	Pas appliqué

RESTAURATION DE L'OBJET DEPUIS LA QUARANTAINE

Kaspersky Anti-Virus place les objets suspects sous une forme cryptée dans le répertoire de quarantaine afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer n'importe quel objet de la quarantaine. La restauration d'un objet peut s'imposer dans les situations suivantes :

- Après l'analyse de la quarantaine à l'aide des bases actualisées, l'état d'un objet est devenu **Fausse alerte** ou **Réparé** ;
- Vous estimez que l'objet ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Anti-Virus n'isole plus cet objet lors des analyses ultérieures, il faut l'exclure du traitement dans la tâche **Protection en temps réel des fichiers** et des tâches d'analyse à la demande. Pour ce faire, attribuez au paramètre Exclusion des objets (selon le nom du fichier) (cf. page 379) ou Exclusion des menaces (cf. page 380) dans ces tâches le nom de l'objet ou ajoutez-le à la zone de confiance (cf. ill. 178).

Lors de la restauration des objets, vous pouvez sélectionner l'endroit où sera placé l'objet : dans l'emplacement d'origine (défini par défaut), dans un dossier de restauration spécial sur le serveur protégé, dans un répertoire désigné de l'ordinateur où est installée la console de Kaspersky Anti-Virus, ou sur un autre ordinateur du réseau.

Pour que Kaspersky Anti-Virus n'analyse pas les objets volumineux lors de la restauration des fichiers depuis la quarantaine, définissez une exclusion pour le dossier %Temp%\wseeqbfiles\.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce dossier est défini dans les paramètres de la quarantaine (cf. page 405).

La restauration d'objets de la quarantaine peut entraîner l'infection de l'ordinateur.

Vous pouvez restaurer l'objet en conservant une copie dans le répertoire de quarantaine afin de pouvoir l'utiliser ultérieurement, par exemple afin de pouvoir analyser une nouvelle fois l'objet après la mise à jour des bases.

Si l'objet placé en quarantaine fait partie d'un objet composé (une archive par exemple), Kaspersky Anti-Virus ne l'inclut pas à nouveau dans cet objet lors de la restauration mais l'enregistre séparément dans le répertoire indiqué.

Vous pouvez restaurer un ou plusieurs objets.

Pour restaurer des objets de la quarantaine, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Quarantaine**.
2. Dans le panneau des résultats, exécutez une des actions suivantes :
   - pour restaurer un seul objet, ouvrez le menu contextuel de l'objet que vous souhaitez restaurer et sélectionnez la commande **Restaurer** ;
   - pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez la commande **Restaurer**.

La boîte de dialogue **Restauration de l'objet** (cf. ill. ci-dessous) s'ouvrira.

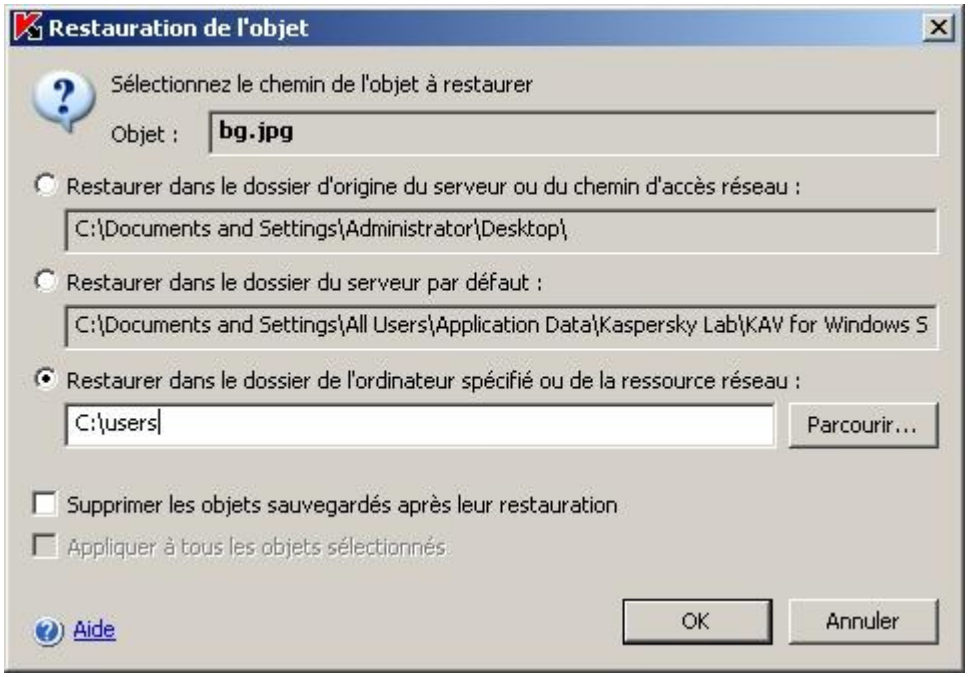


*Illustration 64. Boîte de dialogue **Restauration de l'objet***

3. Dans la boîte de dialogue **Restauration de l'objet**, indiquez pour chaque objet sélectionné le répertoire dans lequel vous souhaitez conserver la copie restaurée (le nom de l'objet figure dans le champ **Objet** de la partie supérieure de la boîte de dialogue ; si vous avez sélectionné plusieurs objets, dans ce champ est le nom du premier objet de la liste qui est affiché).

   Exécutez une des actions suivantes :

   - pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine** ;
   - Pour restaurer l'objet dans le répertoire que vous avez défini en tant que répertoire de restauration dans les paramètres de la quarantaine (cf. page 405), sélectionnez **Restaurer dans le dossier du serveur utilisé par défaut** ;
   - pour restaurer l'objet dans un autre répertoire de l'ordinateur où vous avez installé la console de Kaspersky Anti-Virus ou dans un répertoire de réseau, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis sélectionnez le répertoire souhaité ou saisissez le chemin d'accès à celui-ci.

4. Si vous souhaitez conserver une copie de l'objet dans le dossier de quarantaine après la restauration, désélectionnez la case **Supprimer les objets sauvegardés après leur restauration**.

5. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Si vous avez choisi **Restaurer dans le dossier d'origine du serveu**r ou du chemin d'accès réseau chacun des objets sera enregistré dans son répertoire d'origine ; si vous avez sélectionné **Restaurer dans le dossier du serveur, utilisé par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié** ou de la ressource réseau, tous les objets seront conservés dans le dossier indiqué.

6. Cliquez sur **OK**.

   Kaspersky Anti-Virus commence par restaurer le premier des objets que vous avez sélectionnés.

7. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la boîte de dialogue **Un objet avec ce nom existe déjà** s'ouvrira (cf. ill. ci-dessous).

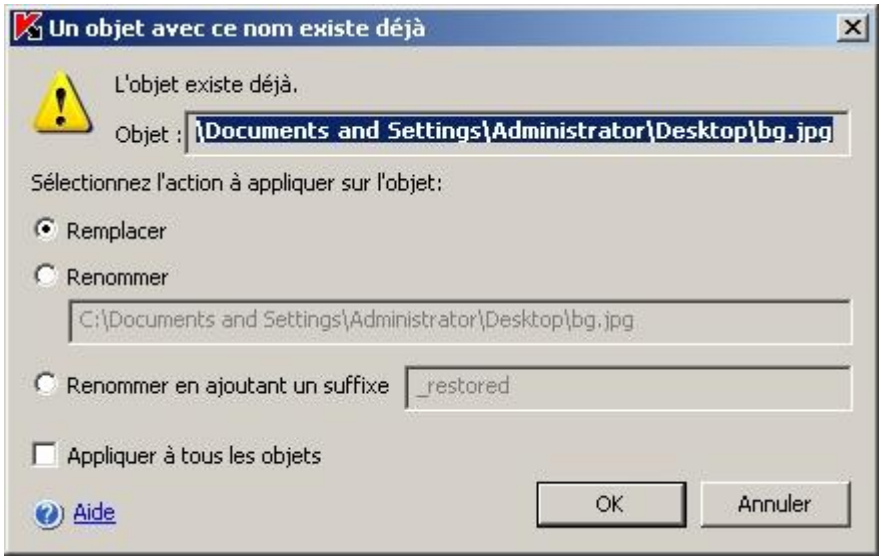


*Illustration 65. Boîte de dialogue **Un objet avec ce nom existe déjà***

a. Choisissez l'une des actions suivantes pour Kaspersky Anti-Virus :

- **Remplacer** afin d'enregistrer l'objet restauré au lieu du fichier existant ;
- **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet et son chemin d'accès dans le champ ;
- **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

b. Si vous avez sélectionné plusieurs objets pour la restauration, alors pour appliquer l'action **Remplacer** ou **Renommer en ajoutant un suffixe** à tous les objets sélectionnés, cochez la case **Appliquer à tous les objets**. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets** ne sera pas accessible).

c. Cliquez sur **OK**.

L'objet sera restauré ; les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets** dans la boîte de dialogue **Restauration de l'objet**, alors la boîte de dialogue **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 3 des présentes instructions).

MISE EN QUARANTAINE DES FICHIERS

Vous pouvez mettre manuellement des fichiers en quarantaine.

Pour mettre un fichier en quarantaine, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Quarantaine** et sélectionnez **Ajouter**.
2. Dans la boîte de dialogue **Ouvrir** sélectionnez le fichier que vous souhaitez placer en quarantaine puis, cliquez sur le bouton **OK**.

   Kaspersky Anti-Virus place le fichier indiqué en quarantaine.

SUPPRESSION DES OBJETS DE LA QUARANTAINE

Conformément aux paramètres de la tâche **Analyse des objets en quarantaine** (cf. page 196), Kaspersky Anti-Virus supprime automatiquement du répertoire de quarantaine les objets dont l'état est devenu **Infecté** suite à l'analyse à l'aide des bases actualisées et qui n'ont pas pu être réparés. Kaspersky Anti-Virus ne supprime pas les autres objets.

Vous pouvez supprimer manuellement un ou plusieurs objets de la quarantaine.

Pour supprimer un ou plusieurs objets de la quarantaine, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Quarantaine**.
2. Exécutez une des actions suivantes :
   - Pour supprimer un objet, ouvrez le menu contextuel de l'objet que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;
   - Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Shift**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez la commande **Supprimer**.
3. Dans la boîte de dialogue ouverte, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

ENVOI DES OBJETS SUSPECTS A KASPERSKY LAB POUR EXAMEN

Si le comportement d'un objet quelconque indique selon vous la présence éventuelle d'une menace et que Kaspersky Anti-Virus le considère comme un fichier sain, il se peut que vous soyez en présence d'un nouveau virus inconnu dont l'algorithme de réparation n'a pas encore été ajouté à la base. Vous pouvez envoyer ce fichier à Kaspersky Lab pour examen. Les experts antivirus de Kaspersky Lab analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de réparation aux bases. Il se peut que lors d'une analyse ultérieure après la mise à jour des bases que Kaspersky Anti-Virus le considère comme un fichier infecté et parvienne à le réparer. Vous pourrez alors non seulement conserver l'objet mais également éviter une épidémie virale.

Seuls les fichiers de la quarantaine peuvent être envoyés pour examen. Ils sont conservés sous forme cryptée et pendant le transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

Vous ne pouvez pas envoyer un objet de la quarantaine à Kaspersky Lab une fois que la licence n'est plus valide.

Pour envoyer un fichier à Kaspersky Lab pour étude, procédez comme suit :

1. Si le fichier ne se trouve pas encore en quarantaine, placez-le à titre préventif (cf. page 200).
2. Dans le nœud **Quarantaine**, dans la liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous souhaitez envoyer à Kaspersky Lab pour examen et sélectionnez la commande **Envoyer l'objet pour examen**.
3. Si un client de messagerie est configuré sur le poste où la console de Kaspersky Anti-Virus est installée, un nouveau message électronique sera créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

   Le champ **Destinataire** du message contient l'adresse électronique de Kaspersky Lab newvirus@kaspersky.com. Le champ **Objet** contient le texte "Objet de la quarantaine".

   Le corps du message contient le texte "Le fichier sera envoyé à Kaspersky Lab pour examen". Vous pouvez reprendre dans le corps du message n'importe quelle information complémentaire sur le fichier : raisons pour lesquelles il vous semble suspect, son comportement et ses effets sur le système.

Le message est accompagné de l'archive <nom de l'objet>.cab. Il contient le fichier <uuid>.klq avec l'objet crypté (où uuid est l'identificateur unique de l'objet dans Kaspersky Anti-Virus), le fichier <uuid>.txt avec les informations récoltées par Kaspersky Anti-Virus sur l'objet et le fichier Sysinfo.txt qui contient les informations relatives à Kaspersky Anti-Virus et au système d'exploitation du serveur :

- Nom et version du système d'exploitation ;
- Nom et version de Kaspersky Anti-Virus ;
- Date d'édition des mises à jour des bases installées ;
- Numéro de série de la licence.

Ces informations sont indispensables aux experts de Kaspersky Lab afin de pouvoir analyser le fichier le plus vite et le plus efficacement possible. Toutefois, si vous ne souhaitez pas les transmettre, vous pouvez supprimer le fichier Sysinfo.txt de l'archive.

Si le client de messagerie n'est pas configuré sur l'ordinateur où est installée la console de Kaspersky Anti-Virus, l'Assistant de connexion à Internet de Microsoft Windows s'ouvrira. Vous pouvez exécuter les opérations suivantes :

- Suivre les instructions de l'Assistant de connexion à Internet, créer un nouveau compte utilisateur et envoyer le fichier de cet ordinateur.
- Quitter l'Assistant et enregistrer l'objet sélectionné crypté dans un fichier. Ce fichier peut être envoyé seul à Kaspersky Lab.

Pour enregistrer l'objet crypté dans un fichier, procédez comme suit :

1. Dans la boîte de dialogue qui vous invite à enregistrer l'objet, cliquez sur le bouton **OK** (cf. ill. ci-après).

Illustration 66. Boîte de dialogue avec invite pour l'enregistrement de l'objet en quarantaine dans un fichier

2. Sélectionnez le répertoire sur le disque du serveur protégé ou le répertoire de réseau dans lequel vous souhaitez enregistrer le fichier avec l'objet.

CONFIGURATION DE PARAMETRES DE LA QUARANTAINE EN MMC

Cette section décrit la configuration des paramètres de la quarantaine. Les nouvelles valeurs des paramètres de la quarantaine sont appliquées directement après l'enregistrement.

La description des paramètres de la quarantaine et de leur valeur par défaut est reprise au point "Paramètres de quarantaine" (cf. page 405).

Pour configurer les paramètres de la quarantaine, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Quarantaine** et sélectionnez l'option **Propriétés** (cf. ill. ci-après).

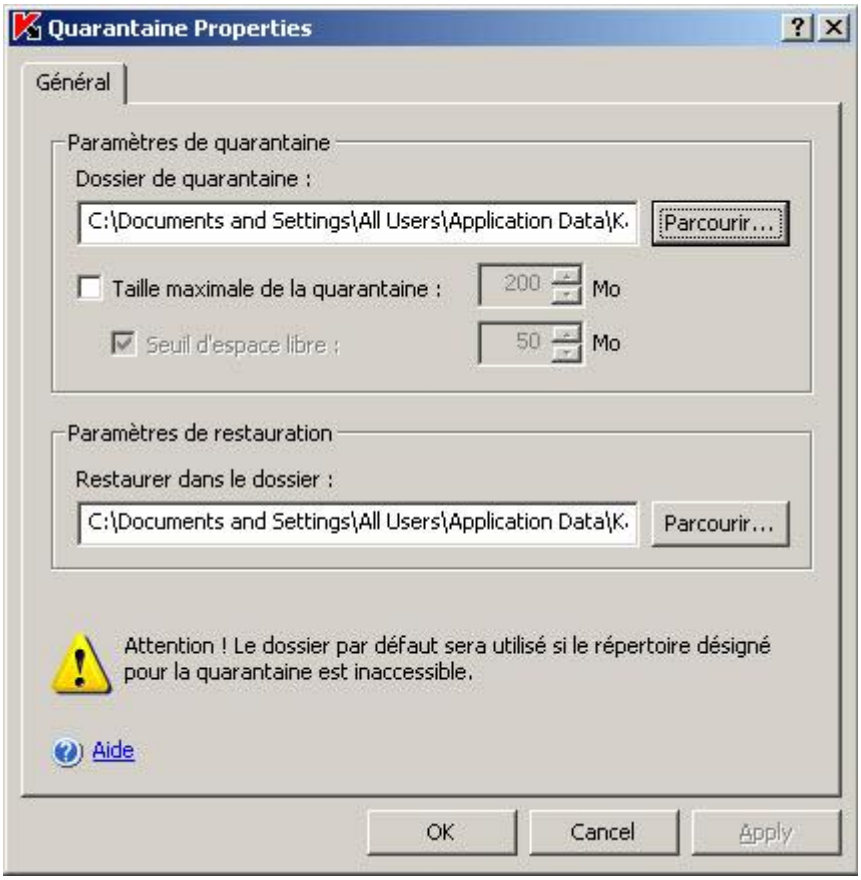


*Illustration 67. Boîte de dialogue **Propriétés : Quarantaine***

2. Dans la boîte de dialogue **Quarantaine Propriétés** configurez les différents paramètres en fonction de vos besoins :

   - Pour désigner un dossier de quarantaine (cf. page 406) différent du dossier par défaut, choisissez le dossier souhaité sur le disque local du serveur protégé dans le champ **Répertoire de quarantaine** ou indiquez son nom et le chemin d'accès complet.

   - pour définir la taille maximale de la quarantaine (cf. page 406), cochez la case **Taille maximale de la quarantaine** et saisissez la valeur souhaitée en mégaoctets dans le champ ;

   - pour définir l'espace disponible minimum dans la quarantaine, cochez la case **Taille maximale de la quarantaine** (cf. page 407), cochez la case **Seuil d'espace libre** et saisissez la valeur souhaitée en mégaoctets dans le champ ;

   - pour désigner un autre répertoire de restauration (cf. page 411), sélectionnez, dans le groupe de paramètres **Paramètres de restauration**, le répertoire souhaité sur le disque local du serveur protégé ou saisissez son nom et son chemin d'accès complet.

3. Cliquez sur **OK**.

STATISTIQUES DE QUARANTAINE

Vous pouvez consulter les informations relatives au nombre d'objets en quarantaine ; il s'agit des statistiques de la quarantaine.

Pour consulter les statistiques de la quarantaine,

ouvrez le menu contextuel du nœud, **Quarantaine** dans l'arborescence de la console et sélectionnez la commande **Statistiques** (cf. ill. ci-après).

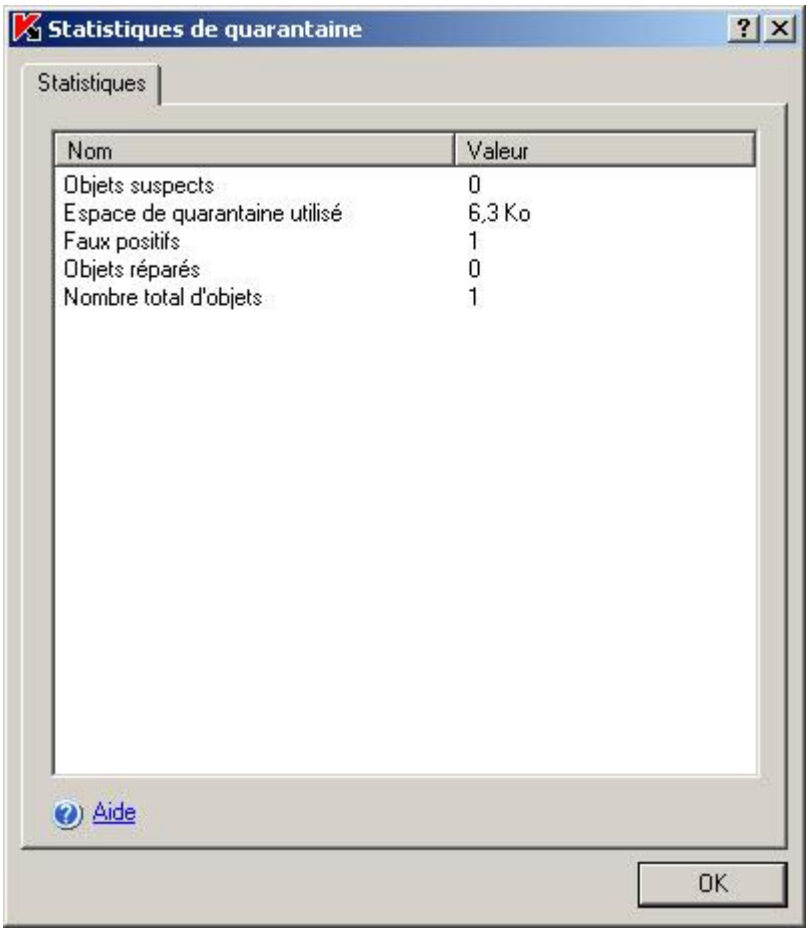


*Illustration 68. Boîte de dialogue **Statistiques de quarantaine***

La boîte de dialogue **Statistiques de quarantaine** reprend les informations sur le nombre d'objets en quarantaine à l'heure actuelle (cf. tableau ci-dessous).

Tableau 20. Informations sur les objets en quarantaine dans la fenêtre Statistiques de quarantaine

CHAMP	DESCRIPTION
Nombre d'objets suspects	Nombre total d'objets en quarantaine.
Espace de quarantaine utilisé	Volume général de données dans le dossier de quarantaine.
Objets en fausse alarme	Nombre d'objets qui ont reçu l'état **Fausse alerte** car l'analyse de la quarantaine à l'aide des bases actualisées a indiqué ces objets comme étant sains.
Objets réparés	Nombre d'objets qui ont reçu l'état **Réparé** après l'analyse de la quarantaine.
Nombre total d'objets	Nombre total d'objets en quarantaine.

BOITES DE DIALOGUE : QUARANTAINE

DANS CETTE SECTION DE L'AIDE

QUARANTAINE (ENTREE)

La Quarantaine est une zone de stockage pour isoler les objets infectés.

Les objets sont placés en quarantaine sous un format chiffré, qui élimine le risque de propagation de l'infection.

L'entrée **Quarantaine** permet d'opérer manuellement sur les objets en quarantaine ; mise en quarantaine, examen, restauration ou suppression, et également de paramétrer la quarantaine.

Panneau de résultats

Le panneau des résultats reprend les informations suivantes pour chaque objet en quarantaine :

Objet – nom de l'objet placé en quarantaine.

Etat – état de l'objet en quarantaine ; peut prendre les valeurs suivantes :

- **Suspect**. L'objet est suspect ; il existe une équivalence partielle entre une partie du code de l'objet et une partie du code d'une menace connue.
- **Infecté**. L'objet est infecté ; il existe une équivalence parfaite entre une partie du code de l'objet et une partie du code d'une menace connue.
- **Fausse alerte**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est sain.
- **Réparé**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est infecté mais qu'il a pu être réparé. Vous pouvez restaurer l'objet sans craintes.
- **Ajouté par l'utilisateur**. L'objet a été placé en quarantaine par l'utilisateur.

Niveau de danger – le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace de l'objet. Le paramètre peut prendre les valeurs suivantes :

- **Haut**. L'objet contient une menace de type vers de réseau, virus traditionnels, chevaux de Troie ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues).

- **Moyen**. L'objet peut contenir une menace du type autres programmes malveillants, logiciels publicitaires ou programmes au contenu pornographique.
- **Bas**. L'objet peut contenir une menace du type programmes présentant un risque potentiel.
- **Événement d'information**. L'objet a été placé en quarantaine par l'utilisateur.

Type de menace : type de la menace selon la classification de Kaspersky Lab. Ce type figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté.

Nom de menace : nom de la menace selon la classification de Kaspersky Lab. Ce nom figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez consulter le nom complet de la menace découverte dans l'objet dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234).

Date d'ajout : date du placement de l'objet en quarantaine.

Chemin d'origine : chemin complet de l'emplacement d'origine de l'objet ; par exemple, le dossier depuis lequel l'objet a été déplacé vers la quarantaine, un fichier contenu dans une archive comprimée, ou un fichier .pst dans une base de données de messagerie.

Taille : taille de l'objet.

Nom d'utilisateur –cette colonne reprend les données suivantes :

- **Si l'objet a été isolé par** Kaspersky Anti-Virus dans la tâche Protection en temps réel des fichiers – le nom du compte utilisateur sous les privilèges duquel l'application a sollicité l'objet au moment de l'interception.
- Si l'objet a été isolé par Kaspersky Anti-Virus dans la tâche d'analyse à la demande – le nom du compte utilisateur sous les privilèges duquel la tâche a été exécuté.
- Si l'utilisateur a placé l'objet en quarantaine manuellement – le nom du compte de cet utilisateur.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Ajouter**- déplace vers la quarantaine un fichier que vous soupçonnez infecté, mais que Kaspersky Anti-Virus n'a pas détecté.
- **Tout analyser** : analyse tous les objets en quarantaine (lancer la tâche **Analyse des objets en quarantaine**).
- **Statistiques** : affiche les informations sur l'état de la quarantaine et des objets contenus.
- **Filtre**- recherche dans la quarantaine des objets qui répondent aux conditions sélectionnées.
- **Supprimer le filtre** : supprime le filtre.
- **Effacer**- supprime tous les objets en quarantaine.
- **Exporter les paramètres/Importer les paramètres** : enregistre les paramètres de quarantaine dans un fichier/restaure les paramètres de quarantaine à partir d'un fichier.
- **Paramètres**- configure les paramètres de quarantaine

Les informations affichées dans le panneau de résultats peuvent être triées par n'importe quelle colonne.

VOIR EGALEMENT

PROPRIETES (FENETRE). QUARANTAINE

La Quarantaine est une zone de stockage pour isoler les objets infectés.

Les paramètres de cet onglet permettent de contrôler l'emplacement du dossier de quarantaine sur le serveur sécurisé, les critères d'état de la quarantaine et les paramètres de restauration des objets placés en quarantaine.

La section **Paramètres de quarantaine** affiche l'adresse du dossier de quarantaine et les paramètres utilisés par Kaspersky Anti-Virus pour surveiller l'état de la quarantaine et pour envoyer des notifications à l'administrateur.

Le dossier de quarantaine doit se trouver sur le serveur sécurisé ou sur un ordinateur équipé de Kaspersky Anti-Virus. %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Quarantaine. Vous pouvez spécifier n'importe quel dossier des unités locales du serveur.

Pour enregistrer des informations sur le dépassement de capacité de la quarantaine, cochez **Taille maximale de la quarantaine** et spécifiez la taille en mégaoctets (200 Mo par défaut). Kaspersky Anti-Virus surveillera alors la taille totale des objets placés en quarantaine. En cas de dépassement, l'événement est enregistré (**Dépassement de la taille maximum de quarantaine**), et une notification est générée conformément aux paramètres pour ce type d'événement.

Pour être informé des dépassements de quarantaine, cochez la case **Seuil d'espace libre** et spécifiez la quantité minimum d'espace libre du dossier de quarantaine en mégaoctets (50 Mo par défaut). Si l'espace libre de la quarantaine est en dessous de ce seuil, l'événement (**Espace libre insuffisant**) est consigné et une notification est générée conformément aux paramètres pour ce type d'événement.

> La caractéristique de **Taille maximale de la quarantaine** n'impose pas de limites à la taille du dossier de quarantaine. Elle fonctionne simplement comme un critère d'événement et permet à l'administrateur de surveiller l'état de la quarantaine. Les objets seront déplacés en quarantaine même après avoir atteint ce seuil.

Dans la section **Paramètres de restauration**, spécifiez dans le champ **Restaurer dans le dossier** le chemin du dossier cible de restauration des objets. Par défaut les objets sont restaurés dans leurs dossiers d'origine. Vous pouvez spécifier un même dossier de restauration pour tous les objets se trouvant sur le serveur sécurisé ou sur un poste différent du réseau local. Le chemin de la ressource doit être noté au format UNC (Universal Naming Convention).

PARAMETRES DU FILTRE (FENETRE). QUARANTAINE

Utilisez cette fenêtre pour créer le critère de recherche des objets présents dans la zone de sauvegarde.

Vous pouvez utiliser de nombreuses conditions dans les critères, combinées avec le lien logique "and" ou "or". Les critères sont créés avec les zones et les boutons sur le côté droit de la fenêtre. La liste des conditions est affichée dans la partie supérieure de la fenêtre.

La liste **Nom du champ** propose les valeurs suivantes:

- **Date d'ajout** : date du placement de l'objet dans la sauvegarde.
- Le **nom d'utilisateur** en fonction de la manière dont l'objet a été placé en sauvegarde reprend :
  - Le nom du compte utilisateur sous lequel l'application sollicitant l'objet a contacté le serveur, si l'objet a été placé en sauvegarde suite à l'exécution de la tâche **Protection en temps réel des fichiers** ;
  - Le nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée, si l'objet a été placé en sauvegarde suite à l'exécution de l'analyse à la demande.
- **Nom de menace** : nom de la menace selon la classification de Kaspersky Lab. Ce nom figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez aussi voir le nom complet de la menace dans le journal relatif à l'exécution de la tâche.
- **Chemin d'origine** : chemin complet de l'emplacement d'origine de l'objet; par exemple, le dossier depuis lequel l'objet a été sauvegardé, un fichier contenu dans une archive comprimée, ou un fichier .pst dans une base de données de messagerie.
- **Objet** : nom sous lequel l'objet a été traité par Kaspersky Anti-Virus.
- **Taille** : taille de l'objet.
- **Etat** : état attribué à l'objet par Kaspersky Anti-Virus pendant l'analyse.
- **Type de menace** : type de la menace selon la classification de Kaspersky Lab.

Niveau de danger : niveau du risque posé par l'objet.

VOIR EGALEMENT

Filtrage des objets en quarantaine 194

Tri des objets en quarantaine 194

Consultation des objets en quarantaine 191

RESTAURATION DE L'OBJET (FENETRE). QUARANTAINE

La restauration d'objets depuis la quarantaine ou la zone de sauvegarde peut produire l'infection du serveur et du réseau tout entier.

Cette fenêtre est utilisée pour configurer les paramètres de restauration de fichiers depuis la quarantaine ou la sauvegarde. Le nom de l'objet restauré est affiché dans la zone **Objet** de la partie supérieure de la fenêtre.

Si l'objet faisait partie d'un objet composé, il ne sera pas restauré dans ce dernier. Il sera enregistré séparément dans le dossier indiqué.

Le chemin où l'objet sera enregistré est déterminé par les paramètres de la quarantaine ou du dossier de sauvegarde. Par défaut, l'objet est restauré dans le dossier d'origine ou, si précisé dans les paramètres de la quarantaine ou du dossier de sauvegarde, dans un dossier de restauration partagé pour tous les objets.

Cette fenêtre permet de spécifier un autre chemin de restauration des objets. Pour ce faire, sélectionnez l'une de ces options :

- **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau** : l'objet restauré sera enregistré dans son dossier d'origine, lorsqu'il a été déplacé vers la quarantaine. Le chemin complet où l'objet sera restauré est affiché dans la zone de saisie.

- **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** : l'objet sera enregistré dans un dossier de restauration partagé pour tous les objets, comme indiqué par les paramètres de la quarantaine ou du dossier de sauvegarde. Le chemin complet où l'objet sera restauré est affiché dans la zone de saisie.

- **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** : l'objet restauré sera enregistré dans un dossier sélectionné sur l'ordinateur où se trouve installé la console de Kaspersky Anti-Virus, ou sur un autre poste du réseau local. Le chemin de la ressource doit être noté au format UNC (Universal Naming Convention) dans la zone de saisie.

L'objet sera enregistré à l'adresse et avec le nom spécifié dans son format d'origine. Toutes les permissions d'accès et attributs du fichier (archive, lecture-seule, etc.) et les autres propriétés de l'objet d'origine seront également restaurées.

Par défaut une copie de l'objet est conservée dans la zone de sauvegarde et peut être supprimée manuellement. Sélectionnez **Supprimer les objets sauvegardés après leur restauration** pour que ces copies soient supprimées automatiquement après une restauration réussie. S'il n'est pas possible de restaurer l'objet, la copie ne sera pas supprimée.

Si vous sélectionnez la restauration de plusieurs objets, vous pouvez appliquer les paramètres de cette fenêtre au reste des objets. Pour ce faire, sélectionnez **Appliquer à tous les objets sélectionnés**.

VOIR EGALEMENT

Restauration de l'objet depuis la quarantaine 198

Suppression des objets de la quarantaine 201

UN OBJET AVEC CE NOM EXISTE DEJA (FENETRE). QUARANTAINE

Cette fenêtre vous indique qu'à l'adresse indiquée, il existe un fichier du même nom que l'objet à restaurer. Le nom complet du fichier (chemin compris) est affiché dans le champ Objet de la partie supérieure de la fenêtre. Observez que le chemin est spécifié conformément aux paramètres de restauration sélectionnés dans la fenêtre précédente.

Vous pouvez remplacer le fichier existant, modifier l'emplacement de l'objet à restaurer, ou le renommer. Pour ce faire, sélectionnez l'une des options suivantes :

- **Remplacer**. Si vous sélectionnez cette option, le fichier existant sera supprimé et l'objet restauré à la même place et sous le même nom.

- **Renommer**. Sélectionnez cette option pour enregistrer l'objet sous un autre nom ou pour changer le chemin où l'objet doit être enregistré. Entrez le nom complet du fichier (chemin compris) avec lequel l'objet restauré sera enregistré.

- **Renommer en ajoutant un suffixe**. Avec cette option, la suite de caractères saisis dans la zone sera ajoutée au nom du fichier. Cette option est utile pour restaurer de nombreux objets avec l'option **Appliquer à tous les objets**. Suite de caractères doit satisfaire les règles de nommage des fichiers.

VOIR EGALEMENT

Restauration de l'objet depuis la quarantaine 198

STATISTIQUES (ONGLET). QUARANTAINE

L'onglet **Statistiques** affiche des informations sur l'état de la quarantaine et des objets contenus. Cet onglet reprend les données suivantes :

- **Objets suspects** : nombre total d'objets qui se distinguent par les propriétés suivantes :
  - sont classés comme suspects, parce qu'une coïncidence partielle a été détectée entre une partie du code de l'objet et le code d'une menace connue ;
  - ont été reconnus comme objets suspects à l'aide de l'analyseur heuristique.
- **Espace de quarantaine utilisé** – taille totale des objets en quarantaine.
- **Objets en fausse alarme** – total des objets classés comme non-infectés, d'après l'analyse de la quarantaine avec une base de données à jour.
- **Objets réparés** – total des objets réparés par l'analyse de la quarantaine avec une base de données à jour.
- **Nombre total d'objets** – nombre total d'objets en quarantaine.

SAUVEGARDE DES OBJETS AVANT LA REPARATION / LA SUPPRESSION. UTILISATION DE LA SAUVEGARDE

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA SAUVEGARDE DES OBJETS AVANT LA REPARATION / LA SUPPRESSION

Kaspersky Anti-Virus enregistre dans le dossier de *sauvegarde* une copie cryptée des objets dont le statut est **Infecté** ou **Suspect** avant de procéder à la réparation ou à la suppression.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Anti-Virus enregistre cet objet composé dans la sauvegarde. Par exemple, si Kaspersky Anti-Virus considère un des objets de la base de messagerie comme étant suspect, il place en sauvegarde l'ensemble de la base de messagerie.

Si la taille l'objet que Kaspersky Anti-Virus copie dans la sauvegarde est importante, le système peut ralentir et l'espace disponible sur le disque dur de l'ordinateur peut être réduit.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur le serveur protégé ou sur un autre ordinateur du réseau local. Vous pouvez restaurer le fichier du dossier de sauvegarde si, par exemple, le fichier original infecté contenait des informations cruciales et que lors de la réparation, Kaspersky Anti-Virus n'a pas réussi à le préserver, ce qui a rendu inaccessibles les informations qu'il contenait.

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

CONSULTATION DES FICHIERS DU DOSSIER DE SAUVEGARDE

Vous pouvez consulter les fichiers du dossier de sauvegarde uniquement via la console de Kaspersky Anti-Virus dans le nœud **Sauvegarde**. Vous ne pouvez pas les consulter à l'aide des gestionnaires de fichiers de Microsoft Windows.

- *Pour consulter les fichiers de la sauvegarde,*

  dans l'arborescence de la console, sélectionnez le nœud **Sauvegarde** (cf. ill. ci-après).

- *Pour trouver l'objet requis dans la liste des objets en quarantaine,*

  vous pouvez les trier (cf. page 213) ou les filtrer (cf. page 214).

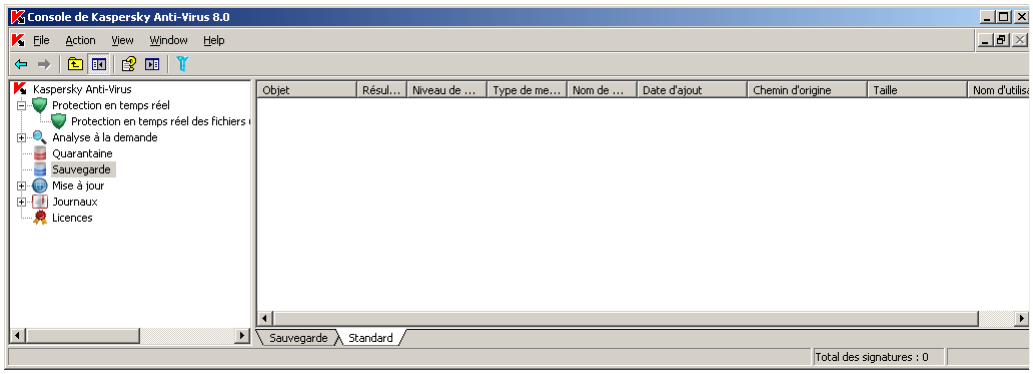


Illustration 69. Informations relatives aux fichiers dans la sauvegarde dans la console de Kaspersky Anti-Virus

Le panneau de résultats reprend les informations sur le fichier se trouvant dans le dossier de sauvegarde (cf. tableau ci-dessous).

Tableau 21. Informations sur le fichier dans le dossier de sauvegarde

CHAMP	DESCRIPTION
Objet	Nom du fichier dont une copie se trouve dans la sauvegarde.
Etat	Etat du fichier concernant la présence ou non de menaces. Peut prendre les valeurs suivantes : • **Infecté**. Le fichier est infecté ; il existe une équivalence parfaite entre une partie du code du fichier et une partie du code d'une menace connue. • **Suspect**. Le fichier est suspect; il existe une équivalence partielle entre une partie du code du fichier et une partie du code d'une menace connue.
Niveau de danger	Le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace de l'objet. Le paramètre peut prendre les valeurs suivantes : • **Haut**. Le fichier contient une menace de type vers de réseau, virus traditionnels, chevaux de Troie ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues). • **Moyen**. Le fichier peut contenir une menace du type autres programmes malveillants, logiciels publicitaires ou programmes au contenu pornographique. • **Bas**. Le fichier peut contenir une menace du type programmes présentant un risque potentiel.
Type de menace	Type de menaces selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez consulter le nom complet de la menace découverte dans l'objet dans le nœud **Journaux**, dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234)
Nom de menace	Nom de la menace selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez consulter le nom complet de la menace découverte dans l'objet dans le nœud **Journaux**, dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234)
Date d'ajout	Date et heure de l'enregistrement du fichier dans la sauvegarde
Chemin d'origine	Chemin d'accès complet au répertoire d'origine : répertoire où se trouvait le fichier avant que sa copie ne soit placée par Kaspersky Anti-Virus dans la sauvegarde.
Taille	Taille du fichier.
Nom d'utilisateur	Cette colonne reprend les informations suivantes : • Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche **Protection en temps réel des fichiers** : nom du compte utilisateur sous les privilèges duquel l'application a sollicité le fichier au moment de l'interception du fichier ; • Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche d'analyse à la demande – nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée.

DANS CETTE SECTION DE L'AIDE

TRI DES FICHIERS DE LA SAUVEGARDE

Par défaut, les fichiers de la sauvegarde sont classés par date d'enregistrement dans l'ordre chronologique inversé. Pour trouver le fichier requis, vous pouvez trier les fichiers selon le contenu de n'importe quelle colonne dans le panneau de résultats.

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Sauvegarde**.

2. Dans la liste des fichiers de la sauvegarde, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les objets.

FILTRAGE DES FICHIERS DE LA SAUVEGARDE

Pour trouver le fichier qu'il vous faut dans la sauvegarde, vous pouvez filtrer les fichiers, c.-à-d. afficher dans le nœud **Sauvegarde** uniquement les fichiers qui répondent aux conditions de filtrage que vous avez définies (les filtres).

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez **Filtre**.

2. La boîte de dialogue **Paramètres du filtre** s'ouvrira (cf. ill. ci-après).

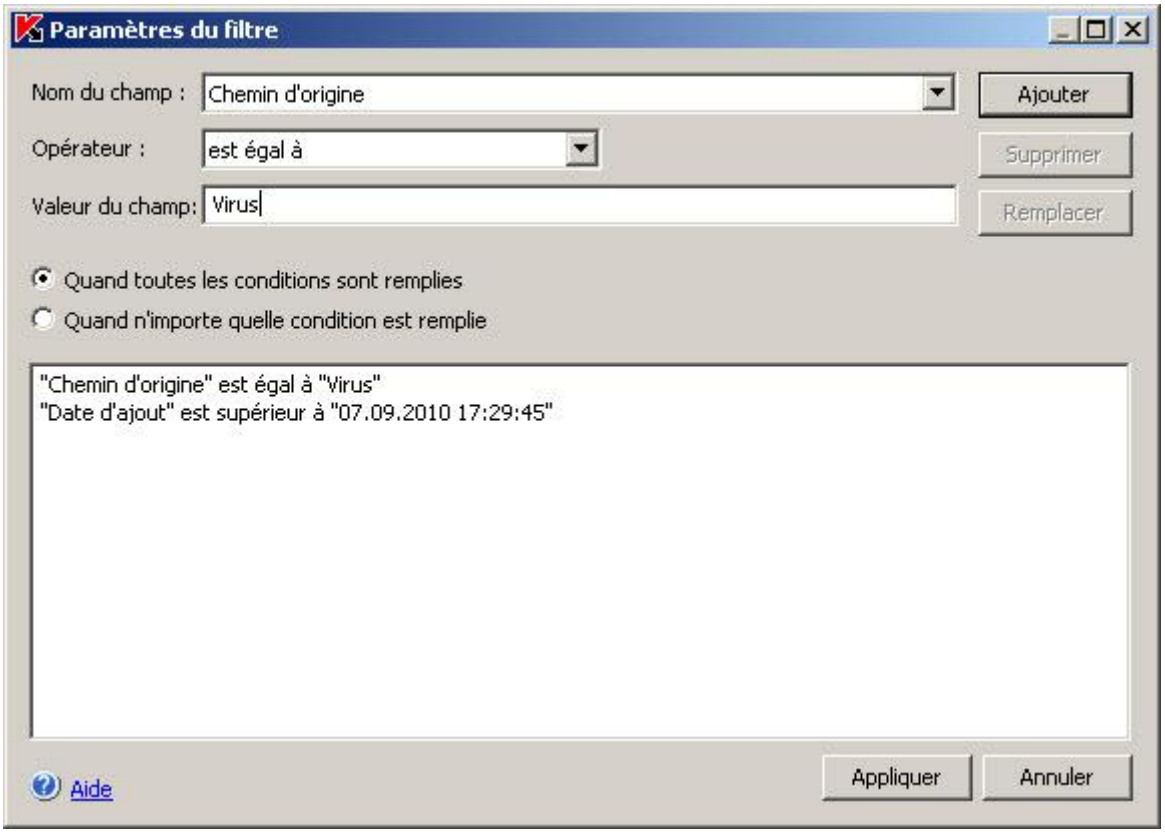


*Illustration 70. Boîte de dialogue **Paramètres du filtre***

3. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ dont la valeur sera comparée à la valeur du filtre.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

d. Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, vous pouvez observer les règles suivantes :

- Afin de réunir quelques filtres selon le " ET " logique, sélectionnez l'option **En cas d'exécution de toutes les conditions**.
- Afin de réunir quelques filtres selon le " OU " logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les fichiers qui répondent aux conditions des filtres.

Pour afficher tous les fichiers dans la liste des fichiers dans la sauvegarde,

dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez la commande **Supprimer le filtre**.

RESTAURATION DES FICHIERS DEPUIS LA SAUVEGARDE

Kaspersky Anti-Virus place les fichiers sous une forme cryptée dans la sauvegarde afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer les fichiers de la sauvegarde.

La restauration d'un fichier peut s'imposer dans les situations suivantes :

- Si le fichier original, qui était infecté, contenait des informations importantes et que Kaspersky Anti-Virus n'a pas pu préserver son intégrité lors de la réparation, ce qui a rendu les informations du fichier inaccessibles ;
- Vous estimez que le fichier ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Anti-Virus ne considère plus ce fichier comme un fichier infecté ou suspect lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche **Protection en temps réel des fichiers** et dans les tâches d'analyse à la demande. Pour ce faire désignez le fichier en tant que valeur du paramètre "Exclusion des objets" (cf. page 379) ou du paramètre "Exclusion des menaces" de ces tâches.

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Lors de la restauration d'un objet, vous pouvez sélectionner l'emplacement où l'objet restauré sera conservé : dans le répertoire d'origine (par défaut), dans un dossier spécial de restauration sur le serveur protégé ou dans un autre dossier indiqué sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou sur un autre ordinateur du réseau.

Pour que Kaspersky Anti-Virus n'analyse pas les objets volumineux lors de la restauration des fichiers depuis la sauvegarde, définissez une exclusion pour le dossier %Temp%\wseeqbfiles\.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce répertoire est défini par les paramètres de la sauvegarde. Cf. rubrique "Configuration des paramètres de la sauvegarde" (à la page 218).

Par défaut, quand Kaspersky Anti-Virus restaure un fichier, il enregistre une copie dans la sauvegarde. Vous pouvez supprimer la copie du fichier de la sauvegarde après la restauration.

Pour restaurer des fichiers depuis la sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Sauvegarde**.

2. Exécutez une des actions suivantes :

   - pour restaurer un fichier, ouvrez le menu contextuel du fichier, dans la liste des fichiers de la sauvegarde, que vous souhaitez restaurer et sélectionnez la commande **Restaurer**.

   - pour restaurer plusieurs objets, sélectionnez les objets souhaités dans la liste à l'aide de la touche **Ctrl** ou **Shift**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez la commande **Restaurer**.

3. Dans la boîte de dialogue **Restauration de l'objet**, spécifiez le répertoire dans lequel le fichier restauré sera enregistré (cf. ill. ci-après).

   Le nom du fichier apparaît dans le champ **Objet** de la partie supérieure de la boîte de dialogue. Si vous avez sélectionné plusieurs objets, dans ce champ est le nom du premier de la liste qui est affiché.

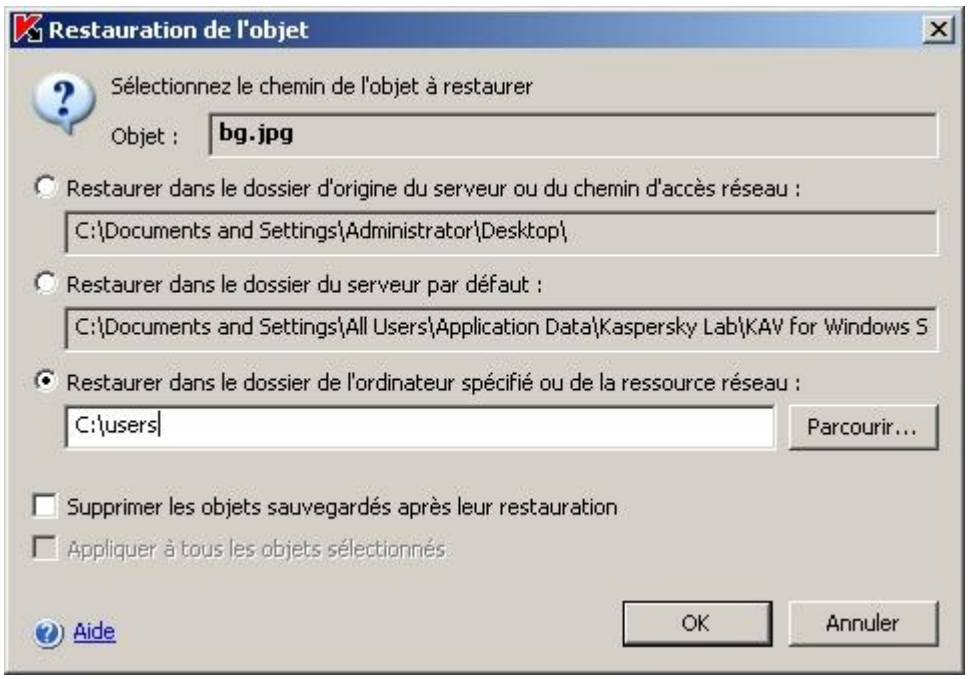


*Illustration 71. Boîte de dialogue **Restauration de l'objet***

Exécutez une des actions suivantes :

- Pour enregistrer le fichier restauré sur le serveur protégé, sélectionnez une des options suivantes :

  - **Restaurer dans le dossier d'origine**, si vous souhaitez restaurer le fichier dans le dossier d'origine.

  - **Restaurer dans le dossier du serveur, utilisé par défaut**, si vous souhaitez restaurer le fichier dans le dossier que vous avez désigné en guise de dossier pour la restauration dans les paramètres de la sauvegarde (cf. page 411).

- Pour enregistrer le fichier restauré dans un autre répertoire, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis sélectionnez le répertoire souhaité (sur l'ordinateur où est installée la console de Kaspersky Anti-Virus ou dans un répertoire de réseau) ou saisissez le chemin d'accès à celui-ci.

4. Si vous souhaitez conserver une copie du fichier dans la sauvegarde après la restauration, désélectionnez la case **Supprimer les objets sauvegardés après leur restauration**.

5. Si vous avez sélectionné plusieurs fichiers pour la restauration, alors pour appliquer les conditions de conservation définies aux autres fichiers sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les fichiers sélectionnés seront restaurés et enregistrés dans le dossier que vous aurez désigné : si vous avez sélectionné l'option **Restaurer dans le dossier d'origine du serveur ou dans le dossier de réseau indiqué**, chacun des fichiers sera enregistré dans son dossier d'origine ; si vous avez sélectionné **Restaurer dans le dossier du serveur par défaut** ou **Restaurer dans le dossier sur l'ordinateur local ou dans une ressource de réseau**, tous les fichiers seront conservés dans le répertoire spécifié.

6. Cliquez sur **OK**.

   Kaspersky Anti-Virus commence par restaurer le premier des fichiers que vous avez sélectionnés.

   Si un fichier portant le même nom existe déjà dans le répertoire indiqué, la boîte de dialogue **Un objet avec ce nom existe déjà** s'ouvrira (cf. ill. ci-après).

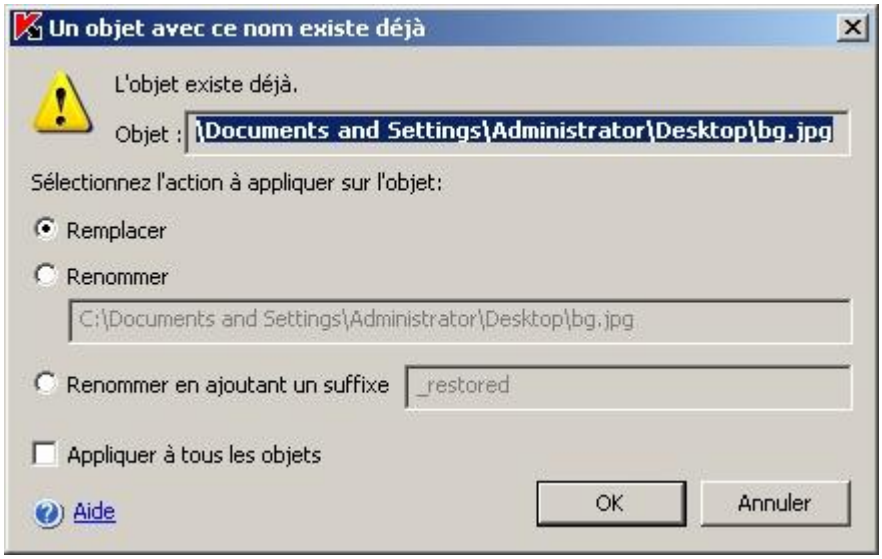


*Illustration 72. Boîte de dialogue **Un objet avec ce nom existe déjà***

7. Exécutez les actions suivantes :

   a. Sélectionnez une des conditions suivantes de conservation du fichier restauré :

      - **Remplacer** afin d'enregistrer le fichier restauré au lieu du fichier existant.
      - **Renommer** afin d'enregistrer le fichier restauré sous un autre nom. Saisissez le nouveau nom du fichier et son chemin d'accès complet dans le champ
      - **Renommer l'objet en ajoutant un suffixe** afin de renommer le fichier en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

   b. Si vous souhaitez appliquer l'action **Remplacer** ou **Renommer** en ajoutant un suffixe aux fichiers restants, cochez la case **Appliquer à tous les objets**.

      Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets** ne sera pas accessible.

   c. Cliquez sur **OK**.

   Le fichier sera restauré. Les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets restants** dans la boîte de dialogue **Restauration de l'objet**, alors la boîte de dialogue **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer le répertoire dans lequel le prochain fichier de la sélection sera enregistré après la restauration (cf. étape 3 des présentes instructions).

SUPPRESSION DES FICHIERS DEPUIS LA SAUVEGARDE

Pour supprimer un ou plusieurs fichiers de la sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Sauvegarde**.

2. Exécutez une des actions suivantes :

   - pour supprimer un fichier, ouvrez le menu contextuel du fichier que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;

   - Pour supprimer plusieurs objets, sélectionnez les objets souhaités dans la liste à l'aide de la touche **Ctrl** ou **Shift**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez la commande **Supprimer**.

3. Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération. Les fichiers sélectionnés seront supprimés.

CONFIGURATION DES PARAMETRES DE LA SAUVEGARDE EN MMC

Cette rubrique décrit la configuration des paramètres de la sauvegarde (cf. page 408).

Les nouvelles valeurs des paramètres de la sauvegarde sont appliquées directement après l'enregistrement.

Pour configurer les paramètres de la sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Sauvegarde** et choisissez l'option **Propriétés** (cf. ill. ci-après).

*Illustration 73. Boîte de dialogue **Propriétés : Sauvegarde***

2. Dans la boîte de dialogue **Propriétés : Sauvegarde**, exécutez les opérations suivantes :

   - Pour définir le dossier qui abritera la sauvegarde (cf. page 409), sélectionnez, dans le champ **Dossier de sauvegarde**, le dossier requis sur le disque local du serveur protégé ou saisissez le chemin d'accès complet à celui-ci.

   - Pour définir la taille maximale de la sauvegarde (cf. page 410), cochez la case **Taille maximale de la sauvegarde** et saisissez la valeur souhaitée en mégaoctets dans le champ.

   - Pour définir le seuil d'espace disponible dans la sauvegarde (cf. page 410), définissez la valeur de **Taille maximale de la sauvegarde**, cochez la case **Seuil d'espace libre** et saisissez la valeur minimale souhaitée d'espace disponible dans la sauvegarde en mégaoctets.

   - Pour indiquer le répertoire de restauration (cf. page 411), dans le groupe de paramètres **Paramètres de restauration**, sélectionnez le répertoire requis sur le disque local du serveur protégé ou dans le champ **Restaurer dans le dossier**, saisissez le nom du dossier et son chemin d'accès complet.

3. Cliquez sur **OK**.

STATISTIQUES DE SAUVEGARDE

Vous pouvez consulter les informations relatives à l'état de la sauvegarde en ce moment ; il s'agit des statistiques de la sauvegarde.

- *Pour consulter les statistiques de la sauvegarde,*

  dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez la commande **Statistiques**.

Dans la boîte de dialogue **Statistiques de sauvegarde** (cf. ill. ci-après), vous pourrez voir les informations relatives à l'état de la sauvegarde à l'heure actuelle (cf. tableau ci-dessous).

Tableau 22. Informations sur l'état de la sauvegarde

CHAMP	DESCRIPTION
Espace de stockage utilisé	Volume de données dans la sauvegarde ; tient compte de la taille des fichiers chiffrés
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde

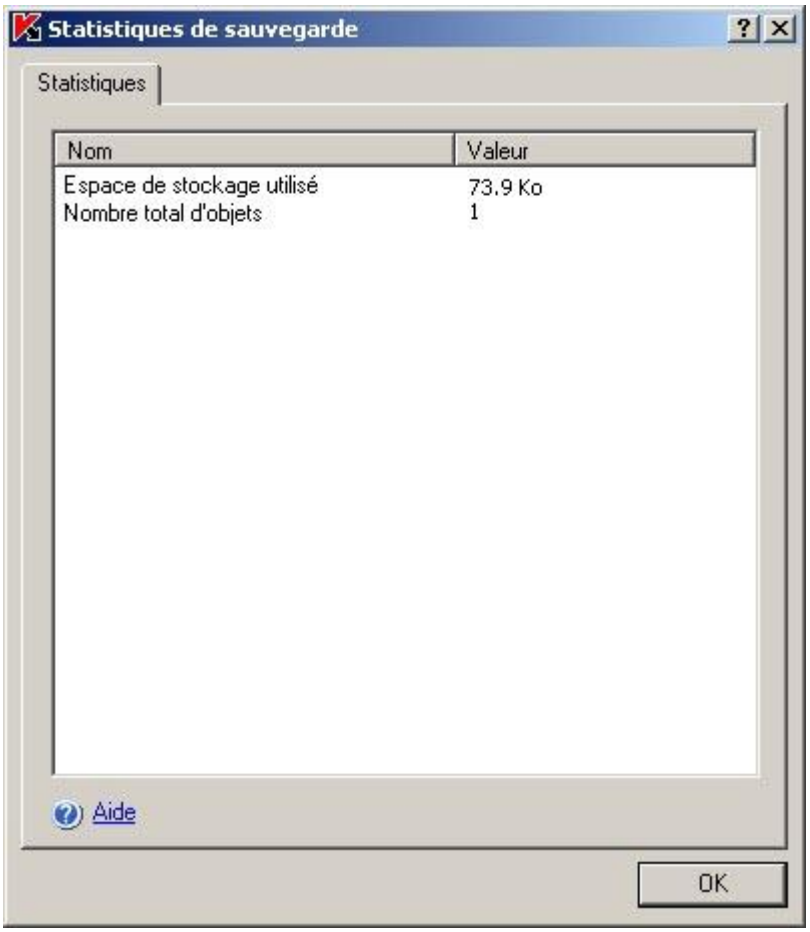


*Illustration 74. Boîte de dialogue **Statistiques de sauvegarde***

BOITES DE DIALOGUE : SAUVEGARDE

DANS CETTE SECTION DE L'AIDE

SAUVEGARDE (ENTREE)

Kaspersky Anti-Virus enregistre dans le dossier de *Sauvegarde* une copie cryptée des objets dont le statut est **Infecté** ou **Suspect** avant de procéder à la réparation ou à la suppression.

Si Kaspersky Anti-Virus juge qu'un objet de l'archive est suspect, il met celui-ci en quarantaine et conserve une copie de l'archive dans le dossier de sauvegarde.

L'élément d'administration **Sauvegarde** est prévu pour la consultation des copies de sauvegarde des objets, leur restauration ou leur suppression ainsi que pour la configuration des paramètres de sauvegarde : emplacement de la sauvegarde, paramètres de restauration des objets et critères d'audit de l'état de la sauvegarde.

Panneau de résultats

Le panneau de résultats affiche la liste des copies de sauvegarde sous forme de tableau. Les informations suivantes sont présentées pour chacun d'eux :

Objet : nom du fichier dont une copie se trouve dans la sauvegarde.

Etat : état du fichier en ce qui concerne la présence ou nom de menaces. Ce paramètre peut prendre les valeurs suivantes :

- **Infecté** : le fichier est infecté ; il existe une équivalence parfaite entre une partie du code du fichier et une partie du code d'une menace connue.
- **Suspect** : l'objet est classé suspect ; une coïncidence partielle a été détectée entre une partie du code de l'objet et le code d'une menace connue.

Niveau de danger – le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace de l'objet. Le paramètre peut prendre les valeurs suivantes :

- **Haut** : le fichier contient une menace de type vers de réseau, virus traditionnels, chevaux de Troie ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues).
- **Moyen** : le fichier peut contenir une menace du type autres programmes malveillants, logiciels publicitaires ou programmes au contenu pornographique.
- **Bas** : le fichier peut contenir une menace du type programmes présentant un risque potentiel.

Type de menace : type de la menace selon la classification de Kaspersky Lab. Ce type figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un fichier comme étant infecté ou suspect. Vous pouvez

consulter le nom complet de la menace dans l'objet dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234)

Nom de menace : nom de la menace selon la classification de Kaspersky Lab. Ce nom figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un fichier comme étant infecté. Vous pouvez consulter le nom complet de la menace dans l'objet dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234)

Date d'ajout : date et heure du placement de l'objet dans la sauvegarde.

Chemin d'origine : chemin d'accès complet au répertoire d'origine : répertoire où se trouvait le fichier avant que sa copie ne soit placée par Kaspersky Anti-Virus dans la sauvegarde.

Taille : taille du fichier.

Nom d'utilisateur –cette colonne reprend les données suivantes :

- Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche **Protection en temps réel des fichiers** : nom du compte utilisateur sous les privilèges duquel l'application a sollicité le fichier au moment de l'interception du fichier.

- Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche d'analyse à la demande : nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée.

Les informations affichées dans le panneau de résultats peuvent être triées par n'importe quelle colonne.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Statistiques** : affiche les informations sur l'état de quarantaine et des objets contenus.

- **Filtre** : recherche dans la zone de sauvegarde des objets qui répondent aux conditions sélectionnées

- **Supprimer le filtre** : supprime le filtre.

- **Effacer** : supprime tous les objets sauvegardés

- **Exporter les paramètres/Importer les paramètres** : enregistre les paramètres de quarantaine dans un fichier/restaure les paramètres de quarantaine à partir d'un fichier.

- **Paramètres** : configure les paramètres de sauvegarde

VOIR EGALEMENT

FENETRE PROPRIETES : SAUVEGARDE

La sauvegarde est une zone de stockage spécialisée dans la copies d'objets, avant leur réparation ou leur suppression.

Les paramètres de cet onglet permettent de contrôler l'emplacement du dossier de sauvegarde sur le serveur sécurisé, les paramètres de restauration des objets qui s'y trouvent et les critères d'état de la sauvegarde.

La section **Paramètres de sauvegarde** affiche l'adresse du dossier de sauvegarde et les paramètres utilisés par Kaspersky Anti-Virus pour surveiller l'état de la zone de sauvegarde et pour envoyer des notifications à l'administrateur.

Les valeurs par défaut sont les mêmes que pour une installation locale du programme. Vous pouvez les modifier si nécessaire.

Le dossier de sauvegarde doit se trouver sur le serveur sécurisé ou sur un ordinateur équipé de Kaspersky Anti-Virus. %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Backup. Vous pouvez spécifier n'importe quel dossier des unités locales du serveur.

Pour enregistrer des informations sur le dépassement de capacité de la sauvegarde, cochez **Taille max. du dossier de sauvegarde** et spécifiez la taille en mégaoctets (200 Mo par défaut). Kaspersky Anti-Virus surveillera alors la taille totale des objets placés en quarantaine. En cas de dépassement, l'événement **Dépassement de la taille maximum de sauvegarde** est enregistré et une notification est générée conformément aux paramètres pour ce type d'événement.

Pour être informé des dépassements de quarantaine, cochez la case **Seuil d'espace libre** et spécifiez la quantité minimum d'espace libre du dossier de quarantaine en mégaoctets (50 Mo par défaut). Si l'espace libre de la sauvegarde est en dessous de ce seuil, l'événement (**Espace libre insuffisant**) est consigné et une notification est générée conformément aux paramètres pour ce type d'événement.

La caractéristique de **Taille max. du dossier de sauvegarde** n'impose pas de limites à la taille du dossier de sauvegarde, elle fonctionne simplement comme un critère d'événement et permet à l'administrateur de surveiller l'état de la zone de sauvegarde. Les objets seront sauvegardés même après avoir atteint ce seuil.

Dans la section **Paramètres de restauration**, spécifiez dans le champ **Restaurer dans le dossier** le chemin du dossier cible de restauration des objets. Par défaut les objets sont restaurés dans leurs dossiers d'origine. Vous pouvez spécifier un même dossier de restauration pour tous les objets se trouvant sur le serveur sécurisé ou sur un poste différent du réseau local. Le chemin de la ressource doit être noté au format UNC (Universal Naming Convention).

FENETRE PARAMETRES DE FILTRE: SAUVEGARDE

Utilisez cette fenêtre pour créer le critère de recherche des objets présents dans la zone de sauvegarde.

Vous pouvez utiliser de nombreuses conditions dans les critères, combinées avec le lien logique "and" ou "or". Les critères sont créés avec les zones et les boutons sur le côté droit de la fenêtre. La liste des conditions est affichée dans la partie supérieure de la fenêtre.

La liste **Nom du champ** propose les valeurs suivantes:

- **Date d'ajout** : date du placement de l'objet dans la sauvegarde.
- Le **nom d'utilisateur** en fonction de la manière dont l'objet a été placé en sauvegarde reprend :
  - Le nom du compte utilisateur sous lequel l'application sollicitant l'objet a contacté le serveur, si l'objet a été placé en sauvegarde suite à l'exécution de la tâche **Protection en temps réel des fichiers** ;
  - Le nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée, si l'objet a été placé en sauvegarde suite à l'exécution de l'analyse à la demande.
- **Nom de menace** : nom de la menace selon la classification de Kaspersky Lab. Ce nom figure dans le nom complet de la menace rendu par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez aussi voir le nom complet de la menace dans le journal relatif à l'exécution de la tâche.

- **Chemin d'origine** : chemin complet de l'emplacement d'origine de l'objet; par exemple, le dossier depuis lequel l'objet a été sauvegardé, un fichier contenu dans une archive comprimée, ou un fichier .pst dans une base de données de messagerie.
- **Objet** : nom sous lequel l'objet a été traité par Kaspersky Anti-Virus.
- **Taille** : taille de l'objet.
- **Etat** : état attribué à l'objet par Kaspersky Anti-Virus pendant l'analyse.
- **Type de menace** : type de la menace selon la classification de Kaspersky Lab.

Niveau de danger : niveau du risque posé par l'objet.

FENETRE RESTAURATION DE L'OBJET: SAUVEGARDE

La restauration d'objets depuis la quarantaine ou la zone de sauvegarde peut produire l'infection du serveur et du réseau tout entier.

Cette fenêtre est utilisée pour configurer les paramètres de restauration de fichiers depuis la quarantaine ou la sauvegarde. Le nom de l'objet restauré est affiché dans la zone **Objet** de la partie supérieure de la fenêtre.

Si l'objet faisait partie d'un objet composé, il ne sera pas restauré dans ce dernier. Il sera enregistré séparément dans le dossier indiqué.

Le chemin où l'objet sera enregistré est déterminé par les paramètres de la quarantaine ou du dossier de sauvegarde. Par défaut, l'objet est restauré dans le dossier d'origine ou, si précisé dans les paramètres de la quarantaine ou du dossier de sauvegarde, dans un dossier de restauration partagé pour tous les objets.

Cette fenêtre permet de spécifier un autre chemin de restauration des objets. Pour ce faire, sélectionnez l'une de ces options :

- **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau** : l'objet restauré sera enregistré dans son dossier d'origine, lorsqu'il a été déplacé vers la quarantaine. Le chemin complet où l'objet sera restauré est affiché dans la zone de saisie.
- **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** : l'objet sera enregistré dans un dossier de restauration partagé pour tous les objets, comme indiqué par les paramètres de la quarantaine ou du dossier de sauvegarde. Le chemin complet où l'objet sera restauré est affiché dans la zone de saisie.
- **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** : l'objet restauré sera enregistré dans un dossier sélectionné sur l'ordinateur où se trouve installé la console de Kaspersky Anti-Virus, ou sur un autre poste du réseau local. Le chemin de la ressource doit être noté au format UNC (Universal Naming Convention) dans la zone de saisie.

L'objet sera enregistré à l'adresse et avec le nom spécifié dans son format d'origine. Toutes les permissions d'accès et attributs du fichier (archive, lecture-seule, etc.) et les autres propriétés de l'objet d'origine seront également restaurées.

Par défaut une copie de l'objet est conservée dans la zone de sauvegarde et peut être supprimée manuellement. Sélectionnez **Supprimer les objets sauvegardés après leur restauration** pour que ces copies soient supprimées automatiquement après une restauration réussie. S'il n'est pas possible de restaurer l'objet, la copie ne sera pas supprimée.

Si vous sélectionnez la restauration de plusieurs objets, vous pouvez appliquer les paramètres de cette fenêtre au reste des objets. Pour ce faire, sélectionnez **Appliquer à tous les objets sélectionnés**.

FENETRE UN OBJET PORTANT CE NOM EXISTE: SAUVEGARDE

Cette fenêtre vous indique qu'à l'adresse indiquée, il existe un fichier du même nom que l'objet à restaurer. Le nom complet du fichier (chemin compris) est affiché dans le champ **Objet** de la partie supérieure de la fenêtre. Observez que le chemin est spécifié conformément aux paramètres de restauration sélectionnés dans la fenêtre précédente.

Vous pouvez remplacer le fichier existant, modifier l'emplacement de l'objet à restaurer, ou le renommer. Pour ce faire, sélectionnez l'une des options suivantes :

- **Remplacer**. Si vous sélectionnez cette option, le fichier existant sera supprimé et l'objet restauré à la même place et sous le même nom.

- **Renommer**. Sélectionnez cette option pour enregistrer l'objet sous un autre nom ou pour changer le chemin où l'objet doit être enregistré. Entrez le nom complet du fichier (chemin compris) avec lequel l'objet restauré sera enregistré.

- **Renommer en ajoutant un suffixe**. Avec cette option, la suite de caractères saisis dans la zone sera ajoutée au nom du fichier. Cette option est utile pour restaurer de nombreux objets avec l'option **Appliquer à tous les objets**. Suite de caractères doit satisfaire les règles de nommage des fichiers.

Si vous sélectionnez la restauration de plusieurs objets, vous pouvez appliquer les paramètres de cette fenêtre au reste des objets. Pour ce faire, sélectionnez **Appliquer à tous les objets**.

FENETRE STATISTIQUES: SAUVEGARDE

La fenêtre **Statistiques** affiche des informations sur l'état de la zone de sauvegarde et sur les objets présents :

Espace de sauvegarde utilisé – taille totale des objets en sauvegarde.

Nombre total d'objets – nombre total d'objets Total des objets actuellement sauvegardés.

CONSIGNATION DES EVENEMENTS. JOURNAUX DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

MOYENS D'ENREGISTREMENT DES EVENEMENTS

Les événements dans Kaspersky Anti-Virus sont scindés entre les événements liés au traitement des objets dans les tâches et les événements liés à l'administration de Kaspersky Anti-Virus. Il s'agit également des événements tels que le lancement de Kaspersky Anti-Virus, la création ou la suppression de tâches, l'exécution de tâches, la modification des paramètres des tâches, etc.

Kaspersky Anti-Virus consigne les événements de la manière suivante :

- Il tient des Journaux d'exécution des tâches. Le journal d'exécution des tâches contient des informations sur l'état actuel de paramètres de la tâche ou sur les événements survenus pendant l'exécution de la tâche.
- Il tient un Journal d'audit système. Y sont consignés les événements liés à l'administration de Kaspersky Anti-Virus.
- Il tient un Journal des événements dans la console "Observateur d'événements" de Microsoft Windows. Y sont consignés les événements importants pour le diagnostic des erreurs.

Si un problème survient durant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus ou une tâche particulière s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un fichier de traçage et un fichier de vidage de la mémoire des processus de Kaspersky Anti-Virus et envoyer ces fichiers avec ces informations au service d'assistance technique de Kaspersky Lab pour analyse. Pour en savoir plus sur la création d'un fichier de traçage et de fichiers de vidage de mémoire, lisez la rubrique "Paramètres généraux de Kaspersky Anti-Virus" (cf. page 324).

JOURNAL D'AUDIT SYSTEME

Kaspersky Anti-Virus réalise un audit système des événements liés à l'administration de Kaspersky Anti-Virus tels que le lancement de Kaspersky Anti-Virus, le lancement et l'arrêt des tâches, la modification des paramètres des tâches, la création et la suppression des tâches d'analyse à la demande ou autres. Les enregistrements relatifs à ces événements figurent dans le nœud **Journal d'audit système**.

Par défaut, Kaspersky Anti-Virus conservera les notes dans le journal d'audit système pendant 60 jours. Vous pouvez modifier la durée de la conservation des enregistrements à l'aide du paramètre **Durée de conservation des événements dans le journal d'audit système**.

Vous pouvez désigner le dossier dans lequel Kaspersky Anti-Virus enregistrera les fichiers du journal d'audit système, différent du dossier choisi par défaut (cf. page 368).

Pour consulter les événements dans le journal d'audit système, sélectionnez le nœud **Journaux** dans l'arborescence de la console, puis le sous-nœud **Journal d'audit système** (cf. ill. ci-après).

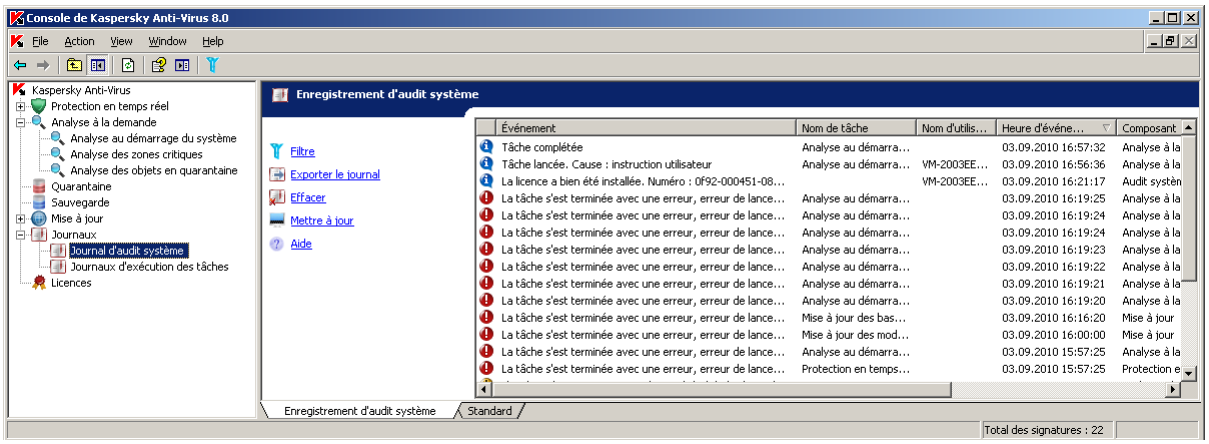


*Illustration 75. Nœud **Journal d'audit système***

Le panneau de résultats reprend les informations sur les événements de Kaspersky Anti-Virus (cf. tableau ci-dessous).

Tableau 23. Notifications relatives aux événements de Kaspersky Anti-Virus

CHAMP	DESCRIPTION
Événement	Description de l'événement ; inclut le type d'événement et des informations complémentaires à son sujet. Les événements sont classés selon les catégories suivantes en fonction du degré d'importance : *informations*, *importants* ou *critiques*.
Nom de la tâche	Nom de la tâche de Kaspersky Anti-Virus à l'exécution de laquelle l'événement est lié.
Nom d'utilisateur	Si l'événement a été provoqué par un utilisateur de Kaspersky Anti-Virus, son nom est affiché dans cette colonne. Si l'action provient non pas de l'utilisateur, mais de Kaspersky Anti-Virus, par exemple la tâche d'analyse à la demande programmée a été lancée, cette colonne affiche l'enregistrement **<domaine><nom de l'ordinateur>$** qui correspond au compte utilisateur **Système local**.
Heure d'événement	Heure d'enregistrement de l'événement selon l'heure du serveur protégé au format défini dans les paramètres régionaux de Microsoft Windows.
Composant	Composant fonctionnel de Kaspersky Anti-Virus pendant le fonctionnement duquel l'événement s'est produit. Si l'événement n'est pas lié au fonctionnement de composants particuliers, mais au fonctionnement de Kaspersky Anti-Virus dans son ensemble, par exemple au lancement de Kaspersky Anti-Virus, cette colonne contient l'enregistrement **Application**.
Objet	Nom de l'objet dont le traitement a provoqué l'événement.
Ordinateur	Nom de l'ordinateur sur lequel l'événement s'est produit.

DANS CETTE SECTION DE L'AIDE

TRI DES EVENEMENTS DANS LE JOURNAL D'AUDIT SYSTEME

Par défaut, les événements sont classés dans le nœud **Journal d'audit système** par ordre chronologique inverse.

Pour trouver un événement dans la liste, vous pouvez trier les événements selon le contenu de n'importe quelle colonne. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Journal d'audit système**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour trier les événements, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journal d'audit système**.

2. Dans le panneau de résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les événements de la liste.

FILTRAGE DES EVENEMENTS DANS LE JOURNAL D'AUDIT SYSTEME

Pour trouver un événement dans le journal d'audit système, vous pouvez filtrer les événements, c.-à-d. afficher dans la liste uniquement les événements qui répondent aux conditions de filtrage que vous aurez définies.

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Journal d'audit système**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour filtrer les événements dans le journal d'audit système, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis ouvrez le menu contextuel du sous-nœud **Journal d'audit système** et sélectionnez l'option **Filtre**.

La boîte de dialogue **Paramètres du filtre** s'ouvrira (cf. ill. ci-après).

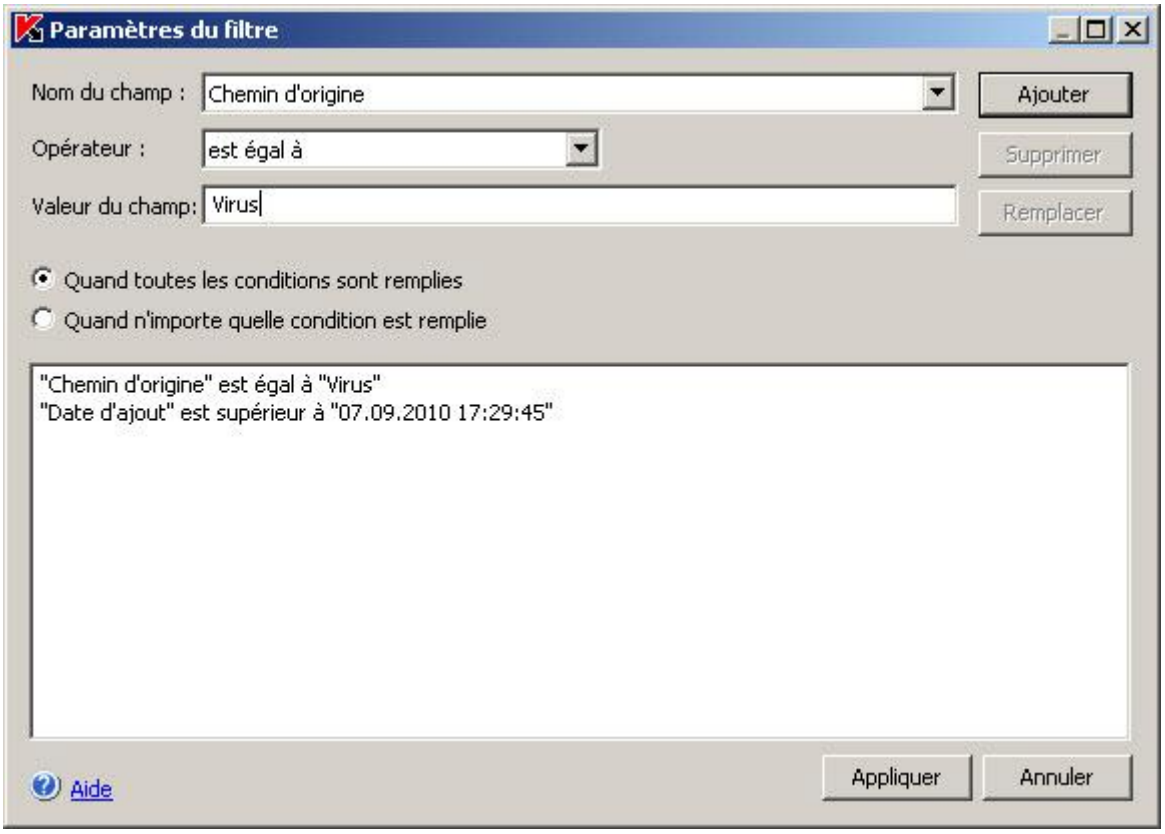


*Illustration 76. Boîte de dialogue **Paramètres du filtre***

2. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste des valeurs disponibles.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, observez les règles suivantes :

   - Afin de réunir quelques filtres selon le " ET " logique, sélectionnez l'option **En cas d'exécution de toutes les conditions**.
   - Afin de réunir quelques filtres selon le " OU " logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
   - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
   - Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les événements qui répondent aux conditions des filtres.

Pour afficher à nouveau tous les événements,

dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis ouvrez le menu contextuel du sous-nœud **Journal d'audit système** et sélectionnez l'option **Supprimer le filtre**.

SUPPRESSION DES EVENEMENTS DU JOURNAL D'AUDIT SYSTEME

Par défaut, Kaspersky Anti-Virus conservera les événements dans le journal d'audit système pendant 60 jours. Vous pouvez modifier la durée de conservation des événements dans le journal.

Vous pouvez supprimer manuellement tous les événements du journal d'audit système.

Pour supprimer tous les événements du journal d'audit système, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis ouvrez le menu contextuel du sous-nœud **Journal d'audit système** et sélectionnez l'option **Effacer**.

2. Dans la boîte de dialogue Confirmation, cliquez sur le bouton **Oui** pour confirmer la suppression.

JOURNAUX D'EXECUTION DES TACHES

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES JOURNAUX D'EXECUTION DES TACHES

Vous pouvez consulter les informations relatives à l'exécution des tâches de Kaspersky Anti-Virus dans la console de ce dernier sous le nœud **Journaux d'exécution des tâches**. Dans la liste des journaux, la *ligne reprenant les informations* relatives au journal indique l'état de la tâche et l'état général des objets traités du point de vue de la sécurité antivirus. *Le journal d'exécution des tâches* contient les statistiques de l'exécution de la tâche (informations sur le nombre d'objets traités), les informations relatives à chaque objet traité par Kaspersky Anti-Virus depuis le lancement de la tâche jusqu'à maintenant ainsi que les paramètres de la tâche.

Par défaut, le journal d'exécution de la tâche est supprimé 30 jours après l'exécution de la tâche. Les enregistrements relatifs aux événements survenus il y a plus de 30 jours sont supprimés des journaux d'exécution des tâches.

Grâce aux paramètres des journaux de Kaspersky Anti-Virus, vous pouvez modifier la durée de conservation des journaux ou désactiver la suppression automatique des journaux afin de les conserver pendant une durée indéterminée. Vous pouvez également sélectionner un journal et le supprimer manuellement.

Vous pouvez modifier l'endroit où Kaspersky Anti-Virus conserver les fichiers des journaux d'exécution des tâches et sélectionner les événements que Kaspersky Anti-Virus consignera dans les journaux.

CONSULTATION DE LA LISTE DES JOURNAUX D'EXECUTION DES TACHES. ETATS DES JOURNAUX

Pour consulter la liste des journaux d'exécution des tâches, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journaux d'exécution des tâches** (cf. ill. ci-après).

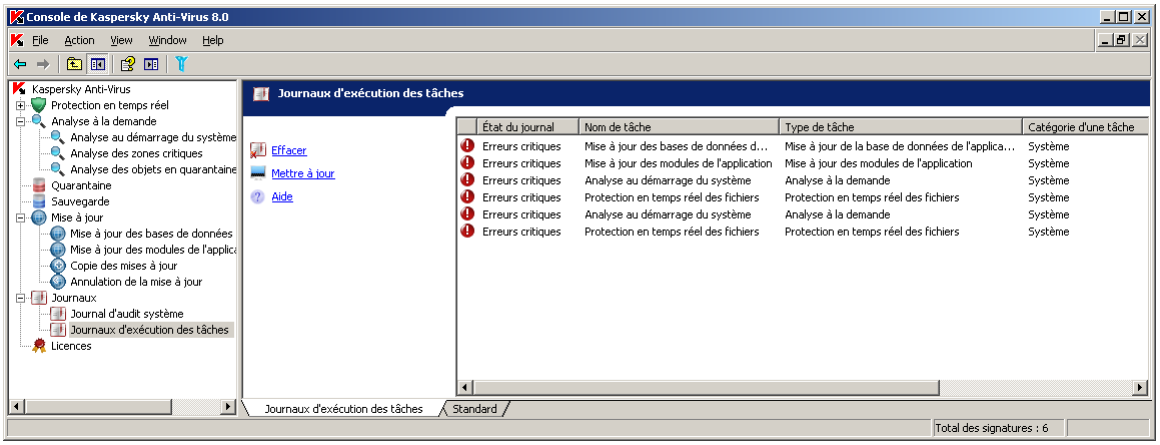


Illustration 77. Liste des journaux d'exécution des tâches dans la console de Kaspersky Anti-Virus

2. Dans le panneau de résultats, trouvez le journal d'exécution de la tâche dont vous souhaitez afficher les informations (cf. tableau ci-après) (pour trouver le journal rapidement, vous pouvez filtrer les journaux ou les trier selon le contenu d'une des colonnes).

Pour savoir comment ouvrir le journal d'exécution de la tâche, lisez la rubrique "Consultation des informations sur la tâche dans le journal" (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234).

La ligne d'informations du journal contient les données de synthèse concernant le journal (cf. tableau ci-dessous).

Tableau 24. Champs contenant des informations sur le journal

CHAMP	DESCRIPTION
Etat du journal	Brève caractéristique qui repose sur les statistiques de la tâche ; affiche l'état global des objets traités du point de vue de la sécurité antivirale. En fonction du niveau d'importance, les journaux sont classés dans les catégories suivantes : *information*, *avertissement* ou *critique*. Les tableaux suivants décrivent les états des journaux des tâches d'analyse à la demande et de mise à jour.
Nom de la tâche	Nom de la tâche dont vous souhaitez consulter le journal d'exécution.
Type de tâche	Le type de tâche correspond au composant fonctionnel dans lequel la tâche est créée (protection en temps réel des fichiers, analyse des scripts, analyse à la demande, mise à jour).
Catégorie de tâche	Catégorie de tâche dans Kaspersky Anti-Virus : *prédéfinie*, *définie par l'utilisateur* ou *de groupe* (cf. page 46).
État de la tâche	L'état actuel de la tâche, par exemple *Exécutée*, *Complétée* ou *En pause*.
Heure de fin	Si la tâche est déjà terminée, cette colonne affiche la date et l'heure de fin d'exécution. Si à ce moment, la tâche est exécutée, le champ est vide.

Tableau 25. États des journaux des tâches d'analyse à la demande

DEGRE D'IMPORTANCE	ETAT DU JOURNAL	DESCRIPTION DE L'ETAT DU JOURNAL
	Aucune menace n'a été découverte	Kaspersky Anti-Virus a analysé tous les objets du secteur sélectionné. Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains.
	Certains objets n'ont pas été traités	Kaspersky Anti-Virus considère tous les objets analysés comme sains ; un ou plusieurs objets ont été ignorés, par exemple parce qu'ils étaient exclus de l'analyse par les paramètres de sécurité ou parce qu'ils étaient utilisés par d'autres applications au moment de l'analyse. Lors de la requête, les fichiers système Windows peuvent être utilisés. Kaspersky Anti-Virus ne les analyse pas et la tâche se termine sur l'état Certains objets n'ont pas été traités.
	Objets endommagés détectés	Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains. Un ou plusieurs objets du secteur sélectionné ont été ignorés : Kaspersky Anti-Virus n'a pas réussi à lire ces objets car leur format est corrompu.
	Des objets suspects ont été découverts	Kaspersky Anti-Virus considère un ou plusieurs objets analysés comme étant suspects. Vous pouvez voir quels objets ont été considérés comme suspects en consultant les informations relatives aux événements dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).
	Des objets infectés ont été découverts	Kaspersky a découvert des menaces dans un ou plusieurs objets. Vous pouvez voir quels objets contiennent des objets en consultant les informations relatives aux événements dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).
	Erreurs de traitement	Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains. Pendant l'analyse d'un ou de plusieurs objets, une erreur est survenue dans Kaspersky Anti-Virus. L'objet analysé lorsque l'erreur s'est produite peut contenir une menace. Nous vous recommandons de placer ces objets en quarantaine et refaire leur analyse près une mise à jour de la base antivirus (cf. page 196). Si l'erreur se reproduit, contactez le Service d'assistance technique de Kaspersky Lab (cf. rubrique "Contacter le service d'assistance technique" à la page17).

DEGRE D'IMPORTANCE	ETAT DU JOURNAL	DESCRIPTION DE L'ETAT DU JOURNAL
	Erreurs critiques	La tâche s'est soldée par un échec. Vous pouvez consulter la cause de l'erreur dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

Tableau 26. Etats des journaux des tâches de mise à jour des base et de copie des mises à jour

DEGRE D'IMPORTANCE	ETAT DU JOURNAL	DESCRIPTION DE L'ETAT DU JOURNAL
	Sans erreur	Kaspersky Anti-Virus a récupéré et installé les mises à jour sans erreur.
	Erreurs critiques	Une erreur s'est produite lors de la récupération ou de l'application des mises à jour. Vous pouvez consulter le nom de la mise à jour qui n'a pas été appliquée et la cause de l'erreur dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

Tableau 27. Etat des journaux des tâches de mise à jour des modules de l'application

DEGRE D'IMPORTANCE	ETAT DU JOURNAL	DESCRIPTION DE L'ETAT DU JOURNAL
	Sans erreur	Kaspersky Anti-Virus a récupéré et installé les modules sans erreur.
	Mise à jour critique disponible	Des mises à jour urgentes des modules de Kaspersky Anti-Virus ont été publiées.
	Une mise à jour prévue des modules d'application est disponible	Des mises à jour prévues des modules de Kaspersky Anti-Virus ont été publiées.
	Des mises à jour critiques et prévues sont disponibles	Des mises à jour urgentes et prévues des modules de Kaspersky Anti-Virus ont été publiées.
	L'installation des mises à jour récupérées est en cours	Kaspersky Anti-Virus a récupéré les mises à jour et les installe.
	La finalisation du processus de mise à jour requiert le redémarrage du serveur	Redémarrez le serveur pour appliquer les mises à jour.
	Erreurs critiques	Une erreur s'est produite lors de la récupération ou de l'application des mises à jour. Vous pouvez consulter le nom de la mise à jour qui n'a pas été appliquée et la cause de l'erreur dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

TRI DES JOURNAUX D'EXECUTION DES TACHES

Les journaux d'exécution des tâches sont classés par défaut dans la liste dans l'ordre chronologique inverse. Vous pouvez les trier selon le contenu de n'importe quelle colonne. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Journaux d'exécution des tâches**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

Pour trier les journaux d'exécution des tâches de la liste, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journaux d'exécution des tâches**.

2. Dans le panneau d'information, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les journaux.

AFFICHAGE DANS LE JOURNAL D'INFORMATIONS RELATIVES A LA TACHE

Le journal d'exécution de la tâche reprend les informations détaillées relatives à tous les événements survenus dans la tâche depuis son lancement jusque maintenant. Par exemple, vous pouvez voir le nom des objets traités dans lesquels une menace a été découverte. Vous pouvez consulter les statistiques d'exécution de la tâche et ses paramètres.

Pour ouvrir le journal d'exécution de la tâche, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journaux d'exécution des tâches**.

2. Dans la liste des journaux d'exécution des tâches, ouvrez le menu contextuel du journal que vous souhaitez consulter puis sélectionnez la commande **Voir le journal**.

3. La boîte de dialogue **Journal d'exécution** contient l'onglet **Événements** qui reprend les informations sur les événements survenus pendant la tâche, l'onglet **Statistiques** qui reprend l'heure de début et de fin de la tâche et ses statistiques et l'onglet **Paramètres** avec les paramètres de la tâche (cf. ill. ci-après).

L'onglet **Evénements** reprend les informations sur les événements survenus pendant la tâche (cf. tableau ci-dessous).

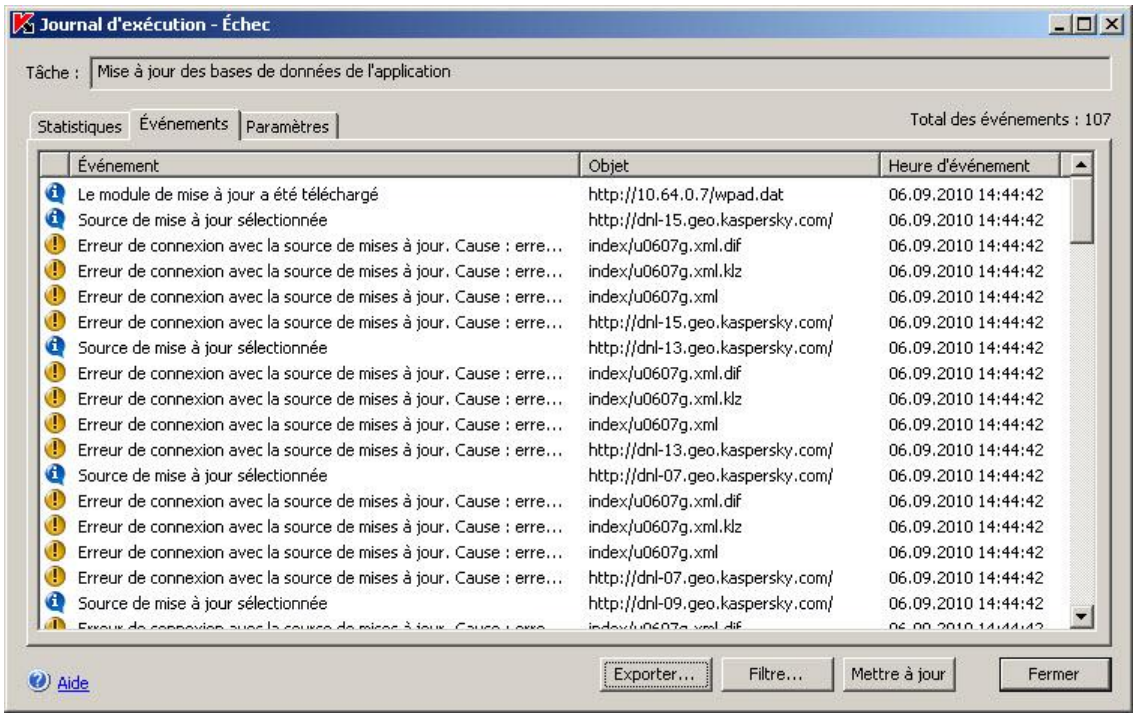


Illustration 78. Exemple de journal d'exécution de la tâche ***Mise à jour des base de l'application***

*Tableau 28. Informations sur les événements survenus pendant la tâche sous l'onglet **Evénements***

CHAMP	DESCRIPTION
Degré d'importance de l'événement	Sur la base du degré d'importance, les événements dans le journal d'exécution de la tâche sont scindés entre les événements informatifs , importants et critiques .
Événement	Type d'événement et informations complémentaires sur l'événement.
Objet	Nom de l'objet traité et chemin d'accès. Pour la tâche **Analyse des scripts**, cette colonne reprend également l'identificateur du processus (PID) qui a exécuté le script intercepté par Kaspersky Anti-Virus.
Heure d'événement	Date et heure auxquelles l'événement s'est produit.

Le journal d'exécution de la tâche **Protection en temps réel des fichiers contient, outre les champs indiqués ci-dessus, les champs Ordinateur** et Nom d'utilisateur ; le journal d'exécution de la tâche **Analyse des scripts** contient le champ **Nom d'utilisateur** (cf. tableau ci-dessous).

Tableau 29. Informations sur l'utilisateur dans les journaux d'exécution des tâches

CHAMP	DESCRIPTION
Ordinateur	Nom de l'ordinateur d'où l'application a sollicité l'objet.
Utilisateur	Nom de l'utilisateur sous le compte duquel l'application a sollicité l'objet. Si l'objet a été sollicité par une application tournant sous le compte **Système local** (**SYSTEM**), cette colonne contiendra l'enregistrement <domaine><nom de l'ordinateur>$. Dans la tâche **Protection en temps réel des fichiers**, Kaspersky Anti-Virus enregistre la valeur localhost en guise de nom de l'ordinateur et non pas le nom de réseau du serveur protégé si l'objet est sollicité par une application qui fonctionne sur le serveur protégé. Si la tâche **Analyse des scripts** a été lancée depuis la console d'administration de Kaspersky Administration Kit, ce champ reprend le nom du compte utilisateur sous les privilèges duquel l'agent d'administration fonctionne.

➧ *Pour consulter les statistiques de la tâche,*

ouvrez l'onglet **Statistiques** (cf. ill. ci-dessous) dans la fenêtre **Journal d'exécution**.

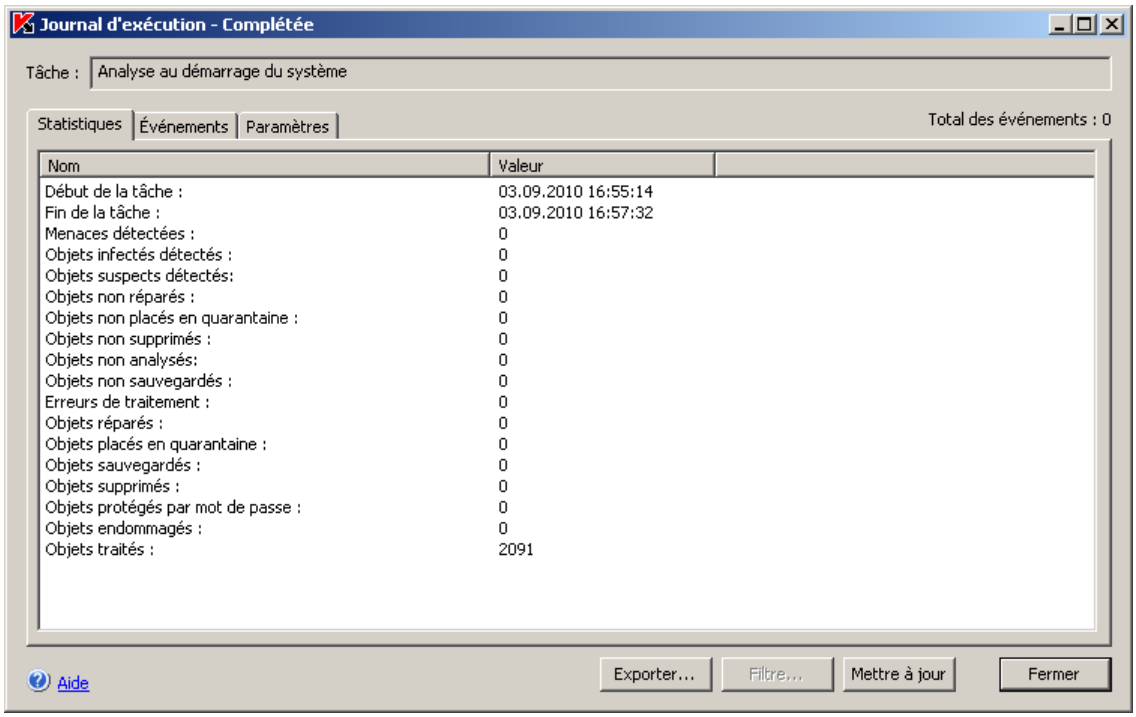


*Illustration 79. Boîte de dialogue **Journal d'exécution de la tâche**, onglet **Statistiques***

- *Pour consulter les paramètres de la tâche,*

  ouvrez l'onglet **Paramètres** (cf. ill. ci-dessous) dans la fenêtre **Journal d'exécution**.

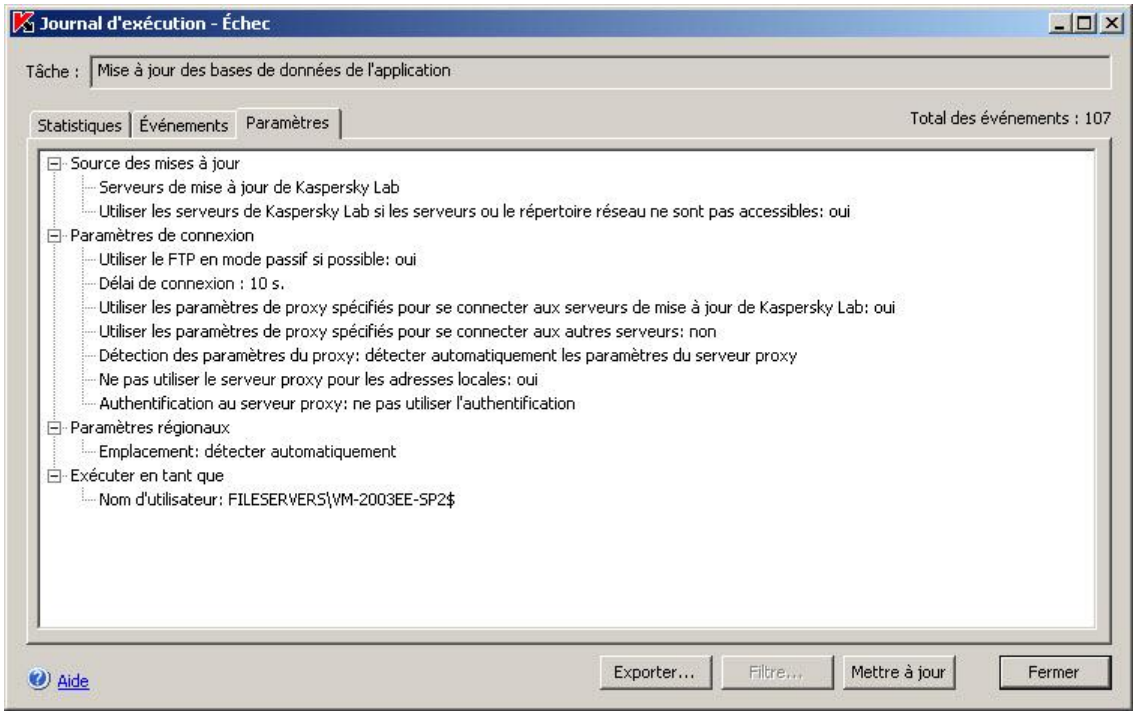


*Illustration 80. Boîte de dialogue **Journal d'exécution de la tâche**, onglet **Paramètres***

Lors de la consultation du rapport détaillé, vous pouvez définir un ou plusieurs filtres pour trouver l'événement souhaité dans l'onglet **Evénements**.

Pour définir un ou plusieurs filtres, procédez comme suit :

1. Cliquez sur le bouton **Filtre** dans la partie inférieure de la boîte de dialogue **Rapport d'exécution**. La boîte de dialogue **Paramètres du filtre** s'ouvrira (cf. ill. ci-après).

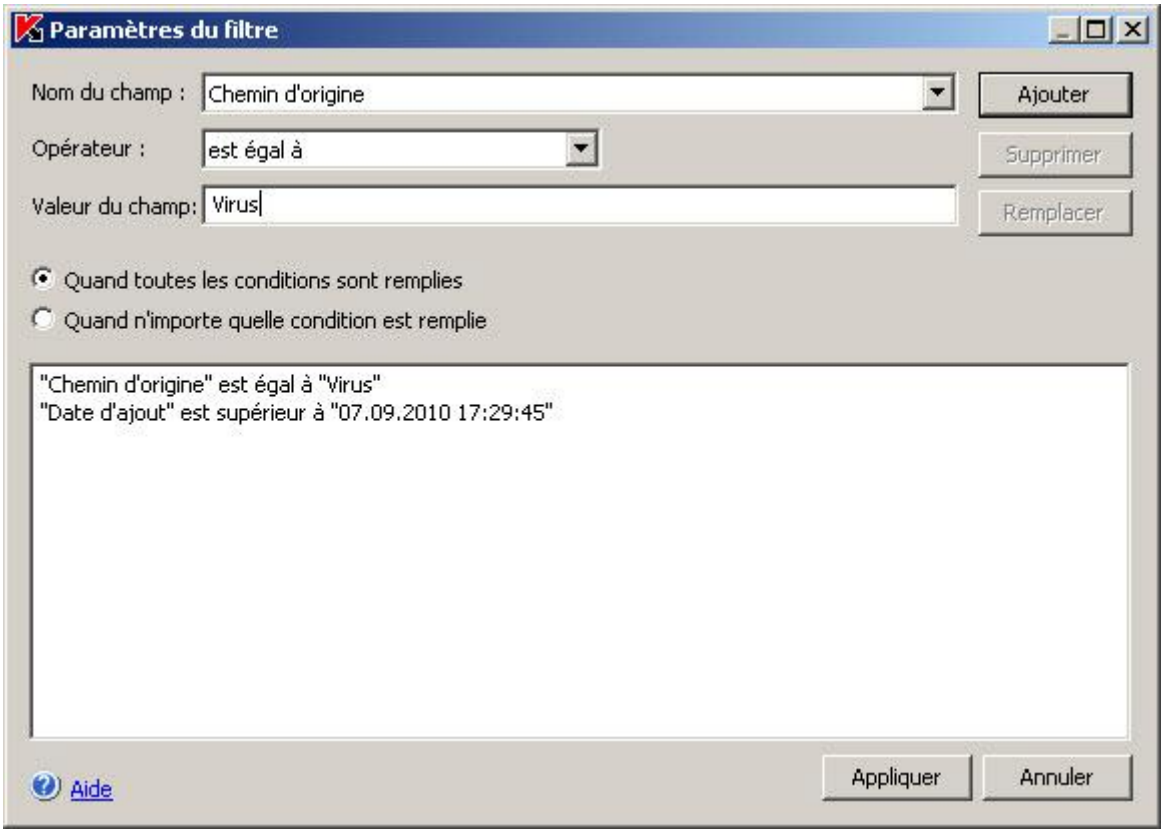


*Illustration 81. Boîte de dialogue **Paramètres du filtre***

2. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste des valeurs disponibles.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, observez les règles suivantes :

   - Afin de réunir quelques filtres selon le " ET " logique, sélectionnez l'option **En cas d'exécution de toutes les conditions**.
   - Afin de réunir quelques filtres selon le " OU " logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
   - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste des objets du journal reprendra uniquement les objets qui répondent aux conditions des filtres.

Pour afficher à nouveau tous les objets,

cliquez à nouveau sur le bouton **Filtre** dans la partie inférieure de la boîte de dialogue **Rapport d'exécution**.

EXPORTATION DES INFORMATIONS DU JOURNAL D'EXECUTION DE LA TACHE DANS UN FICHIER TEXTE

Pour exporter les informations du journal d'exécution de la tâche dans un fichier au format TXT ou CSV, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journaux d'exécution des tâches**.

2. Dans la liste des journaux d'exécution des tâches, ouvrez le menu contextuel du journal que vous souhaitez consulter puis sélectionnez la commande **&Voir le journal**.

3. Dans la partie inférieure de la boîte de dialogue **Journal d'exécution de la tâche**, cliquez sur le bouton **Exporter** et dans la boîte de dialogue **Parcourir**, saisissez le nom du fichier dans lequel vous souhaitez enregistrer les données du journal et choisissez le code (Unicode ou ANSI).

SUPPRESSION DES JOURNAUX D'EXECUTION DES TACHES

Les journaux d'exécution des tâches sont conservés par défaut pendant une période déterminée. Vous pouvez limiter la durée de conservation des enregistrements à l'aide du paramètre général de Kaspersky Anti-Virus **Durée de conservation des journaux** (cf. page 38).

Dans le nœud **Journaux d'exécution des tâches**, vous pouvez supprimer les journaux sélectionnés concernant les tâches terminées.

Pour supprimer un ou plusieurs journaux d'exécution des tâches, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Journaux** puis le sous-nœud **Journaux d'exécution des tâches**.

2. Exécutez une des actions suivantes :

   - pour supprimer un journal, ouvrez le menu contextuel du journal que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;

   - pour supprimer plusieurs journaux, sélectionnez les journaux souhaités dans la liste à l'aide de la touche **Ctrl** ou **Shift**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez la commande **Supprimer**.

3. Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

Les journaux sélectionnés seront supprimés. L'opération sera consignée dans le journal d'audit système.

JOURNAL DES EVENEMENTS DE KASPERSKY ANTI-VIRUS DANS LA CONSOLE OBSERVATEUR D'EVENEMENTS

A l'aide de la console MMC Microsoft Windows **Event Viewer**, vous pouvez consulter le journal des événements de Kaspersky Anti-Virus. Kaspersky Anti-Virus y enregistre les événements importants du point de vue de la sécurité antivirus du serveur protégé et du diagnostic des échecs de Kaspersky Anti-Virus.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements selon les critères suivants :

- **selon le type d'événement** ;
- **selon le niveau de détail**. Le niveau de détail correspond au niveau d'importance des événements consignés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est **Evénements informatifs : les événements de tous les niveaux d'importance sont consignés ; le moins détaillé est le niveau** Evénements critiques où seuls les événements critiques sont consignés Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) ; pour le composant **Mise à jour**, c'est le niveau **Evénements informatifs** qui est sélectionné.

Pour consulter le journal des événements, procédez comme suit :

1. Ajoutez le composant enfichable **Observateur d'événements**. Si vous administrez la défense du serveur à distance depuis le poste de travail de l'administrateur, désignez le serveur protégé en guise d'ordinateur qui devra être administré via le module enfichable.
2. Dans l'arborescence de la console "**Observateur d'événements**", sélectionnez le nœud **Kaspersky Anti-Virus** (cf. ill. ci-après).

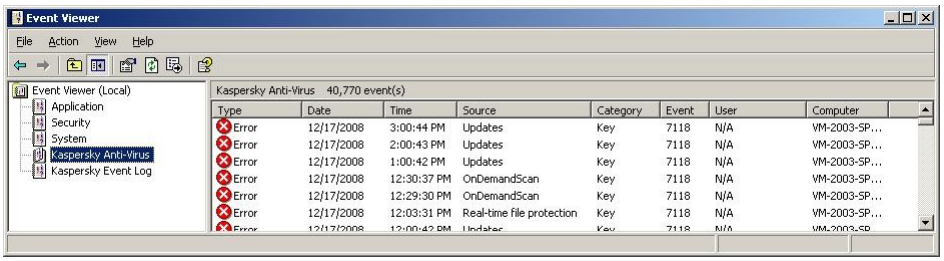


*Illustration 82. Informations sur les événements de Kaspersky Anti-Virus dans la console "**Observateur d'événements**"*

CONFIGURATION DE PARAMETRES DES JOURNAUX DANS MMC

Grâce aux paramètres des journaux de Kaspersky Anti-Virus, vous pouvez modifier la durée de conservation des journaux d'exécution des tâches et du journal d'audit système ou désactiver la suppression automatique des journaux afin de les conserver pendant une durée indéterminée.

Vous pouvez modifier l'emplacement où Kaspersky Anti-Virus conserve les fichiers des journaux d'exécution des tâches et du journal d'audit ainsi que sélectionner les événements que Kaspersky Anti-Virus consignera dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements de Kaspersky Anti-Virus dans la console "Observateur d'événements".

Pour configurer les paramètres des journaux de Kaspersky Anti-Virus, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Journaux** et sélectionnez la commande **Propriétés**.

2. Dans la boîte de dialogue **Journaux Propriétés**, configurez les paramètres des journaux en fonction de vos exigences.

   L'onglet **Général** vous permet de désigner les événements qui seront consignés dans les journaux d'exécution des tâches des composants fonctionnels de Kaspersky Anti-Virus et dans le journal d'audit système et les événements qui seront consignés dans le journal des événements de Kaspersky Anti-Virus dans la console "Observateur d'événements" – configurer le niveau de détails des événements (cf. ill. ci-dessous).

   Pour les composants **Protection en temps réel**, **Analyse des scripts**, **Analyse à la demande** et **Mise à jour**, les événements sont enregistrés dans les journaux relatifs à l'exécution des tâches ainsi que dans le journal d'audit système. Pour ceux-ci, le tableau contient la colonne **Journaux**. Pour les composants **Quarantaine** et **Sauvegarde**, le tableau contient la colonne **Audit**.

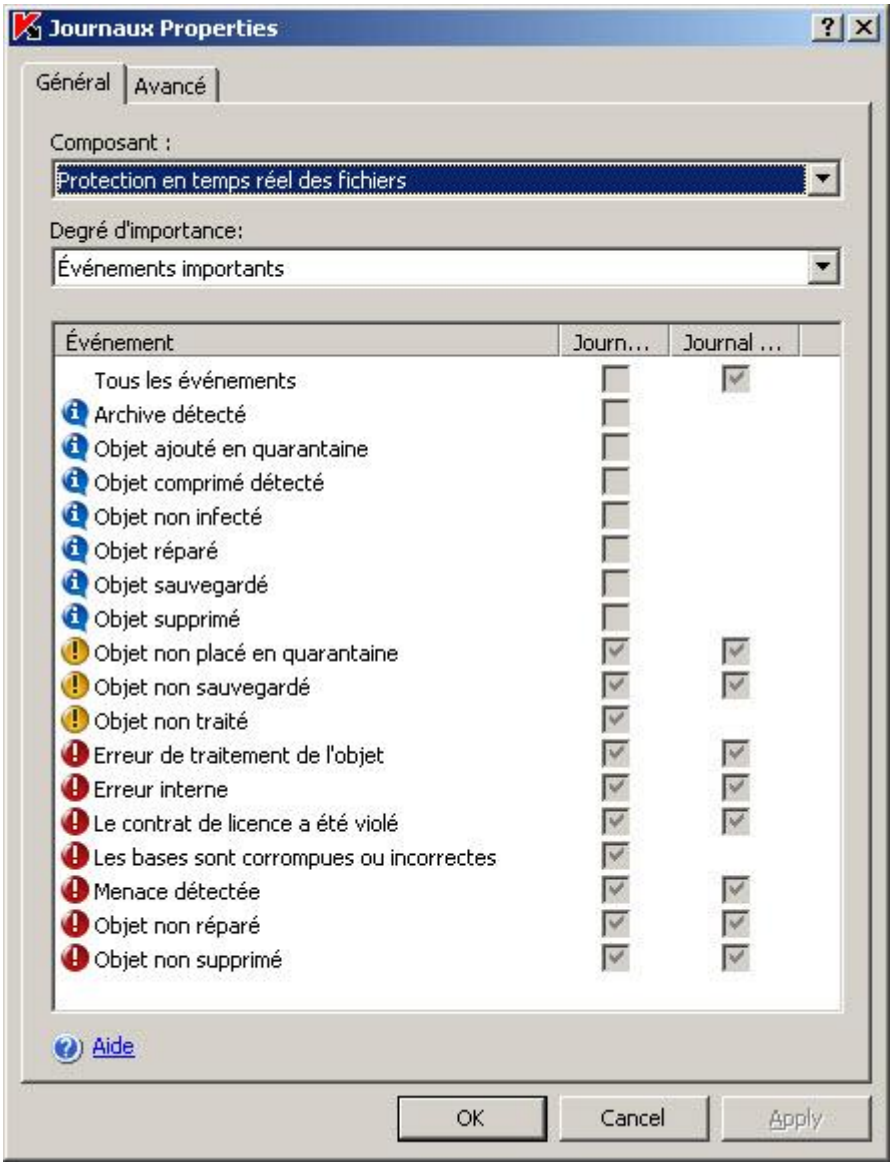


*Illustration 83. Boîte de dialogue **Propriétés : Journaux**, onglet **Général***

Exécutez les actions suivantes :

a. Dans la liste **Composant**, sélectionnez le composant de Kaspersky Anti-Virus pour lequel vous souhaitez indiquer le niveau de détails.

b. Pour définir le niveau de détails dans les journaux d'exécution des tâches et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Degré d'importance**.

Dans la liste des événements, une case cochée apparaîtra à côté des événements qui figureront dans les journaux d'exécution des tâches et dans le journal des événements conformément au niveau de détail sélectionné.

c. Pour activer l'enregistrement d'événements individuels du composant fonctionnel, dans la liste **Degré d'importance**, sélectionnez **Autre** puis, réalisez les opérations suivantes dans la liste des événements du composant :

- Pour activer la consignation des événements dans les journaux d'exécution des tâches, cochez la case **Journaux d'exécution des tâches** correspondante à l'événements ; pour désactiver l'enregistrement des événements dans les journaux d'exécution des tâches, désélectionnez la case **Journaux d'exécution des tâches** correspondante.

- Pour activer l'enregistrement d'un événement dans le journal des événements, cochez la case **Journal des événements** qui lui correspond ; pour désactiver l'enregistrement d'un événement dans le journal des événements, désélectionnez la case **Journal des événements** qui lui correspond.

3. Sous l'onglet **Avancé**, configurez les paramètres de journaux suivants :

- Pour modifier l'emplacement des journaux par défaut (cf. page 368), indiquez le chemin d'accès complet au dossier ou cliquez sur le bouton **Parcourir**.

- Indiquez le nombre de jours pendant lequel les journaux d'exécution des tâches repris dans le nœud **Journaux de la console de Kaspersky Anti-Virus** seront conservés.

- Indiquez le nombre de jours pendant lesquels les informations reprises dans le nœud **Journal d'audit système** (cf. page 369) seront conservées.

*Illustration 84. Boîte de dialogue **Propriétés : Journaux**, onglet **Avancé***

4. Dans la boîte de dialogue **Journaux Propriétés** cliquez sur **OK** afin de conserver les modifications.

BOITES DE DIALOGUE : JOURNAUX

DANS CETTE SECTION DE L'AIDE

JOURNAUX (ENTREE)

Le nœud **Journaux** permet de consulter les journaux de Kaspersky Anti-Virus. Il se compose des sous-entrées **Journal d'audit** et **Journaux relatifs à l'exécution des tâches**.

Panneau de tâches et menu contextuel

À l'aide des liens du panneau de tâches et des commandes du menu contextuel de la tâche sélectionnée dans le panneau de résultats, vous pouvez effectuer les actions suivantes :

- **Exporter la configuration/Importer la configuration** : exporte/restaure les paramètres des journaux vers/à partir d'un fichier.
- **Paramètres**– permet de configurer les journaux : durée de conservation des journaux et des événements dans les journaux, dossier de sauvegarde des journaux, niveau de détail des informations reprises dans les journaux.

VOIR EGALEMENT

NŒUD JOURNAL D'AUDIT SYSTEME

Le **Journal d'audit système** donne accès aux événements enregistrés dans le journal d'audit du programme antivirus.

Panneau de résultats

Le panneau de résultats affiche la liste des événements consignés sous forme de tableau. Les informations suivantes sont présentées pour chacun d'eux :

- **L'icône** indicateur du niveau de gravité de l'événement. Les degrés d'importance suivants sont prévus :

  Critique : événements critiques qui signalent des problèmes de fonctionnement de l'application ou la présence de vulnérabilités dans la sécurité de votre ordinateur. Par exemple : *Menace détectée*, *Erreur générale de mise à jour*.

  Avertissement : événements qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement du programme. Par exemple : *Dépassement du seuil d'espace libre pour la sauvegarde*.

  Pour information : événements de référence qui ne contiennent en général pas d'informations importantes. Par exemple : *Source de mise à jour sélectionnée*.

- **Événement** : type d'événement avec des informations supplémentaires sur lui.

- **Nom de tâche** : nom de la tâche associée à l'événement.

- **Nom d'utilisateur** : nom du compte utilisateur qui a causé l'événement.

  Si l'application qui accède au serveur est exécutée sous le compte **Système local** (**SYSTEM**), la colonne affichera l'entrée **<domaine><nom_ordinateur>$**.

- **Heure d'événement**- date et heure de l'événement. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.

- **Composant** : nom du composant de Kaspersky Anti-Virus associé à l'événement :

  - **Protection en temps réel** : tâches associées à l'activité de la protection en temps réel des fichiers.

  - **Analyse des scripts** : tâches associées à la surveillance des scripts.

  - **Analyse à la demande** : événement associés à l'activité des tâches d'analyse à la demande (tâches système et personnalisées, y compris les tâches créées et exécutées depuis l'invite de commande).

  - **Mise à jour** : événements associés à l'exécution des tâches de mise à jour de la base de Kaspersky Anti-Virus et des modules d'application et de la tâche de distribution des mises à jour : connexion avec la source de mises à jour, avec le serveur proxy, etc.

  - **Quarantaine** : enregistre des informations sur les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de quarantaine, sur l'espace libre dans la quarantaine, etc.

  - **Sauvegarde** : enregistre des informations sur toutes les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de sauvegarde,, sur l'espace libre dans le dossier de sauvegarde, etc.

  - **Audit système** : événements relatifs au démarrage et à l'arrêt de l'application, au renforcement des stratégies de Kaspersky Administration Kit, à l'état des base de données de Kaspersky Anti-Virus et à la gestion des licences.

  - **Journaux** : informations relatives aux opérations liées à l'ajout d'événements dans les journaux d'enregistrement des événements.
  - **Service**: événements liés aux tâches prédéfinies de Kaspersky Anti-Virus.
- **Objet** : nom et chemin complet de l'objet associé à l'événement.
- **Ordinateur** : nom réseau ou adresse IP de l'ordinateur associé à l'événement.

Le contenu et le détail des informations consignées sont déterminées par les paramètres du rapport. Au besoin, vous pouvez modifier les paramètres.

Les informations affichées dans le panneau de résultats peuvent être triées par n'importe quelle colonne.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Filtre** : recherche dans le journal d'audit un événement qui répond aux conditions sélectionnées.
- **Supprimer le filtre** : supprime le filtre.
- **Exporter** : exporter dans un fichier les événements enregistrés dans le journal d'audit.
- **Effacer** : supprime toutes les informations du journal d'audit.

VOIR EGALEMENT

Journal d'audit système 226

Tri des événements dans le journal d'audit système 228

Filtrage des événements dans le journal d'audit système 228

Suppression des événements du journal d'audit système 230

Configuration de paramètres des journaux dans MMC 239

JOURNAUX D'EXECUTION DES TACHES (ENTREE)

Le nœud **Journaux relatifs à l'exécution des tâches** est utilisé pour afficher les journaux relatifs à l'exécution des tâches ainsi que pour paramétrer ceux-ci.

Des journaux sont générés pour toutes les tâches créées : mises à jour, protection en temps réel et analyses à la demande (tâches système, personnalisées et de groupe, ainsi que les tâches créées et exécutées depuis l'invite de commande). Un rapport individuel est généré chaque fois qu'une tâche est exécutée.

Tous les événements enregistrés sur l'activité de Kaspersky Anti-Virus présentent l'un des **niveaux de gravité** suivants :

Événement d'information : messages de référence qui ne contiennent généralement pas d'informations importantes, par exemple : *Objet non infecté*, *Objet réparé*.

Avertissement : événement important qui doit être examiné, car il reflète une situation importante dans le fonctionnement de Kaspersky Anti-Virus, par exemple : *Erreur de connexion avec la source de mises à jour*, *Objet non analysé*.

Critique : événement critique qui signale des problèmes de fonctionnement de l'application ou des vulnérabilités dans la protection du serveur, par exemple : *Menace détectée*, *Erreur générale de mise à jour*.

Panneau de résultats

Le panneau de résultats affiche la liste des rapports générés sous forme de tableau. Les informations suivantes sont présentées pour chacun d'eux :

- L'**icône** indicateur du niveau de gravité du journal, conformément aux résultats d'ensemble de la tâche. Les degrés d'importance suivants sont prévus :

  – La tâche n'a enregistré que des événements avec le niveau de gravité **Événement informatif**.

  – La tâche a rencontré au moins un événement avec le niveau de gravité **Événements critiques**.

  La tâche a rencontré au moins un événement avec le niveau de gravité **Événements critiques**

- **État du rapport** : informations générales sur le niveau de gravité du rapport, d'après l'activité d'ensemble de la tâche, donnant une idée sur la sécurité antivirus :

  Aucune menace détectée : tous les objets ont été analysés avec succès et classés comme non infectés.

  Sans erreur : la tâche de mise à jour s'est déroulée avec succès, les bases de données sont à jour et toutes les mises à jour des modules d'application ont été installées.

  Certains objets n'ont pas été traités : tous les objets analysés ont été classés comme non infectés ; un ou plusieurs des objets ont été **ignorés. Par exemple, il était exclu de l'analyse par les** paramètres de tâche.

  Objets endommagés détectés : tous les objets traités ont été classés comme non infectés; un ou plusieurs des objets ont été **ignorés en raison d'un format endommagé**.

  Objets suspects détectés : un ou plusieurs des objets traités étaient classés suspects.

  Objets infectés détectés : un ou plusieurs des objets traités étaient classés infectés.

  Erreurs de traitement : une erreur est apparue pendant l'analyse d'un ou plusieurs objets.

  L'objet analysé lorsque l'erreur s'est produite peut contenir une menace. Nous vous recommandons de placer ces objets en quarantaine et de refaire leur analyse après une mise à jour de la base antivirus. Si l'erreur se reproduit, contactez le Service d'assistance technique de Kaspersky Lab.

  Erreurs critiques : une erreur est apparue pendant l'exécution de la tâche, ce qui a provoqué une défaillance de la tâche.

- **Nom de tâche** : nom de la tâche sur laquelle le journal est généré.

- Type de tâche : type de la tâche sur laquelle le **journal** est généré.

  - **Mise à jour des base de l'application**.
  - **Mise à jour des modules de l'application**.
  - **Copie des mises à jour**.
  - **Annulation de la mise à jour**.

- **Protection en temps réel des fichier.**
- **Analyse des scripts**.
- **Analyse à la demande** :

- **Catégorie de la tâche** : catégorie de la tâche sur laquelle le rapport est généré. Les catégories de tâche suivantes existent :
  - **Utilisateur** : la tâche a été créée sur le serveur sécurisé depuis une interface locale ou la ligne de commande, ou encore depuis la console d'administration, puis envoyée au serveur en utilisant les outils d'administration à distance de Kaspersky Administration Kit.
  - **Système** : tâches intégrées dans l'application.
  - **Groupe** : tâches de groupe créées et envoyées au serveur à l'aide des outils de Kaspersky Administration Kit.
- **État de la tâche** : état courant de la tâche
- Heure de fin : dans le cas de tâches terminées, cette zone indique **la date et l'heure de fin d'exécution de la tâche.** L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus. Cette zone est vide pour des tâches en cours d'exécution.

Les informations affichées dans le panneau de résultats peuvent être triées par n'importe quelle colonne.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Filtre** : recherche des journaux qui vérifient les critères définis.
- **Supprimer le filtre** : supprime le filtre.
- **Effacer** : supprime tous les journaux.

Les informations qui sont consignées dans les journaux pendant l'activité des tâches sont déterminées par les paramètres des journaux. Par défaut, les informations sur tous les composants de Kaspersky Anti-Virus sont enregistrées. Ceci correspond au niveau **Événements importants**.

VOIR EGALEMENT

Affichage dans le journal d'informations relatives à la tâche 234

FENETRE JOURNAL D'EXECUTION

Cette fenêtre permet de visualiser des informations relatives à la tâche telles que des événements, statistiques et paramètres.

Nombre total d'objets dans rapport, spécifié dans la zone **Total des événements**. Le nom du rapport à générer est affiché dans la partie supérieure de la fenêtre. Les informations sur son activité figurent sur les onglets situés dans la partie centrale de la fenêtre :

Statistiques (onglet)

L'onglet **Statistiques** contient des statistiques sur l'activité de la tâche. Les heures de début et de fin (si la tâche est terminée) sont indiquées pour chaque type de tâche.

Onglet "Evénements"

L'onglet **Événements** contient des informations sur tous les événements enregistrés pendant l'exécution d'une tâche, depuis le démarrage de la tâche jusqu'à l'ouverture du journal.

Les informations de l'onglet **Événements** varient selon le type de tâche et peuvent contenir :

- **L'icône** indicateur du niveau de gravité de l'événement. Les degrés d'importance suivants sont prévus :

  Événement critique, qui signale la présence de vulnérabilités dans la protection de votre ordinateur ou des problèmes dans le fonctionnement de l'application. Menace détectée, *Erreur de traitement de l'objet,* Erreur générale de mise à jour.

  Événements importants : qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement du programme. *Erreur de connexion avec la source de mises à jour*, *Objet non traité*, *Dépassement du seuil d'espace libre pour la sauvegarde*.

  Messages d'information ce sont des messages de référence qui ne contiennent en général pas d'informations importantes. *Objet non infecté*, *Objet réparé*, S*ource de mise à jour sélectionnée.*

- **Événement** : type d'événement avec des informations supplémentaires sur lui.
- **Objet** : nom complet et chemin de l'objet traité (dans le cas de mises à jour, nom du module téléchargé ou installé).
- **Heure d'événement** : date et heure de l'événement. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Ordinateur** : nom de l'ordinateur que l'application a utilisé pour accéder au serveur (uniquement pour les tâches de la **Protection en temps réel des fichiers**). Si une application installée sur le serveur accède au serveur, ce champ contient la valeur **localhost**.
- **Nom d'utilisateur** : nom du compte utilisateur utilisé par l'application pour accéder au serveur.
- Si l'application qui accède au serveur est exécutée sous le compte **Système local** (**SYSTEM**), la colonne affichera l'entrée **<domaine>\<nom_ordinateur>$**.

Les informations sur les événements peuvent être triées par n'importe quelle colonne, sauf la colonne **Événement**.

Vous pouvez rechercher des événements en définissant des critères de recherche. Les recherches s'exécutent avec un filtre : après l'application du filtre, seules les informations qui répondent aux critères de recherche sont affichées.

Paramètres (onglet)

L'onglet **Paramètres** contient la liste des paramètres utilisés pour exécuter une tâche. Dans le cas des tâches de **Protection en temps réel des fichiers** et d'**Analyse des scripts** et d'analyse à la demande, l'historique des modifications des paramètres est affiché.

Boutons

Les boutons de la partie inférieure de la fenêtre permettent de réaliser les opérations suivantes :

- **Exporter** : exporte les informations dans un fichier.

- **Filtre** : recherche des événements qui vérifient les critères définis (disponible uniquement pour l'onglet **Événements).**
- **Mettre à jour** : actualise les informations affichées dans le journal.
- **Fermer** : referme la fenêtre du journal.

VOIR EGALEMENT

Paramètres des tâches de mise à jour 74

Paramètres de protection dans la tâche Protection en temps réel des fichiers et dans les tâches d'analyse à la demande 154

Statistiques de la tâche Protection en temps réel des fichiers 107

Statistiques de la tâche Analyse des scripts 111

JOURNAL D'EXECUTION DES TACHES : FENETRE PARAMETRES DU FILTRE

Utilisez cette fenêtre pour créer le critère de recherche des objets présents dans le journal d'audit.

Vous pouvez utiliser de nombreuses conditions dans le critère, combinées avec le lien logique "and" ou "or". Les critères sont créés avec les zones et les boutons sur le côté droit de la fenêtre. La liste des conditions est affichée dans la partie supérieure de la fenêtre.

La liste **Nom du champ** propose les valeurs suivantes:

- **Heure de fin** : date et heure de fin de l'événement. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Nom de tâche** : nom de la tâche sur laquelle le journal est généré.
- **Catégorie de la tâche** : catégorie de la tâche sur laquelle le rapport est généré.
- **État du rapport** : niveau d'importance du journal, décrit le résultat global de la tâche du point de vue de la sécurité antivirus.
- **État de la tâche** : état courant de la tâche
- Type de tâche : type de la tâche sur laquelle le **journal** est généré.
- **Degré d'importance** – degré d'importance de l'événement.

VOIR EGALEMENT

Affichage dans le journal d'informations relatives à la tâche 234

JOURNAL D'AUDIT SYSTEME : PARAMETRES DU FILTRE (FENETRE)

Utilisez cette fenêtre pour créer le critère de recherche des objets présents dans le journal d'audit.

Vous pouvez utiliser de nombreuses conditions dans le critère, combinées avec le lien logique "and" ou "or". Les critères sont créés avec les zones et les boutons sur le côté droit de la fenêtre. La liste des conditions est affichée dans la partie supérieure de la fenêtre.

La liste **Nom du champ** propose les valeurs suivantes:

- **Heure d'événement**- date et heure de l'événement. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Nom de tâche** : nom de la tâche associée à l'événement.
- **Nom d'utilisateur** : nom du compte utilisateur qui a causé l'événement.
- **Composant** : nom du composant de Kaspersky Anti-Virus associé à l'événement.
- **Ordinateur** : nom réseau ou adresse IP de l'ordinateur associé à l'événement.
- **Objet** : nom et chemin complet de l'objet associé à l'événement.
- **Événement** : type d'événement avec des informations supplémentaires sur lui.
- **Degré d'importance** – degré d'importance de l'événement.

VOIR EGALEMENT

Filtrage des événements dans le journal d'audit système 228

Tri des événements dans le journal d'audit système 228

PROPRIETES D'EVENEMENT (FENETRE)

Cette fenêtre affiche des informations détaillées sur un événement enregistré :

- **Degré d'importance** – degré d'importance de l'événement. Les degrés d'importance suivants sont prévus :

  Critique : événements critiques qui signalent des problèmes de fonctionnement de l'application ou la présence de vulnérabilités dans la sécurité de votre ordinateur. Par exemple : *Menace détectée*, *Erreur de traitement de l'objet*.

  Avertissement : événements qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement du programme. Par exemple : *Objet non analysé*.

  Messages d'information ce sont des messages de référence qui ne contiennent en général pas d'informations importantes. Par exemple : *Objet non infecté*, *Objet réparé*.

- **Heure** : Date et heure d'enregistrement de chacun des événements. L'heure du serveur est indiquée au format défini dans les Paramètres régionaux de Microsoft Windows sur l'ordinateur équipé de la console de Kaspersky Anti-Virus.
- **Nom d'utilisateur** : nom du compte utilisateur qui a causé l'événement.

Si l'application qui accède au serveur est exécutée sous le compte **Système local** (**SYSTEM**), la colonne affichera l'entrée **<domaine><nom_ordinateur>$**.

- **Nom d'ordinateur**- nom de l'ordinateur que l'application utilise pour accéder au serveur (uniquement pour des tâches de **Protection en temps réel des fichiers**). Si une application installée sur le serveur accède au serveur, ce champ contient la valeur localhost.

- **Composant** (affiché uniquement pour les événements du journal d'audit système) : nom du composant de Kaspersky Anti-Virus dans le fonctionnement duquel l'événement a été enregistré. Le système comprend les éléments suivants :

  - **Protection en temps réel** : tâches associées à l'activité de la protection en temps réel des fichiers.

  - **Analyse à la demande** : événement associés à l'activité des tâches d'analyse à la demande (tâches système et personnalisées, y compris les tâches créées et exécutées depuis l'invite de commande).

  - **Analyse des scripts** : tâches associées à la surveillance des scripts.

  - **Quarantaine** : enregistre des informations sur les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de quarantaine, sur l'espace libre dans la quarantaine, etc.

  - **Sauvegarde** : enregistre des informations sur toutes les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de sauvegarde,, sur l'espace libre dans le dossier de sauvegarde, etc.

  - **Mise à jour** : événements associés à l'exécution des tâches de mise à jour de la base antivirus et des modules d'application et de la tâche de distribution des mises à jour : connexion avec la source de mises à jour, avec le serveur proxy, etc.

  - **Audit système** : événements relatifs au démarrage et à l'arrêt de l'application, au renforcement des stratégies de Kaspersky Administration Kit, à l'état des base de données de Kaspersky Anti-Virus et à la gestion des licences.

  - **Journaux** : informations relatives aux opérations liées à l'ajout d'événements dans les journaux d'enregistrement des événements.

  - **Service**: événements liés aux tâches prédéfinies de Kaspersky Anti-Virus.

- **Description** : description et informations avancées sur l'événement, telles que : nom de la tâche associée à l'événement, nom et chemin d'accès de l'objet associé, et nom réseau ou adresse IP de l'ordinateur associé.

Vous pouvez utiliser les boutons "haut" et "bas" pour visualiser les propriétés de l'événement précédent ou suivant. A l'aide du bouton  vous pouvez copier les informations de l'onglet dans le Presse-papiers.

FENETRE PROPRIETES : JOURNAUX, ONGLET GENERAL

Cet onglet présente les paramètres qui déterminent quelles informations sont enregistrées, et leur niveau de détail.

Dans la liste déroulante **Composant**, choisissez le nom du composant pour lesquels vous souhaitez configurer l'enregistrement des événements :

- **Protection en temps réel des fichiers** : enregistre les résultats des tâches de protection en temps réel des fichiers, et tous les événements associés, pendant le fonctionnement de l'application (les événements sont consignés dans le journal d'événements et dans les rapports).

- **Analyse des scripts** : enregistre les résultats des tâches de surveillance des scripts, et tous les événements associés, pendant le fonctionnement de l'application (les événements sont consignés dans le journal d'événements et dans les rapports).

- **Analyse à la demande** : enregistre les résultats des tâches d'analyse à la demande (de groupe, système et personnalisées, y compris celles créées et lancées depuis la ligne de commande) et tous les événements

associés pendant le fonctionnement de l'application (les événements sont consignés dans le journal d'événements et dans les rapports).

- **Mise à jour** : enregistre les résultats des tâches (de groupe et système) de mise à jour et de distribution de la base antivirus et des modules, ainsi que tous les événements associés au fonctionnement de Kaspersky Anti-Virus : connexion avec la source de mises à jour, avec le serveur proxy, etc. (les événements sont enregistrés dans le journal des événements ainsi que dans les journaux relatifs à l'exécution des tâches).

- **Quarantaine** : enregistre des informations sur les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de quarantaine, sur l'espace libre dans la quarantaine, etc. (les événements sont enregistrés dans le journal des événements ainsi que dans le journal d'audit).

- **Sauvegarde** : enregistre des informations sur toutes les opérations de déplacement, suppression ou restauration de fichiers dans le dossier de sauvegarde, sur l'espace libre dans le dossier de sauvegarde, etc. (les événements sont enregistrés dans le journal des événements ainsi que dans le journal d'audit).

Sélectionnez le degré de détail des informations dans la liste déroulante **Niveau de détail** :

- **Événements critiques** : enregistre des événements critiques qui signalent la présence de vulnérabilités dans la protection du serveur ou des problèmes dans le fonctionnement du programme, par exemple : *Menace détectée.*

- **Événements importants** : enregistre les événements critiques et ceux qui doivent être examinés, car ils reflètent des situations importantes du fonctionnement du programme. Par exemple, *Erreur de connexion avec la source de mises à jour*.

- **Événements d'information** : enregistre les événements critiques, les événements importants et les messages de référence qui ne contiennent généralement pas d'informations importantes, par exemple *Objet non infecté*, *Mise à jour de module téléchargée*.

- **Personnalisé** : enregistre des événements spécifiés par l'administrateur.

Le tableau affiche la liste des types d'événements qui répondent au niveau sélectionné. **Le tableau contient un colonne** Enregistrer les événements pour tous les composants. Pour les composants **Protection en temps réel**, **Analyse des scripts**, **Analyse à la demande** et **Mise à jour**, les événements sont enregistrés dans les journaux relatifs à l'exécution des tâches ainsi que dans le journal d'audit système. Pour ceux-ci, le tableau contient une colonne **Journaux**. Pour les composants **Quarantaine** et **Dossier de sauvegarde**, le tableau contient une colonne **Audit**.

Quand un type d'événement est consigné, la case à cocher correspondante est sélectionnée. Si la case n'est pas cochée, cela signifie que la consignation n'est pas prise en charge pour ce type d'événement.

Pour configurer la liste des événements enregistrés manuellement, sélectionnez **Personnalisé** dans le menu déroulant **Niveau de détail.** Dans le tableau inférieur, cochez ensuite les cases selon les événements que vous souhaitez enregistrer et décochez les autres.

Configurez les paramètres d'enregistrement des autres composants.

VOIR EGALEMENT

Configuration de paramètres des journaux dans MMC 239

FENETRE PROPRIETES : JOURNAUX, ONGLET AVANCE

L'onglet **Avancé** vous permet de configurer les journaux relatifs à l'exécution des tâches ainsi que le journal d'audit système.

Dossier des journaux : spécifie le dossier dans lequel Kaspersky Anti-Virus conserve les fichiers des journaux relatifs à l'exécution des tâches et du journal d'audit système.

Supprimer les journaux relatifs à l'exécution des tâches et les événements plus anciens que (jours) – définit le délai de conservation des journaux relatifs à l'exécution des tâches.

Supprimer du journal d'audit les événements plus anciens que (jours) : définit le délai de conservation des événements dans le journal d'audit système.

VOIR EGALEMENT

Dossier de conservation des journaux relatifs à l'exécution des tâches et du journal d'audit système 368

Délai de conservation des journaux relatifs à l'exécution des tâches 368

Durée de conservation des événements dans le journal d'audit système 369

INSTALLATION ET SUPPRESSION DES LICENCES.

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES LICENCES KASPERSKY ANTI-VIRUS

Vous ne pouvez pas utiliser Kaspersky Anti-Virus sans licence. Les informations relatives à la licence, à savoir les privilèges et les restrictions applicables à l'utilisation de Kaspersky Anti-Virus, sont reprises dans une "clé" qui est une fichier texte portant l'extension .key.

Le fichier de la licence contient les données sur la durée de validité de la licence, en jours (par exemple, 365 jours). Kaspersky Lab peut distribuer des licences dont les périodes de validité diffèrent. Le fichier de licence possède sa propre durée de validité : la date après laquelle il n'est plus valide (par exemple, le 31 décembre 2010 si la licence a été délivrée en 2008).

Lors de l'installation de la clé, Kaspersky Anti-Virus calcule la date de fin de validité de la licence : cette date correspond à la fin de la période de validité à partir de l'installation de la licence mais ne peut être postérieure à la date après laquelle le fichier de licence devient invalide. Pendant cette période, vous avez accès aux possibilités suivantes :

- Protection antivirus ;
- Maintient de l'actualité des bases (mises à jour des bases) ;
- Installation automatique des mises à jour urgentes des modules de Kaspersky Anti-Virus (patch).

Pendant cette période, Kaspersky Lab ou son partenaire vous offre une assistance technique pour autant que celle-ci soit prévue dans les conditions de la licence.

Une fois la licence arrivée à échéance, Kaspersky Anti-Virus ne remplit plus ses fonctions : selon la licence que vous utilisiez, vous ne pourrez plus utiliser soit les fonctions de mise à jour des bases et des modules de l'application et le service d'assistance technique, soit l'ensemble des fonctions de Kaspersky Anti-Virus.

Il existe trois types de licence pour Kaspersky Anti-Virus : *test bêta*, *évaluation* et *commerciale*.

Licence pour test bêta

La licence pour test bêta est offerte gratuitement. Elle est proposée uniquement durant les tests bêta de Kaspersky Anti-Virus. Une fois que la licence est parvenue à échéance, toutes les fonctions de Kaspersky Anti-Virus sont désactivées.

Licence d'évaluation

La licence d'évaluation est offerte gratuitement. Elle permet aux utilisateurs de découvrir Kaspersky Anti-Virus. La durée de validité d'une licence d'évaluation n'est pas très longue ; à la fin de celle-ci, toutes les fonctions de Kaspersky Anti-Virus sont désactivées. Vous pouvez installer uniquement une licence d'évaluation de Kaspersky Anti-Virus.

Licence commerciale

Une fois que la licence commerciale est arrivée à échéance, Kaspersky Anti-Virus continue à fonctionner, à l'exception de la mise à jour. L'analyse du serveur s'opère à l'aide des bases installée avant la date de fin de validité de la licence. Il n'identifie pas les menaces ajoutées aux bases par les experts de Kaspersky Lab après la fin de la validité de la licence et il ne répare par les objets infectés par ces menaces. L'assistance technique est également offerte uniquement durant la période de validité de la licence.

Vous pouvez acheter et installer deux licences directement : *une licence active* et une *licence de réserve*. La licence active entre en vigueur dès son installation tandis que la licence complémentaire entre en vigueur automatiquement dès la fin de validité de la licence active.

La licence de Kaspersky Anti-Virus peut imposer des restrictions d'utilisation en fonction du nombre de serveurs.

Avec prise en charge de EMC Celerra

La licence de ce type assure l'intégration de Kaspersky Anti-Virus avec le système réseau de sauvegarde de données EMC Celerra. Kaspersky Anti-Virus transmet à EMC Celerra les informations sur l'état de protection des fichiers enregistrés dans le système, ainsi que les informations sur l'actualité des bases antivirus du produit.

CONSULTATION DES INFORMATIONS RELATIVES AUX CLES INSTALLEES

➧ *Pour consulter les informations sur les licences installées, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le nœud **Licences** (cf. ill. ci-après).

2. Dans le panneau de résultats, ouvrez le menu contextuel de la ligne contenant les informations sur la licence que vous souhaitez consulter et sélectionnez l'option **Propriétés.**

Le panneau de résultats reprend les informations sur la licence (cf. tableau ci-dessous).

Tableau 30. Informations sur la licence

CHAMP	DESCRIPTION
Numéro de la licence	Numéro de série de la licence.
Type de licence	Type de licence: pour test bêta, évaluation ou commerciale ou avec prise en charge d'EMC Celerra (cf. rubrique " Présentation des licences de Kaspersky Anti-Virus " à la page 254).
Fin de validité	Fin de validité : date de fin de validité de la licence déterminée par Kaspersky Anti-Virus lors de l'installation de la licence. La date correspond à la fin de la période de validité de la licence depuis son activation, mais ne peut pas être ultérieure à la fin de validité du fichier de licence.
Etat	État de la licence : active ou complémentaire (cf. rubrique "Présentation des licences Kaspersky Anti-Virus" à la page 254).

Dans la boîte de dialogue **Propriétés :** <**Numéro de série de la licence**>, sous l'onglet **Général** (cf. tableau ci-dessous), vous retrouverez des informations détaillées sur la licence (cf. ill. ci-après).

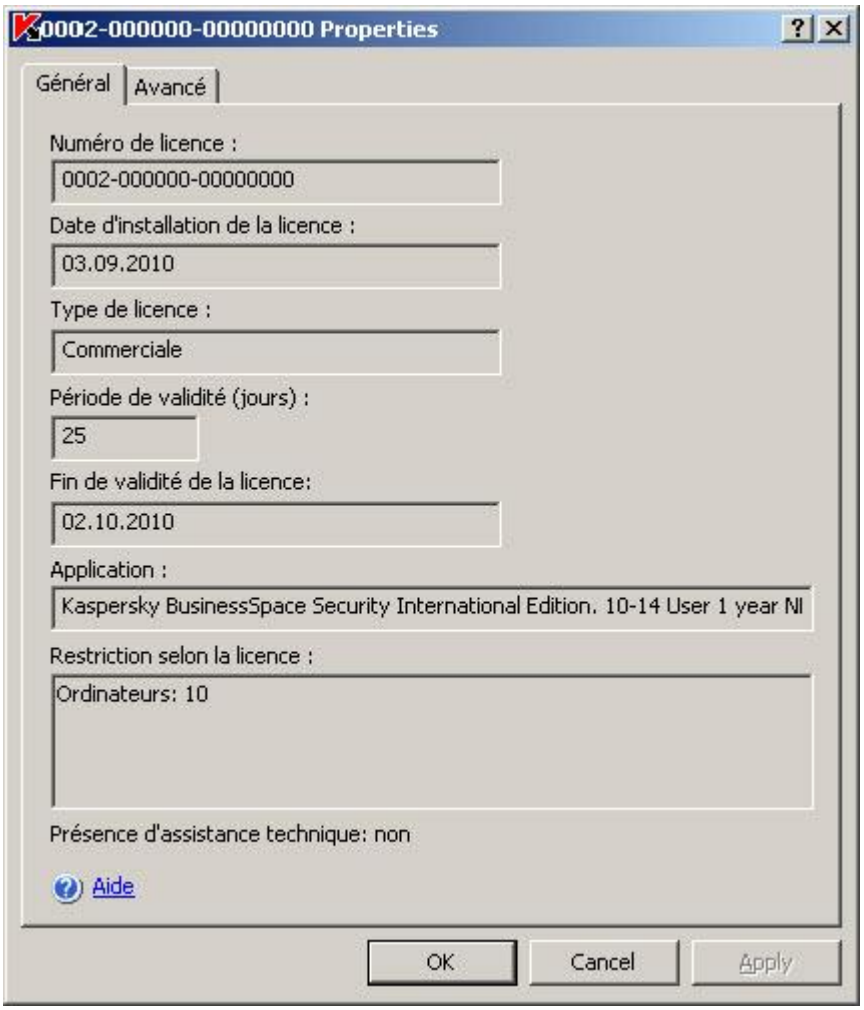


*Illustration 85. Boîte de dialogue **Propriétés**, onglet **Général***

Tableau 31. Informations relatives à la licence

CHAMP	DESCRIPTION
Numéro de la licence	Numéro de série de la licence.
Date d'installation de la licence	Date d'installation de la licence dans Kaspersky Anti-Virus.
Type de licence	Type de licence: pour test bêta, évaluation ou commerciale ou avec prise en charge d'EMC Celerra (cf. rubrique " Présentation des licences de Kaspersky Anti-Virus " à la page 254).
La durée d'évaluation restante est de (jours)	Période d'activité de la licence (en jours), définie au moment de son attribution.
Fin de validité de la licence	Fin de validité : date de fin de validité de la licence déterminée par Kaspersky Anti-Virus lors de l'installation de la licence. La date correspond à la fin de la période de validité de la licence depuis son activation, mais ne peut pas être ultérieure à la fin de validité du fichier de licence.
Application	Nom de Kaspersky Anti-Virus.
Restriction selon la licence	Restrictions prévues par la licence (le cas échéant).
Présence d'assistance technique	Indique si la licence prévoit une assistance technique offerte par Kaspersky Lab ou par ses partenaires.

Dans la boîte de dialogue <**Numéro de série de la licence**> **Propriétés**, sous l'onglet **Avancé**, vous pourrez lire les informations relatives au client ainsi que les coordonnées de Kaspersky Lab ou du distributeur où vous avez acheté Kaspersky Anti-Virus.

INSTALLATION D'UNE LICENCE

Vous pouvez installer la licence à partir du fichier de licence.

Si vous installez la licence en tant qu'active alors qu'une licence active est déjà installée pour Kaspersky Anti-Virus, la nouvelle licence remplacera l'ancienne. La licence active installée auparavant sera supprimée.

Si vous installez la licence en tant que complémentaire alors qu'une licence complémentaire est déjà installée pour Kaspersky Anti-Virus, la nouvelle licence remplacera l'ancienne. La licence complémentaire installée auparavant sera supprimée.

Si vous installez la licence en tant qu'active alors qu'une licence active et une licence complémentaire sont déjà installées pour Kaspersky Anti-Virus, les licences installées auparavant seront supprimées.

➧ *Pour installer une licence, procédez comme suit :*

1. Dans l'arborescence de la console, ouvrez le menu contextuel du nœud **Licences** et sélectionnez **Installer**.

2. Dans la boîte de dialogue **Ajout d'une licence**, indiquez le nom du fichier de licence contenant les informations sur la licence et le chemin d'accès au fichier (cf. ill. ci-après).

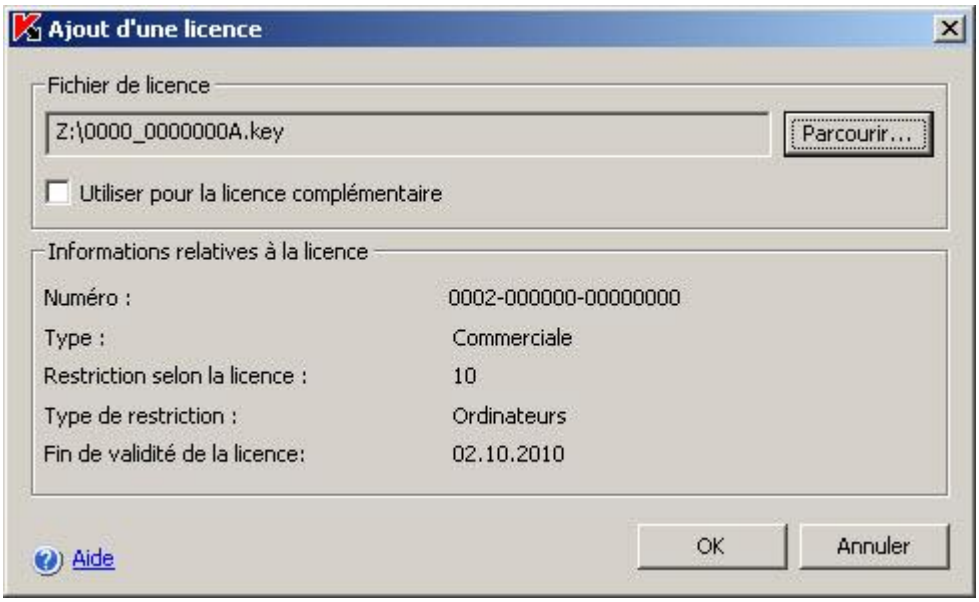


*Illustration 86. Boîte de dialogue **Ajout d'une licence***

3. Si vous installez une licence en guise de licence complémentaire, cochez la case **Utiliser comme licence complémentaire**. Cliquez sur **OK**.

La boîte de dialogue **Ajout d'une licence** reprend les informations sur la licence installée (cf. tableau ci-après).

Tableau 32. Informations sur la licence

CHAMP	DESCRIPTION
Numéro	Numéro de série de la licence
Type	Type de licence: pour test bêta, évaluation ou commerciale (cf. rubrique " Présentation des licences de Kaspersky Anti-Virus" à la page 254).
Restriction selon la licence	Nombre d'objets limités
Type de restriction	Objets limités
Fin de validité de la licence	Date d'expiration de la licence (cf. rubrique "Présentation des licences de Kaspersky Anti-Virus" à la page 254) ; calculée par Kaspersky Anti-Virus ; correspond à la fin de la période de validité de la licence depuis son activation mais pas ultérieur à la fin de validité du fichier de licence.

SUPPRESSION D'UNE LICENCE

Vous pouvez supprimer une licence installée.

Si vous supprimez une licence active alors qu'une licence complémentaire est installée, cette dernière sera activée automatiquement.

Si vous supprimez une licence installée, vous pouvez la rétablir en la réinstallant depuis le fichier de clé.

Pour supprimer la licence installée, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Licences**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur la licence que vous souhaitez supprimer et sélectionnez **Supprimer**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

BOITES DE DIALOGUE : LICENCES

DANS CETTE SECTION DE L'AIDE

LICENCES (ENTREE)

L'entrée **Licences** est conçue pour installer et prolonger les licences Kaspersky Anti-Virus ainsi que pour afficher des informations sur les licences installées.

Vous pouvez installer simultanément deux licences: la licence active et la licence complémentaire. La licence active est d'application dès son installation. La licence complémentaire s'activera automatiquement après expiration de la licence active.

Panneau de résultats

Le panneau des résultats reprend les informations sur les licences installées :

- **Numéro de licence** : numéro de série de la licence ;
- **Type de licence** : type de licence : test bêta, évaluation, commerciale ou avec prise en charge d'EMC Celerra.
- **Date de fin de validité de la licence** : date de fin calculée par Kaspersky Anti-Virus ; correspond à la fin de la période de validité de la licence depuis son activation mais pas ultérieur à la fin de validité du fichier de licence.
- **Etat** : la licence installée est une licence active ou la sauvegarde.

Menu contextuel et panneau de tâches

À l'aide des liens du panneau de tâches et des commandes du menu contextuel, vous pouvez effectuer les actions suivantes :

- **Installer** : installe la licence à partir du fichier de licence.
- **Supprimer** : supprime la licence installée.
- **Propriétés** : affiche les informations détaillées sur la licence.

VOIR EGALEMENT

FENETRE AJOUT D'UNE LICENCE

Cette fenêtre permet de spécifier le fichier de la licence que vous souhaitez installer.

Sélectionnez le fichier de clé à l'aide du bouton **Parcourir**. Les informations relatives à la licence reprises dans le fichier de clé apparaissent dans la rubrique **Renseignements sur la licence**. Vous pouvez consulter les valeurs suivantes :

- **Numéro** : numéro de série de la licence.
- **Type** : un des types de licence suivants : test bêta, évaluation, commerciale ou avec prise en charge d'EMC Celerra.
- **Restriction selon la licence** : restrictions de l'utilisation de Kaspersky Anti-Virus prévues par la licence.
- **Type de restriction** : unité de mesure pour la restriction de l'utilisation de Kaspersky Anti-Virus prévue par la licence, par exemple : ordinateurs.
- **Fin de validité** : date de fin de validité de la licence déterminée par Kaspersky Anti-Virus lors de l'installation de la licence. La date correspond à la fin de la période de validité de la licence depuis son activation, mais ne peut pas être ultérieure à la fin de validité du fichier de licence.

Si la clé doit être installée comme licence active, vérifiez que la case **Utiliser comme licence complémentaire** est décochée.

Si la clé doit être installée comme licence complémentaire, cochez la case **Utiliser comme licence complémentaire**.

PROPRIETES (FENETRE) : <NUMERO DE SERIE DE LA LICENCE>, GENERAL (ONGLET)

Cet onglet affiche des informations suivantes sur la clé de licence de Kaspersky Anti-Virus :

- **Numéro** : numéro de série de la licence.
- **Date d'installation de la licence** : date d'installation de la licence dans Kaspersky Anti-Virus.
- **Type de licence** : type de licence : test bêta, évaluation, commerciale ou avec prise en charge d'EMC Celerra.
- **La durée d'évaluation restante est de** : période de validité de la licence en jours, défini après l'émission de la licence.
- **Fin de validité** : date de fin de validité de la licence déterminée par Kaspersky Anti-Virus lors de l'installation de la licence. La date correspond à la fin de la période de validité de la licence depuis son activation, mais ne peut pas être ultérieure à la fin de validité du fichier de licence.
- **Application** : nom et version de Kaspersky Anti-Virus.

- **Restriction selon la licence** : restrictions prévues par la licence (le cas échéant).
- **Présence d'assistance technique** : indique si les conditions de la licence prévoient une assistance technique par Kaspersky Lab ou par ses partenaires.

PROPRIETES (FENETRE) : <NUMERO DE SERIE DE LA LICENCE>, AVANCE (ONGLET)

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

- **Informations sur la licence** : type de licence, durée de validité, date d'expiration, restrictions pour l'utilisation de Kaspersky Anti-Virus et autres informations générales sur la licence.
- **Informations sur l'assistance** : informations de contact de Kaspersky Lab
- **Renseignements sur le détenteur** : informations sur le bénéficiaire de la licence.

CONFIGURATION DES NOTIFICATIONS

DANS CETTE SECTION DE L'AIDE

MOYENS DE NOTIFICATION DE L'ADMINISTRATEUR ET DES UTILISATEURS

Kaspersky Anti-Virus permet de notifier à l'administrateur et aux utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Anti-Virus et à l'état de la protection antivirus du serveur. Le système assure l'exécution des tâches suivantes

- L'administrateur peut obtenir des informations sur les événements de certains types ;
- Les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peut obtenir des informations sur les événements de type *Une menace a été découverte* qui surviennent pendant la tâche **Protection en temps réel des fichiers**.

L'instruction NETSEND envoie la notification relative à l'objet infecté uniquement si l'utilisateur travaille sur un ordinateur distant. L'instruction NET SEND n'envoie pas la notification sur l'infection à l'utilisateur qui travaille sur le serveur protégé.

Dans la console de Kaspersky Anti-Virus, vous pouvez configurer les notifications de l'administrateur et des utilisateurs de plusieurs manières (cf. tableaux ci-dessous).

Tableau 33. Moyens de notification des utilisateurs

MOYEN DE NOTIFICATION	CONFIGURATION PAR DEFAUT	DESCRIPTION
Fenêtre des services des terminaux	Configuré sur l'événement *Une menace a été découverte* de la tâche **Protection en temps réel des fichiers**	Si le serveur protégé est terminal, vous pouvez appliquer cette méthode afin d'alerter les utilisateurs via terminal.
Notification via le service de messagerie de Microsoft Windows	Configuré sur l'événement *Une menace a été découverte* de la tâche **Protection en temps réel des fichiers**	Ce mode de notification utilise le service de messagerie de Microsoft Windows. Ce mode n'est pas utilisé si le serveur protégé fonctionne sous Microsoft Windows Server 2008. Avant d'opter pour ce mode, assurez-vous que le service de messagerie est activé sur le serveur protégé et sur les postes de travail des utilisateurs du réseau local (il est désactivé par défaut).

Tableau 34. Moyens de notification des administrateurs

MOYEN DE NOTIFICATION	CONFIGURATION PAR DEFAUT	DESCRIPTION
Notification via le service de messagerie de Microsoft Windows	Non configuré	Ce mode de notification utilise le service de messagerie de Microsoft Windows. Ce mode n'est pas utilisé si le serveur protégé fonctionne sous Microsoft Windows Server 2008. Avant d'opter pour ce mode de notification, assurez-vous que le service de messagerie est activé sur le serveur protégé et sur l'ordinateur qui fait office de poste de travail de l'administrateur (si l'administrateur administre Kaspersky Anti-Virus à distance). Le service de messagerie est désactivé par défaut.
Lancement du fichier exécutable	Non configuré	Ce mode de notification lance le fichier exécutable indiqué quand un événement défini survient. Le fichier exécutable doit se trouver sur le disque local du serveur protégé.
Notification par courrier électronique	Non configuré	Ce mode transmet les notifications via le courrier électronique.

Vous pouvez créer un texte différent pour chaque type d'événement. Ce texte peut contenir des champs avec les informations sur l'événement. Le texte prédéfini du message est utilisé par défaut pour les notifications des utilisateurs (cf. tableau ci-dessous).

Tableau 35. Texte du message composé par défaut pour la notification des utilisateurs

TACHE	TYPE D'EVENEMENT	TEXTE DU MESSAGE
Protection en temps réel des fichiers	*Une menace a été découverte*	Kaspersky Anti-Virus a bloqué l'accès à %OBJECT% sur l'ordinateur %FROM_COMPUTER% à %EVENT_TIME%. Cause : %EVENT_TYPE%. Type de menace : %VIRUS_TYPE%: %VIRUS_NAME%. Nom de l'utilisateur de l'objet : %USER_NAME%. Nom du poste de l'utilisateur de l'objet : %USER_COMPUTER%

MOYENS DE NOTIFICATION DE L'ADMINISTRATEUR ET DES UTILISATEURS

La configuration des notifications sur les événements porte sur le mode de notification et sur la composition du texte du message.

Pour configurer les notifications sur les événements, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Paramètres de notification**.

   La boîte de dialogue **Notifications** s'ouvrira (cf. ill. ci-après).

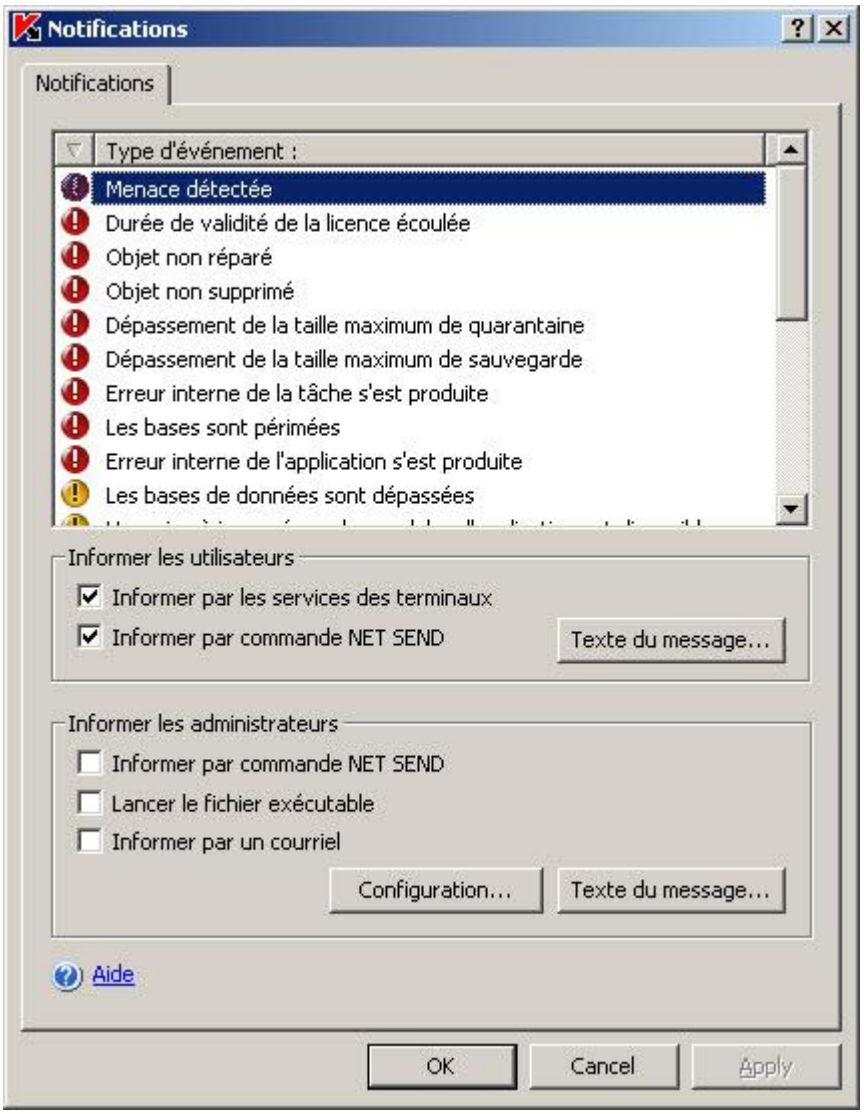


*Illustration 87. Boîte de dialogue **Notifications***

2. Dans la boîte de dialogue **Notifications**, onglet **Notifications**, sélectionnez les événements et définissez le mode de notification pour ceux-ci :

   - Pour définir les moyens de notification de l'administrateur, réalisez les actions suivantes :

     a. Dans la liste **Type d'événement**, sélectionnez les types d'événements.

b. Dans le groupe de paramètres **Informer les administrateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

c. Dans le groupe de paramètres **Informer les utilisateurs**, cochez la case contre les modes de notification que vous souhaitez configurer pour l'événement **Menace détectée**.

Vous pouvez composer un texte du message de notification pour plusieurs types d'événements : après avoir choisi le mode de notification pour un type d'événement, sélectionnez, à l'aide de la touche **Ctrl** ou **Shift**, les autres types d'événements pour lesquels vous souhaitez créer ce même texte du message.

3. Pour composer le texte du message, cliquez sur le bouton **Texte du message** dans le groupe de paramètres correspondant. Dans la boîte de dialogue **Texte du message**, saisissez le texte qui sera affiché dans le message sur l'événement.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Macro** et sélectionnez les champs désirés dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette rubrique.

   Pour revenir au texte prévu par défaut pour l'événement, cliquez sur le bouton **Par défaut**.

   Pour configurer les modes de notifications de l'administrateur sur les événements sélectionnés, cliquez sur le bouton **Configuration** dans la boîte de dialogue **Notifications** et dans la boîte de dialogue **Configuration avancés**, procédez à la configuration des modes sélectionnés. Pour ce faire, exécutez les actions suivantes :

   a. Pour les notifications via courrier électronique, ouvrez l'onglet **Courriel** et saisissez les adresses électroniques des destinataires (séparez les adresses par un point virgule), le nom ou l'adresse de réseau du serveur SMTP, ainsi que son port, dans les champs prévus à cet effet (cf. ill. ci-après). Si nécessaire, indiquez le texte qui figurera dans les champs **Objet** et **De**. Le texte du champ **Objet** peut contenir des valeurs de champs d'informations (cf. tableau ci-dessous).

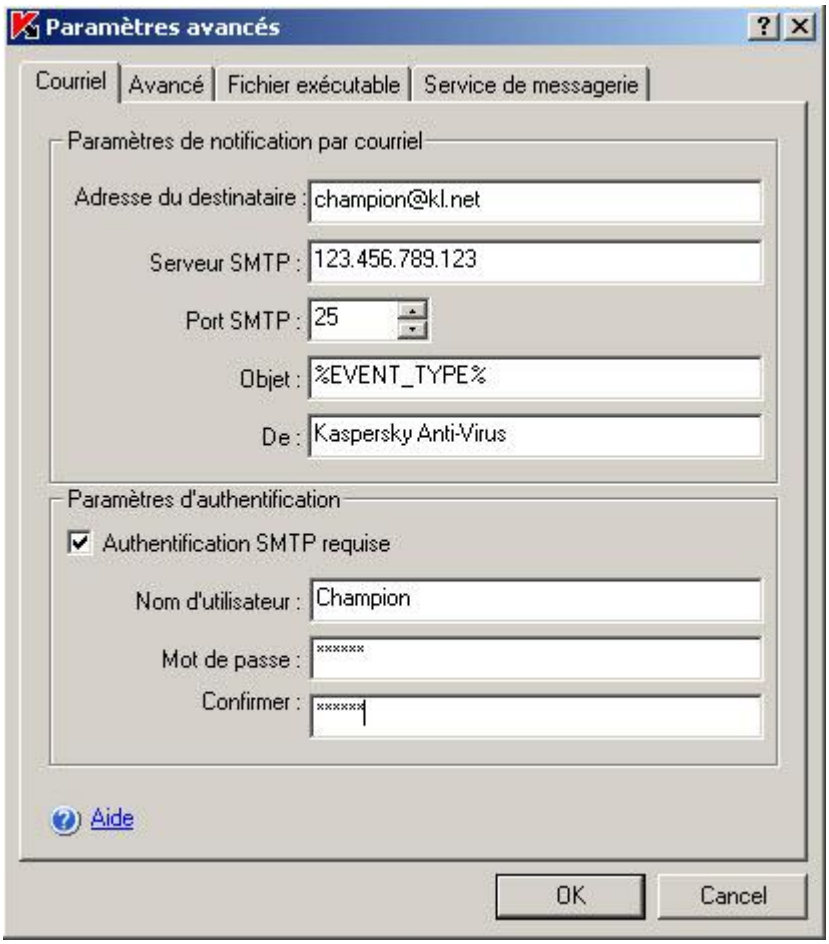


*Illustration 88. Boîte de dialogue **Configuration avancée**, onglet **Courrier électronique** (pour Windows Server 2003)*

b. Si vous souhaitez utiliser la vérification de l'authenticité selon le compte utilisateur lors de la connexion au serveur SMTP, il faudra dans ce cas cochez la case **Authentification SMTP** requise dans le groupe **Paramètres d'authentification** et saisir le nom et le mot de passe de l'utilisateur dont l'authenticité sera vérifiée

c. Pour les notifications via le service de messagerie, sous l'onglet **Service de messagerie**, composez la liste des ordinateurs des destinataires des messages : pour chaque ordinateur que vous souhaitez ajouter, cliquez sur le bouton **Ajouter** et dans le champ, saisissez son nom de réseau (cf. ill. ci-après).

   N'oubliez pas que les notifications via le **Service de messagerie** ne sont pas utilisées si le serveur protégé tourne sous Microsoft Windows Server 2008.

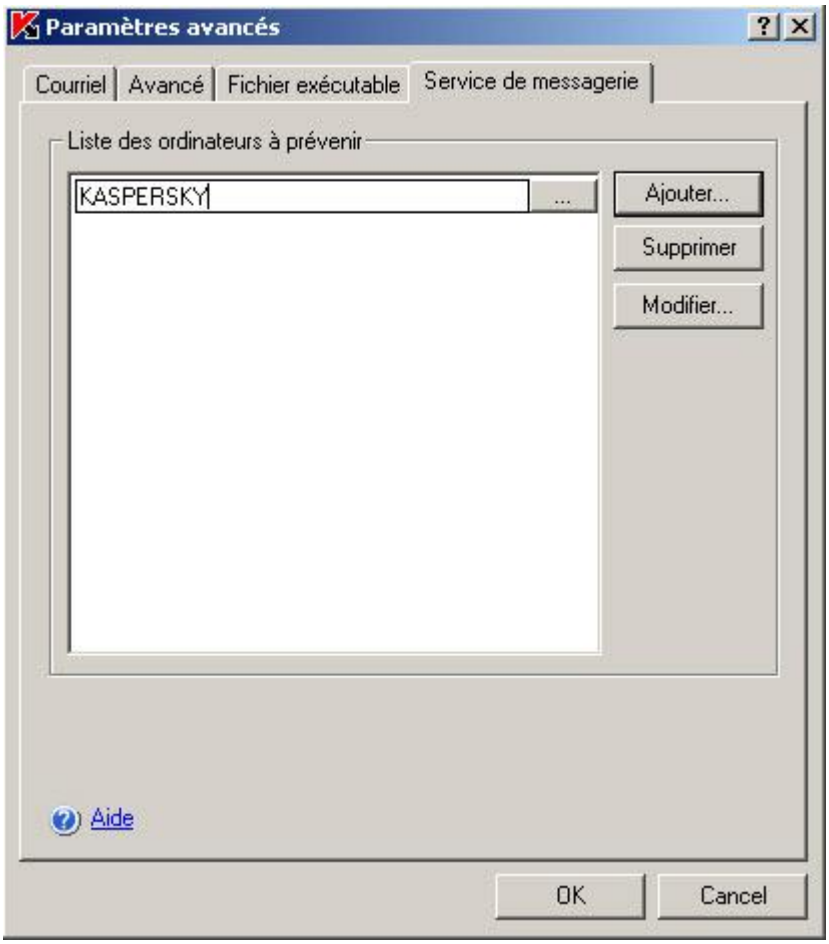


*Illustration 89. Boîte de dialogue **Configuration avancée**, onglet **Service de messagerie***

d. Pour le lancement d'un fichier exécutable, sélectionnez le fichier sur le disque local du serveur protégé qui sera exécuté sur le serveur lorsque l'événement se produira dans l'onglet **Fichier exécutable** ou saisissez le chemin d'accès à ce dernier. Saisissez le nom et le mot de passe de l'utilisateur sous le compte duquel le fichier sera exécuté (cf. ill. ci-après).

   En indiquant le chemin d'accès au fichier exécutable, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

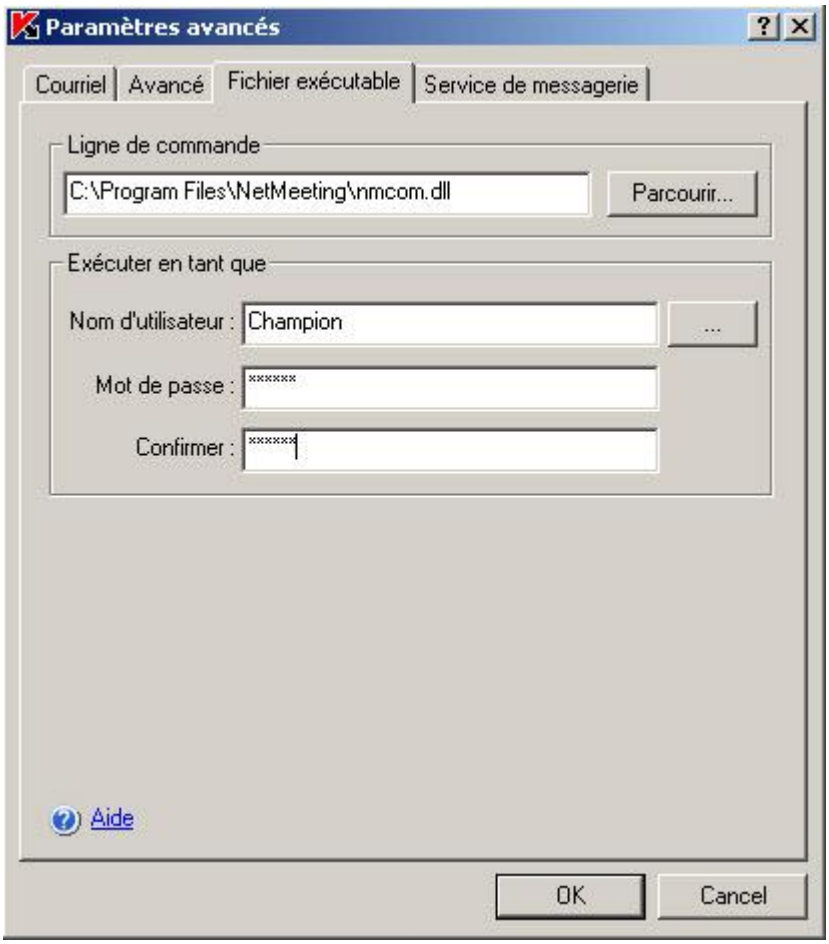


*Illustration 90. Boîte de dialogue **Paramètres avancés**, onglet **Fichier exécutable***

Si vous souhaitez limiter le nombre de messages de notification en fonction d'événements d'un même type par unité de temps, cochez la case **Ne pas répéter la notification plus de** sous l'onglet **Avancé** et indiquez la valeur souhaitée par unité de temps (cf. ill. ci-après).

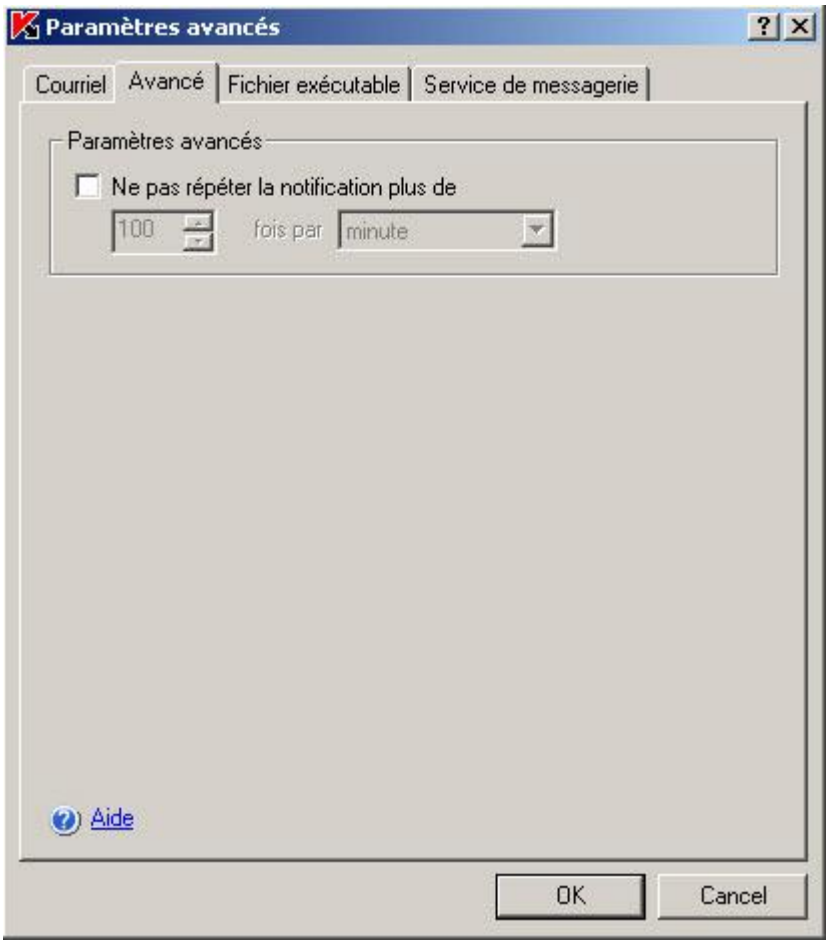


*Illustration 91. Boîte de dialogue **Paramètres avancés**, onglet **Avancé***

4. Cliquez sur **OK**.

Tableau 36. Champs d'information sur les événements

CHAMP	DESCRIPTION
%EVENT_TYPE%	Type d'événement
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%EVENT_SEVERITY%	Degré d'importance de l'événement.
%OBJECT%	Nom de l'objet (dans les tâches de protection en temps réel et d'analyse à la demande) Dans la tâche **Mise à jour des modules de l'application**, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.
%VIRUS_NAME%	Nom de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande).
%VIRUS_TYPE%	Type de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande)
%USER_COMPUTER%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'ordinateur dont l'utilisateur a sollicité un objet sur le serveur.
%USER_NAME%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'utilisateur qui a sollicité un objet sur le serveur.
%FROM_COMPUTER%	Nom du serveur protégé d'où provient la notification
%REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements)
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement erreur interne de la tâche)
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)

BOITES DE DIALOGUE : NOTIFICATIONS

DANS CETTE SECTION DE L'AIDE

PROPRIETES DE KASPERSKY ANTI-VIRUS : ONGLET NOTIFICATIONS

Cet onglet affiche les paramètres de notification des utilisateurs et des administrateurs sur l'état de la protection antivirus sur le serveur, sur la base antivirus ainsi que sur les résultats des tâches et d'autres événements enregistrés par le fonctionnement de l'application.

La liste des types d'événements dont vous pouvez des notifications est présentée dans la partie supérieure de l'onglet.

Sélectionnez dans la liste le type d'événement dont vous souhaitez configurer et spécifiez ses paramètres. Pour sélectionner plus d'un type d'événement, utilisez les touches **Maj** et **Ctrl**.

Dans la section **Informer les utilisateurs**, sélectionnez la méthode de notification de l'utilisateur utilisée quand un événement se produit. Pour ce faire, cochez les cases :

- **Informer par les services des terminaux** : les utilisateurs des services Terminal Server seront informés de l'événement.
- **Informer par commande NET SEND** : en cas d'événement, une notification sera envoyée par **NET SEND**.

Créer le texte du message. Pour ce faire, cliquez sur **Texte du message**.

La section **Informer les utilisateurs** n'est disponible que pour les types d'événement liés directement aux actions de l'utilisateur. Par exemple, la tentative de copie d'un objet infecté sur le serveur ou l'accès à ce même objet génère un événement de **Menace détectée**. Ces types d'événements contiennent généralement des informations sur l'utilisateur.

Dans la section **Informer les administrateurs**, sélectionnez les méthodes de notification des administrateurs pour les types d'événements sélectionnés. Pour ce faire, cochez les cases :

- **Informer par commande NET SEND** : l'administrateur recevra une notification d'événement via **NET SEND**.
- **Lancer le fichier exécutable** : si un événement se produit sur le serveur sécurisé, ce programme est lancé sous le compte utilisateur spécifié.
- **Informer par un courriel** : l'administrateur recevra une notification d'événement par le serveur de messagerie.

Créer le texte du message. Pour ce faire, cliquez sur **Texte du message**.

Configurez les méthodes de notification sélectionnées. Pour ce faire, cliquez sur **Configuration**.

Vérifiez que les paramètres des services qui distribuent les notifications sont activés à la fois sur le serveur sécurisé et les postes de travail des utilisateurs.

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs 262

Moyens de notification de l'administrateur et des utilisateurs 264

TEXTE DU MESSAGE (FENETRE)

Cette fenêtre permet de créer un modèle pour les messages utilisés pour les notifications d'événements.

Entrez le texte du message. Le texte peut inclure des informations sur l'événement enregistré. Pour ce faire, choisissez les champs (cf. tableau ci-dessous) à ajouter au modèle dans la liste déroulante ouverte avec le bouton **Macro.**

Pour restaurer le texte prévu par défaut dans les notifications, cliquez sur **Par défaut**.

Tableau 37. Paramètres génériques pour les notifications sur l'événement enregistré

CHAMP	DESCRIPTION
%EVENT_SEVERITY%	Degré d'importance de l'événement.
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)
%EVENT_TYPE%	Type d'événement
%USER_COMPUTER%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'ordinateur dont l'utilisateur a sollicité un objet sur le serveur.
%OBJECT%	Nom de l'objet (dans les tâches de protection en temps réel et d'analyse à la demande) Dans la tâche **Mise à jour des modules de l'application**, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.
%USER_NAME%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'utilisateur qui a sollicité un objet sur le serveur.
%VIRUS_NAME%	Nom de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande).
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement erreur interne de la tâche)
%REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements)
%FROM_COMPUTER%	Nom du serveur protégé d'où provient la notification
%VIRUS_TYPE%	Type de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande)

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs 262

Moyens de notification de l'administrateur et des utilisateurs 264

CONFIGURATION DES NOTIFICATIONS : ONGLET SERVICE DE MESSAGERIE

Cet onglet permet de créer la liste des postes auxquels les notifications seront envoyées via NET SEND.

Vous pouvez modifier la liste des ordinateurs destinataires à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Il ne faut utiliser que les noms réseau des ordinateurs.

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs 262

Moyens de notification de l'administrateur et des utilisateurs 264

CONFIGURATION DES NOTIFICATIONS : ONGLET COURRIEL

Cet onglet permet de configurer les paramètres utilisés pour envoyer des notifications par courrier électronique sur les événements enregistrés. Dans la zone **Paramètres de notification par courriel**, spécifiez :

- **Adresse du destinataire** : Adresse de messagerie du destinataire de la notification. Vous pouvez indiquer plusieurs adresses séparées par un point-virgule.
- **Serveur SMTP** : Adresse du serveur de messagerie. Vous pouvez utiliser une adresse IP ou le nom de l'ordinateur sur le réseau.
- **Port SMTP** : Numéro de port du serveur SMTP. Le numéro 25 correspond au port par défaut.
- **Objet** : Ligne objet du message.
- **De** : Adresse de l'expéditeur.

Si le serveur SMTP nécessite une authentification, indiquez ses données d'identification dans les zones **Paramètres d'authentification** : cochez la case **Authentification SMTP requise** et complétez les zones **Nom d'utilisateur**, **Mot de passe** et **Confirmer**.

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs..... 262

Moyens de notification de l'administrateur et des utilisateurs..... 264

CONFIGURATION DES NOTIFICATIONS : ONGLET FICHIER EXECUTABLE

Cet onglet affiche les paramètres permettant de déterminer quel programme sera démarré si un événement se produit sur le serveur.

Spécifiez le fichier à exécuter dans la zone **Ligne de commande**. Indiquez le chemin et le nom de fichier manuellement. Le fichier doit être enregistré sur une unité locale du serveur sécurisé ou sur un ordinateur équipé du produit Anti-Virus 8.0 pour Windows Servers Enterprise Edition.

Dans les zones **Exécuter en tant que**, entrez un nom d'utilisateur avec des privilèges suffisants pour exécuter le fichier, ou sélectionnez-le dans la liste ouverte avec le bouton  . Spécifiez le mot de passe et confirmez-le.

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs..... 262

Moyens de notification de l'administrateur et des utilisateurs..... 264

CONFIGURATION DES NOTIFICATIONS : ONGLET AVANCE

Cet onglet permet de limiter le nombre de messages envoyés pour un certain type d'événement, pendant une durée de temps spécifique. Pour ce faire, sélectionnez **Ne pas répéter la notification** plus de et spécifiez le nombre et limite de durée souhaités.

VOIR EGALEMENT

Moyens de notification de l'administrateur et des utilisateurs..... 262

Moyens de notification de l'administrateur et des utilisateurs..... 264

ADMINISTRATION DE LA SAUVEGARDE HIERARCHIQUE

Kaspersky Anti-Virus permet d'analyser les fichiers placer dans les sauvegardes hiérarchiques et dans les systèmes de sauvegarde.

DANS CETTE SECTION DE L'AIDE

PRESENTATION DU SYSTEME D'ADMINISTRATION DE LA SAUVEGARDE HIERARCHIQUE

Le système d'administration du la sauvegarde hiérarchique (Hierarchical Storage Management, HSM) (ci-après système HSM) permet de déplacer des données entre des disques locaux rapides et des périphériques lents de conservation de données à long terme. Malgré les avantages évidents des périphériques de rappel rapides, leur utilisation reste chère pour la majorité des entreprises. Les systèmes HSM garantissent le transfert des informations non utilisées vers des périphériques bon marché de stockage à distance, ce qui réduit les dépenses de la société.

Les systèmes HSM enregistrent une partie des informations dans des référentiels distants et les restaure en cas de besoin. Les systèmes HSM assurent un contrôle permanent de l'utilisation des fichiers et définissent ceux qui peuvent être déplacés dans le stockage distant et ceux qu'il est préférable de laisser sur les périphériques de stockage local. Les fichiers sont déplacés vers le stockage distant s'ils ne sont pas sollicités pendant une période définie. Si l'utilisateur sollicite le fichier situé dans le stockage distant, celui est transféré à nouveau vers le disque local. Ce principe garantit à l'utilisateur un accès rapide à un volume important d'informations qui est bien supérieur à la capacité du disque.

Lors du déplacement d'un fichier depuis le disque local vers le stockage distant, le système HSM conserve le lien vers l'emplacement effectif de ce fichier. En cas de sollicitation d'un fichier contenant un lien, le système définit l'emplacement des données sur le périphérique d'archives. Le remplacement des fichiers par des liens dans l'emplacement de stockage permet d'obtenir un stockage à la capacité quasiment illimitée.

Certains systèmes HSM permettent de conserver une partie des fichiers dans le stockage local. Dans ce cas, une grande partie du fichier est déplacée vers stockage distant tandis qu'une petite partie du fichier source reste sur le stockage local.

Les systèmes HSM proposent deux méthodes d'accès aux informations situées dans le stockage hiérarchique :

- points de traitement réitéré ;
- attributs élargis du fichier.

CONFIGURATION DE L'ACCES A LA SAUVEGARDE HIERARCHIQUE

Les paramètres de fonctionnement du système HSM dépendent du mode d'accès à la sauvegarde hiérarchique qu'il prend en charge.

Pour désigner le mode d'accès au stockage hiérarchique, procédez comme suit :

1. Ouvrez la boîte de dialogue de configuration. Pour ce faire, réalisez une des opérations suivantes :

   - Dans l'arborescence de la console, ouvrez le menu contextuel du nom du composant enfichable de Kaspersky Anti-Virus et choisissez l'option **Sauvegarde hiérarchique** ;

   - Dans l'arborescence de la console, sélectionnez le nom du composant enfichable de Kaspersky Anti-Virus et choisissez l'option **Sauvegarde hiérarchique** sur le volet d'accès rapide.

   La fenêtre **Paramètres du système HSM** (cf. ill. ci-après) s'ouvre.

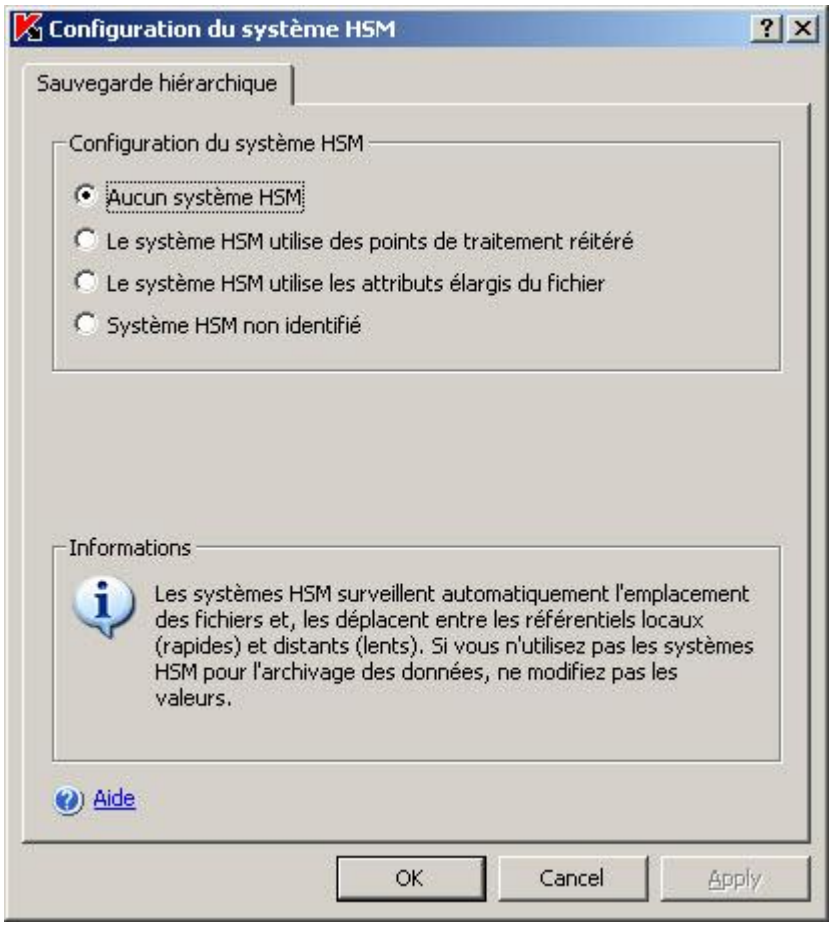


Illustration 92. Paramètres des systèmes HSM

2. Sous l'onglet **Sauvegarde hiérarchique**, indiquez le **Type d'accès au stockage hiérarchique**.

   Les paramètres d'accès au stockage hiérarchique varient en fonction du système HSM utilisé. Pour bien configurer ces paramètres, il faut absolument connaître comment le système HSM définit l'emplacement du fichier analysé. Pour obtenir les informations indispensables, consultez la documentation relative au système HSM utilisé.

   Vous avez le choix entre les options suivantes pour l'accès au stockage hiérarchique :

   - **Aucun système HSM**.

   - **Le système HSM utilise des points de traitement réitéré**.

   - **Le système HSM utilise les attributs élargis du fichier**.

- **Système HSM non identifié**.

3. Cliquez sur le bouton **OK** pour conserver le paramètre désigné.

Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut du paramètre **Type d'accès à la sauvegarde hiérarchique** (**Aucun système HSM**).

IMPORTATION ET EXPORTATION DES PARAMETRES

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE L'IMPORTATION ET DE L'EXPORTATION DES PARAMETRES

Si vous devez attribuer la même valeur à plusieurs paramètres de Kaspersky Ani-Virus sur plusieurs serveurs protégés, vous pouvez configurer Kaspersky Anti-Virus sur un serveur, exporter la configuration au format XML puis importer ce fichier dans les copies de Kaspersky Anti-Virus installées sur les autres serveurs.

Vous pouvez enregistrer tous les paramètres de Kaspersky Anti-Virus ou les paramètres des composants distincts.

En cas d'exportation de tous les paramètres de Kaspersky Anti-Virus, les paramètres généraux de Kaspersky Anti-Virus et les paramètres des composants suivants sont enregistrés dans le fichier :

- Protection en temps réel des fichiers.
- Analyse des scripts.
- Analyse à la demande :
- Mise à jour des base et des modules logiciels de Kaspersky Anti-Virus.
- Quarantaine.
- Sauvegarde.
- Journaux
- Notifications.
- Zone de confiance.

  Enregistrez dans le fichier les paramètres généraux de Kaspersky Anti-Virus et les permissions des comptes utilisateur.

Kaspersky Anti-Virus n'exporte pas les paramètres des tâches de groupe.

Kaspersky Anti-Virus exporte tous les mots de passe qu'il utilise, par exemple les données des comptes pour l'exécution des tâches ou la connexion au serveur proxy, et les conserve dans le fichier de configuration dans une forme cryptée. Ils peuvent être importés uniquement par Kaspersky Anti-Virus sur ce même ordinateur, s'il n'y a pas eu de réinstallation ou de mise à jour. Kaspersky Anti-Virus sur un autre ordinateur ne les importera pas. Après l'importation des paramètres sur un autre ordinateur, vous devrez saisir tous les mots de passe manuellement.

Si une stratégie de Kaspersky Administration Kit est active au moment de l'exportation des paramètres, Kaspersky Anti-Virus exporte non pas les valeurs appliquées par la stratégie mais celles en vigueur avant son application.

Vous pouvez importer les paramètres depuis le fichier de configuration qui contient les paramètres uniquement de certains composants de Kaspersky Anti-Virus (par exemple, créé dans une version de Kaspersky Anti-Virus sans la totalité des composants). Après l'importation des paramètres dans Kaspersky Anti-Virus, seuls les paramètres repris dans le fichier de configuration sont modifiés. Les autres paramètres conservent leur valeur antérieure.

Les paramètres importés ne sont pas appliqués aux tâches en exécution. Ils sont appliqués uniquement au lancement suivant. Il est conseillé d'interrompre les tâches des composants avant d'importer les paramètres.

EXPORTATION DES PARAMETRES.

Pour exporter les paramètres dans un fichier de configuration, procédez comme suit :

1. Si vous avez modifié les paramètres dans la console de Kaspersky Anti-Virus avant d'exporter les paramètres, cliquez sur le bouton **Enregistrer** pour enregistrer leurs nouvelles valeurs.

2. Exécutez une des actions suivantes :

   - pour importer tous les paramètres de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus dans l'arborescence de la console et sélectionnez la commande **Exporter les paramètres** ;

   - Pour exporter les paramètres d'un composant individuel, ouvrez le menu contextuel du nœud correspond à cette fonction dans l'arborescence de la console et sélectionnez la commande **Exporter les paramètres**.

   La fenêtre de bienvenue de l'Assistant d'exportation des paramètres s'ouvre.

3. Suivez les instructions affichées dans les fenêtres de l'Assistant : indiquez le nom du fichier de configuration dans lequel vous souhaitez enregistrer les paramètres ainsi que le chemin d'accès à celui-ci.

   Pour désigner le chemin d'accès, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

   Si une stratégie de Kaspersky Administration Kit est active au moment de l'exportation des paramètres, Kaspersky Anti-Virus exporte non pas les valeurs appliquées par la stratégie mais celles en vigueur avant son application.

4. Dans la fenêtre **Fin de l'exportation** cliquez sur le bouton **OK** afin de fermer l'Assistant d'exportation des paramètres.

IMPORTATIONS DES PARAMETRES

Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :

1. Exécutez une des actions suivantes :

   - pour importer tous les paramètres de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus dans l'arborescence de la console et sélectionnez la commande **Importer les paramètres** ;

   - pour importer les paramètres d'un composant individuel, ouvrez le menu contextuel du nœud correspond à cette fonction dans l'arborescence de la console et sélectionnez la commande **Importer les paramètres**.

   La fenêtre de bienvenue de l'Assistant d'importation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : identifiez le fichier de configuration que vous souhaitez importer.

Une fois que les paramètres de Kaspersky Anti-Virus et de ses composants auront été importés, vous ne pourrez plus revenir à leurs valeurs antérieures.

3. Dans la fenêtre **Fin de l'importation** cliquez sur le bouton **OK** afin de fermer l'Assistant d'importation des paramètres.

4. Dans la barre d'outils de la console de Kaspersky Anti-Virus, cliquez sur le bouton **Mettre à jour** pour afficher les paramètres importés.

Kaspersky Anti-Virus n'importe pas les mots de passe (les données des comptes utilisateur pour l'exécution de tâches ou la connexion au serveur proxy) d'un fichier créé sur un autre ordinateur ou sur ce même ordinateur après une réinstallation ou de mise à jour de Kaspersky Anti-Virus. Après la fin de l'importation, vous devrez saisir les mots de passe manuellement.

ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA LA LIGNE DE COMMANDE

DANS CETTE SECTION DE L'AIDE

ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA LA LIGNE DE COMMANDE

Vous pouvez exécuter les principales instructions d'administration de Kaspersky Anti-Virus via la ligne de commande du serveur protégé, si vous avez inclus le composant **Utilitaire de ligne de commande** dans la liste des composants à installer lors de l'installation de Kaspersky Anti-Virus.

La ligne de commande permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Anti-Virus.

Certaines des instructions de Kaspersky Anti-Virus sont exécutées en mode synchrone : l'administration revient à la console uniquement après la fin de l'exécution de l'instruction ; d'autres instructions sont exécutées en mode asynchrone : l'administration revient à la console directement après le lancement de l'instruction.

Pour interrompre l'exécution d'une commande en mode synchrone,

appuyez sur la combinaison de touches **Ctrl**+**C**.

Lors de la saisie d'une instruction de Kaspersky Anti-Virus, respectez les règles suivantes :

- saisissez les paramètres et les instructions en majuscules ou en minuscules ;
- séparez les paramètres par des espaces ;
- si le nom du fichier attribué en tant que valeur d'un paramètre contient un espace, alors saisissez ce nom (et son chemin d'accès) entre guillemets, par exemple : "C:\TEST\test cpp.exe" ;
- le cas échéant, vous pouvez utiliser des caractères génériques dans les noms des fichiers ou des chemins, par exemple : " C:\Temp\Temp*\ ", " C:\Temp\Temp???.doc ", " C:\Temp\Temp*.doc "

La ligne de commande vous permet d'effectuer toutes les opérations de gestion et d'administration de Kaspersky Anti-Virus (cf. tableau ci-dessous).

Tableau 38. Instructions de Kaspersky Anti-Virus

INSTRUCTION	DESCRIPTION
KAVSHELL HELP (cf. page 282)	Affiche l'aide sur les instructions de Kaspersky Anti-Virus.
KAVSHELL START (cf. page 283)	Lance le service de Kaspersky Anti-Virus.
KAVSHELL STOP (cf. page 283)	Arrête le service de Kaspersky Anti-Virus.
KAVSHELL SCAN (cf. page 283)	Crée et lance une tâche d'analyse à la demande temporaire dont la couverture d'analyse et les paramètres de sécurité sont définis par les arguments de l'instruction.
KAVSHELL SCANCRITICAL (cf. page 287)	Lance la tâche prédéfinie **Analyse des zones critiques**.
KAVSHELL TASK (cf. page 288)	Lance/suspend/relance/arrête la tâche indiquée en mode asynchrone/rend l'état actuelle de la tâche/les statistiques de la tâche.
KAVSHELL RTP (cf. page 289)	Lance ou arrête toutes les tâches de protection en temps réel.
KAVSHELL UPDATE (cf. page 290)	Lance la tâche de mise à jour des bases de Kaspersky Anti-Virus selon les paramètres définis à l'aide des arguments de l'instruction.
KAVSHELL ROLLBACK (cf. page 292)	Remet les bases à l'état antérieur à la mise à jour.
KAVSHELL LICENSE (cf. page 293)	Gère les licences.
KAVSHELL TRACE (cf. page 294)	Active ou désactive la création du fichier de traçage, gère les paramètres du fichier de traçage.
KAVSHELL DUMP (cf. page 295)	Active ou désactive la création d'un vidage de mémoire des processus de Kaspersky Anti-Virus en cas d'arrêt suite à une erreur.
KAVSHELL IMPORT (cf. page 296)	Importe les paramètres généraux de Kaspersky Anti-Virus, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration créé au préalable.
KAVSHELL EXPORT (cf. page 297)	Exporte tous les paramètres de Kaspersky Anti-Virus et des tâches existantes dans un fichier de configuration.

AFFICHAGE DE L'AIDE SUR LES INSTRUCTIONS DE KASPERSKY ANTI-VIRUS KAVSHELL HELP

Pour obtenir la liste de toutes les instructions de Kaspersky Anti-Virus, saisissez une des commandes suivantes :

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une instruction, saisissez une des instructions suivantes :

```
KAVSHELL HELP <instruction>

KAVSHELL <instruction> /?
```

Exemples d'instruction KAVSHELL HELP

Pour consulter des informations plus détaillées sur l'instruction KAVSHELL SCAN, exécutez l'instruction suivante :

```
KAVSHELL HELP SCAN
```

LANCEMENT ET ARRET DU SERVICE DE KASPERSKY ANTI-VIRUS. KAVSHELL START, KAVSHELL STOP

Pour lancer le service de Kaspersky Anti-Virus, utilisez l'instruction `KAVSHELL START`.

Le lancement du service de Kaspersky Anti-Virus s'accompagne par défaut de l'activation de la **Protection en temps réel des fichiers**, de l'**Analyse des scripts**, de l'**Analyse au démarrage du système** ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Pour arrêter le service de Kaspersky Anti-Virus, utilisez l'instruction `KAVSHELL STOP`.

Codes de retour des instructions KAVSHELL START et KAVSHELL STOP (cf. page 298).

ANALYSE DU SECTEUR INDIQUE. KAVSHELL SCAN

Pour lancer la tâche d'analyse de secteurs définis du serveur protégé, utilisez l'instruction `KAVSHELL SCAN`. Les arguments de cette instruction définissent les paramètres de la tâche (couverture d'analyse et paramètres de sécurité).

La tâche d'analyse à la demande lancée à l'aide de l'instruction `KAVSHELL SCAN` est temporaire. Elle apparaît dans la console de Kaspersky Anti-Virus uniquement pendant son exécution (la console de Kaspersky Anti-Virus ne vous permet pas de consulter les paramètres de la tâche). Le journal d'exécution de la tâche est enregistré en même temps ; il apparaît dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Anti-Virus. De même, les stratégies de l'application Kaspersky Administration Kit peuvent être appliquées aux tâches d'analyse à la demande créées dans la console de Kaspersky Anti-Virus et aux tâches créées et lancées à l'aide de l'instruction SCAN. Pour en savoir plus sur l'administration de Kaspersky Anti-Virus à l'aide de Kaspersky Administration Kit, lisez la rubrique "Administration de Kaspersky Anti-Virus via Kaspersky Administration Kit" (cf. page 304).

L'instruction `KAVSHELL SCAN` est exécutée en mode synchrone.

Vous pouvez employer une variable système pour désigner le chemin dans la tâche d'analyse à la demande. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction KAVSHELL SCAN avec les privilèges de cet utilisateur.

Pour lancer une tâche existante d'analyse à la demande depuis la ligne de commande, utilisez l'instruction KAVSHELL TASK (cf. page 288).

Syntaxe de l'instruction KAVSHELL SCAN

```
KAVSHELL SCAN <zones d'analyse> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:< nom du fichier contenant la liste des zones d'analyse >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"masque">] [/ES:<taille>] [/ET:<nombre de
secondes>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<nom du fichier du
journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>] [/ANSI]
```

L'instruction KAVSHELL SCAN contient les arguments obligatoires et complémentaires dont l'utilisation n'est pas obligatoire (cf. tableau ci-dessous).

Exemples d'instruction KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.ff?;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL /NOISWIFT:1 /W:report.log

KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Tableau 39. Syntaxe de l'instruction KAVSHELL SCAN et destination de ces arguments

CLE	DESCRIPTION
Couverture de l'analyse. Argument obligatoire.	
<fichiers> <répertoires> <chemin de réseau>	Couverture d'analyse : liste de fichiers, de répertoires, de chemins de réseau et de zones prédéfinies. Indiquez les chemins de réseau au format UNC (Universal Naming Convention). Dans l'exemple suivant, le répertoire Folder4 est indiqué sans son chemin d'accès. Il se trouve dans le répertoire d'où l'instruction KAVSHELL est exécutée : KAVSHELL SCAN Folder4 Si le nom de l'objet à analyser contient des espaces, il faudra l'indiquer entre guillemets. Si vous avez choisi un dossier, Kaspersky Anti-Virus analysera également tous les sous-dossiers du dossier en question. Pour analyser un groupe de fichiers, vous pouvez utiliser les caractères * ou ?
/MEMORY	Analyse les objets dans la mémoire vive.
/SHARED	Analyse les dossiers partagés sur le serveur.
/STARTUP	Analyse les objets de démarrage.
/REMDRIVES	Analyse les disques amovibles.
/FIXDRIVES	Analyse les disques durs.
/MYCOMP	Analyse tous les secteurs du serveur protégé.
/L: <nom du fichier contenant la liste des couvertures d'analyse>	Nom du fichier contenant la liste des couvertures d'analyse, y compris le chemin d'accès complet au fichier. Les zones d'analyse dans le fichier sont séparées par un retour à la ligne. Vous pouvez indiquer les couvertures d'analyse prédéfinies comme indiqué dans l'exemple ci-après de fichier contenant la liste des couvertures d'analyse : C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Objets à analyser (File types). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus analysera les objets en fonction du format.	
/FA	Analyse tous les objets
/FC	Analyse les objets en fonction du format (par défaut). Kaspersky Anti-Virus analyse uniquement les objets dont le format figure dans la liste des formats propres aux objets pouvant être infectés.
/FE	Analyse les objets en fonction de l'extension. Kaspersky Anti-Virus analyse uniquement les objets dont l'extension figure dans la liste des extensions propres aux objets pouvant être infectés.
/NEWONLY	Analyser uniquement les nouveaux fichiers et les fichiers modifiés (cf. page 382). Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus analysera tous les objets.
/AI: **Actions à exécuter sur les objets infectés**. Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus appliquera l'action **Ignorer**.	
DISINFECT	Réparer, ignorer si la réparation est impossible
DISINFDEL	Réparer, supprimer si la réparation est impossible

CLE	DESCRIPTION
DELETE	Supprimer Les paramètres DISINFECT et DELETE ont été préservés dans la version actuelle de Kaspersky Anti-Virus pour garantir la compatibilité avec les versions antérieures. Vous pouvez utiliser ces paramètres au lieu des arguments de commande /AI: et /AS:. Dans ce cas, Kaspersky Anti-Virus ne traitera pas les objets suspects.
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée
/AS: **Actions à exécuter sur les objets suspects** (**actions**). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus appliquera l'action **Ignorer**.	
QUARANTINE	Quarantaine
DELETE	Supprimer
REPORT	Envoie un rapport (par défaut)
AUTO	Exécute l'action recommandée
Exclusions (Exclusions)	
/E:ABMSPO	L'argument exclut les objets composés des types suivants : A : archives SFX ; B : bases de données de messagerie électronique ; M : message de texte plat ; S : archives (y compris les archives SFX) ; P : objets compactés ; O : objets OLE intégrés.
/EM:<"masque">	Exclut les fichiers en fonction du masque. Vous pouvez définir plusieurs masques, par exemple : EM:"*.txt;*.png; C\Videos*.avi".
/ET:<nombre de secondes>	Arrête le traitement de l'objet s'il dure plus longtemps que la durée indiquée en secondes. Par défaut, l'analyse n'est pas limitée dans le temps.
/ES:<taille>	Exclut de l'analyse les objets composés dont la taille, en mégaoctets, dépasse la valeur de l'argument <taille>. Par défaut, Kaspersky Anti-Virus analyse les objets de n'importe quelle taille.
/TZOFF	Annule les exclusions de la zone de confiance.
/AI: **actions sur les fichiers autonomes** (Options)	
/SKIP	Ignore les fichiers autonomes.
/RESIDENT	Analyser seulement la partie résidente du fichier.
/SCAN	Analyse tous les fichiers autonomes.
/SCAN=<jours>	Analyse uniquement les fichiers autonomes sollicités par Kaspersky Anti-Virus durant la période indiquée (jours).

CLE	DESCRIPTION
/SCAN NORECALL	Analyse les fichiers autonomes sans les copier, si possible, sur le disque dur.
/SCAN=<jours>	Analyse uniquement les fichiers autonomes sollicités par Kaspersky Anti-Virus durant la période indiquée (jour) sans les copier, dans la mesure du possible, sur le disque dur.
Paramètres complémentaires (Options)	
/NOICHECKER	Désactive l'utilisation de la technologie iChecker (activée par défaut).
/NOISWIFT	Désactive l'utilisation de la technologie iSwift (activée par défaut).
/ANALYZERLEVEL:<niveau d'analyse>	Active l'utilisation de l'analyseur heuristique (cf. page 393), configure le niveau d'analyse. L'analyse heuristique peut être effectuée à plusieurs niveaux : 1 – superficielle ; 2 – moyenne ; 3 – profonde. Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus n'utilisera pas l'analyseur heuristique.
/NOCHECKMSSIGN	Ne vérifie pas la signature de Microsoft Corporation dans les fichiers (désactivé par défaut).
/ALIAS:<nom alternatif de la tâche>	L'argument permet d'attribuer un nom temporaire à la tâche d'analyse à la demande. Ce nom permet de consulter la tâche durant son exécution, par exemple pour consulter les statistiques à l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Anti-Virus. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple update_1234. Dans la console de Kaspersky Anti-Virus, la tâche reçoit le nom Scan objects (<date heure>), par exemple, Scan objects 8/16/2007 5:13:14 PM.
Paramètres des journaux d'exécution des tâches (Report settings)	
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Anti-Virus enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Anti-Virus dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier de journal existant. Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de journal, il n'interrompt pas l'exécution de l'instruction mais affiche pas de message sur l'erreur.

CLE	DESCRIPTION
/ANSI	La clé permet d'enregistrer les événements dans le journal d'exécution des tâches dans l'encodage ANSI. La clé ANSI ne sera pas appliquée, si la clé W n'est pas définie. Si la clé ANSI n'est pas spécifiée, alors le journal d'exécution des tâches s'effectue dans l'encodage UNICODE.

Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL298 (cf. page)

LANCEMENT DE LA TACHE ANALYSE DES ZONES CRITIQUES. KAVSHELL SCANCRITICAL

Utilisez l'instruction `KAVSHELL SCANCRITICAL` pour lancer la tâche prédéfinie d'analyse à la demande **Analyse des zones critiques** selon les paramètres définis dans la console de Kaspersky Anti-Virus.

Vous pouvez employer une variable système pour désigner le chemin dans la tâche d'analyse à la demande. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL SCAN` avec les privilèges de cet utilisateur.

Syntaxe de l'instruction KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<nom du fichier du journal d'exécution de la tâche>]
```

Exemple de l'instruction KAVSHELL SCANCRITICAL

Pour exécuter la tâche d'analyse à la demande **Analyse des zones critiques** ; enregistrer le journal d'exécution de la tâche dans le fichier scancritical.log dans le répertoire en cours, exécutez l'instruction suivante :

```
KAVSHELLSCANCRITICAL /W:scancritical.log
```

Vous pouvez configurer l'emplacement du fichier journal d'exécution de la tâche en fonction de la syntaxe de l'argument (cf. tableau ci-dessous).

Syntaxe de l'argument `/W` de l'instruction `KAVSHELL SCANCRITICAL`

CLE	DESCRIPTION
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Anti-Virus enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Anti-Virus dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier de journal existant. Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de journal, il n'interrompt pas l'exécution de l'instruction mais affiche pas de message sur l'erreur.

Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL (cf. page 298).

ADMINISTRATION DE LA TACHE INDIQUEE EN MODE ASYNCHRONE. KAVSHELL TASK

A l'aide de l'instruction `KAVSHELL TASK`, vous pouvez administrer la tâche indiquée : lancer, suspendre, reprendre ou arrêter la tâche ainsi que consulter son état actuel et ses statistiques. L'instruction est exécutée en monde asynchrone.

A l'aide de l'instruction vous pouvez administrer les tâche créées dans Kaspersky Administration Kit.

Instruction de la commande KAVSHELL TASK

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemples de l'instruction KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

L'instruction `KAVSHELL TASK` peut être exécutée sans clé de licence ou avec une ou plusieurs clés de licence (cf. tableau ci-dessous).

Tableau 40. Instruction de la commande KAVSHELL TASK

CLE	DESCRIPTION
Sans argument	L'instruction renvoie la liste de toutes les tâches existantes de Kaspersky Anti-Virus. La liste contient les champs : nom alternatif de la tâche, catégorie de tâche (tâche prédéfinie et tâche définie par utilisateur) et état actuel de la tâche.
<nom alternatif de la tâche>	Au lieu du nom de la tâche dans la commande SCAN TASK, utilisez son nom alternatif : bref nom complémentaire attribué aux tâches par Kaspersky Anti-Virus. Pour consulter les noms alternatifs des tâches dans Kaspersky Anti-Virus, saisissez l'instruction KAVSHELL TASK sans argument.
/START	Lance la tâche indiquée en mode asynchrone
/STOP	Arrête la tâche indiquée
/PAUSE	Suspend la tâche indiquée
/RESUME	Relance la tâche indiquée en mode asynchrone
/STATE	Récupère l'état actuel de la tâche (par exemple, **Exécution en cours**, **Complétée**, **En pause**, **Arrêtée**, **Echec**, **Lancement en cours**, **Restauration en cours**)
/STATISTICS	Affiche les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche jusqu'à ce moment.

Codes de retour de l'instruction KAVSHELL TASK (cf. page 299)

LANCEMENT ET ARRET DES TACHES DE PROTECTION EN TEMPS REEL. KAVSHELL RTP

L'instruction `KAVSHELL RTP` vous permet de lancer ou d'arrêter toutes les tâches de protection en temps réel.

Syntaxe de l'instruction KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Exemples de l'instruction KAVSHELL RTP

Pour lancer toutes les tâches de protection en temps réel, exécutez l'instruction suivante :

```
KAVSHELL RTP /START
```

L'instruction `KAVSHELL RTP` peut inclure n'importe quel des deux arguments obligatoires (cf. tableau ci-dessous).

Arguments de l'instruction KAVSHELL RTP

CLE	DESCRIPTION
/START	Lance toutes les tâches de protection en temps réel
/STOP	Arrête toutes les tâches de protection en temps réel

Codes de retour de l'instruction KAVSHELL RTP (cf. page 299)

LANCEMENT DE LA TACHE DE MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS. KAVSHELL UPDATE

La commande `KAVSHELL UPDATE` vous permet de lancer la tâche de mise à jour des bases de Kaspersky Anti-Virus en mode synchrone.

La tâche de mise à jour des bases de Kaspersky Anti-Virus, lancée à l'aide de la commande `KAVSHELL UPDATE`, est une tâche temporaire. Elle est affichée dans la console de Kaspersky Anti-Virus uniquement pendant son exécution. Le journal d'exécution de la tâche est enregistré en même temps ; il est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Anti-Virus. Les stratégies de l'application Kaspersky Administration Kit peuvent s'appliquer aux tâches de mise à jour créées et lancées via l'instruction `KAVSHELL UPDATE`, ainsi qu'aux tâches de mises à jour créées dans la console de Kaspersky Anti-Virus. Pour en savoir plus sur l'administration de Kaspersky Anti-Virus sur les serveurs à l'aide de Kaspersky Administration Kit, lisez la rubrique "Administration de Kaspersky Anti-Virus via Kaspersky Administration Kit" (cf. page 304).

Vous pouvez utiliser des variables système pour indiquer la source des mises à jour dans cette tâche. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL UPDATE` avec les privilèges de cet utilisateur.

Syntaxe de l'instruction KAVSHELL UPDATE

```
KAVSHELL UPDATE < Source de la mise à jour | /AK | /KL> [/NOUSEKL]
[/PROXY:<adresse>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nom d'utilisateur>]
[/PROXYPWD:<mot de passe>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<nombre de secondes>] [/REG:<code iso3166>] [/W:<nom du fichier
du journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction KAVSHELL SCAN contient les arguments obligatoires et complémentaires dont l'utilisation n'est pas obligatoire (cf. tableau ci-dessous).

Exemples de l'instruction KAVSHELL UPDATE

Pour lancer une tâche de mise à jour des bases créée par l'utilisateur, exécutez l'instruction suivante :

```
KAVSHELL UPDATE
```

Pour lancer une tâche de mise à jour des bases, les fichiers de mise à jour se trouvent dans le dossier \\Server\bases, exécutez l'instruction suivante :

```
KAVSHELL UPDATE \\Server\bases
```

Pour lancer une tâche de mise à jour depuis le serveur FTP ftp://dnl-ru1.kaspersky-labs.com/ et enregistrer tous les événements de la tâche dans le fichier journal c:\update_report.log, exécutez l'instruction suivante :

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log
```

Pour recevoir les mises à jour des bases de Kaspersky Anti-Virus depuis le serveur de mise à jour de Kaspersky Lab ; connectez-vous à la source des mises à jour via le serveur proxy (adresse du serveur proxy : proxy.company.com, port : 8080) ; pour accéder au serveur, utilisez la vérification intégrée de l'authenticité de Microsoft Windows (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser, mot de passe : 123456), puis exécutez l'instruction suivante :

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456 :
```

Tableau 41. Arguments de l'instruction KAVSHELL UPDATE

CLE	DESCRIPTION
Sources de la mise à jour (argument obligatoire). Indiquez une ou plusieurs sources. Kaspersky Anti-Virus contactera chacune des sources dans l'ordre de la liste. Séparez les sources par un espace.	
<chemin au format UNC>	Source de mise à jour définie par l'utilisateur : chemin d'accès au répertoire de réseau contenant les mises à jour au format UNC (Universal Naming Convention).
<URL>	Source des mises à jour définie par l'utilisateur : adresse du serveur FTP ou HTTP sur lequel se trouve le répertoire contenant les mises à jour.
<Dossier local>	Source des mises à jour définie par l'utilisateur : dossier sur le serveur protégé
/AK	Serveur d'administration de Kaspersky Administration Kit en guise de source des mises à jour
/KL	Serveurs de mises à jour de Kaspersky Lab en guise de source des mises à jour
/NOUSEKL	N'utilise pas les serveurs de mise à jour de Kaspersky Lab si les autres sources des mises à jour indiquées sont inaccessibles (utilisés par défaut).
Paramètres du serveur proxy	
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas cet argument, Kaspersky Anti-Virus identifiera automatiquement les paramètres du serveur proxy utilisé dans le réseau local.
/AUTHTYPE:<0-2>	Cet argument définit la méthode de vérification de l'authenticité pour l'accès au serveur proxy. Le paramètre peut prendre les valeurs suivantes : **0** : analyse de l'authenticité de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Anti-Virus contactera le serveur proxy sous le compte **Système local** (**SYSTEM**) ; **1** : analyse de l'authenticité de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Anti-Virus contactera le serveur proxy sous le compte utilisateur dont les données sont définies par les arguments /PROXYUSER et /PROXYPWD ; **2** : analyse de l'authenticité selon le nom et le mot de passe de l'utilisateur définis par les arguments /PROXYUSER et /PROXYPWD (Basic authentication). Si l'accès au serveur proxy ne requiert pas l'authentification, alors il n'est pas nécessaire d'indiquer cet argument.
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur employé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> è /PROXYPWD:<mot de passe> sont ignorés.</Z1>
/PROXYPWD:<mot de passe>	Mot de passe qui utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> è /PROXYPWD:<mot de passe> sont ignorés.</Z1> Si vous définissez l'argument /PROXYUSER mais pas l'argument /PROXYPWD, le système considère que le mot de passe est vide.
/NOPROXYFORKL	N'utilise pas les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab (utilisés par défaut)
/USEPROXYFORCUSTOM	Utilise les paramètres du serveur proxy pour la connexion aux sources de mises à jour définies par l'utilisateur (non utilisées par défaut)
/USEPROXYFORLOCAL	Utilise les paramètres du serveur proxy pour la connexion aux sources locales des mises à jour. Si cet argument n'est pas indiqué, la valeur **Ne pas utiliser les paramètres de proxy spécifiés pour se connecter aux sources des mises à jour locales est appliquée**. Pour plus d'informations sur ces paramètres, consultez la section "Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour" (cf. page 398).
Paramètres généraux du serveur FTP ou HTTP	
/NOFTPPASSIVE	Si vous utilisez cet argument, Kaspersky Anti-Virus utilisera le mode actif du serveur FTP pour se connecter au serveur protégé. Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus utilisera le mode passif du serveur FTP si cela est possible.

CLE	DESCRIPTION
/TIMEOUT:<nombre de secondes>	Délai d'attente lors de la connexion au serveur FTP ou HTTP. Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus appliquera, par défaut, la valeur 10 sec. Cet argument accepte uniquement des nombres entiers.
/REG:<code iso3166>	L'argument des paramètres régionaux intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mises à jour le plus proche. En guise de valeur pour cet argument, saisissez le code alphabétique du pays où se trouve le serveur protégé conformément à la norme ISO 3166-1, par exemple /REG:gr ou /REG:RU. Si vous n'utilisez pas cet argument ou si vous indiquez un code inexistant, alors Kaspersky Anti-Virus identifiera l'emplacement du serveur protégé selon les paramètres régionaux du serveur protégé (pour Microsoft Windows 2003 Server ou suivant, il s'agit de la variable **Emplacement** (Location)).
/ALIAS:<nom alternatif de la tâche>	Cet argument permet d'attribuer un nom temporaire à la tâche afin de pouvoir la consulter durant l'exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à la l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Anti-Virus. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple, update_1234. Dans la console de Kaspersky Anti-Virus, la tâche reçoit le nom Update-bases (<date time>), par exemple, Update-bases 8/16/2007 05:41:02 PM.
/W:<nom du fichier du journal d'exécution de la tâche>	Si vous désignez cet argument, Kaspersky Anti-Virus enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument. Le fichier du journal d'exécution de la tâche contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Anti-Virus dans la console "Observateur d'événements". Vous pouvez indiquer un chemin absolu ou relatif au fichier du journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du journal sera créé dans le répertoire en cours. Un nouveau lancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier de journal existant. Vous pouvez consulter le fichier du journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution des tâches** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de journal, il n'interrompt pas l'exécution de l'instruction et n'affiche pas de message sur l'erreur.

Codes de retour de l'instruction KAVSHELL UPDATE (cf. rubrique "Code de retour de l'instruction KAVSHELL RTP" à la page 299)

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS. KAVSHELL ROLLBACK

L'instruction `KAVSHELL ROLLBACK` vous permet d'exécuter la tâche prédéfinie **Annulation de la mise à jour** pour remettre les bases de Kaspersky Anti-Virus à l'état antérieur à la mise à jour. La commande est exécutée en mode synchrone.

Syntaxe de l'instruction

```
KAVSHELL ROLLBACK
```

Codes de retour de l'instruction KAVSHELL ROLLBACK (cf. page 300)

INSTALLATION ET SUPPRESSION DES LICENCES. KAVSHELL LICENSE

L'instruction `KAVSHELL LICENSE` vous permet d'installer et de supprimer les licences de Kaspersky Anti-Virus.

Syntaxe de l'instruction KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD: <nom du fichier de clé> [/R] | /DEL: <numéro de série>]
```

Exemples de l'instruction KAVSHELL LICENSE

Pour installer la licence depuis le fichier de licence, exécutez l'instruction suivante :

```
KAVSHELL LICENSE /ADD:C:/License.key
```

Pour obtenir les informations sur les licences installées, exécutez l'instruction suivante :

```
KAVSHELL LICENSE
```

Pour supprimer la licence installée avec le numéro de série 0000-000000-00000001, exécutez l'instruction suivante :

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

L'instruction `KAVSHELL LICENSE` peut être exécutée avec ou sans les clés de licence (cf. tableau ci-dessous).

Tableau 42. Arguments de l'instruction KAVSHELL LICENSE

CLE	DESCRIPTION
Sans argument	L'instruction affiche les informations suivantes sur les licences installées : • Numéro de série de la licence ; • Type de licence (test bêta, commerciale, évaluation ou avec prise en charge d'EMC Celerra) ; • Numéro de série de la clé ; • Licence complémentaire ou non. Si la valeur * est définie, la licence installée est une licence complémentaire.
/ADD:<nom du fichier de clé>	Installe la licence depuis un fichier de licence dont le nom est défini par la valeur /ADD. Indiquez le nom du fichier de licence et le chemin d'accès complet à celui-ci. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
/R	L'argument /R est complémentaire à l'argument /ADD. Il indique que la licence installée est une licence de complémentaire.
/DEL: <numéro de série>	Supprime la licence dont le numéro de série correspond à la valeur de l'argument /DEL.

Codes de retour de l'instruction KAVSHELL LICENSE (cf. page 301)

ACTIVATION, CONFIGURATION ET DESACTIVATION DE LA CONSTITUTION D'UN JOURNAL DE TRAÇAGE. KAVSHELL TRACE

L'instruction `KAVSHELL TRACE` vous permet d'activer ou de désactiver sur-le-champ la création d'un journal de traçage de tous les sous-systèmes de Kaspersky Anti-Virus ainsi que de définir le niveau de détail des informations reprises dans le journal.

Syntaxe de l'instruction KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<dossier contenant les fichiers du journal de traçage> [/S:<taille maximale du fichier de traçage en mégaoctets>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Si le journal de traçage est constitué et vous souhaitez modifier ses paramètres, saisissez l'instruction `KAVSHELL TRACE` avec l'argument /ON et définissez les paramètres du journal à l'aide des arguments /S et /LVL (cf. tableau ci-dessous).

Tableau 43. Arguments de l'instruction KAVSHELL TRACE

CLE	DESCRIPTION
/ON	Active la constitution du journal de traçage.
/F:<dossier contenant les fichiers du journal de traçage>	Cet argument indique le chemin d'accès complet au dossier dans lequel les fichiers du journal de traçage seront conservés (argument obligatoire). Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Vous pouvez indiquer les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques de réseau du serveur protégé. Si le nom du dossier dont vous saisissez le chemin d'accès pour cet argument contient un espace, il faudra saisir le nom entre guillemets, par exemple /F:"C\Trace Folder". Pour désigner le chemin d'accès au dossier contenant les fichiers du journal de traçage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
/S:<Taille maximale du fichier journal en mégaoctets>	Cet argument définit la taille maximale d'un fichier du journal de traçage. Dès que la taille du journal atteint la valeur maximale, Kaspersky Anti-Virus consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé. Si vous ne définissez pas cet argument, la taille maximale d'un journal sera limitée à 50 Mo.
/LVL:debug|info|warning|error|critical	Cette clé définit le niveau de détail du journal depuis le niveau le plus détaillé (**informations de débogage**) où tous les événements sont enregistrés jusqu'au niveau minimum (**Critiques**) où seuls les événements critiques sont consignés dans le journal. Si vous ne définissez pas cet argument, le journal de traçage contiendra les événements correspondant au niveau de détail **Informations de débogage**.
/OFF	Cet argument désactive la constitution du journal de traçage.

Exemples de l'instruction KAVSHELL TRACE :

Pour activer le contenu du journal de traçage avec le niveau de détail Informations de débogage et la taille maximale du fichier du journal de 200 Mo et enregistrer le fichier du journal dans le répertoire C:\Trace Folder, exécutez l'instruction suivante :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

Pour activer le contenu du journal de traçage avec le niveau de détail Evénements importants et enregistrer le fichier journal dans le répertoire C:\Trace Folder, exécutez l'instruction suivante :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

Pour désactiver le contenu du journal de traçage, exécutez l'instruction suivante :

```
KAVSHELL TRACE OFF
```

Codes de retour de l'instruction KAVSHELL TRACE (cf. page 301)

PURGE DE LA BASE ISWIFT. KAVSHELL FBRESET

Kaspersky Anti-Virus utilise la technologie iSwift qui permet de ne pas devoir analyser à nouveau un fichier si celui-ci n'a pas été modifié depuis l'analyse antérieure (cf. rubrique Application de la technologie iSwift).

Dans le répertoire système %SYSTEMDRIVE%\System Volume Information, Kaspersky Anti-Virus crée les fichiers fidbox.dat et fidbox2.dat qui contiennent les informations relatives aux objets sains déjà analysés. Plus le nombre de fichiers différents analysés par Kaspersky Anti-Virus est élevé, plus la taille du fichier fidbox.dat (fidbox2.dat) sera importante. Ce fichier contient uniquement les informations actuelles sur les fichiers existant vraiment dans le système : si un fichier quelconque est supprimé, Kaspersky Anti-Virus supprime les informations qui le concerne du fichier fidbox.dat (fidbox2.dat).

Pour purger ce fichier, utilisez l'instruction `KAVSHELL FBRESET`.

Tenez compte des particularités suivantes de l'instruction `KAVSHELL FBRESET` :

- Lors de la purge du fichier fidbox.dat à l'aide de l'instruction KAVSHELL FBRESET, Kaspersky Anti-Virus ne désactive pas la protection (à la différence de la suppression manuelle du fichier).
- Après la remise à zéro du fichier fidbox.dat, Kaspersky Anti-Virus peut augmenter la charge sur le serveur. Dans ce cas, le logiciel antivirus analyse tous les fichiers sollicités pour la première fois après la remise à zéro du fichier fidbox.dat. Après l'analyse, Kaspersky Anti-Virus introduit à nouveau dans le fichier fidbox.dat les informations relatives à l'objet analysé. Lorsque cet objet sera à nouveau sollicité, la technologie iSwift permet de ne pas devoir l'analyser à nouveau, pour autant qu'il n'ait pas été modifié.

Si votre système d'exploitation utilise le contrôle des comptes utilisateur (UAC, User Account Control), pour pouvoir exécuter l'instruction `KAVSHELL FBRESET`, **il faudra posséder les autorisations d'administrateur.**

ACTIVATION ET DESACTIVATION DE LA CREATION DE FICHIERS DE VIDAGE. KAVSHELL DUMP

L'instruction `KAVSHELL DUMP` vous permet d'activer ou de désactiver sur le champ la création de modèles de mémoire (dumps) des processus de Kaspersky Anti-Virus en cas d'arrêt provoqué par une erreur (cf. tableau ci-dessous). De plus, vous pouvez prendre à n'importe quel moment un exemple de la mémoire des processus de Kaspersky Anti-Virus en cours d'exécution.

Syntaxe de l'instruction KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<dossier contenant les fichiers de vidage>|/SNAPSHOT /F:<dossier
contenant les fichiers de vidage> / P:<pid> | /OFF>
```

Exemples d'instruction KAVSHELL DUMP

Pour activer la création des dumps ; enregistrer les dumps dans le répertoire C:\Dump Folder, exécutez l'instruction suivante :

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Pour faire un dump de la mémoire du processus avec l'identificateur 1234 dans le répertoire C:/Dumps, exécutez l'instruction suivante :

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

Pour désactiver la création des dumps, exécutez l'instruction suivante :

```
KAVSHELL DUMP OFF
```

Tableau 44. Arguments de l'instruction KAVSHELL DUMP

CLE	DESCRIPTION
/ON	Active la création d'un vidage de mémoire du processus en cas d'arrêt suite à une erreur.
/F:<dossier contenant les fichiers de vidage>	Argument obligatoire ; indique le chemin d'accès au répertoire où le fichier de vidage sera enregistré. Si vous saisissez un chemin d'accès à un répertoire inexistant, le fichier ne sera pas créé. Vous pouvez indiquer les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques de réseau du serveur protégé. Pour désigner le chemin d'accès au dossier contenant les fichiers de vidage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
/SNAPSHOT	Crée un instantané du modèle de mémoire du processus de Kaspersky Anti-Virus en exécution indiqué et enregistre le fichier de vidage dans le dossier dont le chemin d'accès est défini par l'argument /F.
/P	Identificateur du processus PID ; repris dans le **gestionnaire des tâches** de Microsoft Windows
/OFF	Désactive la création d'un vidage de mémoire du processus en cas d'arrêt suite à une erreur.

Codes de retour de l'instruction KAVSHELL DUMP (cf. page 302)

IMPORTATIONS DES PARAMETRES. KAVSHELL IMPORT

L'instruction `KAVSHELL IMPORT` vous permet d'importer les paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches depuis un fichier de configuration dans Kaspersky Anti-Virus sur le serveur protégé (cf. tableau ci-dessous). Vous pouvez créer le fichier de configuration à l'aide de l'instruction `KAVSHELL EXPORT`.

Syntaxe de l'instruction KAVSHELL IMPORT

```
KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de l'instruction KAVSHELL IMPORT

```
KAVSHELL IMPORT Server1.xml
```

Tableau 45. Arguments de l'instruction KAVSHELL IMPORT

CLE	DESCRIPTION
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration d'où les paramètres vont être importés. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL IMPORT (cf. page 302)

EXPORTATION DES PARAMETRES. KAVSHELL EXPORT

L'instruction `KAVSHELL EXPORT` vous permet d'exporter tous les paramètres de Kaspersky Anti-Virus et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Anti-Virus sur d'autres serveurs (cf. tableau ci-dessous).

Syntaxe de l'instruction KAVSHELL EXPORT

```
KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de l'instruction KAVSHELL EXPORT

```
KAVSHELL EXPORT Server1.xml
```

Tableau 46. Arguments de l'instruction KAVSHELL EXPORT

CLE	DESCRIPTION
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration dans lequel les paramètres vont être enregistrés. Vous pouvez attribuer n'importe quelle extension au fichier de configuration. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL EXPORT (cf. page 303)

CODE DE RETOUR

DANS CETTE SECTION DE L'AIDE

CODES DE RETOUR DES INSTRUCTIONS KAVSHELL START ET KAVSHELL STOP

Tableau 47. Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

DESCRIPTION	
0	L'opération a réussi
-3	Erreur de privilèges d'accès
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (par exemple, le service de Kaspersky Anti-Virus est déjà exécuté ou est déjà arrêté)
-7	Le service n'est pas enregistré
-8	Le lancement du service est interdit
-9	La tentative d'exécution du service sous un autre compte utilisateur a échoué (par défaut, le service de Kaspersky Anti-Virus fonctionne sous compte utilisateur **Système local**).
-99	Erreur inconnue

CODES DE RETOUR DES INSTRUCTIONS KAVSHELL SCAN ET KAVSHELL SCANCRITICAL

Tableau 48. Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi (Aucune menace n'a été découverte)
1	L'opération a été annulée
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le fichier avec la liste des couvertures d'analyse est introuvable).
-5	Syntaxe de l'instruction incorrecte ou couverture d'analyse non définie.
-80	Des objets infectés ont été découverts
-81	Des objets suspects ont été découverts
-82	Des erreurs de traitement ont été découvertes
-83	Des objets non analysés ont été découverts
-84	Objets endommagés détectés
-85	Impossible de créer le fichier du journal d'exécution de la tâche
-99	Erreur inconnue
-301	Licence non valide

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL TASK

Tableau 49. Codes de retour de l'instruction KAVSHELL TASK

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (la tâche est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (par exemple, la tâche n'est pas lancée, est déjà lancée ou ne peut être arrêtée)
-99	Erreur inconnue
-301	Licence non valide
401	La tâche n'est pas lancée (pour l'argument /STATE)
402	La tâche est déjà lancée (pour l'argument /STATE)
403	La tâche est déjà arrêtée (pour l'argument /STATE)
-404	Erreur d'exécution de l'opération (la modification de l'état de la tâche a entraîné son échec)

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL RTP

Tableau 50. Codes de retour de l'instruction KAVSHELL RTP

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (une des tâches de protection en temps réel ou toutes les tâches de protection en temps réel sont introuvables)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (par exemple, la tâche est déjà exécutée ou est déjà arrêtée)
-99	Erreur inconnue
-301	Licence non valide

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL UPDATE

Tableau 51. Codes de retour de l'instruction KAVSHELL UPDATE

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
200	Tous les objets sont d'actualité (les bases ou les modules logiciels sont d'actualité)
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe de l'instruction incorrecte
-99	Erreur inconnue
-206	Les fichiers des mises à jour ne sont pas présents dans la source indiquée ou leur format est inconnu
-209	Erreur de connexion à la source des mises a jour
-232	Erreur d'authentification lors de la connexion au serveur proxy
-234	Erreur de connexion à l'application Kaspersky Administration Kit
-235	Kaspersky Anti-Virus n'a pas réussi la vérification de l'authenticité lors de la connexion à la source des mises à jour
-236	Les bases de Kaspersky Anti-Virus sont corrompues
-301	Licence non valide

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL ROLLBACK

Tableau 52. Codes de retour de l'instruction KAVSHELL ROLLBACK

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-99	Erreur inconnue
-221	La copie de sauvegardé des bases est introuvable
-222	La copie de sauvegardé des bases est corrompue

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL LICENSE

Tableau 53. Codes de retour de l'instruction KAVSHELL LICENSE

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Privilèges insuffisants pour l'administration des licences
-4	Objet introuvable (la licence portant ce numéro de série est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (la licence est déjà installée).
-99	Erreur inconnue
-301	Licence non valide
-303	Licence prévue pour une autre application

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL TRACE

Tableau 54. Codes de retour de l'instruction KAVSHELL TRACE

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin d'accès indiqué en tant que chemin d'accès au dossier contenant les fichiers du journal de traçage est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (tentative d'exécution de KAVSHELL TRACE /OFF si la création du journal de traçage a déjà été désactivée)
-99	Erreur inconnue

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL FBRESET

Tableau 55. Codes de retour de l'instruction KAVSHELL FBRESET

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-99	Erreur inconnue

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL DUMP

Tableau 56. Codes de retour de l'instruction KAVSHELL DUMP

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin indiqué en guise de chemin d'accès au dossier contenant les fichiers de vidage est introuvable ; le processus avec le PID indiqué est introuvable)
-5	Syntaxe de l'instruction incorrecte
-6	Opération invalide (tentative d'exécution de KAVSHELL DUMP /OFF si la création des fichiers de vidage a déjà été désactivée)
-99	Erreur inconnue
-237	Des sources de mises à jour incompatibles ont été définies

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL IMPORT

Tableau 57. Codes de retour de l'instruction KAVSHELL IMPORT

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le fichier de configuration à importer est introuvable)
-5	Syntaxe incorrecte
-99	Erreur inconnue
501	L'opération a réussi, toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple Kaspersky Anti-Virus n'a pas importé des paramètres d'un composant fonctionnel quelconque
-502	Le format du fichier à importer est inconnu ou le fichier manque
-503	Paramètres incompatibles (le fichier de configuration provient d'une autre application ou d'une version de Kaspersky Anti-Virus postérieure ou incompatible)

CODES DE RETOUR DE L'INSTRUCTION KAVSHELL EXPORT

Tableau 58. Codes de retour de l'instruction KAVSHELL EXPORT

CODE DE RETOUR	DESCRIPTION
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe incorrecte
-10	Impossible de créer le fichier de configuration (par exemple, accès interdit au répertoire indiqué dans le chemin d'accès au fichier)
-99	Erreur inconnue
501	L'opération a réussi, toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple Kaspersky Anti-Virus n'a pas exporté des paramètres d'un composant fonctionnel quelconque

ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA KASPERSKY ADMINISTRATION KIT

Si l'entreprise pour laquelle vous travaillez utilise Kaspersky Administration Kit pour l'administration centralisée des logiciels antivirus, vous pouvez administrer Kaspersky Anti-Virus sur les serveurs protégés et le configurer via la console d'administration Kaspersky Administration Kit.

DANS CETTE SECTION DE L'AIDE

CONFIGURATION DE KASPERSKY ANTI-VIRUS DANS LA BOITE DE DIALOGUE PARAMETRES DE L'APPLICATION

DANS CETTE SECTION DE L'AIDE

BOITE DE DIALOGUE PARAMETRES DE L'APPLICATION

Dans la boîte de dialogue **Paramètres de l'application**, vous pouvez réaliser l'administration à distance de Kaspersky Anti-Virus et sa configuration sur le serveur protégé sélectionné.

*Pour ouvrir la boîte de dialogue **Paramètres de l'application**, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

2. Dans le volet des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur le serveur protégé et choisissez l'option **Propriétés**.

3. Dans la boîte de dialogue **Propriétés** <**Nom de l'ordinateur**> sous l'onglet **Applications,** sélectionnez la commande dans la liste des applications installées, puis cliquez sur le bouton **Propriétés** (cf. ill. ci-après).

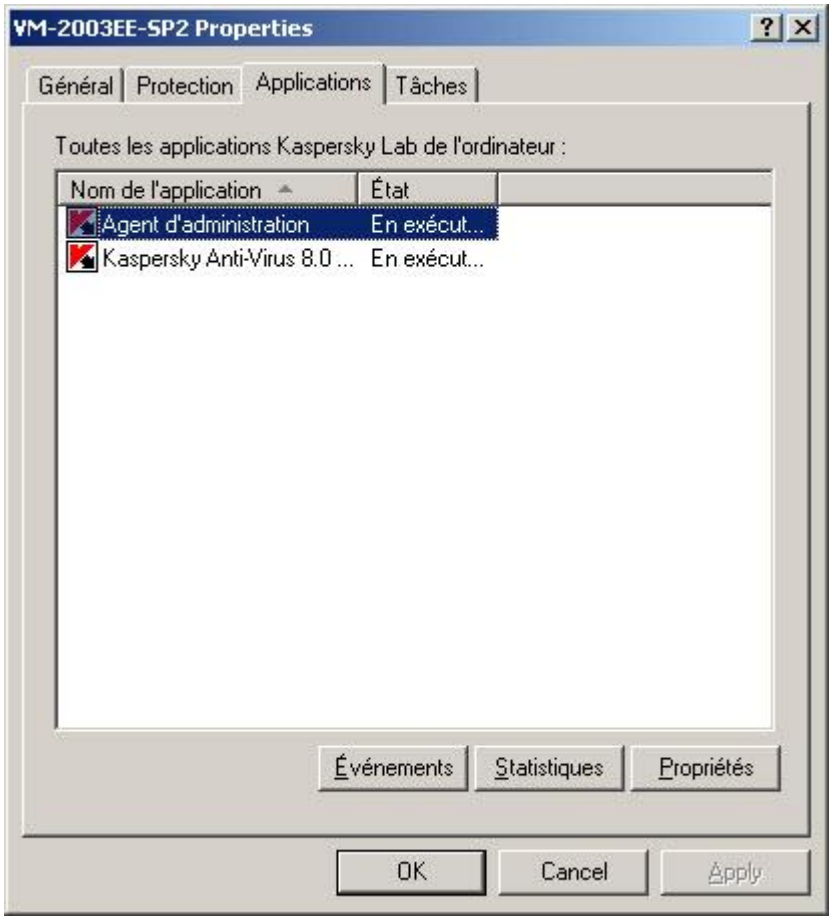


Illustration 93. Liste des applications antivirus dans la boîte de dialogue ***Propriétés : <nom de l'ordinateur>***

La boîte de dialogue **Paramètres de l'application** s'ouvrira (cf. ill. ci-après).

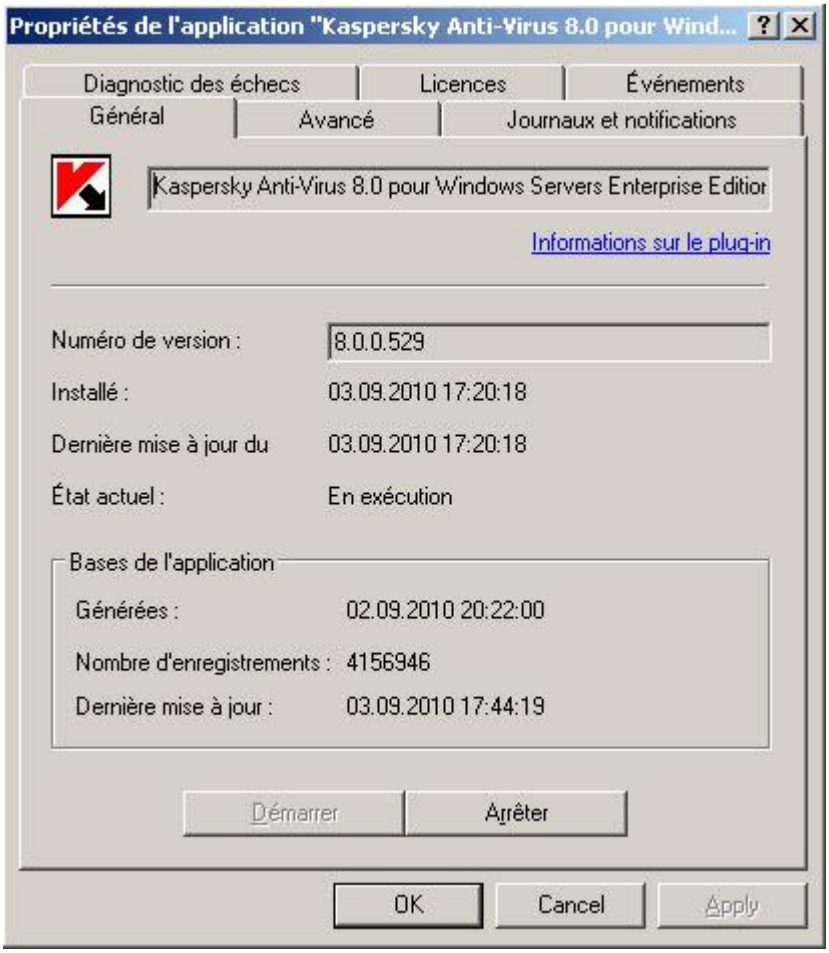


*Illustration 94. Boîte de dialogue **Paramètres de l'application**, onglet **Général***

Quand une stratégie de Kaspersky Administration Kit est appliquée, la valeur des paramètres de la stratégie accompagné de l'icône 🔒 ne peut être modifiée dans la boîte de dialogue **Paramètres de l'application** de la console d'administration.

ADMINISTRATION DES OBJETS EN QUARANTAINE ET CONFIGURATION DES PARAMETRES DE LA QUARANTAINE

DANS CETTE SECTION DE L'AIDE

FONCTIONS DE LA QUARANTAINE ET LEUR CONFIGURATION

Le tableau ci-après énumère les fonctions de la quarantaine et les outils d'administration qui vous permettent de gérer ces fonctions.

Tableau 59. Fonctions de la quarantaine et leur configuration

FONCTION DE LA QUARANTAINE	CONSOLE D'ADMINISTRATION DE KASPERSKY ADMINISTRATION KIT	CONSOLE DE KASPERSKY ANTI-VIRUS
Consultation, tri et suppression des objets	Oui (cf. document *Kaspersky Administration Kit. Manuel de l'administrateur*)	Oui
Filtrage des objets	Non	Oui
Envoi des objets suspects de la quarantaine à Kaspersky Lab pour examen	Non	Oui
Placement des objets en quarantaine manuellement	Non	Oui
Restauration des objets de la quarantaine	Oui Les options de restauration des objets suivantes sont disponibles : • Dans l'emplacement d'origine ; • Dans l'emplacement désigné dans la Console d'administration Kaspersky Administration Kit (cf. document *Kaspersky Administration Kit. Manuel de l'administrateur*)	Oui
Analyse des objets en quarantaine	Oui Lancez la tâche **Analyse des objets en quarantaine**.	Oui
Configuration de paramètres de la quarantaine	Oui	Oui
Consultation des statistiques de la quarantaine	Oui	Oui

CONFIGURATION DE PARAMETRES DE QUARANTAINE DANS KASPERSKY ADMINISTRATION KIT

La boîte de dialogue **Paramètres de l'application** du serveur sélectionné permet de configurer les paramètres de la quarantaine.

Kaspersky Anti-Virus isole les objets qu'il considère suspects dans la quarantaine : ils sont déplacés de leur emplacement d'origine vers un dossier spécial où ils cryptés pour raison de sécurité.

Pour configurer les paramètres de la quarantaine, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).

2. Sous l'onglet **Avancé** du groupe **Configuration de la quarantaine et de la sauvegarde**, cliquez sur le bouton **Configuration** (cf. ill. ci-après).

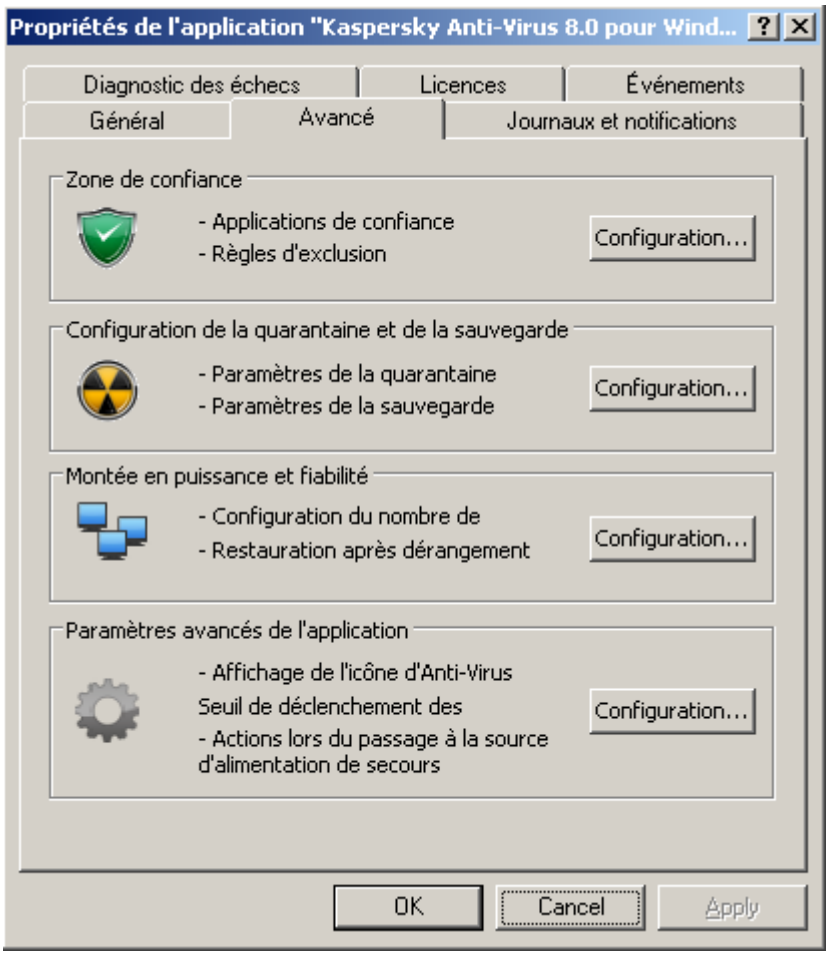


*Illustration 95. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

3. Sous l'onglet **Quarantaine** de la boîte de dialogue **Configuration de la quarantaine et de la sauvegarde**, configurez le cas échéant les paramètres suivants de la quarantaine (cf. ill. ci-après) :

   - Pour désigner un dossier de quarantaine (cf. page 406) différent du dossier proposé par défaut, indiquez le chemin d'accès complet au dossier sur le disque local du serveur protégé dans le champ **Dossier de quarantaine**.

   - Pour définir la taille maximale de la quarantaine (cf. page 406), cochez la case **Taille maximale de la quarantaine** et saisissez la valeur souhaitée en mégaoctets dans le champ.

   - pour définir l'espace disponible minimum(cf. page 407) dans la quarantaine, cochez la case **Taille maximale de la quarantaine**, cochez la case **Seuil d'espace libre** et saisissez la valeur souhaitée en mégaoctets dans le champ ;

- Pour sélectionner un autre dossier de restauration (cf. page 411), indiquez le chemin d'accès complet au dossier sur le disque local de l'ordinateur protégé dans le groupe de paramètres **Paramètres de restauration**.

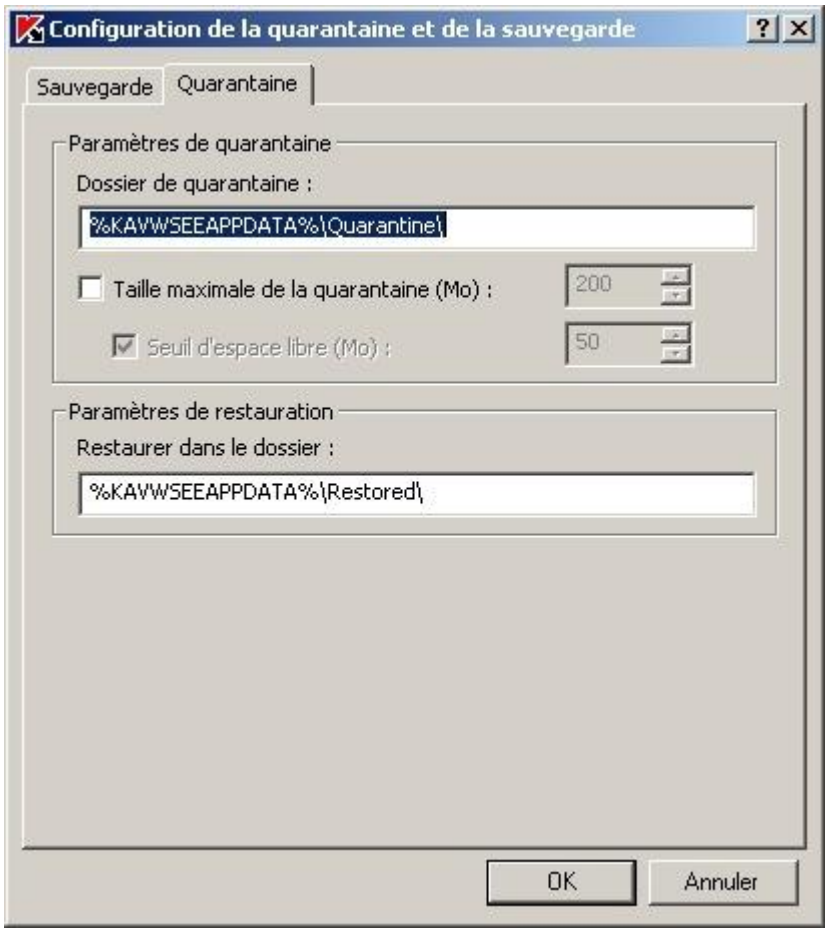


*Illustration 96. Boîte de dialogue **Paramètres de l'application**, onglet **Quarantaine***

4. Cliquez sur **OK**.

ADMINISTRATION DES FICHIERS DE LA SAUVEGARDE ET CONFIGURATION DES PARAMETRES DE LA SAUVEGARDE

DANS CETTE SECTION DE L'AIDE

FONCTIONS DE LA SAUVEGARDE ET MODES DE CONFIGURATION

Le tableau ci-après énumère les fonctions de la sauvegarde et les outils d'administration qui vous permettent de gérer ces fonctions.

Tableau 60. Fonctions de la sauvegarde

FONCTIONS DE LA SAUVEGARDE	CONSOLE SERVEUR DE KASPERSKY ADMINISTRATION KIT	CONSOLE DE KASPERSKY ANTI-VIRUS
Consultation, tri et suppression des fichiers	Oui	Oui
Filtrage des fichiers	Non	Oui
Restauration des fichiers depuis la sauvegarde	Oui Les options de restauration des objets suivantes sont disponibles : • Dans l'emplacement d'origine ; • Dans l'emplacement désigné dans la Console d'administration Kaspersky Administration Kit (cf. document *Kaspersky Administration Kit. Manuel de l'administrateur*)	Oui
Configuration des paramètres de la sauvegarde	Oui	Oui
Consultation des statistiques de la sauvegarde	Oui	Oui

CONFIGURATION DE LA SAUVEGARDE DANS KASPERSKY ADMINISTRATION KIT

La boîte de dialogue **Paramètres de l'application** du serveur sélectionné permet de configurer les paramètres de la sauvegarde.

Lisez la rubrique de présentation de la sauvegarde des objets avant la réparation ou la suppression (cf. page 211).

➧ *Pour configurer les paramètres de la sauvegarde, procédez comme suit :*

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).
2. Sous l'onglet **Avancé** du groupe **Configuration de la quarantaine et de la sauvegarde**, cliquez sur le bouton **Configuration** (cf. ill. ci-après).

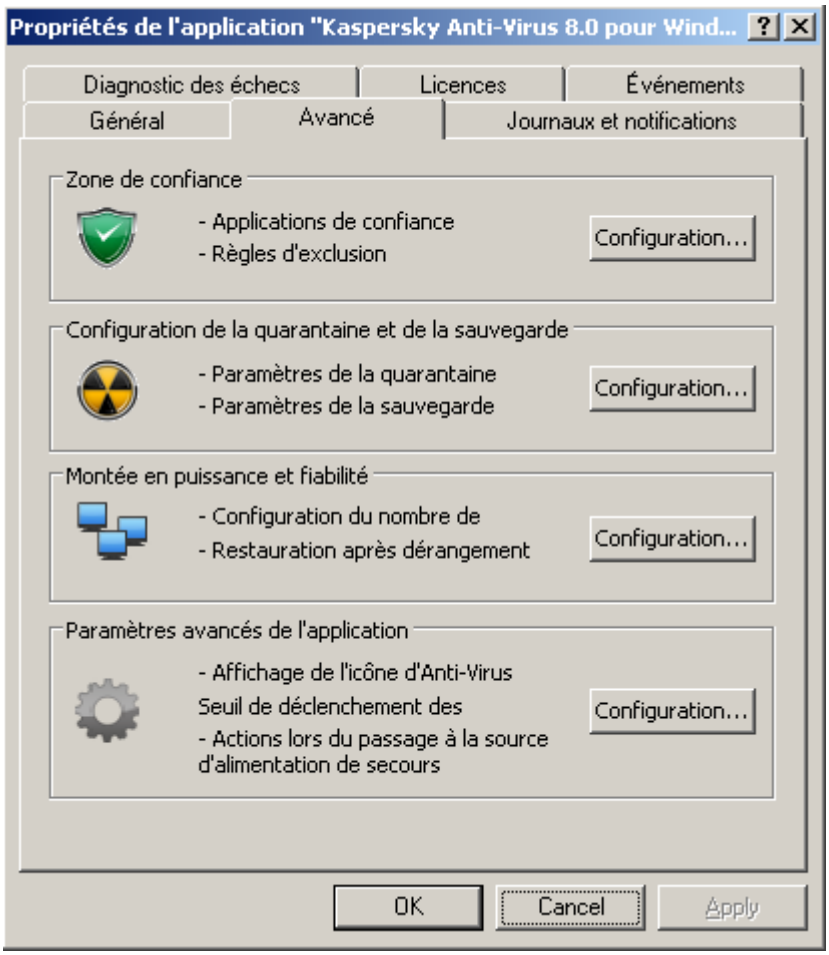


*Illustration 97. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

3. Sous l'onglet **Sauvegarde** de la boîte de dialogue **Configuration de la quarantaine et de la sauvegarde**, configurez le cas échéant les paramètres suivants de la sauvegarde (cf. ill. ci-après) :

   - Pour définir le dossier qui abritera la sauvegarde (cf. page 409), sélectionnez, dans le champ **Dossier de sauvegarde**, le dossier requis sur le disque local du serveur protégé ou saisissez le chemin d'accès complet à celui-ci.

   - Pour définir la taille maximale de la sauvegarde (cf. page 410), cochez la case **Taille maximale de la sauvegarde** et saisissez la valeur souhaitée en mégaoctets dans le champ.

   - Pour définir le seuil d'espace disponible dans la sauvegarde (cf. page 410), définissez la valeur de **Taille maximale de la sauvegarde**, cochez la case **Seuil d'espace libre** et saisissez la valeur minimale souhaitée d'espace disponible dans la sauvegarde en mégaoctets.

- Pour indiquer le répertoire de restauration (cf. page 411), dans le groupe de paramètres **Paramètres de restauration**, sélectionnez le répertoire requis sur le disque local du serveur protégé ou dans le champ **Restaurer dans le dossier**, saisissez le nom du dossier et son chemin d'accès complet.

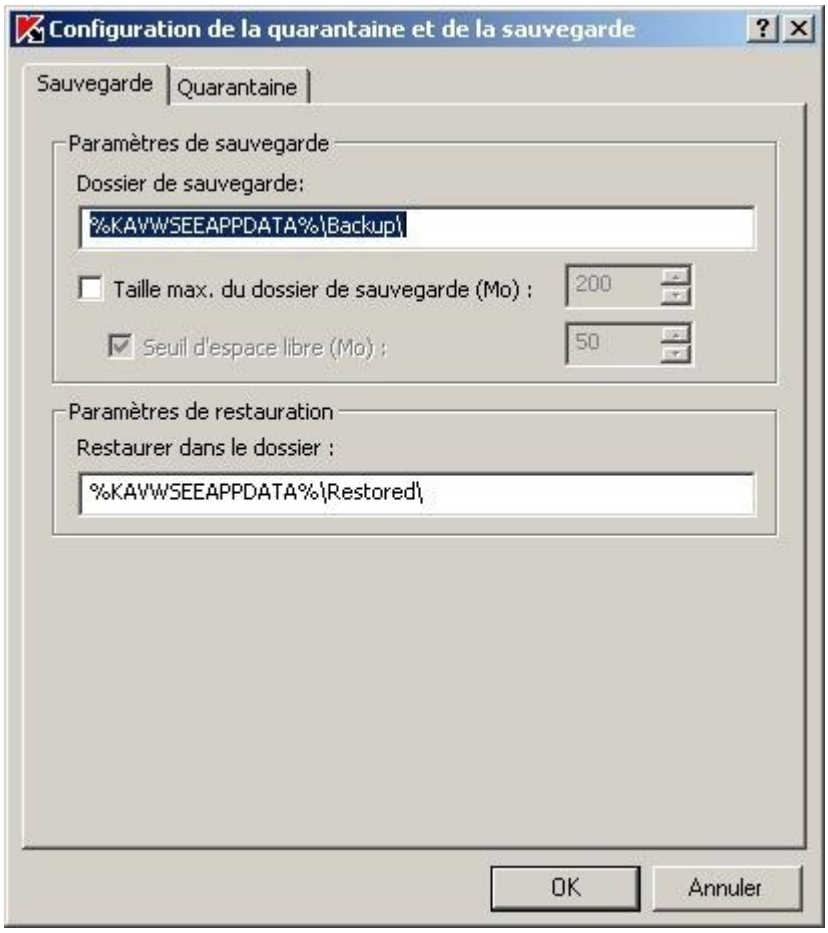


*Illustration 98. Boîte de dialogue **Configuration de la sauvegarde et de la quarantaine**, onglet **Sauvegarde***

4. Cliquez sur **OK**.

ADMINISTRATION DE LA ZONE DE CONFIANCE

Vous pouvez administrer la zone de confiance de Kaspersky Anti-Virus dans Kaspersky Administration Kit.

DANS CETTE SECTION DE L'AIDE

AJOUT DE PROCESSUS A LA LISTE DES PROCESSUS DE CONFIANCE (KASPERSKY ADMINISTRATION KIT)

La console d'administration de Kaspersky Administration Kit permet d'ajouter les fichiers exécutables des processus sur le disque du serveur protégé à la zone de confiance ; vous ne pouvez pas ajouter des processus de la liste des processus actifs sur le serveur.

En savoir plus sur la zone de confiance de Kaspersky Anti-Virus (cf. page 178).

Pour ajouter le processus à la liste des processus de confiance de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la boîte de dialogue **Paramètres de l'application** (cf. page 304),

2. Sous l'onglet **Avancé**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Zone de confiance** (cf. ill. ci-après).

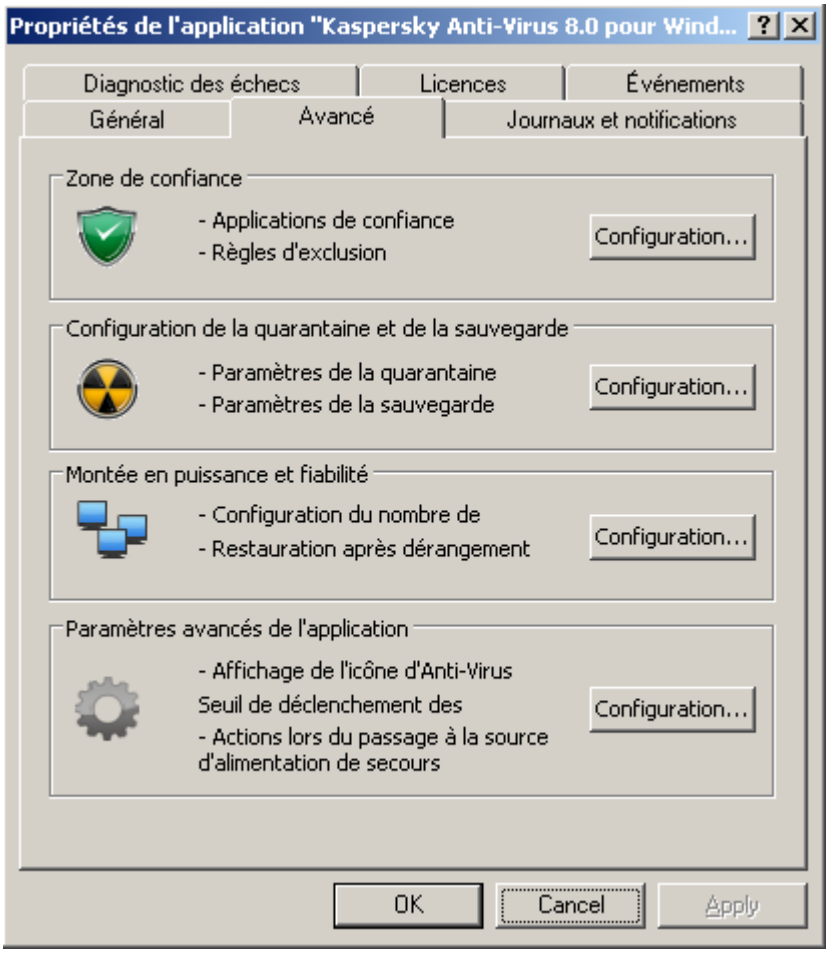


*Illustration 99. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

3. Dan la boîte de dialogue **Configuration de la zone de confiance**, sous l'onglet **Applications** de confiance, activez la fonction **Processus de confiance** : cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** (cf. ill. ci-après).

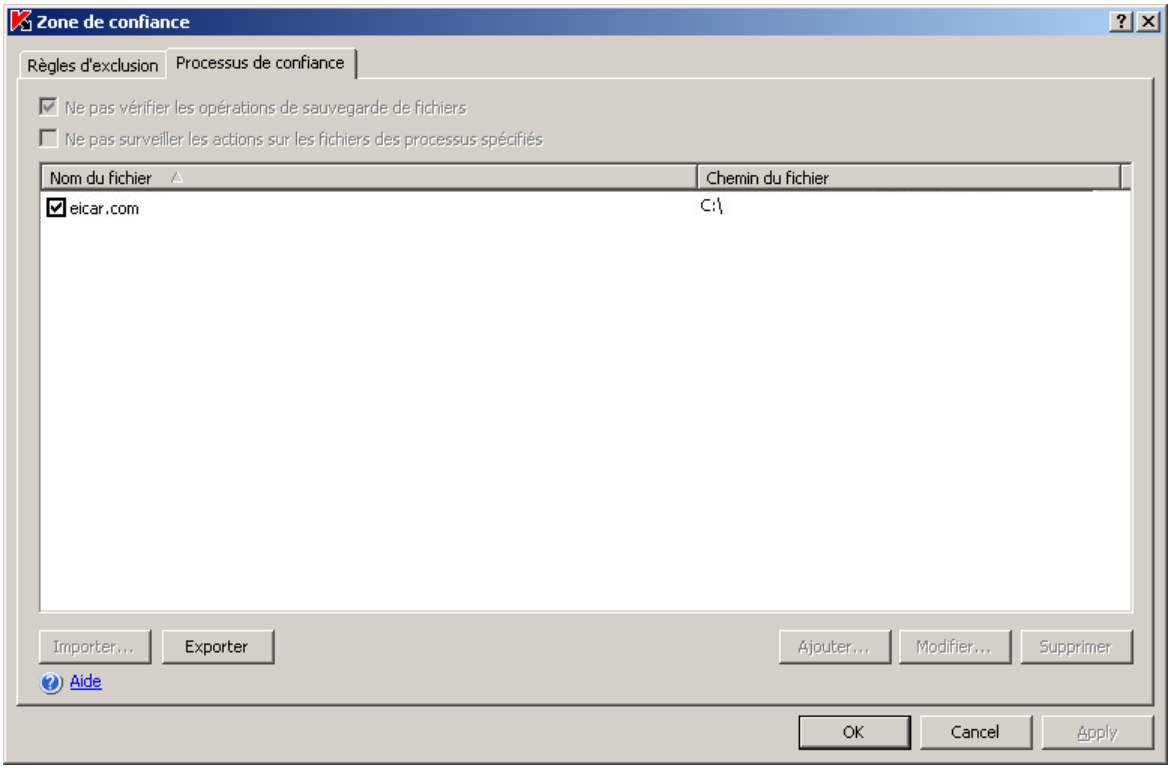


*Illustration 100. Boîte de dialogue **Configuration de la zone de confiance**, onglet **Applications de confiance***

4. Si vous avez exporté les paramètres de la zone de confiance de Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition dans un fichier de configuration, vous pouvez importer la zone de confiance de ce fichier. Pour ce faire, exécutez les actions suivantes :

   a. Cliquez sur **Import**.

   b. Dans la fenêtre **Sélection du fichier**, désignez le fichier de configuration contenant les paramètres de la zone de confiance.

   c. Cliquez sur **OK**.

   N'oubliez pas que tous les paramètres de la zone de confiance seront importés depuis ce fichier.

5. Pour sélectionner le fichier exécutable du processus sur le disque du serveur protégé, procédez de la manière suivante :

   a. Cliquez sur **Ajouter**.

   b. Dans la boîte de dialogue **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du processus sur le disque local du serveur protégé.

   c. Le nom du fichier et le chemin d'accès à celui-ci apparaît dans la boîte de dialogue **Ajout d'un processus de confiance**.

   d. Cliquez sur **OK**.

   Le nom du fichier exécutable du processus sélectionné apparaît dans la liste des processus de confiance de l'onglet **Processus de confiance**.

6. Cliquez sur **OK** pour enregistrer les modifications.

DESACTIVATION DE LA PROTECTION EN TEMPS REEL DES FICHIERS PENDANT LA CREATION DE LA SAUVEGARDE

Pendant la création d'une copie de sauvegarde des fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités durant les opérations de copie de sauvegarde. Kaspersky Anti-Virus n'analyse pas les fichiers que l'application de sauvegarde ouvre en lecture avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Pour désactiver la protection en temps réel des fichiers pendant la copie de sauvegarde, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).

2. Sous l'onglet **Avancé**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Zone de confiance** (cf. ill. ci-après).

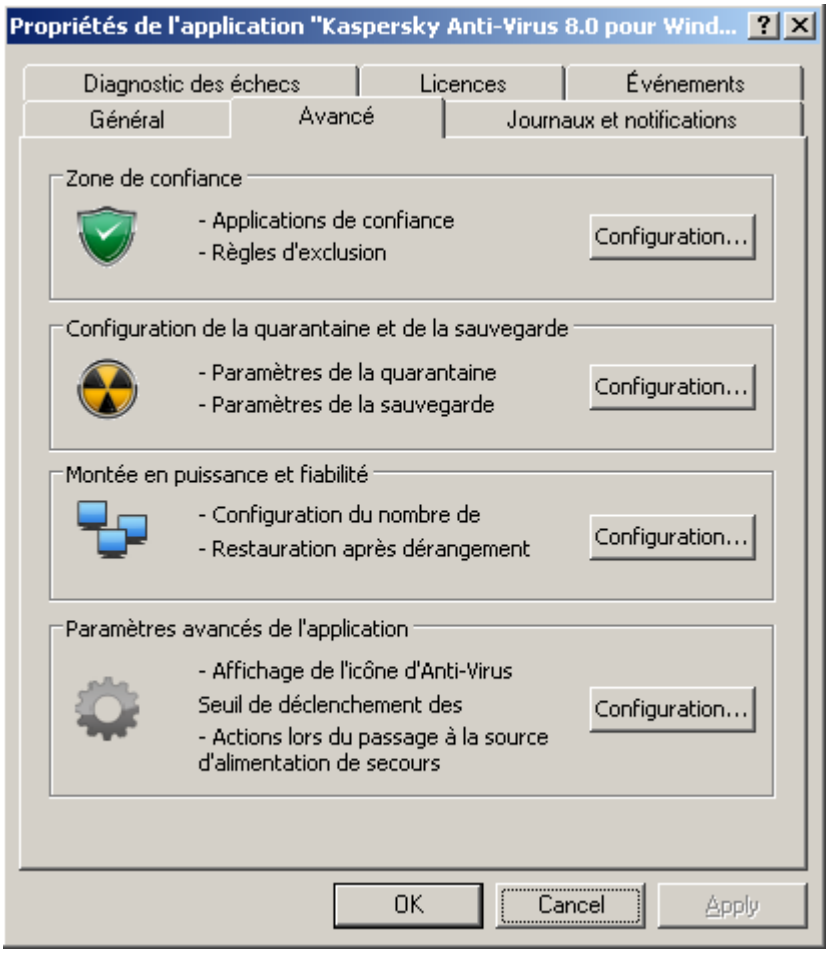


*Illustration 101. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

3. Pour désactiver la protection en temps réel des fichiers sollicités durant la copie de sauvegarde, cochez sous l'onglet **Applications de confiance** la case **Ne pas vérifier les opérations de sauvegarde de fichiers** (cf. ill. ci-après).

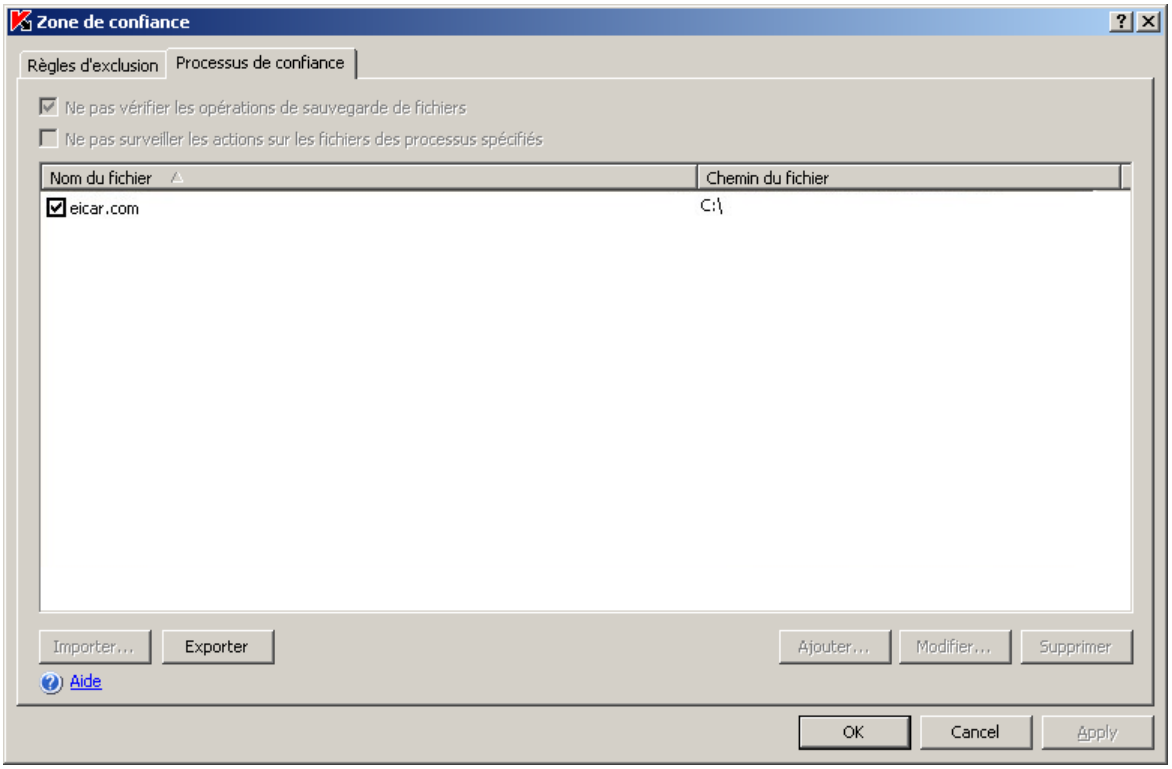


*Illustration 102. Boîte de dialogue **Configuration de la zone de confiance**, onglet **Applications de confiance***

4. Cliquez sur **OK** pour enregistrer les modifications.

5. Le cas échéant, appliquez les exclusions de la zone de confiance dans les tâches sélectionnées et dans les stratégies (cf. rubrique "Application de la zone de confiance dans l'application Kaspersky Administration Kit" à la page 320).

AJOUT D'EXCLUSIONS A LA ZONE DE CONFIANCE

Vous pouvez ajouter des objets à la zone de confiance pour les exclure de l'analyse. En savoir plus sur la zone de confiance de Kaspersky Anti-Virus (cf. page 178).

Pour ajouter une exclusion dans la zone de confiance, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).

2. Sous l'onglet **Avancé**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Zone de confiance** (cf. ill. ci-après).

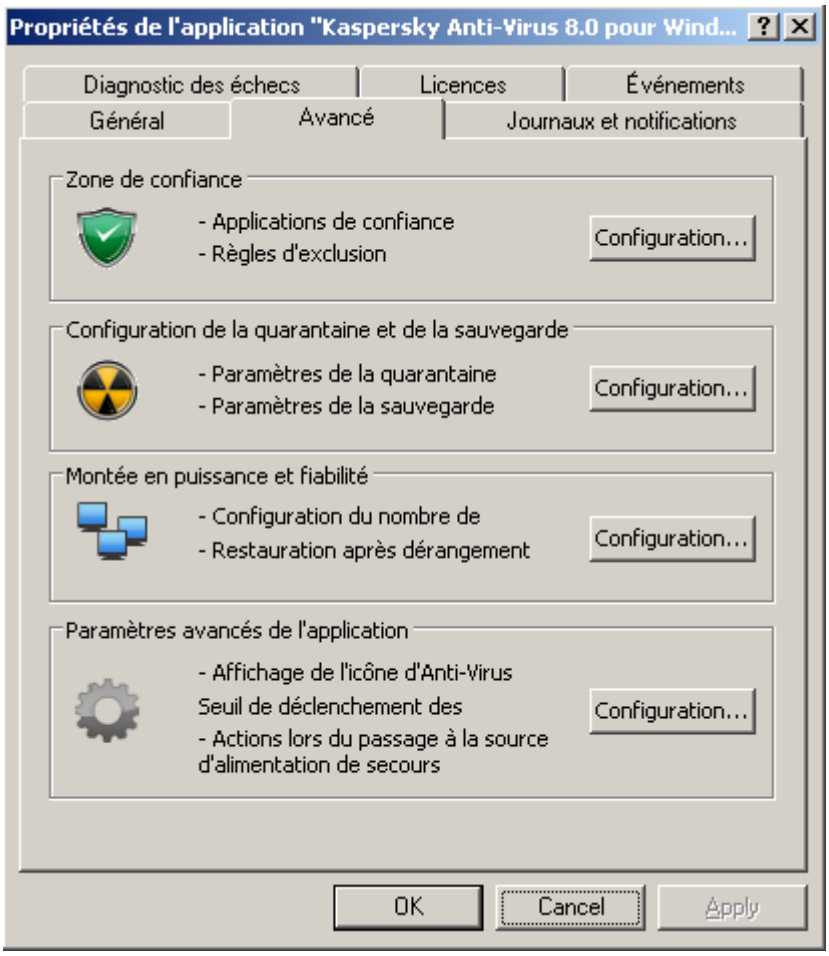
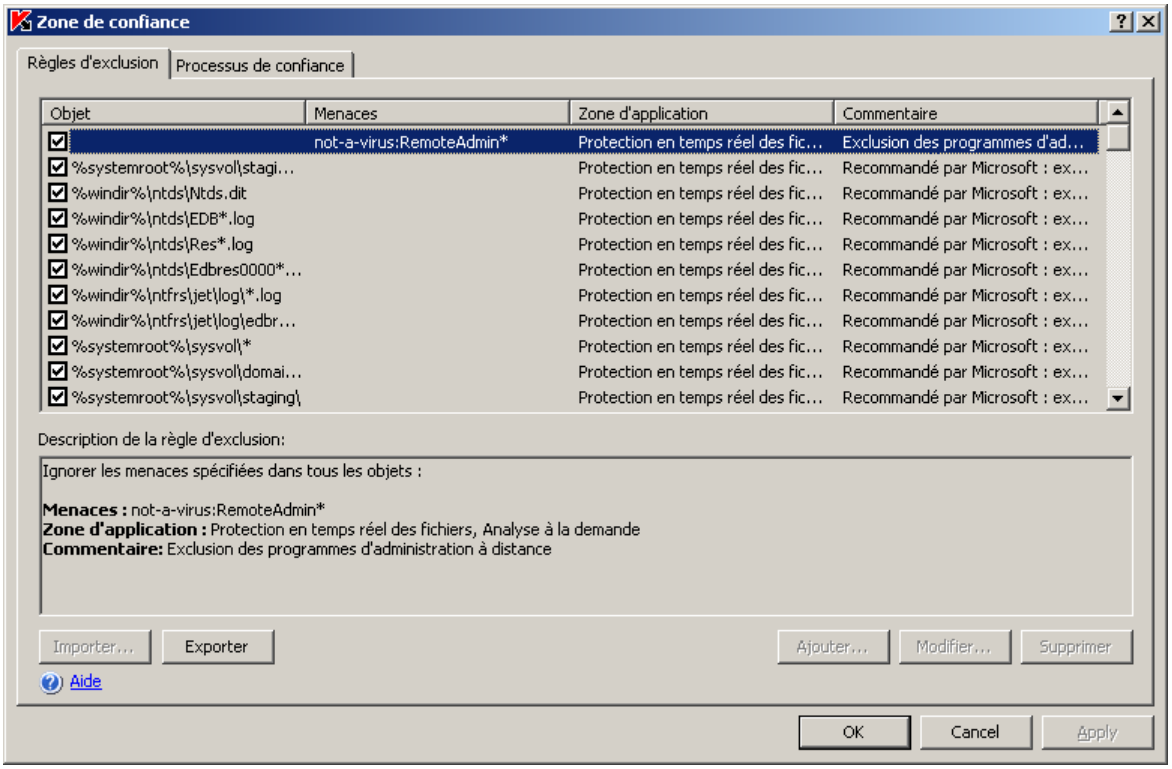


*Illustration 103. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

3. Dans la boîte de dialogue **Configuration de la zone de confiance**, ouvrez l'onglet **Règles d'exclusion** (cf. ill. ci-après)**.**



4. Si vous avez exporté les paramètres de la zone de confiance de Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition dans un fichier de configuration, vous pouvez importer la zone de confiance de ce fichier.

   a. Cliquez sur **Import**.

   b. Dans la fenêtre **Sélection du fichier**, désignez le fichier de configuration contenant les paramètres de la zone de confiance.

   c. Cliquez sur **OK**.

   N'oubliez pas que tous les paramètres de la zone de confiance seront importés depuis ce fichier.

5. Pour ajouter les exclusions recommandées par Microsoft à la zone de confiance, cliquez sur l'onglet **Règles d'exclusion**, cliquez sur le bouton **Règles** et dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer l'opération.

6. Pour ajouter une nouvelle règle d'exclusion, cliquez sur le bouton **Ajouter** sous le titre **Description de la règle d'exclusion**. La boîte de dialogue **Règle d'exclusion** s'ouvre.

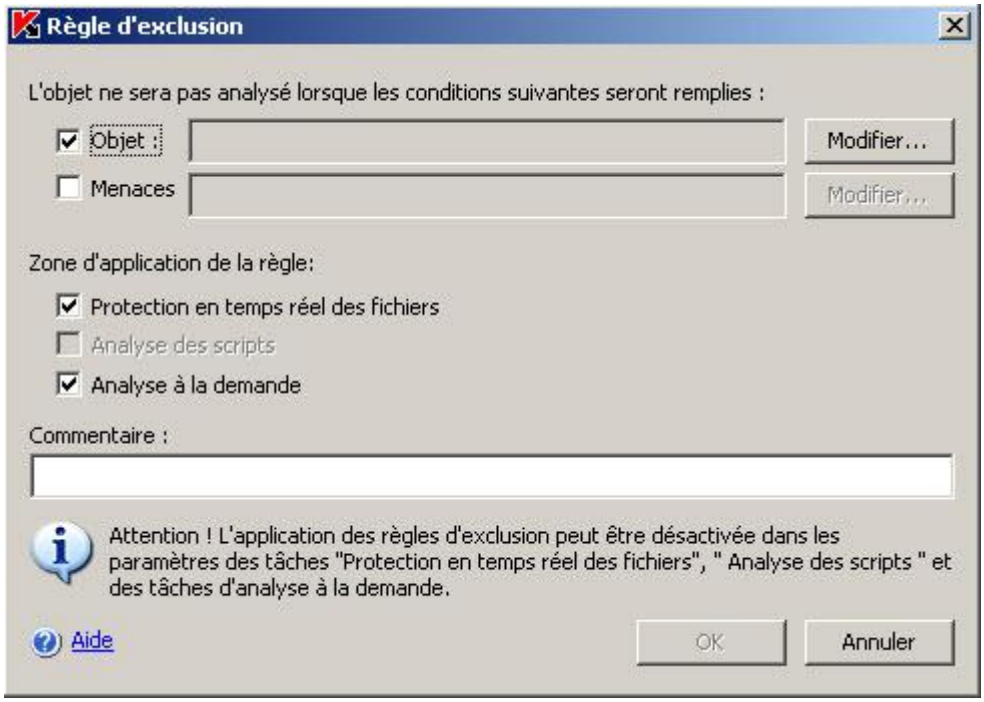


*Illustration 104. Boîte de dialogue **Règle d'exclusion**.*

Indiquez la règle selon laquelle Kaspersky Anti-Virus va exclure les objets. Respectez les recommandations suivantes :

- Pour exclure toutes les menaces dans les dossiers et fichiers indiqués, cochez la case **Objet** et désélectionnez la case **Menaces**.
- Pour exclure toutes les menaces dans les dossiers et fichiers indiqués, cochez la case **Objet** et désélectionnez la case **Menaces**.
- Pour exclure les menaces définies dans toute la couverture d'analyse, désélectionnez la case **Objet** et cochez la case **Menaces**.

Si vous souhaitez indiquer l'emplacement de l'objet, cochez la case **Objet**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Sélection de l'objet**, sélectionnez l'objet qui sera exclu de l'analyse (cf. ill. ci-dessous), puis cliquez sur **OK.** Vous pouvez sélectionner les emplacements suivants pour l'objet :

- **Couverture de l'analyse prédéfinie**. Sélectionnez une des zones d'analyse prédéfinie dans la liste.
- **Disque ou répertoire**. Indiquez le disque du serveur ou le répertoire sur le serveur ou dans le réseau local.
- **Fichier**. Indiquez le fichier sur le serveur ou dans le réseau local.
- **Fichier ou URL du script**. Désignez le script sur le serveur protégé, dans le réseau local ou sur Internet.

Vous pouvez définir des masques pour les noms de dossiers ou de fichiers à l'aide des caractères génériques **?** et *****.

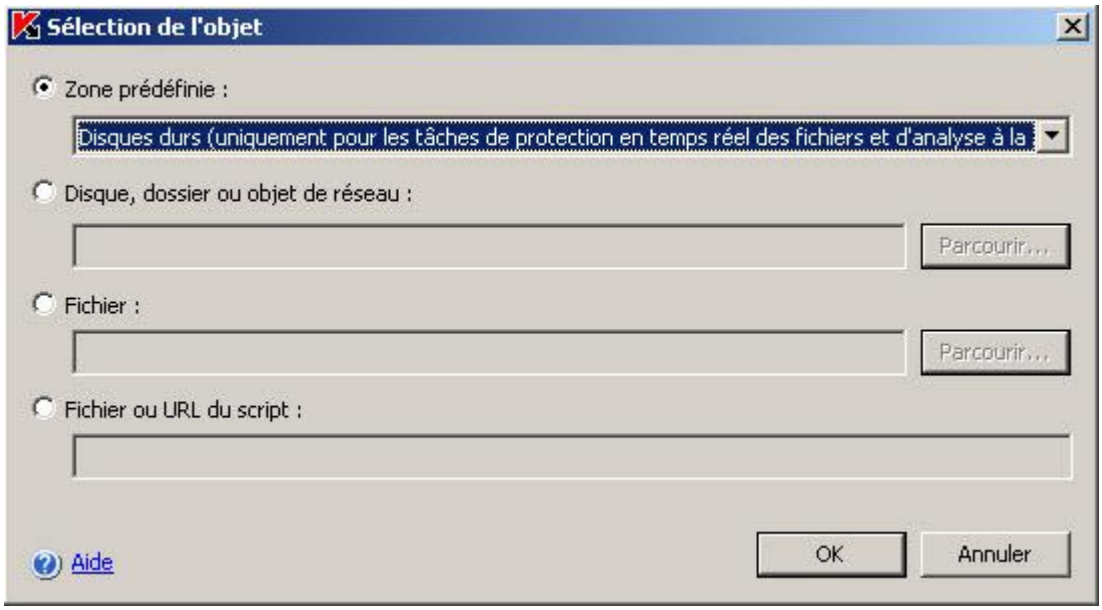


*Illustration 105. Boîte de dialogue **Sélection de l'objet***

7. Si vous souhaitez indiquer le nom de la menace, cochez la case **Menaces**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Liste des exclusions des menaces**, ajoutez le nom de la menace. Lisez la description du paramètre exclusion des menaces (cf. page 380).

8. Cochez la case en regard des composants fonctionnels dans les tâches desquels la règle d'exclusion sera appliquée.

   Cliquez sur **OK**. Exécutez une des actions suivantes :

   - Pour modifier la règle, sélectionnez sous l'onglet **Règles d'exclusion**, la règle que vous voulez modifier, puis cliquez sur le bouton **Modifier** et introduisez les modifications dans la boîte de dialogue **Règle d'exclusion**.

   - Pour supprimer une règle, sous l'onglet **Règles d'exclusion**, sélectionnez la règle que vous voulez supprimer, cliquez sur le bouton **Supprimer** et confirmez l'opération.

9. Cliquez sur le bouton **OK** dans la boîte de dialogue **Configuration de la zone de confiance**.

10. Le cas échéant, appliquez les exclusions de la zone de confiance dans les tâches sélectionnées et dans les stratégies (cf. rubrique "Application de la zone de confiance dans l'application Kaspersky Administration Kit" à la page 320).

APPLICATION DE LA ZONE DE CONFIANCE DANS KASPERSKY ADMINISTRATION KIT

Vous pouvez activer ou désactiver l'application de la zone de confiance dans les stratégies existantes et dans les tâches (lors de la création d'une tâche ou dans la boîte de dialogue **Propriétés:<Nom de la tâche>**).

La zone de confiance est appliquée par défaut dans les nouvelles tâches ou stratégies (cf. page 178).

➧ *Pour appliquer la zone de confiance à une stratégie, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés** puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie puis déployez le nœud **Stratégies**.

2. Ouvrez le menu contextuel de la stratégie dont vous souhaitez configurer les paramètres, puis choisissez l'option **Propriétés**.

3. Dans la boîte de dialogue **Propriétés : <Nom de la stratégie>**, exécutez les opérations suivantes :

   - Pour exclure les *processus de confiance*, assurez-vous que la case **Ne pas surveiller les actions sur fichiers des processus spécifiés** est cochée et fermez le cadenas dans le groupe de paramètres **Liste des processus de confiance**.

   - Pour exclure les *opérations de la sauvegarde*, assurez-vous que la case **Ne pas vérifier les opérations de sauvegarde de fichiers** est cochée et fermez le cadenas dans le groupe de paramètres **Liste des processus de confiance**.

4. Pour appliquer les exclusions définies par l'utilisateur, verrouillez les paramètres du groupe **Exclusions**.

5. Cliquez sur **OK**.

Pour appliquer la zone de confiance à une tâche, procédez comme suit :

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

2. Dans le volet des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur le serveur protégé et choisissez l'option **Propriétés**.

3. Sous l'onglet **Tâches** de la boîte de dialogue **Propriétés: <Nom de la tâche>**, ouvrez le menu contextuel de la tâche que vous souhaitez configurer et choisissez l'option **Propriétés**.

4. Dans la boîte de dialogue **Propriétés : <Nom de tâche>**, sous l'onglet **Avancé**, cochez la case **Appliquer la zone de confiance**.

Vous pouvez également appliquer la zone de confiance lors de la création de la tâche.

CONFIGURATION DES NOTIFICATIONS DANS KASPERSKY ADMINISTRATION KIT

DANS CETTE SECTION DE L'AIDE

INFORMATIONS GENERALES SUR LA CONFIGURATION DES NOTIFICATIONS DANS KASPERSKY ADMINISTRATION KIT

La console d'administration de Kaspersky Administration Kit permet de configurer les notifications adressées à l'administrateur et aux utilisateurs relatives aux événements liés à l'utilisation de Kaspersky Anti-Virus et à l'état de la protection antivirus du serveur protégé :

- L'administrateur peut obtenir des informations sur les événements de certains types ;

- les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peut obtenir des informations sur les événements de type *Une menace a été découverte*.

Vous pouvez configurer les notifications relatives aux événements de Kaspersky Anti-Virus pour un serveur dans la fenêtre **Propriétés** du serveur sélectionné ou pour un groupe de serveurs dans la fenêtre **Propriétés: <nom de la stratégie>** du groupe sélectionné.

Vous pouvez configurer les notifications sous l'onglet **Événements** ou dans la boîte de dialogue **Configuration des notifications**. Vous pouvez configurer les types suivants de notification :

- L'onglet **Événements** (onglet standard de Kaspersky Administration Kit) permet de configurer les notifications adressées à l'administrateur sur les événements de certains types. Pour connaître les modes de notification que vous pouvez configurer et la marche à suivre, consultez le document *Kaspersky Administration Kit. Manuel de l'administrateur*.

- La boîte de dialogue **Configuration des notifications** permet de configurer les notifications pour l'administrateur et pour les utilisateurs.

  En savoir plus sur les modes de notification que vous pouvez configurer dans la boîte de dialogue **Configuration des notifications** (cf. page 262).

Les notifications relatives à certains types d'événements peuvent être configurées uniquement dans une des fenêtres tandis que d'autres notifications peuvent être configurées dans les deux.

Si vous configurez les notifications sur les événements d'un type d'une manière sur les deux onglets, sous l'onglet **Événements** et dans la boîte de dialogue **Configuration des notifications**

CONFIGURATION DES NOTIFICATIONS DE L'ADMINISTRATEUR ET DES UTILISATEURS DANS LA BOITE DE DIALOGUE CONFIGURATION DES NOTIFICATIONS

Pour configurer les notifications, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).

2. Sous l'onglet **Journaux** et notifications, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Notifications sur les événements**.

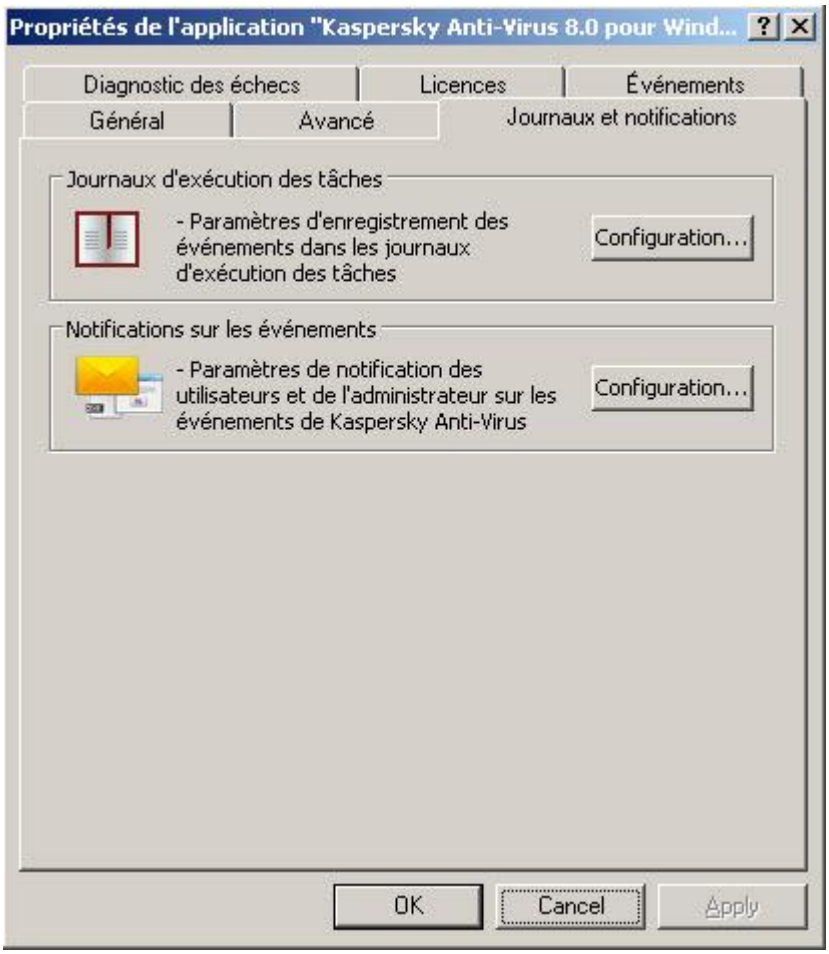


*Illustration 106. Boîte de dialogue **Paramètres de l'application**, onglet **Journaux et notifications***

3. Dans la boîte de dialogue **Configuration des notifications**, configurez les notifications sur les événements requis, puis cliquez sur **OK**.

La configuration des notifications dans la boîte de dialogue **Configuration des notifications** est similaire à la configuration des notifications dans la boîte de dialogue **Notifications** de la console de Kaspersky Anti-Virus.

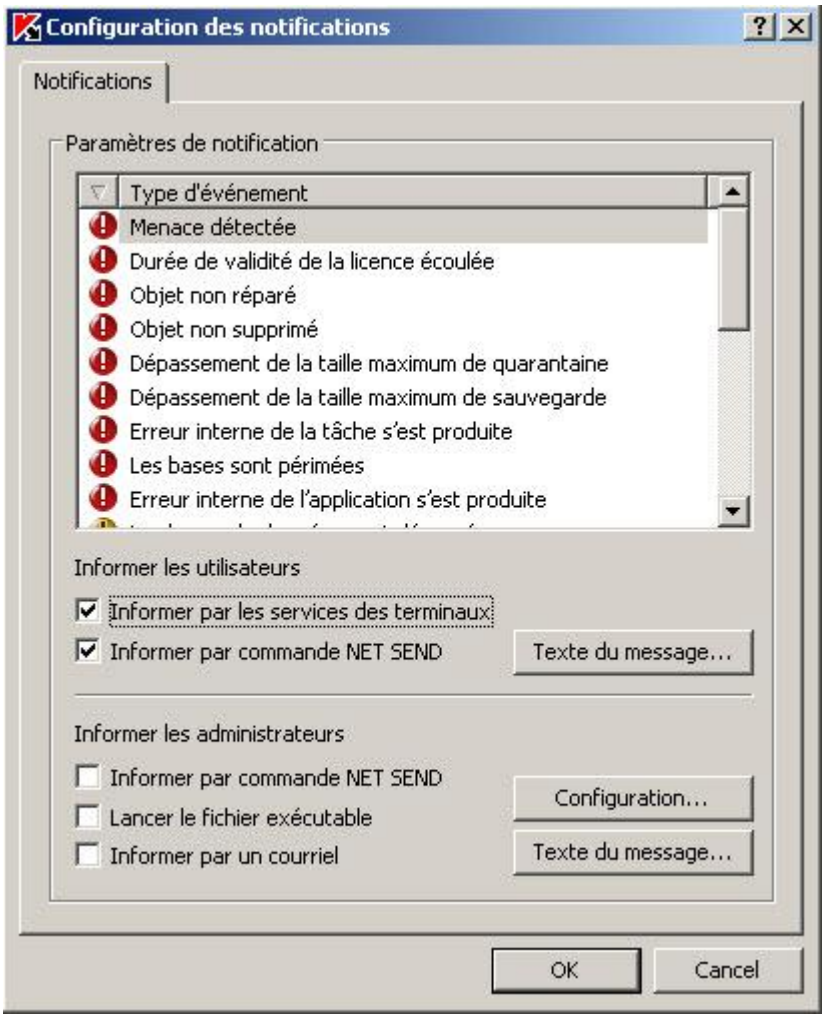


*Illustration 107. Boîte de dialogue **Paramètres des notifications***

CONFIGURATION DES PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS DANS KASPERSKY ADMINISTRATION KIT

Pour configurer les paramètres des journaux de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304). Configurez les paramètres de Kaspersky Anti-Virus selon vos besoins sous les onglets suivants.

2. Sous l'onglet **Diagnostic des échecs**, configurez les paramètres de diagnostic des échecs (cf. ill. ci-après) :

   - activez ou désactivez la création du journal de traçage (cf. page 360) ;

   - le cas échéant, configurez les paramètres du journal ;

- activez ou désactivez la création de fichiers de vidage de mémoire des processus de Kaspersky Anti-Virus (cf. page 365).

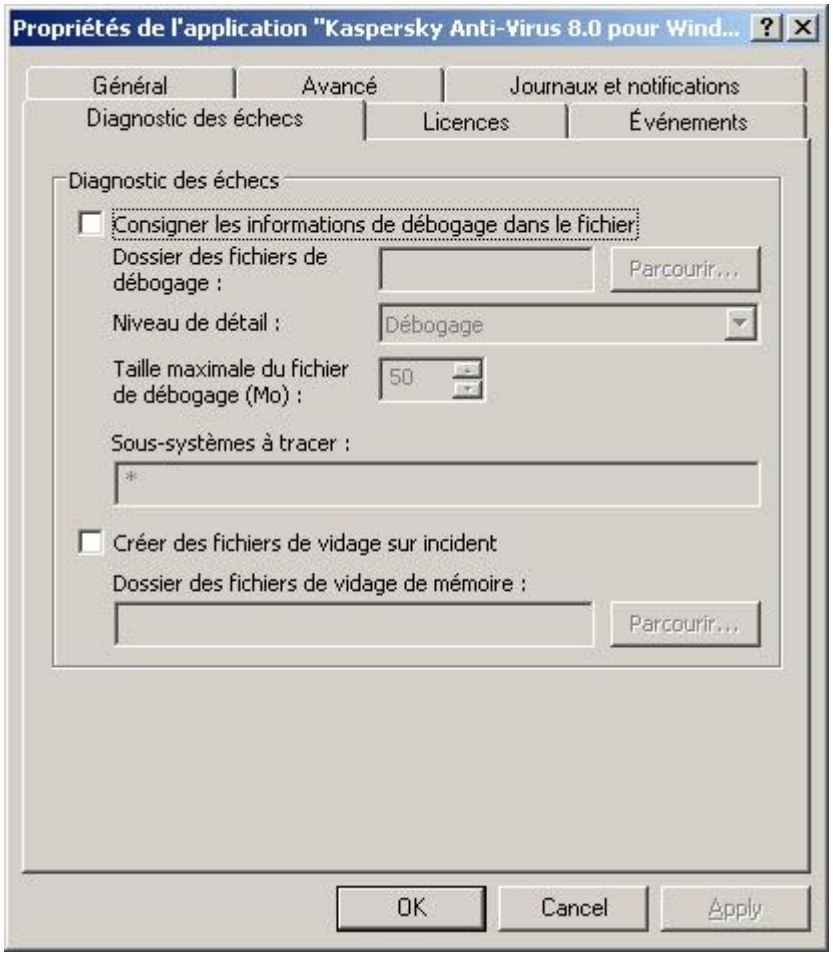


*Illustration 108. Boîte de dialogue **Paramètres de l'application**, onglet **Diagnostic des échecs***

3. Sur l'onglet **Avancé**, exécutez les actions suivantes (cf. ill. ci-après).

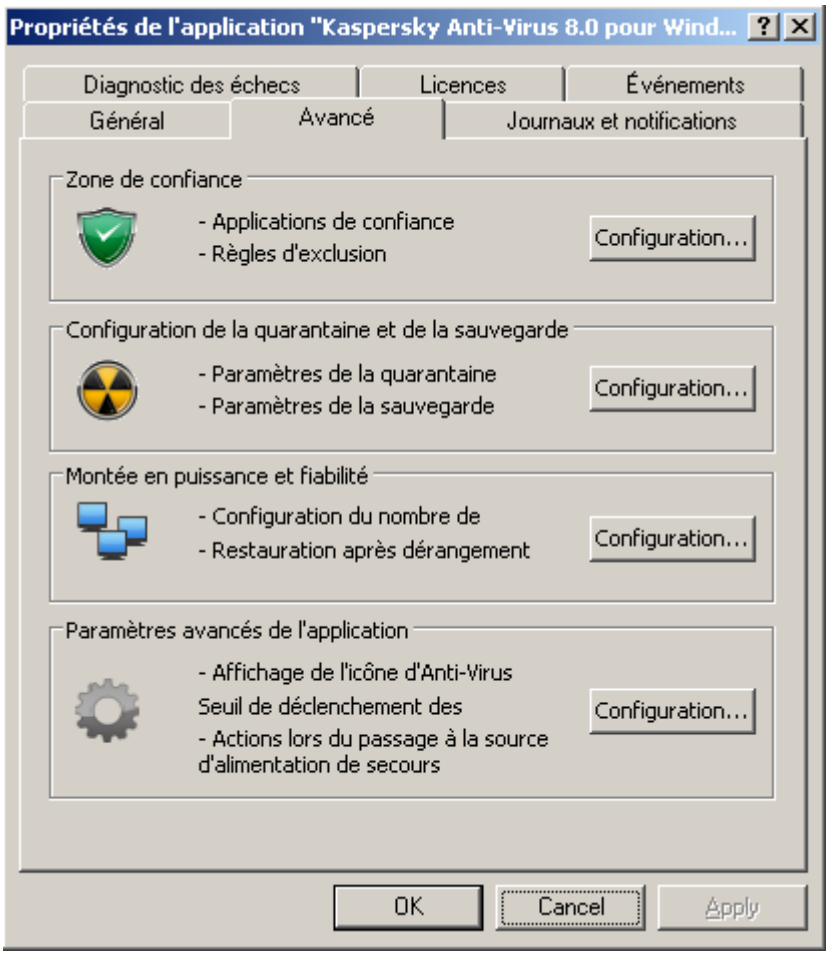


*Illustration 109. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé***

- Pour configurer les paramètres de répartition des processus de travail et de restauration du système, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Paramètres d'adaptabilité** et **Paramètres de fiabilité** et dans la boîte de dialogue qui s'ouvre (cf. ill. ci-après), configurez les paramètres suivants de Kaspersky Anti-Virus en fonction de vos besoins :

  - Nombre maximum de processus de travail actifs que Kaspersky Anti-Virus peut lancer (cf. page 356) ;

  - Nombre de processus pour les tâches de protection en temps réel (cf. page 357) ;

  - Nombre de processus de travail pour les tâches d'analyse à la demande en arrière-plan (cf. page 358) ;

  - Nombre de tentatives de restauration des tâches après un arrêt sur un échec (cf. page 359).

Cliquez sur **OK**.

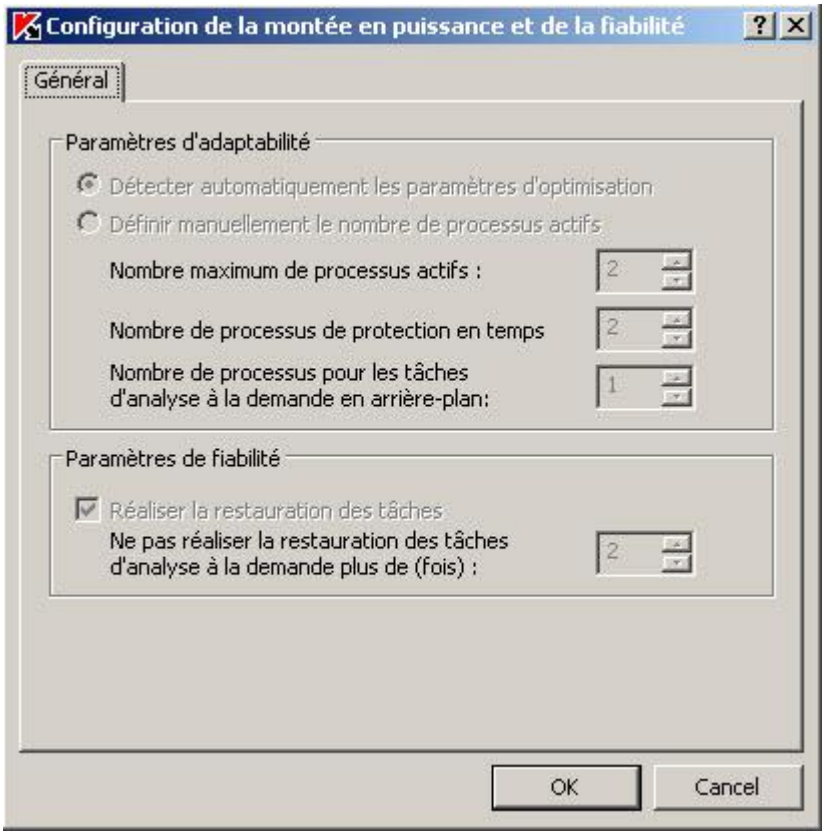


*Illustration 110. Boîte de dialogue **Paramètres de montée en puissance et de fiabilité***

4. Sous l'onglet **Avancé**, cliquez sur le bouton **Configuration** du groupe de paramètres **Paramètres avancés de l'application** et dans la boîte de dialogue (cf. ill. ci-après) qui s'ouvre, configurez les paramètres suivants de Kaspersky Anti-Virus selon vos besoins :

   - afficher ou non l'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches du serveur chaque fois que Kaspersky Anti-Virus est lancé automatiquement après le redémarrage du serveur. Pour en savoir plus, lisez le chapitre "Icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches" (cf. ill. 23).

   - actions de Kaspersky Anti-Virus en cas d'alimentation via un onduleur (cf. ill. 359) ;

   - nombre de jours à l'issue desquels les événements *Les bases doivent être actualisées*, *Les bases sont fortement dépassées* et *L'analyse des zones critiques n'a plus été réalisées depuis longtemps* seront déclenchés (cf. page 360).

   Cliquez sur **OK**.

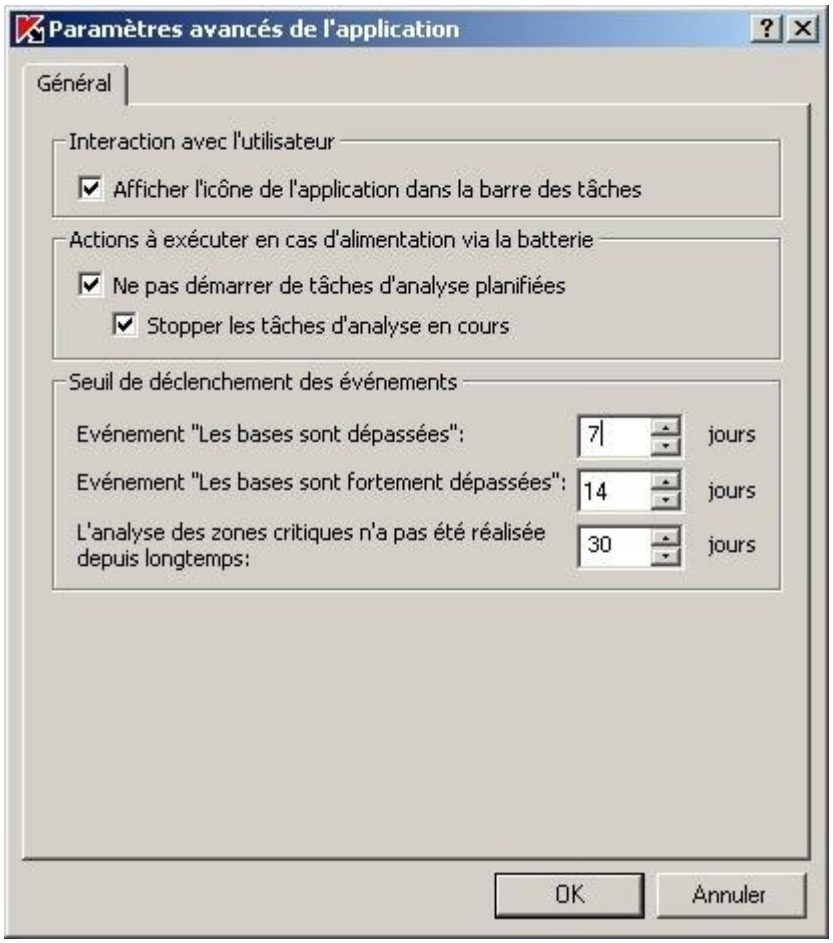


*Illustration 111. Boîte de dialogue **Paramètres avancés de l'application**, onglet **Général***

Sous l'onglet **Sauvegarde hiérarchique**, sélectionnez une des options suivantes d'accès à la sauvegarde hiérarchique (cf. ill. ci-après) :

- **Aucun système HSM**.
- **Le système HSM utilise des points de traitement réitéré**.
- **Le système HSM utilise les attributs élargis du fichier**.

- **Système HSM non identifié**.

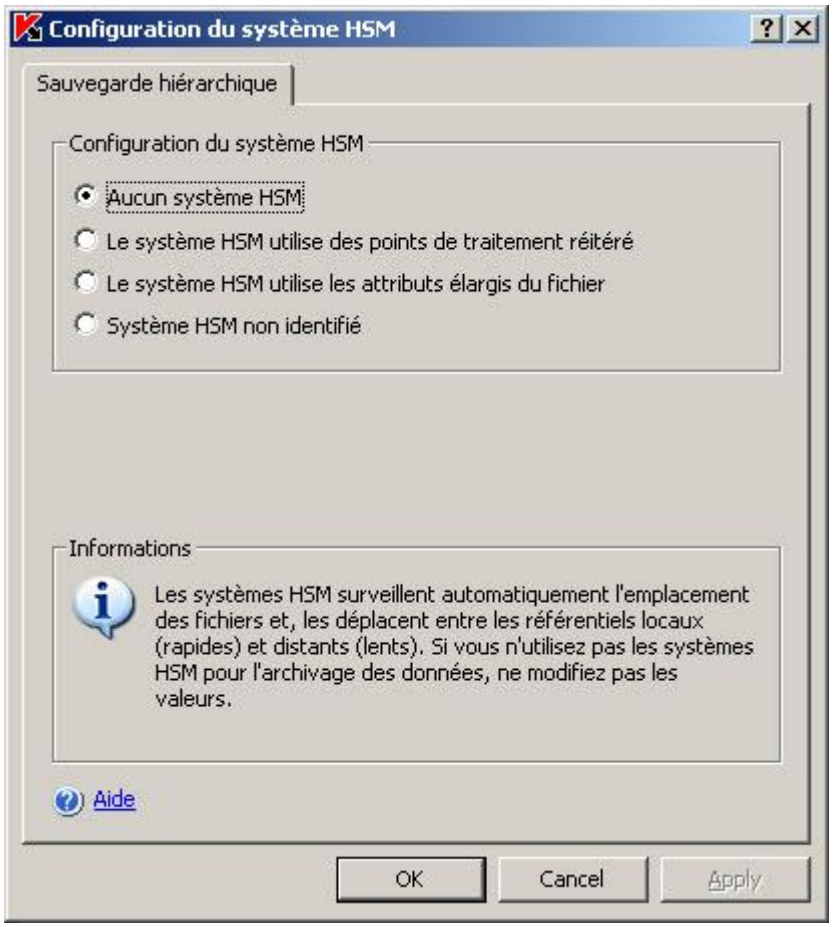


*Illustration 112. Boîte de dialogue **Paramètres avancés de l'application**, onglet **Sauvegarde hiérarchique***

Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut du paramètre **Type d'accès à la sauvegarde hiérarchique** (**Aucun système HSM**).

5. Après avoir modifié les valeurs des paramètres requis de Kaspersky Anti-Virus, cliquez sur **OK** dans la boîte de dialogue **Paramètres de l'application**.

CONFIGURATION DE PARAMETRES DES JOURNAUX DANS KASPERSKY ADMINISTRATION KIT

Pour configurer les paramètres des journaux de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvre la boîte de dialogue **Paramètres de l'application** (cf. page 304).

2. Sous l'onglet **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Journaux d'exécution des tâches** (cf. ill. ci-après).

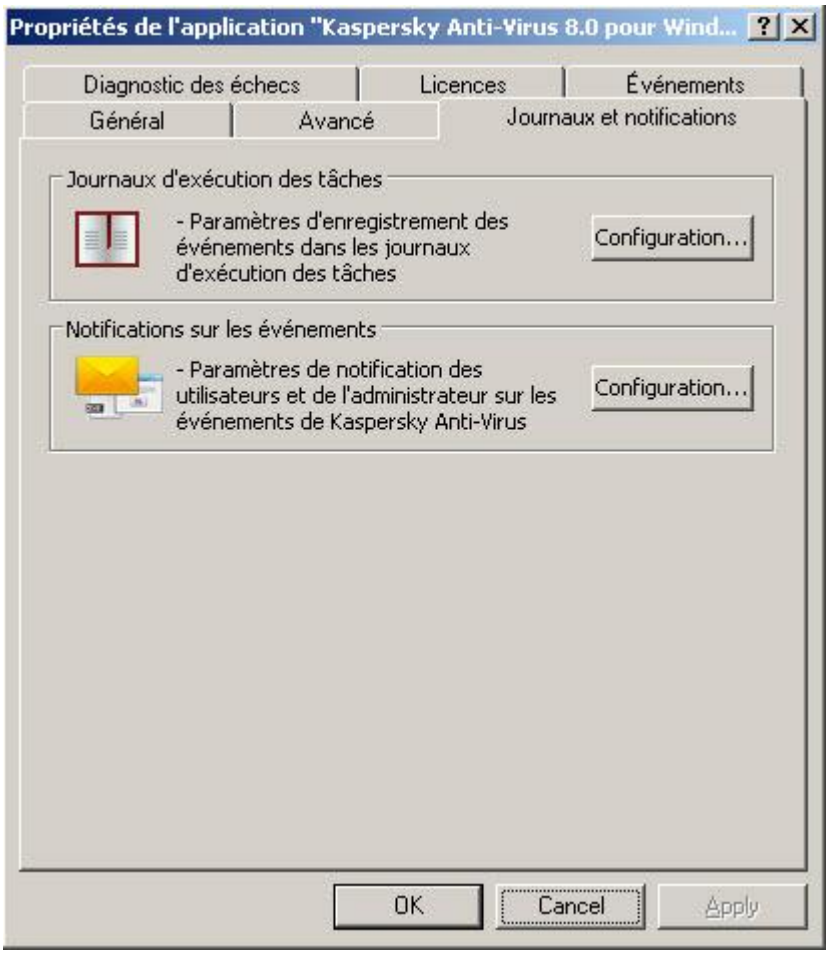


*Illustration 113. Boîte de dialogue **Paramètres de l'application**, onglet **Journaux et notifications***

3. Dans la boîte de dialogue **Propriétés des journaux**, configurez les paramètres suivants de Kaspersky Anti-Virus en fonction de vos besoins (cf. ill. ci-après) :

   - Configurez le niveau de détail des événements dans les journaux (cf. page 367). Pour ce faire, exécutez les actions suivantes :

     a. Dans la liste **Composant**, sélectionnez le composant de Kaspersky Anti-Virus pour lequel vous souhaitez indiquer le niveau de détails.

     b. Pour définir le niveau de détails dans les journaux d'exécution des tâches et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Degré d'importance**.

   - Pour modifier l'emplacement des journaux par défaut (cf. page 368), indiquez le chemin d'accès complet au dossier ou cliquez sur le bouton **Parcourir**.

   - Indiquez la durée de conservation en jour des journaux d'exécution des tâches (cf. page 368).

- Indiquez le nombre de jours pendant lesquels les informations reprises dans le nœud **Journal d'audit système** (cf. page 369) seront conservées.

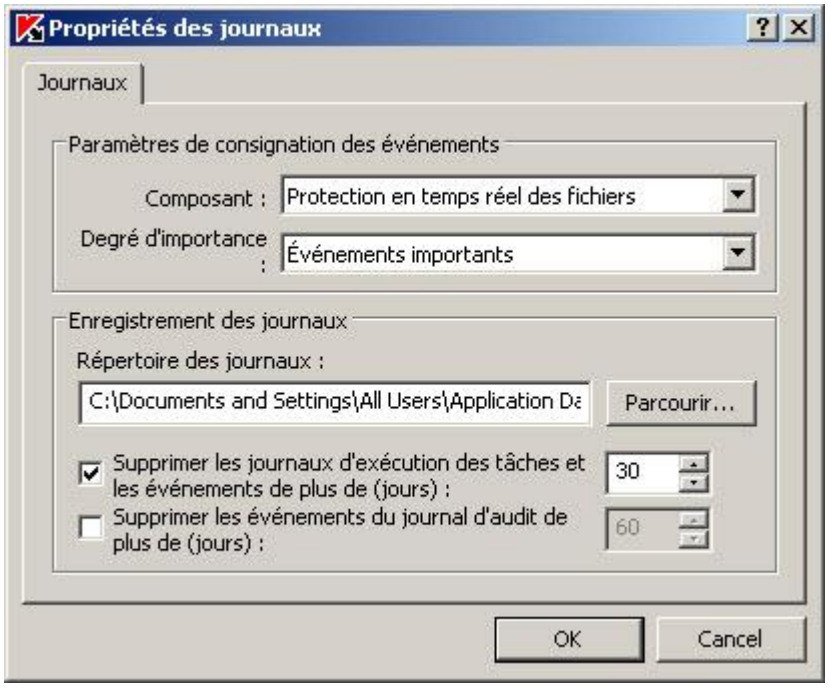


*Illustration 114. Boîte de dialogue **Propriétés des journaux***

4. Après avoir modifié les valeurs des paramètres des journaux de Kaspersky Anti-Virus, cliquez sur **OK**.

5. Cliquez sur **Ok** dans la boîte de dialogue **Paramètres de l'application**.

CREATION ET CONFIGURATION DE STRATEGIES

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES STRATEGIES

Vous pouvez créer des stratégies de Kaspersky Administration Kit unique pour l'administration de la protection de plusieurs serveurs sur lesquels Kaspersky Anti-Virus est installé.

Une stratégie applique les paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches à l'ensemble des serveurs protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la console d'administration, la stratégie active dans le groupe en ce moment possède l'état *active*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Anti-Virus. Vous pouvez la consulter dans la console de Kaspersky Anti-Virus dans le nœud **Journal d'audit système**.

N'oubliez pas que Kaspersky Administration Kit 8.0 permet uniquement d'appliquer les stratégies selon le mode **Modifier les paramètres obligatoires**. Dans le cadre de la stratégie, Kaspersky Anti-Virus applique les valeurs des paramètres en regard desquels vous avez coché la case dans les propriétés de la stratégie au lieu de la valeur des paramètres effectifs avant l'application de la stratégie. Les paramètres accompagnés de l'icône dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Anti-Virus. Dès que l'action de la stratégie est terminée, les paramètres dont la valeur ont été modifiés par la stratégie, reprennent la valeur qu'ils avaient avant l'exécution de celle-ci.

Tandis que la stratégie est appliquée, la console de Kaspersky Anti-Virus et la boîte de dialogue **Paramètres de l'application** de la console d'administration affichent les valeurs des paramètres marqués dans la stratégie par l'icône ; ils ne peuvent être modifiés. Les valeurs des autres paramètres (indiqués dans la stratégie par l'icône) peuvent être modifiés dans la console de Kaspersky Anti-Virus et dans la boîte de dialogue **Paramètres de l'application** de la console d'administration.

Si la stratégie défini les paramètres d'une tâche quelconque de protection en temps réel et si cette tâche est en exécution, les paramètres définis par la stratégie sont appliqués directement après que la stratégie devient active. Si la tâche n'est pas exécutée, alors les paramètres sont appliqués à son lancement. Si la stratégie définit les paramètres de tâches de mise à jour ou de tâches d'analyse à la demande, alors quand la stratégie devient active, ces paramètres ne sont pas appliqué aux tâches en cours d'exécution mais uniquement lors du prochain lancement de la tâche.

CREATION D'UNE STRATEGIE DANS KASPERSKY ADMINISTRATION KIT

La création d'une stratégie comporte les étapes suivantes :

1. Vous pouvez créer une stratégie à l'aide de l'Assistant de création de stratégie. Vous pouvez définir les paramètres de la protection en temps réel dans les fenêtres de l'Assistant.

2. Dans la boîte de dialogue **Propriétés** de la stratégie créée, vous pouvez configurer les paramètres de la protection en temps réel, les paramètres généraux de Kaspersky Anti-Virus, les paramètres de la quarantaine et de la sauvegarde, le niveau de détail des journaux d'exécution des tâches, les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Anti-Virus. Lisez la rubrique consacrée à la configuration de la stratégie créée (cf. page 336).

Pour créer une stratégie pour un groupe de serveurs sur lesquels Kaspersky Anti-Virus est installé, procédez comme suit :

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis déployez le groupe d'administration pour lequel vous souhaitez créer une stratégie.

2. Dans le menu contextuel du nœud **Stratégies**, sélectionnez la commande **Créer → Stratégie**.

   Cette action entraîne l'ouverture de l'Assistant de création de stratégies.

3. Dans le champ de saisie de la fenêtre **Nom de la stratégie**, tapez le nom de la stratégie à créer (il ne doit pas contenir les caractères **" * < : > ? \ / |**).

4. Sous l'onglet **Nom de l'application** de la fenêtre **Application**, sélectionnez l'option **Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition**.

5. Sélectionnez un des états de stratégie suivant dans la fenêtre **Nouvelle stratégie** :

   - **Stratégie active**, si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, celle-ci deviendra inactive et la stratégie que vous venez de créer sera activée.

   - **Stratégie inactive**, si vous ne voulez pas utiliser immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.

6. Sélectionnez une des options suivantes (cf. ill. ci-après) dans la fenêtre **Sélection du type** :

- **Créer** pour créer une stratégie reprenant les paramètres définis pour les stratégies créées par défaut ;
- **Importer la stratégie de la version d'Anti-Virus précédente** afin d'utiliser en guise de modèle une stratégie de Kaspersky Anti-Virus 6.0 pour Windows Servers ou Kaspersky Anti-Virus 6.0 pour Windows Servers Enterprise Edition.

Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de configuration dans lequel vous aviez enregistré la stratégie existante.

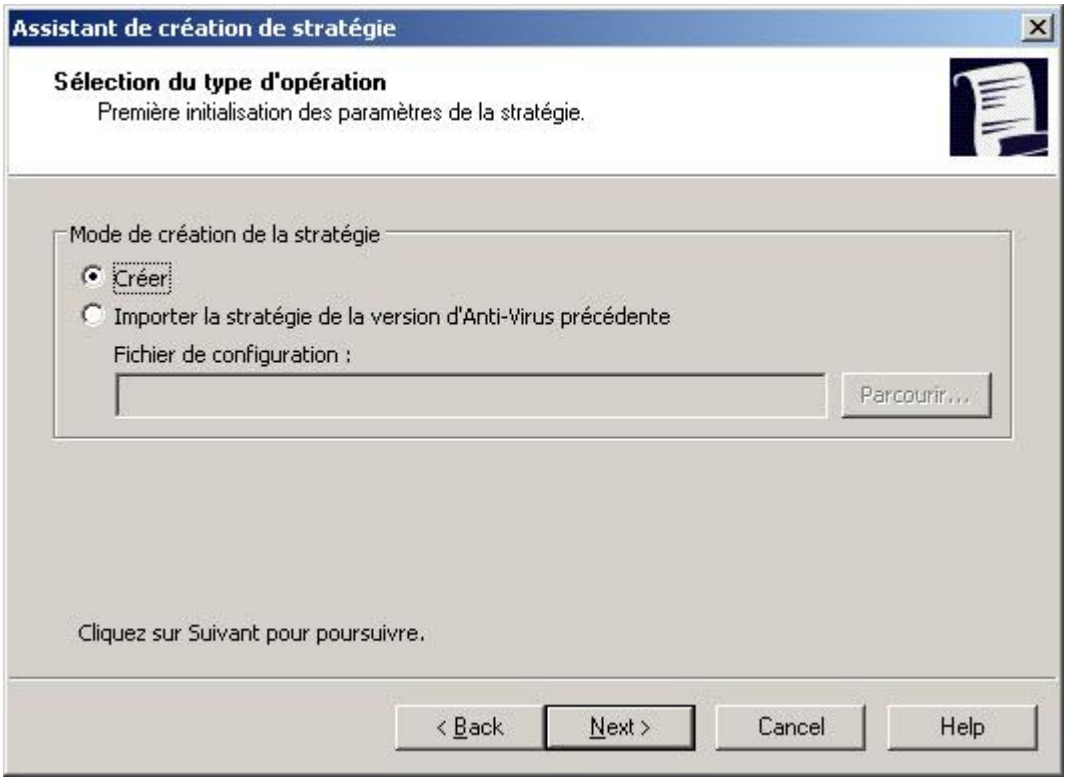


Illustration 115. ***Mode de création de la stratégie*** *(fenêtre)*

7. Dans la fenêtre **Protection en temps réel**, configurez, le cas échéant, les paramètres de la tâche **Protection en temps réel des fichiers** et de la tâche **Analyse des scripts** en fonction de vos besoins (cf. ill. ci-après).

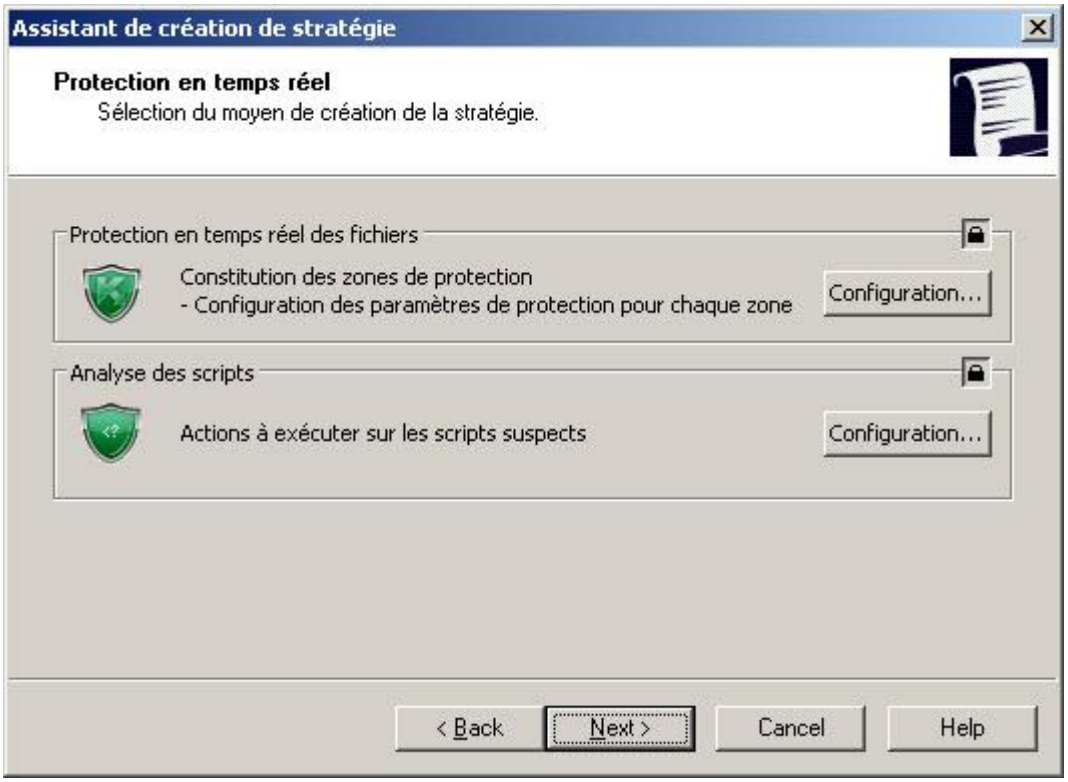


*Illustration 116. **Protection en temps réel** (fenêtre)*

Dans la nouvelles stratégie, les paramètres de la tâche **Protection en temps réel des fichiers** sont définis par défaut (cf. rubrique "Configuration de la tâche Protection en temps réel des fichiers" à la page 87), les paramètres de la tâche **Analyse des scripts** sont également définis par défaut (cf. page 108).

- Pour modifier les paramètres de la tâche **Protection en temps réel des fichiers**, cliquez sur le bouton **Configuration** du groupe de paramètres **Protection en temps réel des fichiers** et dans la boîte de dialogue **Paramètres**, configurez la zone de protection et choisissez un des niveaux de protection prédéfinis ou configurez manuellement les paramètres de la protection (cf. rubrique "Paramètres de la protection de la tâche Protection en temps réel des fichiers et des tâches d'analyse à la demande" à la page 375), sélectionnez le mode de protection des objets, configurez l'utilisation de l'analyseur heuristique, configurez l'application de la zone de confiance (cf. ill. ci-après). Programmez l'exécution de la tâche. Cliquez sur **OK**.

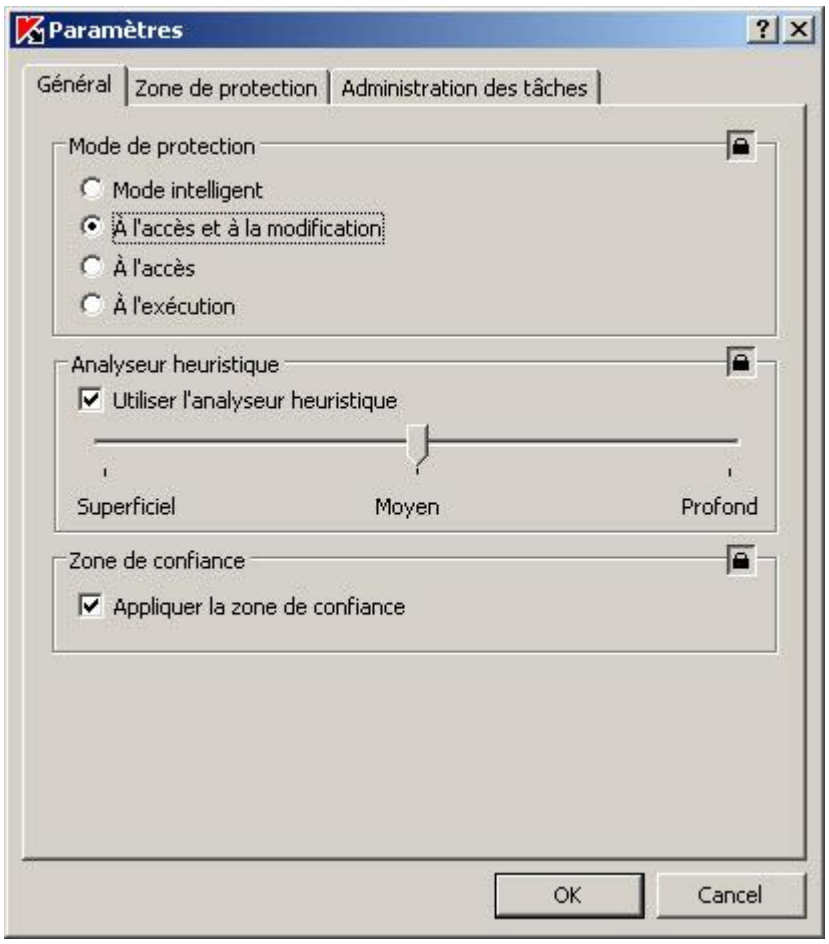


Illustration 117. Configuration des paramètres de la protection en temps réel

- Pour modifier les paramètres de la tâche **Analyse des scripts**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Analyse des scripts** et dans la boîte de dialogue **Paramètres**, configurez les paramètres de la tâche conformément à vos exigences (cf. ill. ci-après). Programmez l'exécution de la tâche. Cliquez sur **OK**.

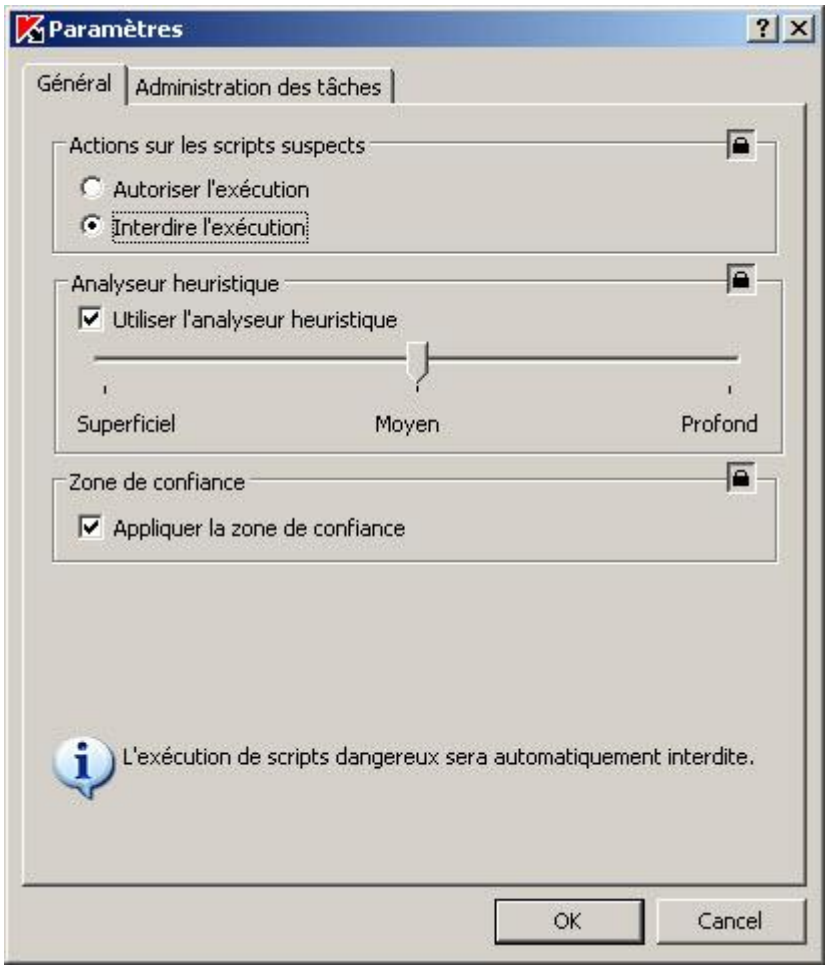


Illustration 118. Configuration des paramètres d'analyse des scripts

8. Dans la fenêtre **Fin du travail** de l'Assistant, cliquez sur le bouton **Terminer**.

   La stratégie créée est reprise dans la liste des stratégies du nœud **Stratégies** du groupe d'administration sélectionné. Dans la boîte de dialogue **Propriétés : <Nom de la stratégie>**, vous pouvez configurer d'autres paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches.

CONFIGURATION DE STRATEGIES DANS KASPERSKY ADMINISTRATION KIT

Dans la boîte de dialogue **Propriétés : <nom de la stratégie>** de la stratégie existante, vous pouvez configurer les paramètres uniques de la protection en temps réel, les paramètres généraux de Kaspersky Anti-Virus, les paramètres de la quarantaine et de la sauvegarde, le niveau de détail des journaux d'exécution des tâches, les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Anti-Virus.

➧ *Pour configurer les paramètres de la stratégie dans la boîte de dialogue **Propriétés : <nom de la stratégie>**, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés** puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie puis déployez le nœud **Stratégies**.

2. Dans l'arborescence de la console d'administration, déployez le nœud **Stratégie**, ouvrez le menu contextuel de la stratégie dont vous souhaitez configurer les paramètres et choisissez l'option **Propriétés**.

   Dans la boîte de dialogue **Propriétés : <nom de la stratégie>**, configurez les paramètres requis de la stratégie (cf. ill. ci-après).

*Illustration 119. Exemple de boîte de dialogue **Propriétés : <nom de la stratégie>***

L'onglet **Protection en temps réel** permet de configurer les paramètres suivants de la protection en temps réel :

- dans la tâche **Protection en temps réel des fichiers** :
  - Zone de protection ;
  - Paramètres de protection pour la zone de protection sélectionnée : niveau de protection prédéfini (cf. page 144) ou configuration manuelle des paramètres de protection (comme dans la console de Kaspersky Anti-Virus) (cf. page 147).
  - mode de protection (cf. page 375) ;
  - application de l'analyseur heuristique (cf. page 393) ;
  - application de la zone de confiance (cf. page 178).
- dans la tâche **Analyse des scripts** :
  - autorisation ou interdiction de l'exécution de scripts suspects (cf. page 87) ;

- application de l'analyseur heuristique (cf. page 393) ;
- application de la zone de confiance (cf. page 178).

L'onglet **Avancé** permet de configurer les paramètres généraux de Kaspersky Anti-Virus, les paramètres de la quarantaine et de la sauvegarde de la même manière que dans la boîte de dialogue **Paramètres de l'application** (cf. ill. ci-après).

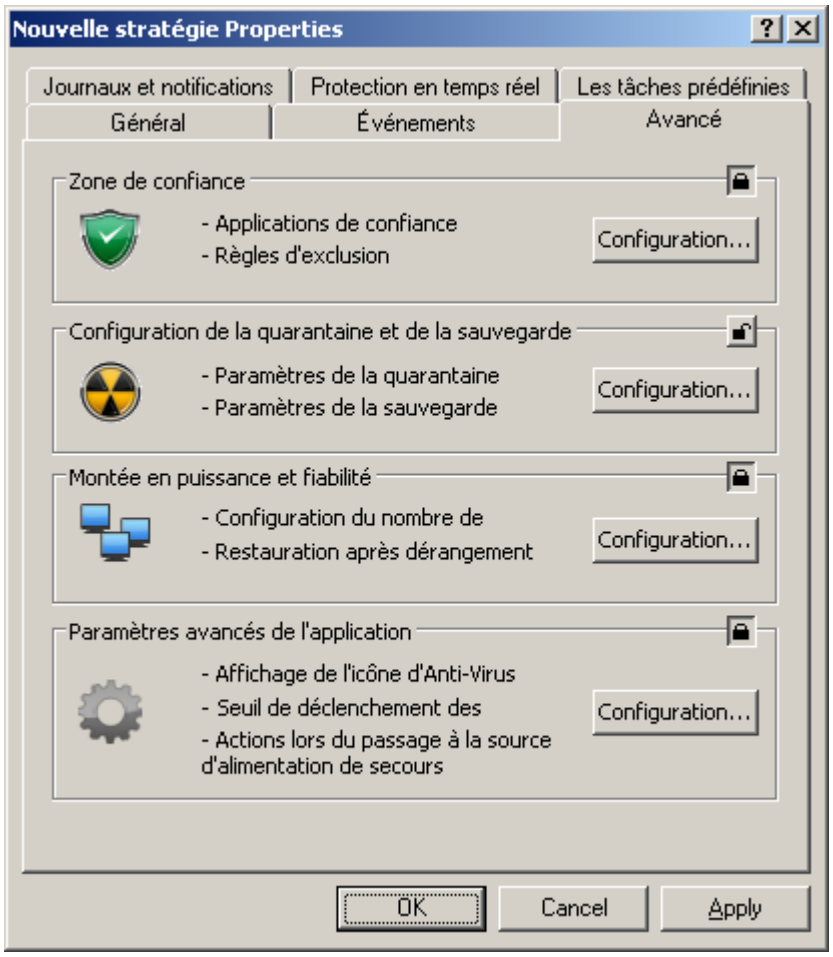


*Illustration 120. Boîte de dialogue **Propriétés : <nom de la stratégie>**, onglet **Avancé***

Sous l'onglet **Journaux** et notifications, configurez les paramètres des objets suivants (cf. ill. ci-après) :

- Journaux d'exécution des tâches et du journal d'audit système. Comme dans la boîte de dialogue **Paramètres de l'application** (cf. page 329).

- Notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Anti-Virus. Comme dans la boîte de dialogue **Paramètres de l'application** (cf. page 322).

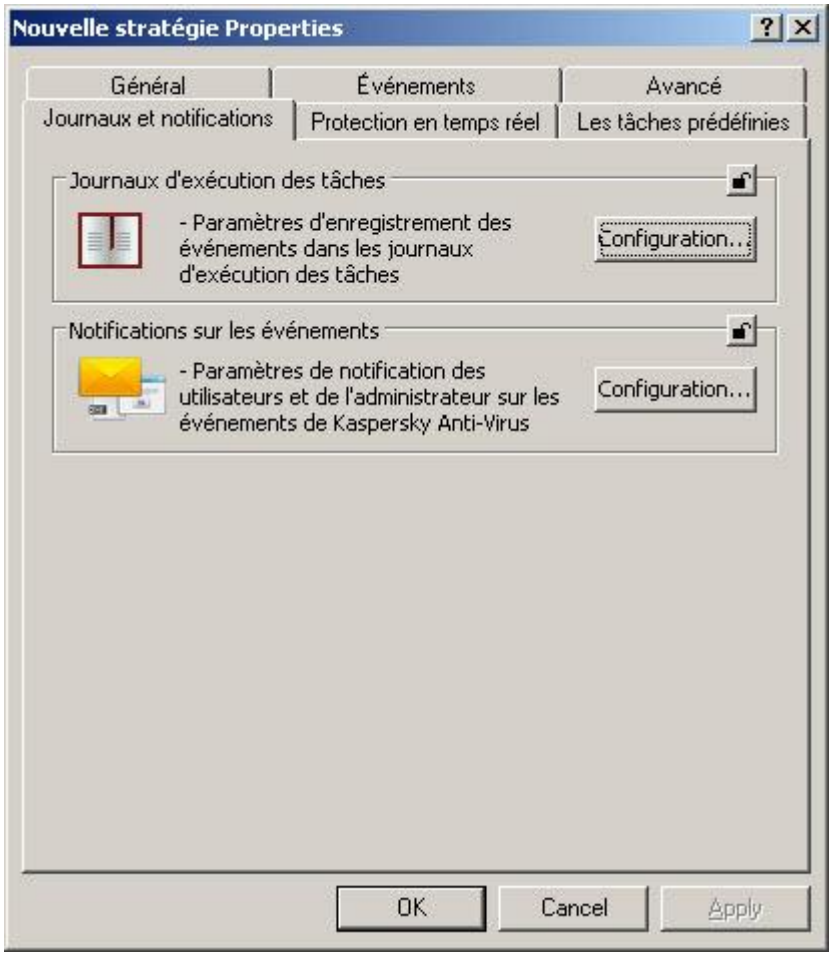


*Illustration 121. Boîte de dialogue **Propriétés : <nom de la stratégie>**, onglet **Journaux et notifications***

3. Une fois que vous aurez configuré les paramètres requis, cliquez sur le bouton **OK** pour enregistrer les modifications.

DESACTIVATION DE L'EXECUTION PROGRAMMEE DES TACHES PREDEFINIES LOCALES

Grâce aux stratégies, vous pouvez désactiver la planification des tâches prédéfinies locales suivantes sur l'ensemble des serveurs d'un groupe d'administration :

- tâches d'analyse à la demande : **Analyse des zones critiques**, **Analyse des objets en quarantaine** et **Analyse au démarrage du système** ;
- tâches de mise à jour : **Mise à jour des bases de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**.

Si vous excluez le serveur protégé du groupe d'administration, la planification des tâches prédéfinies sera automatiquement activée.

Pour désactiver l'exécution programmée d'une tâche prédéfinie de Kaspersky Anti-Virus sur les serveurs du groupe, procédez comme suit :

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, déployez ensuite le groupe requis puis, sélectionnez le nœud **Stratégies**.

2. Dans le volet des résultats, ouvrez le menu contextuel de la stratégie à l'aide de laquelle vous souhaitez désactiver l'exécution programmée des tâches système de Kaspersky Anti-Virus sur les serveurs du groupe et choisissez l'option **Propriétés**.

3. Dans la boîte de dialogue **Propriétés : <nom de la stratégie>**, ouvrez l'onglet **Tâches prédéfinies** (cf. ill. ci-après).

4. Décochez la case en regard des tâches prédéfinies proposées dont vous souhaitez suspendre l'exécution programmée.

   Pour rétablir l'exécution programmée des tâches prédéfinies du type requis, cochez la case en regard des tâches requises.

5. Cliquez sur **OK**.

Si vous désactivez l'exécution programmée des tâches prédéfinies, vous pourrez les lancer manuellement aussi bien au départ de la Console de Kaspersky Anti-Virus qu'au départ de la console d'administration Kaspersky Administration Kit.

CREATION ET CONFIGURATION DES TACHES

DANS CETTE SECTION DE L'AIDE

PRESENTATION DE LA CREATION DES TACHES

Vous pouvez créer des tâches locales définies par l'utilisateur, des tâches pour une sélection d'ordinateurs et des tâches de groupes des types suivants :

- analyse à la demande ;
- tâches de mise à jour ;
- retour à l'état antérieur à la mise à jour des bases ;
- installation d'une licence.

Vous créez les tâches locales pour le serveur sélectionné protégé dans la boîte de dialogue **Paramètres** de l'application sous l'onglet **Tâches** ; les tâches de groupe sont créées dans le nœud **Tâches de groupe** du groupe sélectionné, tandis que les tâches pour plusieurs ordinateurs qui n'appartiennent pas à un groupe sont créées dans le nœud **Tâches pour les sélections d'ordinateurs**.

Les stratégies permettent de suspendre la programmation des tâches locales système de mise à jour et d'analyse à la demande sur tous les serveurs protégés appartenant à un groupe d'administration.

Vous trouverez toutes les informations sur les tâches de Kaspersky Administration Kit dans le document intitulé *Kaspersky Administration Kit. Manuel de l'administrateur*.

CREATION D'UNE TACHE DANS KASPERSKY ADMINISTRATION KIT

Pour créer une tâche dans la console d'administration Kaspersky Administration Kit :

1. Lancez l'Assistant de création de tâche de la catégorie requise :

   - *Pour créer une tâche locale* :

     a. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

     b. Dans le volet des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur le serveur protégé et choisissez l'option **Propriétés**.

     c. Sous l'onglet **Tâches**, cliquez sur le bouton **Ajouter**.

   - *Pour créer une tâche de groupe* :

     a. Dans l'arborescence de la console d'administration, sélectionnez le groupe pour lequel vous souhaitez créer une tâche de groupe.

     b. Ouvrez le menu contextuel du sous-répertoire **Tâches de groupe** et choisissez la commande **Créer → Tâche**.

   - *Pour créer une tâche pour une sélection quelconque d'ordinateurs,* ouvrez, dans l'arborescence de la console d'administration, le menu contextuel du nœud **Tâches pour une sélection d'ordinateurs** et choisissez l'option **Créer → Tâche**.

   La fenêtre d'accueil de l'Assistant de création de tâche s'ouvre.

2. Dans la fenêtre **Nom de tâche** de l'Assistant de création de tâche, saisissez le nom de la tâche (100 caractères maximum, ne peut contenir les caractères **I * < > ? \ / | :)**. Il est conseillé d'indiquer le type de tâche dans son nom (par exemple, Analyse à la demande du dossier partagé).

3. Dans la fenêtre **Type de tâche**, sous l'onglet **Kaspersky Anti-Virus 8.0 pour Windows Servers Enterprise Edition**, sélectionnez le type de la tâche créée.

4. Si vous avez choisi n'importe quel type de tâche, à l'exception de **Annulation de la mise à jour des bases** ou de **Installation de la licence**, la fenêtre **Configuration** (cf. ill. ci-après) s'ouvre. Sélectionnez une des options suivantes :

   - **Créer** pour créer une tâche selon les paramètres définis par défaut pour les tâches du type que vous avez sélectionné ;

   - **Importer la tâche de la version d'Anti-Virus précédente** afin d'utiliser en guise de modèle une tâche de Kaspersky Anti-Virus 6.0 pour Windows Servers ou Kaspersky Anti-Virus 6.0 pour Windows Servers Enterprise Edition.

Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de configuration dans lequel vous aviez enregistré la tâche existante.

*Illustration 122. Fenêtre **Sélection du mode de création de la tâche** de l'Assistant*

5. En fonction du type de tâche créée, exécutez une des actions suivantes :

   - *Si vous créez une tâche d'analyse à la demande* :

     a. Dans la fenêtre **Zone d'analyse**, définissez la couverture de l'analyse.

La zone d'analyse reprend par défaut les secteurs critiques du serveur (cf. ill. ci-après). Les zones analysées sont accompagnées d'une coche dans le tableau ☑.

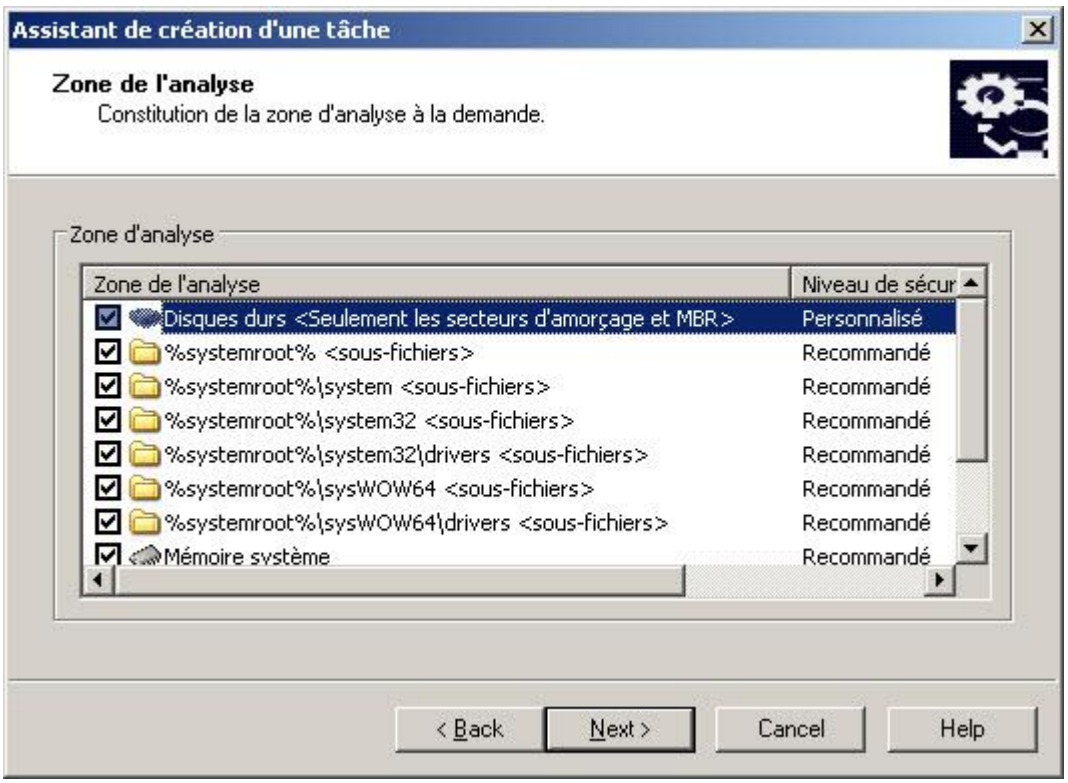


*Illustration 123. Fenêtre **Zone d'analyse** de l'Assistant de création de tâche*

Vous pouvez modifier la zone d'analyse, y inclure des zones distinctes prédéfinies, des disques, des dossiers et des fichiers et définir les paramètres particuliers de la protection pour chaque zone ajoutée.

- Pour exclure tous les secteurs critiques de l'analyse, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.

- Pour inclure une zone prédéfinie, un disque, un dossier ou un fichier à la zone d'analyse, cliquez avec le bouton droit de la souris dans le tableau **Zone d'analyse** et choisissez l'option **Ajouter une zone d'analyse**. Dans la fenêtre **Ajout d'objets à la zone d'analyse** (cf. ill. ci-dessous), sélectionnez une zone prédéfinie dans la liste **Zone de l'analyse prédéfinie**, désignez le disque du serveur, le dossier ou le fichier sur le serveur ou un autre ordinateur du réseau, puis cliquez sur **OK**.

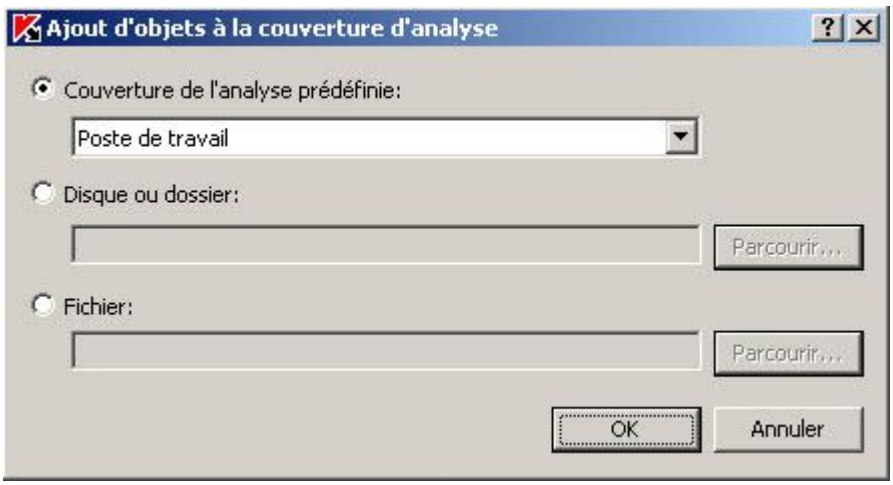


*Illustration 124. Boîte de dialogue **Ajout d'objets à la zone d'analyse***

- Pour exclure des dossiers ou fichiers intégrés de l'analyse, sélectionnez le dossier (ou le disque) ajouté dans la fenêtre **Zone d'analyse** de l'Assistant, ouvrez le menu contextuel et choisissez l'option **Configurez**, puis dans la fenêtre **Configuration de l'analyse à la demande**, cliquez sur le bouton **Configuration** et sous l'onglet **Général**, décochez la case **Sous-dossiers** (**Sous-fichiers**).

- Pour modifier les paramètre de la protection de la zone d'analyse, ouvrez le menu contextuel de la zone dont vous souhaitez modifier les paramètres et choisissez l'option **Configurer**. Dans la boîte de dialogue **Configuration de l'analyse à la demande**, sélectionnez un des niveaux de protection prédéfinis ou cliquez sur le bouton **Configuration** afin de configurer manuellement les paramètres de l'analyse. La configuration se déroule de la même manière que dans la console de Kaspersky Anti-Virus (cf. page 147).

- Pour exclure les objets intégrés de la zone d'analyse ajoutée, cliquez sur le bouton droit de la souris dans le tableau **Zone d'analyse**, sélectionnez **Ajouter une exclusion** et désignez les objets que vous voulez exclure : sélectionnez une zone définie dans la liste **Zone de l'analyse prédéfinie**, désignez le disque du serveur, le dossier ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur le bouton **OK**.

  Les zones exclues de l'analyse sont marquées de l'icône ☐ dans le tableau.

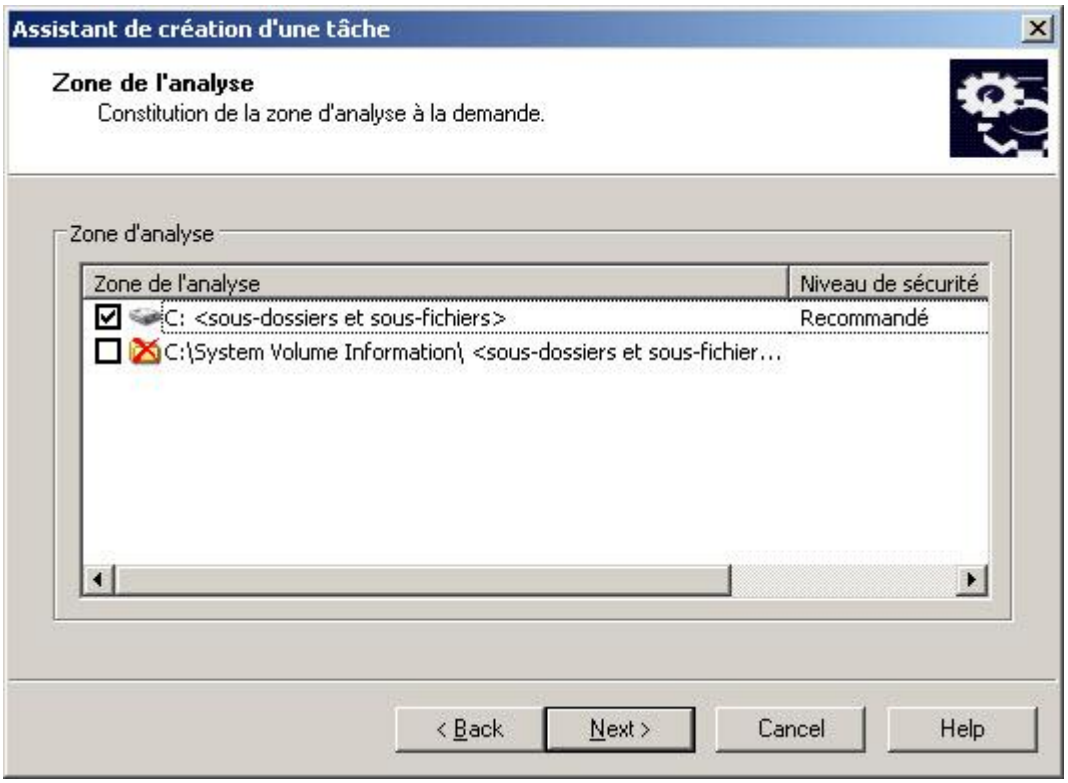


Illustration 125. Ajout d'exclusions à la zone d'analyse

a. Réalisez les actions suivantes dans la fenêtre **Avancé** (cf. ill. ci-après).

   Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure de l'analyse les objets décrits dans la zone de confiance de Kaspersky Anti-Virus. Lisez la rubrique consacrée à la zone de confiance de Kaspersky Anti-Virus (cf. page 178) pour en savoir plus ; lisez également la rubrique sur l'ajout d'exclusions à la zone de confiance dans l'application Kaspersky Administration Kit (cf. page 312).

   Si vous avez l'intention d'utiliser la tâche créée en tant que tâche d'analyse des secteurs critiques de l'ordinateur, cochez la case **Considérer comme une tâche d'analyse de secteurs critiques** dans la fenêtre **Avancé**. L'application Kaspersky Administration Kit évalue l'état de la sécurité du serveur (des serveurs) sur la base des résultats de l'exécution des tâches avec l'état "Tâche d'analyse des secteurs critiques" (cf. rubrique "Administration de l'analyse des serveurs. Attribution de l'état Tâche d'analyse

des secteurs critiques à la tâche d'analyse à la demande" à la page 354) et non pas seulement sur la base des résultats de l'exécution de la tâche prédéfinie **Analyse des secteurs critiques**.

Pour attribuer la priorité de base **Basse** (**Low**) au processus de travail dans lequel la tâche sera exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Avancé**. Par défaut, les processus dans lesquels les tâches de Kaspersky Anti-Virus sont exécutées ont la priorité de base **Moyenne** (**Normal**). La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

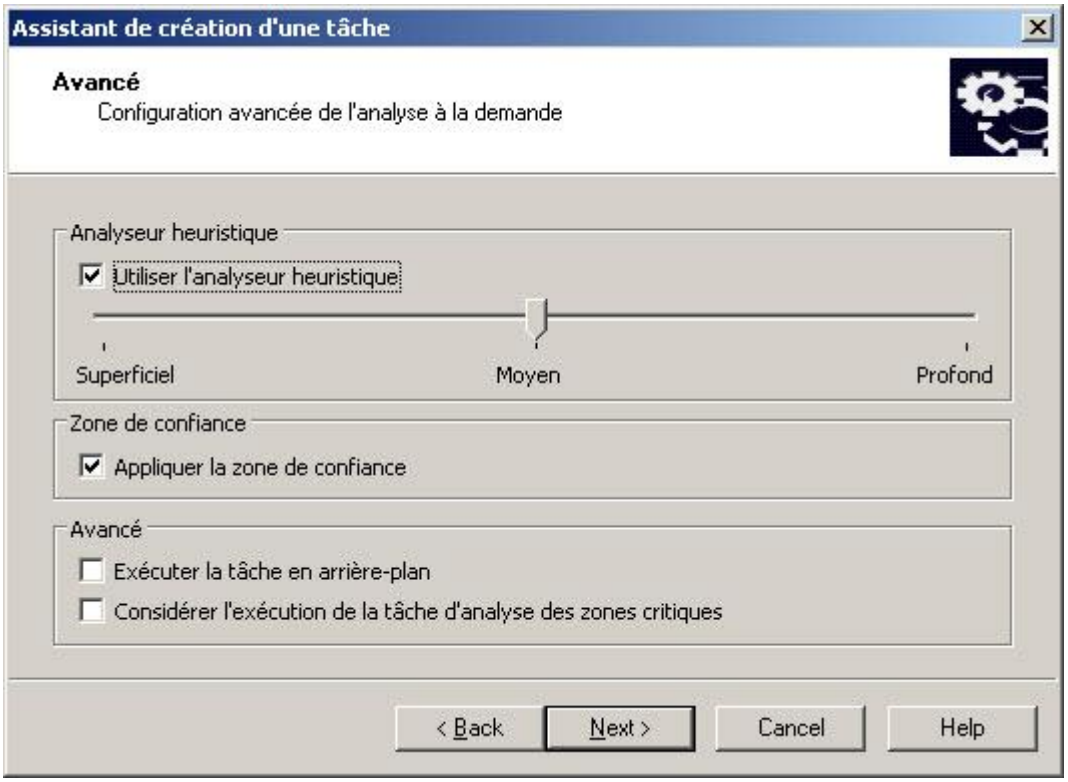


*Illustration 126. Fenêtre **Avancé** de l'Assistant de création d'une tâche d'analyse à la demande*

- *Si vous créez une des tâches de mise à jour*, définissez les paramètres de la tâche conformément à vos exigences:

a. Sélectionnez la source des mises à jour dans la fenêtre **Source des mises à jour** (cf. page 396).

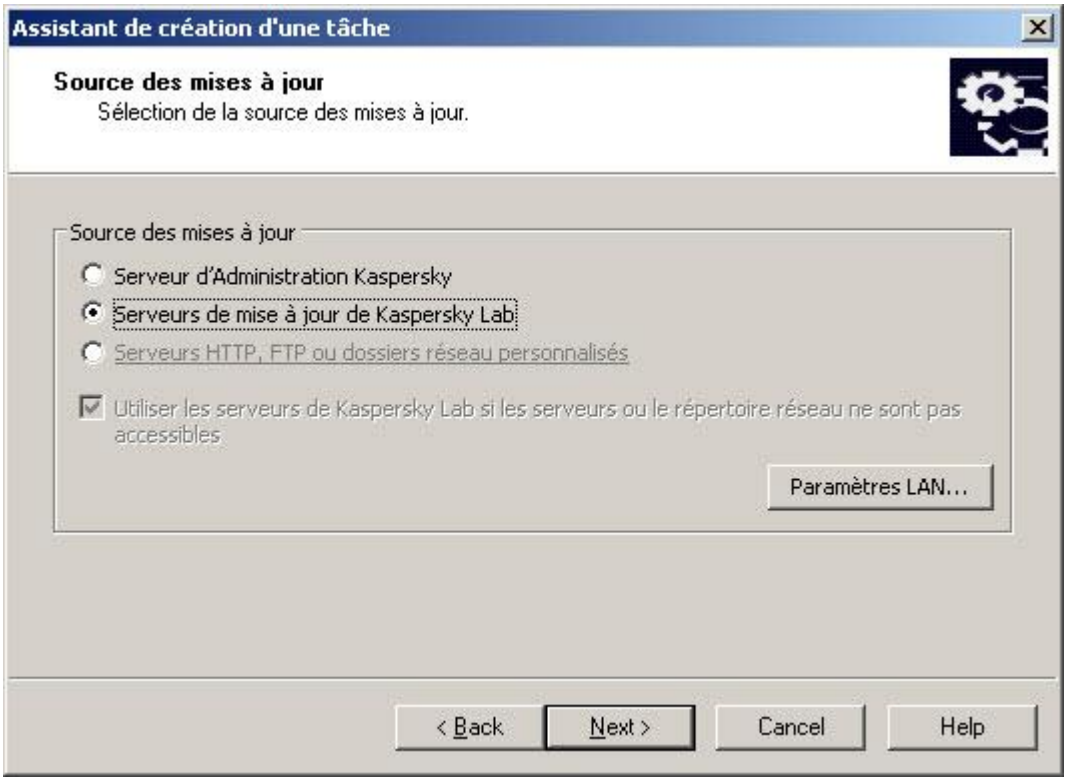


*Illustration 127. Fenêtre **Source des mises à jour** de l'Assistant de création de tâches*

b. Cliquez sur le bouton **Paramètres LAN**. La boîte de dialogue **Configuration de connexion** s'ouvre.

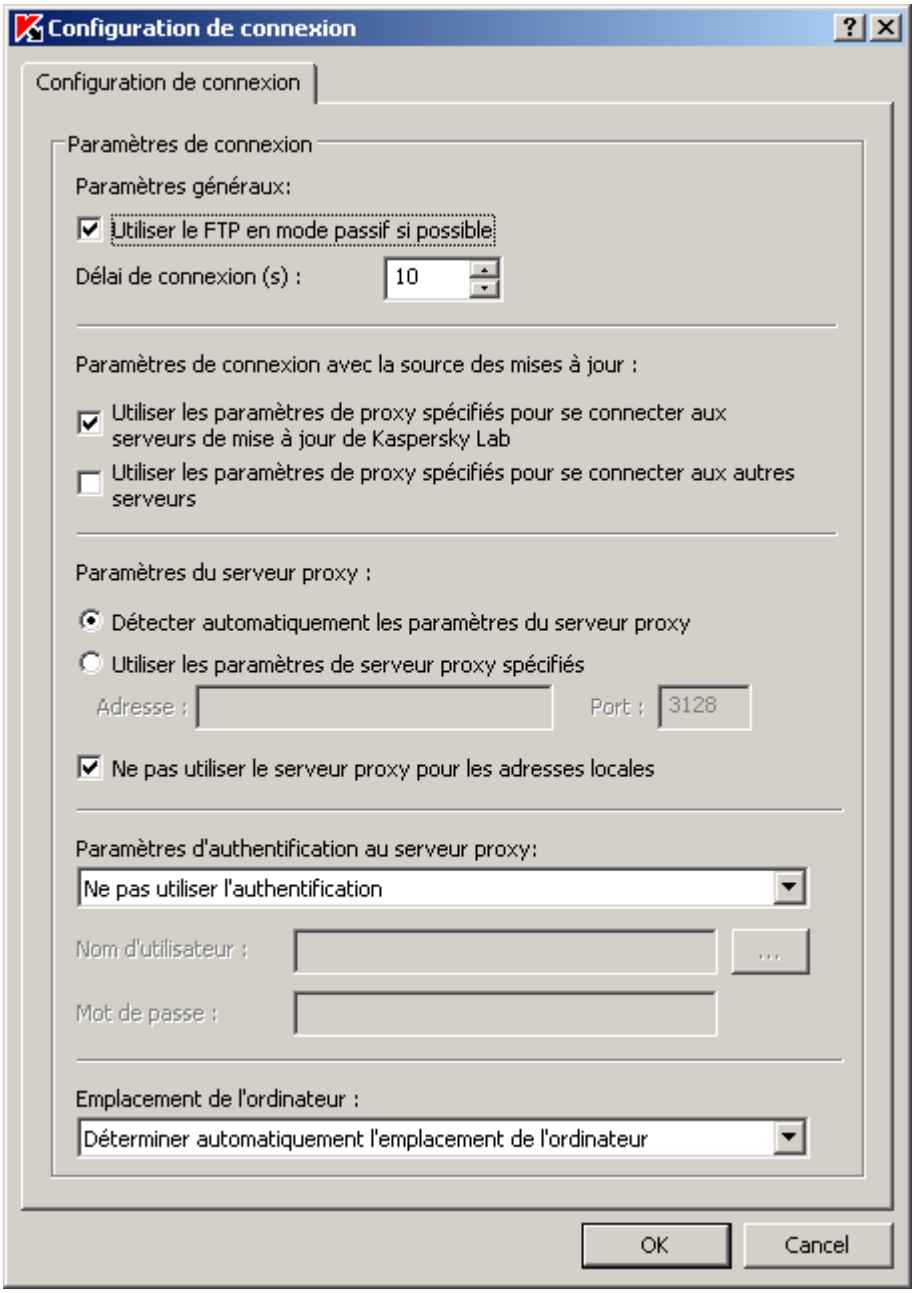


*Illustration 128. Boîte de dialogue **Configuration de connexion**.*

c. Sous l'onglet **Configuration de connexion**, procédez comme suit :

Sélectez Mode du serveur FTP pour la connexion au serveur protégé (cf. page 397).

Le cas échéant, modifiez le délai d'attente pour la connexion au serveur de mise à jour (cf. page 397).

Configurez les paramètres d'accès au serveur proxy lors de la connexion à la source des mises à jour (cf. page 399).

Indiquez l'emplacement du serveur protégé (ou des serveurs) pour optimiser la récupération des mises à jour (cf. page 401).

- *Si vous créez une tâche "Mise à jour des modules de l'application"*, configurez les paramètres requis de la mise à jour des modules de l'application dans la fenêtre **Configuration de la mise à jour** :

a. Décidez si vous souhaitez copier et installer les mises à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles (cf. page 402).

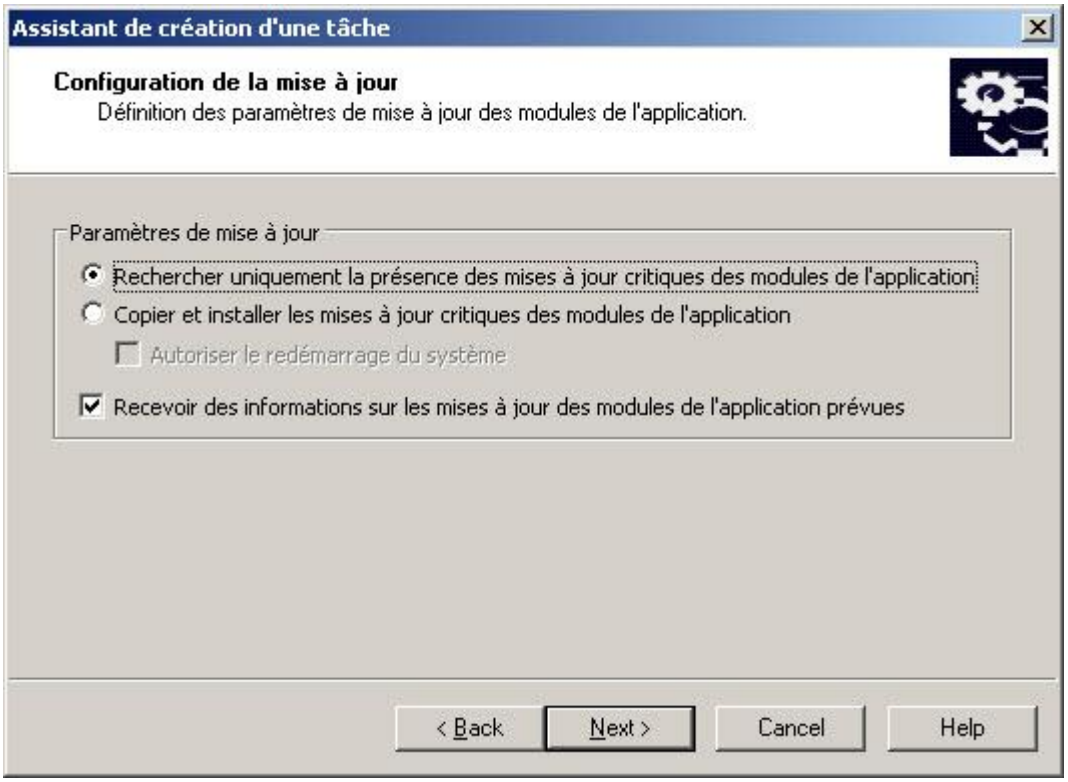


*Illustration 129. Fenêtre **Configuration des mises à jour** dans la tâche **Mise à jour des modules de l'application***

b. Si vous avez choisi **Copier et installer les mises à jour critiques des modules de l'application**, le redémarrage du serveur peut être requis pour terminer l'installation des modules de l'application. Pour que Kaspersky Anti-Virus relance automatiquement le serveur après la fin de la tâche, cochez la case **Autoriser le redémarrage du système**. Pour annuler le redémarrage automatique après la fin de la tâche, désélectionnez la case **Autoriser le redémarrage du système**.

c. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement **Des mises à jour prévues des modules de Kaspersky Anti-Virus sont disponibles**. Celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées. Vous trouverez des informations complémentaires sur la configuration des notifications dans la rubrique "Configuration des notifications"" (cf. page 262).

- *Si vous créez la tâche "Copie des mises à jour"*, indiquez, dans la fenêtre **Copie des mises à jour**, la composition des mises à jour (cf. page 404) et le dossier d'enregistrement de celles-ci.

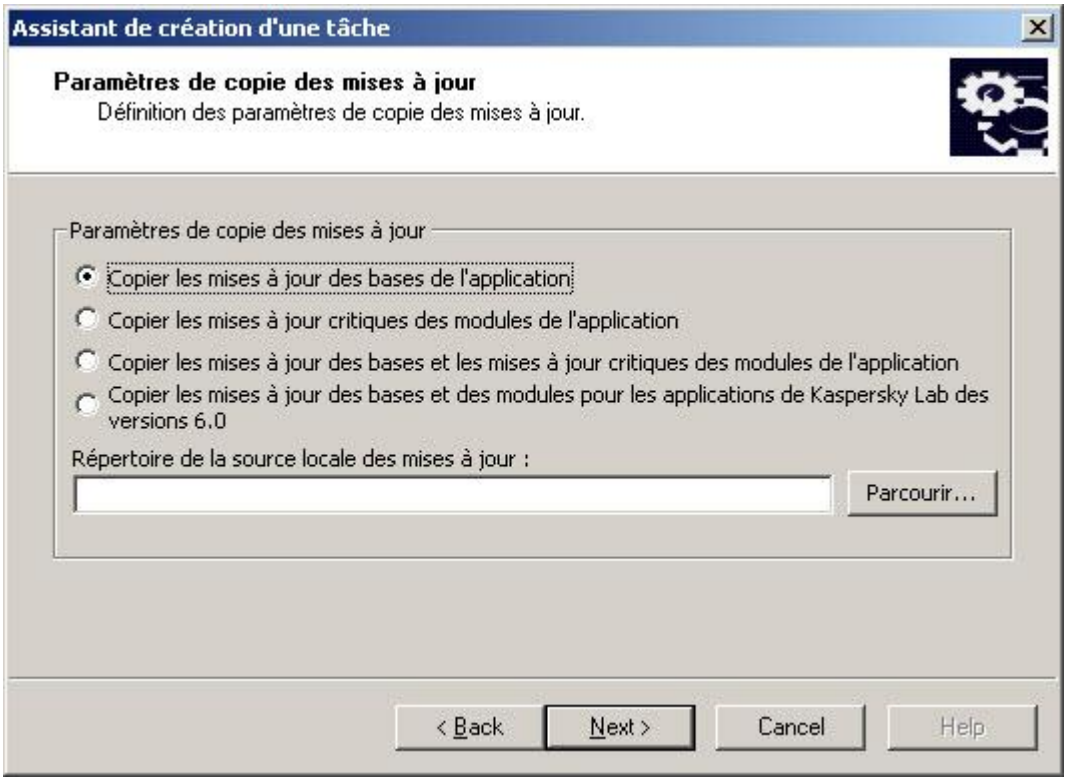


Illustration 130. ***Configuration de copie des mises à jour*** *(fenêtre)*

- *Si vous créez la tâche "Installation de la licence"*, dans le champ **Fichier de licence** de la fenêtre **Installation de la licence**, indiquez le nom du fichier de licence avec l'extension .key et le chemin d'accès complet à celui-ci.

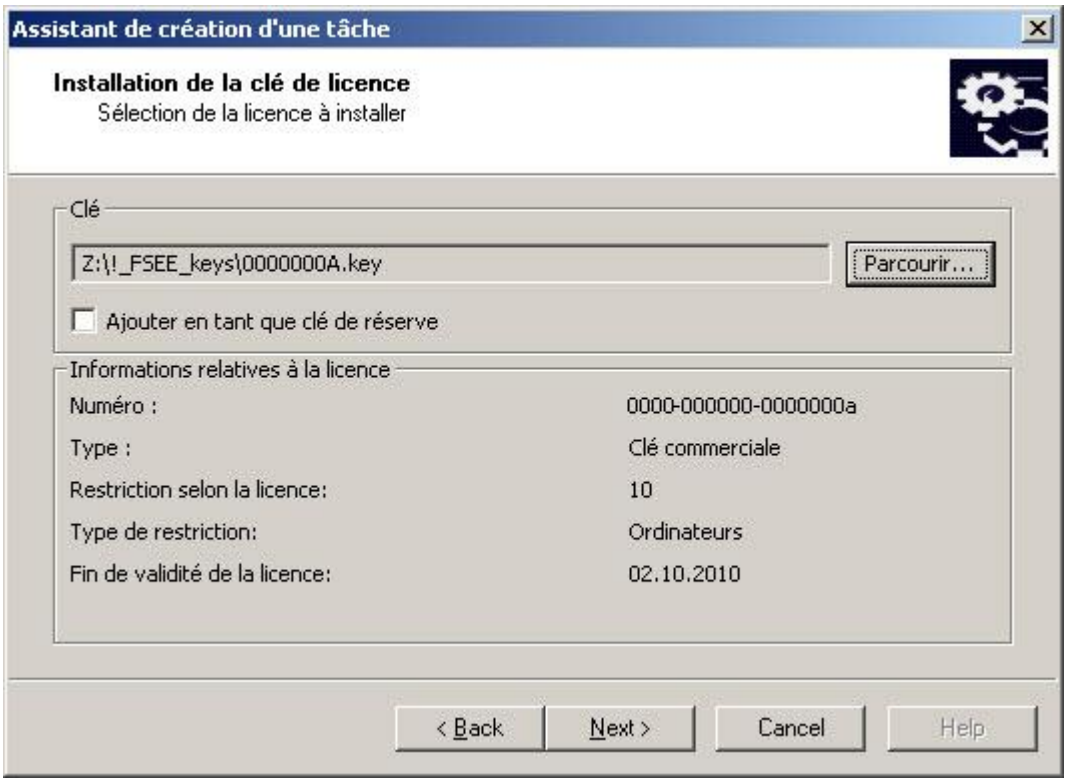


*Illustration 131. **Installation des licences** (fenêtre)*

6. Configurez les paramètres de la programmation de la tâche (vous pouvez configurer la programmation des tâches de tous les types à l'exception des tâches **Installer la licence** et **Annulation de la mise à jour**). Exécutez les actions suivantes dans la fenêtre **Planification** :

   a. Pour activer la planification, cochez la case **Exécuter de manière planifiée** ;

   b. Désignez la fréquence d'exécution de la tâche (cf. page 370): choisissez une des valeurs suivantes dans la liste **Fréquence d'exécution** : **Chaque heure**, **Chaque jour**, **Chaque semaine**, **Au lancement de l'application**, **À la mise à jour de la base antivirus** (dans les tâches **Mise à jour des bases de données de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**, vous avez également la possibilité de choisir la fréquence **Après réception des mises à jour par le serveur d'administration**) :

      - si vous avez sélectionné **Chaque heure**, indiquez le nombre d'heures dans le champ **Tous les <chiffres> heure(s)** du groupe de paramètres **Configuration du démarrage des tâches** ;

      - si vous avez sélectionné **Chaque jour**, indiquez le nombre de jours dans le champ **Tous les <chiffres> jour(s)** du groupe de paramètres **Configuration du démarrage des tâches** ;

- si vous avez sélectionné **Chaque semaine**, indiquez le nombre de semaines dans le champ **Tous les <chiffres> semaine(s)** du groupe de paramètres **Configuration du démarrage des tâches**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;

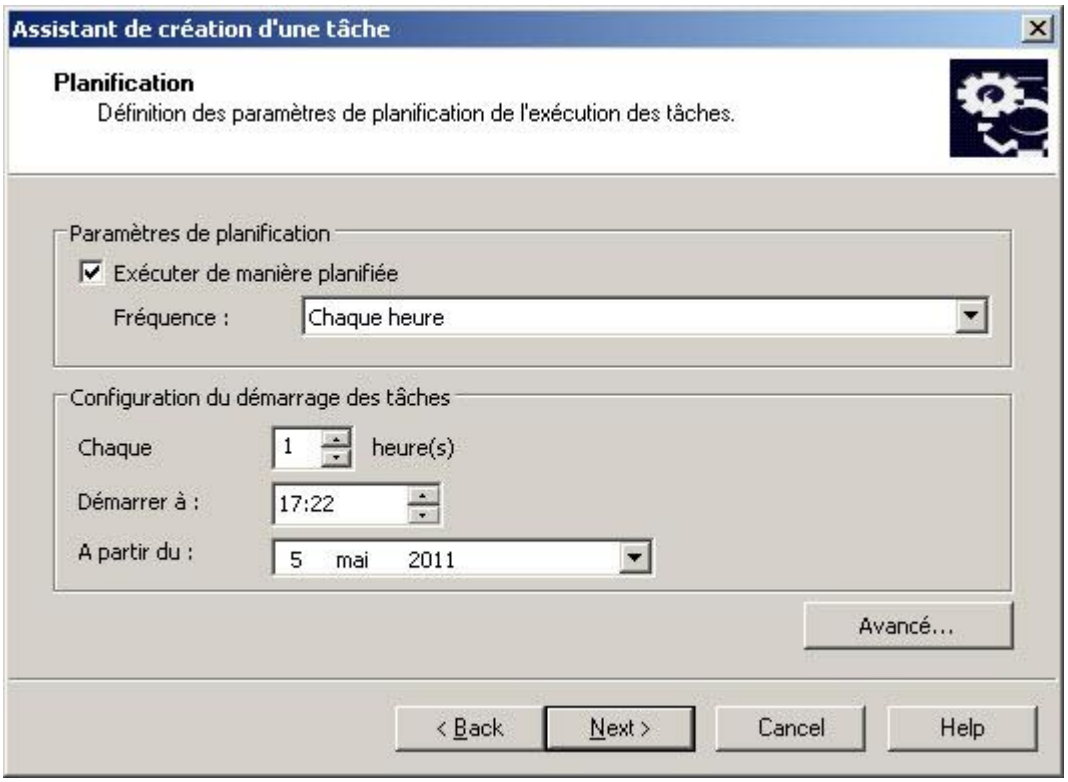


*Illustration 132. Exemple de la fenêtre **Programmation**, fréquence d'exécution **Chaque heure***

c. Dans le champ **A partir du**, indiquez l'heure de la première exécution de la tâche ;dans le champ **A partir du**, indiquez la date d'entrée en vigueur de la planification (cf. page 371).

d. Au besoin, définissez les paramètres complémentaires de la programmation : **Avancé** et dans la boîte de dialogue **Paramètres de planification avancé** procédez comme suit :

- Pour définir la durée maximale de l'exécution d'une tâche (cf. page 372), dans le groupe **Informations sur l'arrêt de la tâche**, champ **Durée**, saisissez le nombre d'heures et de minutes.

*Illustration 133. Boîte de dialogue **Paramètres de planification avancés***

- Indiquez l'intervalle de temps au cours d'une période de 24 heures pendant lequel l'exécution de la tâche sera suspendue (cf. page 373) : dans le groupe **Paramètres d'arrêt de la tâche**, saisissez l'heure de début et de fin de l'intervalle dans le champ **Pause à partir de … jusqu'à**.

- Indiquez la date à partir de laquelle la programmation ne sera plus active (cf. page 372) : cochez la case **Annuler la programmation à partir de** et à l'aide de la boîte de dialogue **Calendrier**, choisissez la date à partir de laquelle la programmation ne sera plus active.

- Activez le lancement des tâches ignorées (cf. page 373) : cochez la case **Lancer les tâches non exécutées**.

- Activez l'utilisation du paramètre de répartition de l'heure d'exécution (cf. page. 374) : cochez la case **Répartir l'heure d'exécution de la tâche dans l'intervalle** et indiquez la valeur du paramètre en minute.

e. Cliquez sur **OK**.

7. Si la tâche créée est une tâche pour une sélection quelconque d'ordinateurs, sélectionnez les ordinateurs du réseau (groupes) sur lesquels elle sera exécutée.

8. Dans la fenêtre **Fin de l'Assistant de création de tâches**, cliquez sur le bouton **Terminer**.

9. La tâche créée apparaît dans la boîte de dialogue **Tâches**.

CONFIGURATION D'UNE TACHE DANS KASPERSKY ADMINISTRATION KIT

Une fois la tâche créée, vous pouvez configurez les paramètres suivants :

- Modifier les paramètres de la tâche ;

- Configurer/modifier la planification de la tâche ;

- Indiquer le compte utilisateur sous lequel la tâche sera exécutée ;

- Configurer les notifications sur les résultats de l'exécution des tâches.

Pour configurer la tâche, procédez comme suit :

1. Dans l'arborescence de la console d'administration, déployez le nœud **Ordinateurs administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

2. Dans le volet des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur le serveur protégé et choisissez l'option **Propriétés**.

3. Sous l'onglet **Tâches** de la boîte de dialogue **Propriétés : <Nom de l'ordinateur>**, ouvrez le menu contextuel de la tâche que vous souhaitez configurer et choisissez l'option **Propriétés**.

4. Le cas échéant, modifiez les paramètres de la tâche. Pour ce faire, exécutez les actions suivantes :

   - Dans la tâche **Protection en temps réel des fichiers**, sous l'onglet **Configuration**:

     - Composez la zone de protection (pour en savoir plus, lisez la rubrique sur les zones de protection prédéfinies (cf. page 91)) ;

     - Appliquez la zone de confiance : sous l'onglet **Avancé,** cochez la case **Appliquer la zone de confiance**. Pour savoir comment constituer la zone de confiance, lisez la rubrique "Ajout d'exclusions à la zone de confiance" (cf. page 316) ;

     - Modifiez le mode de protection des objets : sous l'onglet **Avancé**, sélectionnez le mode requis de protection des objets (cf. page 375) ;

   - Dans la tâche **Analyse des scripts** sous l'onglet **Configuration** :

     - décidez s'il faut autoriser ou interdire l'exécution des scripts considérés comme suspects par Kaspersky Anti-Virus ;

     - Appliquez la zone de confiance. Pour savoir comment constituer la zone de confiance, lisez la rubrique "Ajout d'exclusions à la zone de confiance" (cf. page 316) ;

   - dans la tâche **Analyse des zones critiques** sous l'onglet **Configuration** :

     - sous l'onglet **Configuration**, composez la zone d'analyse. Pour en savoir plus sur les secteurs prédéfinis, lisez la rubrique "Zones d'analyse prédéfinies" (cf. page 134).

     - sous l'onglet **Avancé** , modifiez la priorité du processus de travail dans lequel la tâche va être exécutée (cf. page 152) ;

     - sous l'onglet **Avancé**, le cas échéant, attribuez à la tâche l'état "Tâche d'analyse des secteurs critiques de l'ordinateur" (cf. rubrique "Administration de l'analyse des serveurs. Attribution de l'état Analyse des zones critiques à la tâche d'analyse à la demande" (cf. page 354)

     - sous l'onglet **Avancé**, appliquez la zone de confiance. Pour savoir comment constituer la zone de confiance, lisez la rubrique "Ajout d'exclusions à la zone de confiance" (cf. page 316) ;

   - dans la tâche **Copie des mises à jour** :

     - sous l'onglet **Configuration de la copie des mises à jour**, désignez la composition des mises à jour (cf. page 404) et le dossier d'enregistrement ;

     - sous l'onglet **Source des mises à jour**, indiquez la source des mises à jour (cf. page 396) ;

     - sous l'onglet **Planification**, programmez l'exécution de la tâche. Étape 5 Instructions sur la création d'une tâche (cf. page 341);

     - sous l'onglet **Compte utilisateur**, désignez le compte utilisateur sous les privilèges duquel la tâche va être exécutée (cf. page 54).

- sous l'onglet **Notification**, configurez la notification sur les résultats de l'exécution de la tâche (pour en savoir plus, lisez le document *Kaspersky Administration Kit. Manuel de l'utilisateur*).

Pendant l'application de la stratégie de Kaspersky Administration Kit, les valeurs des paramètres accompagnés dans la stratégie de l'icône dans la boîte de dialogue **Propriétés : <nom de la tâche>** de la console d'administration ne peuvent être modifiés.

5. Cliquez sur **OK**.

6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés : <nom de la tâche>** afin d'enregistrer les modifications.

ADMINISTRATION DE L'ANALYSE DES SERVEURS ATTRIBUTION DE L'ETAT ANALYSE DES ZONES CRITIQUES A LA TACHE D'ANALYSE A LA DEMANDE

Kaspersky Administration Kit attribue par défaut l'état **Avertissement** au serveur si la tâche **Analyse des zones critiques** est exécutée moins souvent que la valeur du paramètre de Kaspersky Anti-Virus **Seuil de déclenchement de l'événement "L'analyse des secteurs critiques n'a plus eu lieu depuis longtemps"**.

Pour configurer l'analyse de tous les serveurs appartenant à un groupe d'administration, procédez comme suit :

1. Créez une tâche de groupe d'analyse à la demande. Dans la fenêtre **Configuration de l'Assistant de création de tâches**, attribuez l'état "Tâche d'analyse des secteurs critiques" à la tâche créée. Les paramètres que vous aurez définis (zone d'analyse et paramètres de protection) seront identiques pour tous les serveurs du groupe. Programmez l'exécution de la tâche. Obtenez de plus amples informations sur la manière de créer une tâche (cf. page 341).

Vous pouvez attribuer l'état "Tâche d'analyse des zones critiques" à la tâche d'analyse à la demande aussi bien lors de sa création que plus tard, dans la boîte de dialogue **Propriétés : <Nom de la tâche>**.

2. À l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez la tâche prédéfinie **Analyse des secteurs critiques** sur les serveurs du groupe (cf. rubrique "Désactivation de l'exécution programmée des tâches prédéfinies" à la page 339).

Dès ce moment, le Serveur d'administration de Kaspersky Administration Kit évalue la protection du serveur protégé et vous informe à l'issue de la dernière exécution de la tâche avec l'état "Tâche d'analyse de zones critiques" et non pas sur la base des résultats de la tâche prédéfinie **Analyse des zones critiques**.

Vous pouvez attribuer l'état "Tâche d'analyse des zones critiques" à des tâches de groupe d'analyse à la demande ou à des tâches pour des sélections d'ordinateurs.

La console de Kaspersky Anti-Virus permet de voir si la tâche d'analyse à la demande est une tâche d'analyse des zones critiques de l'ordinateur.

Dans la console de Kaspersky Anti-Virus, la case **Considérer l'exécution de la tâche d'analyse des zones critiques** apparaît dans la propriété des tâches mais elle ne peut être modifiée.

PARAMETRES DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

NOMBRE MAXIMUM DE PROCESSUS ACTIFS

*Tableau 61. Paramètre **Nombre maximum de processus actifs***

Paramètre	Nombre maximum de processus actifs
Description	Ce paramètre appartient au groupe de paramètres Montée en capacité de Kaspersky Anti-Virus. Il définit le nombre maximum de processus de travail qui peuvent être exécutés simultanément par Kaspersky Anti-Virus. Les processus de travail de Kaspersky Anti-Virus sont chargés de la protection en temps réel, de l'analyse à la demande et de la mise à jour. L'augmentation du nombre de processus de travail exécutés en parallèle accélère la vitesse d'analyse des fichiers et la résistance de Kaspersky Anti-Virus aux échecs. Toutefois, si cette valeur est trop élevée, les performances globales du serveur peuvent chuter et la mémoire vive requise peut augmenter. N'oubliez pas que la console d'administration de l'application Kaspersky Administration Kit vous permet de définir le paramètre **Nombre maximum de processus actifs** uniquement pour Kaspersky Anti-Virus sur un serveur séparé (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.
Valeurs possibles	1– 8
Valeur par défaut	Kaspersky Anti-Virus réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :

Nombre de processeurs	Nombre maximum de processus actifs
1	1
1< nbre de processeurs < 4	2
4 et plus	4

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

NOMBRE DE PROCESSUS POUR LA PROTECTION EN TEMPS REEL

*Tableau 62. Paramètre **Nombre de processus pour la protection en temps réel***

Paramètre	Nombre de processus pour la protection en temps réel.
Description	Ce paramètre appartient au groupe de paramètres **Montée en capacité** de Kaspersky Anti-Virus. Grâce à ce paramètre, vous pouvez définir un nombre fixe de processus qui serviront à Kaspersky Anti-Virus pour l'exécution de la protection en temps réel. La valeur plus élevée de ce paramètres accélère l'analyse des objets dans les tâches liées à la protection en temps réel. Toutefois, plus le nombre de processus de travail affectés à Kaspersky Anti-Virus est élevé, plus grand sera l'effet sur les performances globales du serveur protégé et sur son utilisation de la mémoire vive. N'oubliez pas que la console d'administration de l'application Kaspersky Administration Kit vous permet de définir le paramètre **Nombre de processus de protection en temps réel** uniquement pour Kaspersky Anti-Virus sur un serveur distinct (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.
Valeurs possibles	Valeurs possibles: 1-N, où N est la valeur définie par le paramètre **Nombre maximum de processus de travail actifs**. Si le **Nombre de processus** pour la protection en temps réel spécifié est égal au Nombre maximum de processus actifs, vous diminuez l'impact de Kaspersky Anti-Virus sur la vitesse de l'échange de fichiers entre les postes de travail et le serveur, tout en augmentant sa vitesse de réaction pendant la protection en temps réel. Toutefois, les tâches de mise à jour et les tâches d'analyse à la demande avec la priorité de base **Moyenne** (**Normal**) seront exécutées dans les processus de Kaspersky Anti-Virus déjà lancés. Les tâches d'analyse à la demande seront exécutées plus lentement. Si l'exécution de la tâche entraîne un échec, son redémarrage prendra plus de temps. Les tâches d'analyse à la demande avec la priorité de base **Faible** (**Low**) sont toujours exécutées dans un ou plusieurs processus séparés (cf. rubrique "Nombre de processus pour les tâches d'analyse à la demande des processus" à la page 358).
Valeur par défaut	Kaspersky Anti-Virus réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :

Nombre de processeurs	Nombre de processus pour la protection en temps réel
=1	1
>1	2

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

NOMBRE DE PROCESSEURS POUR LES TACHES D'ANALYSE A LA DEMANDE EN ARRIERE-PLAN

*Tableau 63. Paramètre **Nombre de processus pour les tâches d'analyse à la demande en arrière-plan***

Paramètre	Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan.
Description	Ce paramètre appartient au groupe de paramètres **Montée en capacité** de Kaspersky Anti-Virus. Grâce à ce paramètre, vous pouvez définir le nombre maximum de processus que Kaspersky Anti-Virus utilisera pour l'exécution de l'analyse à la demande en arrière-plan. Le nombre de processus que vous définissez à l'aide de ce paramètre ne fait pas partie du total des processus de travail de Kaspersky Anti-Virus défini à l'aide du paramètre **Nombre maximum de processus actifs**. Par exemple, si vous spécifiez les valeurs des paramètres comme ci-dessous : • Nombre maximum de processus actifs – 3 ; • Nombre de processus pour les tâches de protection en temps réel – 3 ; • Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan – 1 ; et puis que vous lancez la tâche de protection en temps réel et une tâche d'analyse à la demande en arrière-plan, le nombre total de processus de travail de kavfswp.exe de Kaspersky Anti-Virus est de 4. Un processus de travail de faible priorité peut exécuter plusieurs tâches d'analyse à la demande. Vous pouvez augmenter le nombre de processus de travail, par exemple si vous lancez simultanément plusieurs tâches en arrière-plan, afin d'attribuer des processus distincts à chaque tâche. L'attribution de processus distincts aux tâches augmente la fiabilité de l'exécution de ces tâches ainsi que la vitesse.
Valeurs possibles	1-4
Valeur par défaut	1

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

RECUPERATION AUTOMATIQUE

*Tableau 64. Paramètre **Restauration des tâches***

Paramètre	Restauration des tâches (**Réaliser la restauration du logiciel**).
Description	Ce paramètre appartient au groupe de paramètres **Fiabilité** de Kaspersky Anti-Virus. Il active la restauration des tâches lorsque celles-ci se solde par une erreur et définit le nombre de tentatives de restauration des tâches d'analyse à la demande. Lorsqu'une tâche se solde par un échec, le processus kavfs.exe de Kaspersky Anti-Virus tente de relancer le processus dans lequel cette tâche était exécutée au moment de l'arrêt. Si la restauration des tâches est désactivée, Kaspersky Anti-Virus ne restaure pas les tâches d'analyse à la demande et de protection en temps réel. Si la restauration des tâches est activée, Kaspersky Anti-Virus tente de restaurer les tâches de protection en temps réel jusqu'à la réussite de l'opération et tente de restaurer les tâches d'analyse à la demande autant de fois que le précise le paramètre.
Valeurs possibles	Activée / désactivée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 1-10.
Valeur par défaut	La restauration des tâches est activée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 2

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

ACTIONS DANS LE FONCTIONNEMENT SUR LA SOURCE D'ALIMENTATION DE SECOURS

*Tableau 65. Paramètre **Utilisation de la source d'alimentation de secours***

Paramètre	Utilisation de la source d'alimentation de secours.
Description	Ce paramètre définit les actions exécutées par Kaspersky Anti-Virus lorsque le serveur fonctionne sur l'alimentation électrique de secours.
Valeurs possibles	Lancer/ne pas lancer les tâches d'analyse à la demande qui ont été programmées ; Exécuter / arrêter toutes les tâches d'analyse à la demande lancées.
Valeur par défaut	Par défaut, lorsque le serveur utilise une source d'alimentation de secours, Kaspersky Anti-Virus fonctionne en mode suivant : • N'exécute pas les tâches d'analyse à la demande qui ont été programmées ; • Arrête automatiquement toutes les tâches d'analyse à la demande lancées.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

ACTIONS DANS LE FONCTIONNEMENT SUR LA SOURCE D'ALIMENTATION DE SECOURS

*Tableau 66. Paramètre **Seuils de déclenchement des événements***

Paramètre	Seuils de déclenchement des événements.
Description	Vous pouvez définir le seuil de déclenchement des événements des trois types suivants : • *Les bases de données sont dépassées* et *Les bases de données sont périmées*. Cet événement se déclenche lorsque les bases de Kaspersky Anti-Virus ne sont pas actualisées durant une période (nombre de jours) définie depuis la création des dernières mises à jour des bases. Vous pouvez configurer la notification de l'administrateur lorsque ces événements surviennent. • *L'analyse des zones critiques n'a pas été réalisée depuis longtemps*. Cet événement se déclenche si aucune des tâches accompagnées de la case Considérer l'exécution de la tâche d'analyse des zones critiques n'a été exécutée au cours du nombre de jours indiqué (cf. rubrique "Administration de l'analyse des serveurs. Attribution de l'état Analyse des zones critiques à la tâche d'analyse à la demande" à la page 354)
Valeurs possibles	Nombre de jours compris entre 1 et 365
Valeur par défaut	Les bases de données sont dépassées – 7 jours ; Les bases de données sont périmées – 14 jours ; L'analyse des zones critiques n'a pas été réalisée depuis longtemps 30 jours.

CF. INSTRUCTION DE LA CONFIGURATION

PARAMETRES DU JOURNAL DE TRAÇAGE

DANS CETTE SECTION DE L'AIDE

CONSTITUTION D'UN JOURNAL DE TRAÇAGE

*Tableau 67. Paramètre **Constitution d'un journal de traçage***

Paramètre	Constitution d'un journal de traçage (**Consigner les informations de débogage dans le fichier**).
Description	Le paramètre **Constitution d'un journal de traçage** appartient au groupe de paramètres **Diagnostic des échecs**. Si un problème est survenu pendant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus ou une tâche en particulier s'arrête suite à une erreur ou ne se lance pas) et que vous souhaitez le diagnostiquer, vous pouvez créer un journal de traçage et envoyer les fichiers de ce journal au Service d'assistance technique de Kaspersky Lab pour l'analyse (cf. rubrique "Contacter le service d'assistance technique" à la page 17). Le journal de traçage de chaque processus de Kaspersky Anti-Virus est conservé dans un fichier distinct.
Valeurs et certaines recommandations quant à leur utilisation	Le journal de traçage est constitué/n'est pas constitué. Pour activer la constitution du fichier de traçage, il faut définir le répertoire dans lequel ces fichiers seront enregistrés Si vous administrez Kaspersky Anti-Virus sur un serveur protégé par une console installée sur un autre ordinateur, vous devrez indiquer les paramètres du journal de traçage dans la clé de registre de Microsoft Windows de cet ordinateur, puis fermer et rouvrir la console de Kaspersky Anti-Virus afin d'activer la constitution du journal de traçage du sous-système gui. *Si la version 32 bits de Microsoft Windows est installée sur l'ordinateur,* modifiez la valeur suivante du registre : HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVWSEE\6.0\Trace\Configuration =sub-system=gui;level=info;sink=folder(<répertoire pour les fichiers journaux et chemin d'accès>);roll=50000;layout=basic;logging=on *Si la version 64 bits de Microsoft Windows est installée sur l'ordinateur,* modifiez la valeur suivante du registre : HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVWSEE\6.0\Trace\Configuration =sub-system=gui;level=info;sink=folder(<répertoire pour les fichiers journaux et chemin d'accès>);roll=50000;layout=basic;logging=on Pour désigner le chemin d'accès au répertoire, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
Valeur par défaut	Le journal de traçage n'est pas constitué.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

DOSSIER CONTENANT LES FICHIERS DU JOURNAL DE TRAÇAGE

*Tableau 68. Paramètre **Dossier contenant les fichiers du journal de traçage***

Paramètre	Dossier contenant les fichiers du journal de traçage(**Dossier des fichiers de débogage**)
Description	Pour activer la constitution du fichier de traçage, il faut définir le répertoire dans lequel ces fichiers seront enregistrés
Valeurs et certaines recommandations quant à leur utilisation	Identifiez le répertoire sur le disque local du serveur protégé. Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Les répertoires de réseau ou les répertoires créés à l'aide de la commande SUBST ne peuvent faire office de répertoire pour l'enregistrement du fichier de traçage. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur. Pour désigner le chemin d'accès au dossier contenant les fichiers du journal de traçage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
Valeur par défaut	Non définie.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit..... 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC..... 38

NIVEAU DE DETAIL DU JOURNAL DE TRAÇAGE.

*Tableau 69. Paramètre **Niveau de détail du journal de traçage***

Paramètre	Niveau de détail du journal de traçage
Description	Vous pouvez sélectionner le niveau de détail du journal de traçage (**Informations de mise au point**, **Evénements d'information**, **Événements importants**, **Erreurs** ou **Événements critiques**).
Valeurs et certaines recommandations quant à leur utilisation	Le niveau le plus détaillé est le niveau **Informations de mise au point** où tous les événements sont consignés dans le journal tandis que le niveau le moins détaillé est le niveau **Événements critiques** où seuls les événements critiques sont consignés. N'oubliez pas que le journal de traçage peut prendre beaucoup de place sur le disque.
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé sa constitution, Kaspersky Anti-Virus réalisera le traçage de tous les sous-systèmes de Kaspersky Anti-Virus au niveau de détails **Informations de mise au point**.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit..... 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC..... 38

TAILLE D'UN FICHIER DU JOURNAL DE TRAÇAGE.

*Tableau 70. Paramètre **Taille d'un fichier du journal de traçage***

Paramètre	Taille d'un fichier de journal de traçage.
Description	Vous pouvez modifier la taille maximale d'un fichier du journal.
Valeurs et certaines recommandations quant à leur utilisation	1 à 999 Mo. Dès que la taille du fichier de rapport atteint la valeur maximale, Kaspersky Anti-Virus consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé.
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé son contenu, la taille maximale d'un fichier du journal sera de 50 Mo.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

TRAÇAGE DE SOUS-SYSTEMES INDIVIDUELS DE KASPERSKY ANTI-VIRUS

*Tableau 71. Paramètre **Traçage de certains sous-systèmes uniquement de Kaspersky Anti-Virus***

Paramètre	Traçage de certains sous-systèmes uniquement de Kaspersky Anti-Virus.
Description	Vous pouvez consigner dans le journal uniquement certains sous-systèmes de Kaspersky Anti-Virus si vous le souhaitez.
Valeurs et certaines recommandations quant à leur utilisation	Dans la boîte de dialogue de configuration des paramètres de Kaspersky Anti-Virus, groupe de paramètres **Diagnostic des échecs**, cliquez sur le bouton **Avancé** et dans la boîte de dialogue **Paramètres avancés**, champ **Sous-systèmes à tracer** au point, saisissez les codes des sous-systèmes pour lesquels vous souhaitez un traçage. Les codes des sous-systèmes doivent être séparés par une virgule. La saisie des codes est sensible à la casse. Les codes et les noms des sous-systèmes de Kaspersky Anti-Virus sont repris dans le tableau suivant. Les paramètres de traçage du sous-système **gui** (module enfichable de Kaspersky Anti-Virus) sont appliqués après le redémarrage de la console de Kaspersky Anti-Virus ; les paramètres de traçage du sous-système **AK_conn** (sous-système d'intégration à l'Agent d'administration de Kaspersky Administration Kit), après le redémarrage de l'agent d'administration de Kaspersky Administration Kit ; les paramètres de traçage des autres sous-systèmes de Kaspersky Anti-Virus sont appliqués directement après l'enregistrement des paramètres.
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé sa constitution, Kaspersky Anti-Virus réalisera le traçage de tous les sous-systèmes de Kaspersky Anti-Virus

Le tableau suivant reprend la liste des codes des sous-systèmes de Kaspersky Anti-Virus dont les informations peuvent être ajoutées au fichier de traçage.

Tableau 72. Liste des codes des sous-systèmes pouvant être ajoutés au journal de traçage

CODE DE SOUS-SYSTEME	NOM DU SOUS-SYSTEME
*	Tous les sous-systèmes (par défaut)
gui	Composant enfichable de Kaspersky Anti-Virus
ak_conn	Sous-système d'intégration à l'agent d'administration de Kaspersky Administration Kit
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Anti-Virus
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance de Kaspersky Anti-Virus
ods	Sous-système d'analyse à la demande
oas	Sous-système de protection en temps réel des fichiers
qb	Sous-système de la quarantaine et du dossier de sauvegardé
scandll	Module auxiliaire de l'analyse Anti-Virus
core	Sous-système de la fonction antivirus de base
avscan	Sous-système de traitement antivirus
avserv	Sous-système d'administration du moteur antivirus
prague	Sous-système de fonction de base
scsrv	Sous-système de gestion des requêtes émanant de l'intercepteur de scripts
script	Intercepteur de scripts
updater	Sous-système de mise à jour des bases et des modules d'application

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres généraux de Kaspersky Anti-Virus dans Kaspersky Administration Kit 324

Configuration des paramètres généraux de Kaspersky Anti-Virus dans MMC 38

CREATION DE FICHIERS DE VIDAGE DE LA MEMOIRE DES PROCESSUS DE KASPERSKY ANTI-VIRUS

*Tableau 73. Paramètre **Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus***

Paramètre	Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (**Créer des fichiers de vidage sur incident**).
Description	Le paramètre **Création de fichiers de vidage des processus de Kaspersky Anti-Virus** appartient au groupe de paramètres **Diagnostic des échecs**. Si un problème survient durant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez activer la création de fichiers de vidage de mémoire des processus de Kaspersky Anti-Virus et envoyer ces fichiers au Service d'assistance technique de Kaspersky Lab pour l'analyse (cf. rubrique "Contacter le service d'assistance technique" à la page 17).
Valeurs et certaines recommandations quant à leur utilisation	Les fichiers de vidages sont créés / ne sont pas créés. Pour activer la création de fichiers de vidage, indiquez le dossier où ces fichiers seront enregistrés. Si vous saisissez un chemin d'accès à un répertoire inexistant, les fichiers de vidage ne seront pas créés. Si vous administrez Kaspersky Anti-Virus sur un serveur protégé par la console Kaspersky Anti-Virus installée sur un autre ordinateur, vous devrez indiquer les paramètres de la création des fichiers de vidage dans la clé de registre de Microsoft Windows de cet ordinateur, puis fermer et rouvrir la console de Kaspersky Anti-Virus afin d'activer le vidage du processus de la console de Kaspersky Anti-Virus. *Si la version 32 bits de Microsoft Windows est installée sur l'ordinateur,* modifiez les valeurs suivantes du registre : • HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVWSEE\8.0\CrashDump\Enable=0x00000000 • HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVWSEE\8.0\CrashDump\Folder=C:\Temp *Si la version 64 bits de Microsoft Windows est installée sur l'ordinateur,* modifiez les valeurs suivantes du registre : • HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVWSEE\8.0\CrashDump\Enable=0x00000000 • HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVWSEE\8.0\CrashDump\Folder=C:\Temp Spécifiez les valeurs suivantes des paramètres sélectionnés du registre : • 0x00000000 : désactive la création de fichiers de vidage du processus de la console de Kaspersky Anti-Virus ; • 0x00000001 : active la création de fichiers de vidage du processus de la console de Kaspersky Anti-Virus ; Folder=C:\Temp : répertoire dans lequel le fichier de vidage du processus de la console de Kaspersky Anti-Virus sera enregistré en cas d'arrêt suite à une erreur. Pour désigner le chemin d'accès au dossier contenant les fichiers de vidage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
Valeur par défaut	Les fichiers de vidage ne sont pas créés.

CF. INSTRUCTION DE LA CONFIGURATION

PARAMETRES DES JOURNAUX

DANS CETTE SECTION DE L'AIDE

NIVEAU DE DETAIL DES JOURNAUX D'EXECUTION DES TACHES, DU JOURNAL D'AUDIT SYSTEME ET DU JOURNAL DES EVENEMENTS DE KASPERSKY ANTI-VIRUS DANS LA CONSOLE OBSERVATEUR D'EVENEMENTS

*Tableau 74. Paramètre **Niveau de détail des journaux d'exécution des tâches, du journal d'audit système et du journal des événements de Kaspersky Anti-Virus dans la console Observateur d'événements***

Paramètre	Niveau de détail des journaux d'exécution des tâches, du journal d'audit système et du journal des événements de Kaspersky Anti-Virus dans la console **Observateur d'événements**.
Description	Les événements de Kaspersky Anti-Virus sont répartis en trois catégories selon le degré d'importance : *informatifs*, *importants* et *critiques*. Les types d'événement se caractérisent par les particularités suivantes : • **Les événements informatifs**, par exemple *Aucune menace n'a été découverte* ou *Sans erreur*, reprennent les résultats du fonctionnement de Kaspersky Anti-Virus et les conditions dans lesquels aucune menace pour la sécurité de l'ordinateur n'a été découverte. • Les **Evénements importants** tels que *Erreur de connexion à la source de mise à jour* peuvent avoir un impact sur l'exécution des fonctions de Kaspersky Anti-Virus. • Les **Evénements critiques** peuvent entraîner une violation de la sécurité antivirus du serveur protégé. Il s'agit par exemple des événements *L'intégrité du module a été violée*, *Une menace a été découverte* ou *Erreur interne de la tâche*. Le niveau de détail des journaux d'exécution des tâches ou du journal des événements correspond au degré d'importance des événements qui y sont consignés.
Valeurs et certaines recommandations quant à leur utilisation	Vous pouvez définir un des trois niveaux de détail depuis **Informatif** où les événements de tous les degrés d'importance sont consignés jusqu'à **Critiques** où seuls les événements critiques sont enregistrés. Vous pouvez également inclure manuellement des événements particuliers dans les événements à consigner dans les journaux d'exécution des tâches et le journal des événements. N'oubliez pas que les journaux peuvent occuper beaucoup de place sur le disque.
Valeur par défaut	Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) ; pour le composant **Mise à jour**, c'est le niveau **Evénements informatifs** qui est sélectionné.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres des journaux dans Kaspersky Administration Kit 329

Configuration de paramètres des journaux dans MMC 239

DOSSIER D'ENREGISTREMENT DES JOURNAUX D'EXECUTION DES TACHES ET DU JOURNAL D'AUDIT SYSTEME

*Tableau 75. Paramètre **Dossier d'enregistrement des journaux relatifs à l'exécution des tâches et du journal d'audit système***

Paramètre	Dossier d'enregistrement des journaux d'exécution des tâches et du journal d'audit système
Description	Dossier sur le disque local du serveur où Kaspersky Anti-Virus enregistre les fichiers des journaux d'exécution des tâches et du journal d'audit système. Vous ne pouvez pas consulter les journaux de ce dossier à l'aide du navigateur.
Valeurs et certaines recommandations quant à leur utilisation	Identifiez le répertoire sur le disque local du serveur protégé. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur. Pour indiquer le chemin d'accès au répertoire d'enregistrement des journaux, vous pouvez utiliser des variables ; vous ne pouvez pas utiliser des variables d'utilisateur.
Valeur par défaut	%ALLUSERSPROFILE%\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Reports\

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres des journaux dans Kaspersky Administration Kit 329

Configuration de paramètres des journaux dans MMC 239

DELAI DE CONSERVATION DES JOURNAUX RELATIFS A L'EXECUTION DES TACHES

*Tableau 76. Paramètre **Durée de conservation des journaux d'exécution des tâches***

Paramètre	Durée de conservation des journaux d'exécution des tâches (**Ne pas conserver les journaux d'exécution des tâches plus de ... jours**).
Description	Ce paramètre détermine le nombre de jours de conservation des journaux d'exécution des tâches qui apparaissent dans le nœud **Journaux d'exécution des tâches** dans la console de Kaspersky Anti-Virus. Vous pouvez désactiver ce paramètre afin de conserver indéfiniment les journaux d'exécution des tâches. Dans ce cas, la taille du fichier qui abrite les informations des journaux peut devenir très grande.
Valeurs possibles	1–365
Valeur par défaut	Les enregistrements relatifs aux événements survenus il y a plus de 30 jours sont supprimés des journaux d'exécution des tâches de Kaspersky Anti-Virus. Les journaux d'exécution des tâches des tâches exécutées sont supprimés 30 jours après la fin des tâches.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres des journaux dans Kaspersky Administration Kit 329

Configuration de paramètres des journaux dans MMC 239

DUREE DE CONSERVATION DES EVENEMENTS DANS LE JOURNAL D'AUDIT SYSTEME

*Tableau 77. Paramètre **Durée de conservation du journal d'audit système***

Paramètre	Durée de conservation du journal d'audit système (**Ne pas conserver les événements plus de ... jours**).
Description	Vous pouvez limiter la durée de conservation des événements qui figurent dans le nœud **Journal d'audit système** de la console Kaspersky Anti-Virus.
Valeurs possibles	1–365
Valeur par défaut	Les événements de l'enregistrement d'audit système sont supprimés après 60 jours.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres des journaux dans Kaspersky Administration Kit 329

Configuration de paramètres des journaux dans MMC 239

PARAMETRES DE PLANIFICATION DES TACHES

DANS CETTE SECTION DE L'AIDE

FREQUENCE D'EXECUTION

*Tableau 78. Paramètre **Fréquence d'exécution***

Paramètre	Fréquence d'exécution.
Description	Ce paramètre est obligatoire. La tâche peut être exécutée selon une fréquence que vous définirez en heures, en jours ou en semaines, les jours indiqués de la semaine, après le lancement de Kaspersky Anti-Virus, la mise à jour des bases ou la récupération des mises à jour par le serveur d'administration.
Valeurs et certaines recommandations quant à leur utilisation	Les valeurs suivantes sont possibles : • **Chaque heure**. La tâche sera exécutée selon la fréquence horaire que vous avez définie. • **Chaque jour**. La tâche sera exécutée selon la fréquence journalière que vous avez définie. • **Chaque semaine**. La tâche sera exécutée selon la fréquence hebdomadaire que vous avez définie. • **Au lancement de l'application**. La tâche sera lancée chaque fois que Kaspersky Anti-Virus sera ouvert. • **À la mise à jour de la base antivirus** (cette option ne s'applique pas aux tâches de mise à jour). La tâche sera exécutée après chaque mise à jour des bases de Kaspersky Anti-Virus. • **Après la réception des mises à jour par le serveur d'administration** (s'applique uniquement aux tâches **Mise à jour de la base de données de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**, s'affiche uniquement dans la console d'administration Kaspersky Administration Kit, ne s'affiche pas dans la console de Kaspersky Anti-Virus). La tâche sera lancée chaque fois que le serveur d'administration recevra la mise à jour des bases.
Valeur par défaut	Dans les tâches prédéfinies locales, les valeurs par défaut du paramètre **Fréquence** sont les suivantes : • **Protection en temps réel des fichiers** : au lancement de l'application ; • **Analyse des scripts** :au lancement de l'application ; • **Analyse au démarrage du système** :au lancement de l'application ; • **Analyse des zones critiques** : chaque semaine (le vendredi à 20h00) ; • **Analyse des objets en quarantaine** : après la mise à jour des bases ; • **Mise à jour de la base de données de l'application** : toutes les heures ; • **Mise à jour des modules de l'application** : chaque semaine (le vendredi à 16h00) ; • **Copie des mises à jour** : programmation désactivée ; • **Annulation de la mise à jour** : programmation non prévue. Dans les tâches d'analyse à la demande définies par l'utilisateur recréées, la programmation est désactivée :

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

DATE D'ENTREE EN VIGUEUR DE LA PLANIFICATION ET HEURE DE LA PREMIERE EXECUTION DE LA TACHE

*Tableau 79. Paramètre **Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche***

Paramètre	Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche.
Description	Les paramètres suivants sont obligatoires : • **Date d'entrée en vigueur de la planification** (**A partir du**). Kaspersky Anti-Virus lancera la tâche à la date désignée selon la fréquence définie. • **A partir du** (appliquée si la valeur du paramètre **Fréquence** est **Chaque heure**). Kaspersky Anti-Virus lance la tâche la première fois à l'heure indiquée. • **Démarrer à** (appliquée si la valeur du paramètre **Fréquence** est **Chaque jour** ou **Chaque semaine**). Kaspersky Anti-Virus lancera la tâche à l'heure indiquée selon la fréquence définie par le paramètre **Fréquence**.
Valeurs possibles	Indiquez la date et l'heure.
Valeur par défaut	Ces paramètres sont désactivés dans les tâches d'analyse à la demande définies par l'utilisateur recréées. Dans les tâches prédéfinies locales, ces paramètres possèdent les valeurs par défaut suivantes : • **Analyse des zones critiques** : tous les vendredi à 20h00 selon la configuration de l'heure sur le serveur protégé ; • **Mise à jour de la base de données de l'application** : toutes les trois heures. Ces paramètres sont désactivés dans la programmation des autres tâches prédéfinies.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

DATE DE LA FIN DE VALIDITE DE LA PLANIFICATION

*Tableau 80. Paramètre **Date de la fin de validité de la planification***

Paramètre	Date de la fin de validité de la planification (**Suspendre la planification à partir du**).
Description	A partir de la date que vous aurez saisie, la programmation ne sera plus valide : la tâche programmée ne sera pas exécutée. Ce paramètre ne s'applique pas si la valeur du paramètre **Fréquence** est **Au lancement de l'application** ou **A la mise à jour de la base antivirus**.
Valeurs possibles	Saisissez la date ou sélectionnez-la dans la fenêtre **Calendrier**.
Valeur par défaut	Non définie

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

DUREE MAXIMALE DE L'EXECUTION D'UNE TACHE

*Tableau 81. Paramètre **Durée maximale de l'exécution d'une tâche***

Paramètre	Durée maximale de l'exécution d'une tâche.
Description	Si l'exécution de la tâche prend plus de temps que la durée que vous avez saisie en heures et en minutes, la tâche sera arrêtée par Kaspersky Anti-Virus. Une tâche arrêtée de la sorte ne sera pas considérée comme ignorée. Ce paramètre vous permettra également de définir l'heure d'arrêt automatique des tâches de protection en temps réel. Ce paramètre ne concerne pas les tâches de mise à jour.
Valeurs possibles	Indiquez la durée en heures et en minutes.
Valeur par défaut	Désactivée

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

INTERVALLE DE TEMPS AU COURS D'UNE JOURNEE PENDANT LEQUEL LA TACHE SERA SUSPENDUE

*Tableau 82. Paramètre **Intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue***

Paramètre	Intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue (**Pause à partir de... jusqu'à**).
Description	Le cas échéant, vous pouvez suspendre une tâche pendant un intervalle déterminé durant la journée, par exemple suspendre la tâche d'analyse à la demande si la charge du serveur à ce moment de la journée est élevée et que vous ne souhaitez pas l'augmenter en exécutant cette tâche. Ce paramètre ne concerne pas les tâches de mise à jour. Si en plus de ce paramètre vous activez le paramètre **Durée maximale de l'exécution d'une tâche**, n'oubliez pas que l'intervalle de suspension de la tâche indiqué entre dans la durée maximale d'exécution de la tâche.
Valeurs possibles	Définissez le nombre d'heures et de minutes.
Valeur par défaut	Désactivé.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

EXECUTION DES TACHES NON EXECUTEES

*Tableau 83. Paramètre **Lancement des tâches non exécutées***

Paramètre	Exécution des tâches non exécutées.
Description	Vous pouvez activer le lancement des tâches non exécutées. Si Kaspersky Anti-Virus ne peut pas exécuter la tâche à l'heure définie (par exemple, l'ordinateur est éteint), Kaspersky Anti-Virus considère cette tâche comme ignorée et l'exécutera automatiquement dès qu'il sera à nouveau lancé. La tâche n'est pas considérée comme ignorée si elle s'exécute déjà au moment de son démarrage prévu. Ce paramètre ne s'applique pas si la valeur du paramètre **Fréquence** est **Au lancement de l'application** ou **A la mise à jour de la base antivirus**.
Valeurs possibles	Activé/désactivé
Valeur par défaut	Désactivé

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

REPARTITION DES LANCEMENTS DANS L'INTERVALLE, MIN

*Tableau 84. Paramètre **Répartition des lancements dans l'intervalle***

Paramètre	Répartition des lancements dans l'intervalle, min.
Description	Si vous attribuez une valeur à ce paramètre, la tâche sera lancée à tout moment dans l'intervalle entre le moment calculé de son exécution programmée et le moment de l'exécution plus la valeur dudit paramètre. Vous pouvez appliquer ce paramètre, par exemple en cas d'utilisation d'un ordinateur intermédiaire pour la diffusion des mises à jour sur de nombreux serveurs afin de réduire la charge sur cet ordinateur et dans le trafic de réseau. Ce paramètre ne s'applique pas si le type de lancement sélectionné est **Au lancement de l'application**, **A la mise à jour de la base antivirus** ou **Après réception des mises à jour par le serveur d'administration**.
Valeurs possibles	Désignez le nombre de minutes
Valeur par défaut	Désactivé.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de planification des tâches en MMC 50

Configuration d'une tâche dans Kaspersky Administration Kit 352

PARAMETRES DE PROTECTION DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS ET DANS LES TACHES D'ANALYSE A LA DEMANDE

DANS CETTE SECTION DE L'AIDE

MODE DE PROTECTION

Le paramètre de sécurité **Mode de protection** concerne uniquement la tâche **Protection en temps réel des fichiers** (voir le tableau ci-dessous).

*Tableau 85. Paramètre **Mode de protection***

Paramètre	Mode de protection.
Description	Ce paramètre concerne uniquement la tâche **Protection en temps réel des fichiers**. Il définit le type d'accès aux objets qui entraînera une analyse de Kaspersky Anti-Virus. Le paramètre **Mode de protection** possède une valeur unique pour toutes les couvertures d'analyse reprises dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les nœuds particuliers.
Valeurs et certaines recommandations quant à leur utilisation	Sélectionnez un des modes de protection en fonction de vos exigences de sécurité pour le système, des types de formats de fichiers enregistrés sur le serveur et du type d'informations qu'ils renferment : • **Mode intelligent**. Kaspersky Anti-Virus analyse l'objet à l'ouverture et le vérifie à nouveau après l'enregistrement, si l'objet a été modifié. Si le processus pendant son exécution contacte plusieurs fois l'objet et le modifie, Kaspersky Anti-Virus le vérifiera à nouveau uniquement après la dernière sauvegardé par ce processus. • **Ouverture et modification**. Kaspersky Anti-Virus analyse l'objet à l'ouverture et le vérifie à nouveau à la fermeture s'il a été modifié. • **Ouverture**. Kaspersky Anti-Virus analyse l'objet à l'ouverture aussi bien en écriture qu'en exécution ou en modification. • **Exécution**. Kaspersky Anti-Virus analyse l'objet uniquement en cas d'ouverture pour exécution. Par défaut, les objets sont analysés en mode de protection **A l'accès et à la modification**.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

OBJETS A ANALYSER

Le paramètre de sécurité **Objets à analyser** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande (voir le tableau ci-dessous).

*Tableau 86. Paramètre **Objets à analyser***

Paramètre	Objets à analyser.
Description	Ce paramètre définit si tous les objets de la couverture de protection seront analysés ou uniquement les objets d'un format ou dotés d'une extension défini. Les experts de Kaspersky Lab composent des listes des formats et des extensions qui peuvent contenir des objets susceptibles d'être infectés. Ces listes sont reprises dans Kaspersky Anti-Virus. Grâce au paramètre **Objets à analyser**, vous pouvez composer votre propre liste des extensions.
Valeurs et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Analyser tous les objets**. Kaspersky Anti-Virus analyse tous les objets, quel que soit leur format ou leur extension. • **Objets analysés en fonction du format**. Avant d'analyser l'objet, Kaspersky Anti-Virus définit son format. Si le format figure dans la liste des formats des objets pouvant être infectés, l'objet sera analysé par Kaspersky Anti-Virus. Si le format ne figure pas dans cette liste (par exemple, un fichier txt ne peut être infecté), alors Kaspersky Anti-Virus ne l'analyse pas. • **Objets analysés en fonction d'une liste d'extensions**. Kaspersky Anti-Virus analyse uniquement les objets dont l'extension figure dans la liste des extensions d'objets pouvant être infectés. Si l'extension de l'objet ne figure pas dans cette liste, Kaspersky Anti-Virus l'ignorera. Si vous sélectionnez la valeur **Objets en fonction de la liste définie des extensions**, la vitesse d'analyse sera plus rapide que si vous choisissez la valeur **Objets en fonction du format**. Toutefois, le risque d'infection sera supérieur car l'extension d'un objet ne correspond pas toujours à son format. Par exemple, un fichier portant l'extension .txt n'est pas nécessairement un fichier au format texte. Il peut s'agir d'un fichier exécutable contenant une menace. Mais Kaspersky Anti-Virus n'analysera pas l'objet car l'extension .txt ne figure pas dans la liste des extensions des objets pouvant être infectés. • **Objets analysés en fonction de masques d'extensions**. Kaspersky Anti-Virus analyse les objets dont les extensions figurent dans la liste indiquée (par défaut, cette liste est vide). Vous pouvez ajouter des extensions ou des masques d'extension à la liste ainsi que supprimer des extensions ou des masques existants. Les masques d'extension acceptent les caractères suivants : Vous pouvez ajouter toutes les extensions de la liste des extensions livrée avec Kaspersky Anti-Virus. Pour ce faire, cliquez sur le bouton **Valeur par défaut** dans la boîte de dialogue de modification de la liste. • **Analyser les secteurs d'amorçage et la partition MBR**. Ce paramètre intervient si la couverture d'analyse contient les couvertures prédéfinies **Disques durs** et **Disques amovibles**, la couverture prédéfinie **Poste de travail** ou des disques créés dynamiquement. Ce paramètre n'intervient pas si la couverture d'analyse contient uniquement **Mémoire système**, **Objets exécutés au démarrage du système**, **Dossiers partagés** ou si la couverture d'analyse contient des fichiers ou des dossiers distincts. • **Analyser les flux NTFS alternatifs**. Kaspersky Anti-Virus analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

CF. INSTRUCTION DE LA CONFIGURATION

ACTIONS EN FONCTION DU TYPE DE MENACE

Le paramètre de sécurité **Actions en fonction du type de menace** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande (voir le tableau ci-dessous).

*Tableau 87. Paramètre **Actions en fonction du type de menace***

Paramètre	Actions en fonction du type de menace (**Agir en fonction du type des menaces**).
Description	Les menaces de certains types représentent un plus grand danger pour le serveur que d'autres. Par exemple, un cheval de Troie peut causer plus de dommages qu'un logiciel publicitaire (adware). A l'aide des paramètres de ce groupe, vous pouvez configurer diverses actions de Kaspersky Anti-Virus pour les objets qui contiennent les menaces de différents types. Quand vous définissez les valeurs de ce paramètres, Kaspersky Anti-Virus les appliquera en même temps que les paramètres **Actions à exécuter sur les objets infectés** et **Actions à exécuter sur les objets suspects**.
Valeurs et certaines recommandations quant à leur utilisation	Pour chaque type de menaces, sélectionnez dans la liste des actions qui pourront être exécutées sur les objets infectés et suspects deux actions que Kaspersky Anti-Virus tentera d'exécuter s'il découvre une menace du type précisé dans l'objet. Kaspersky Anti-Virus exécutera la deuxième action sur l'objet s'il ne parvient pas à exécuter la première. Kaspersky Anti-Virus appliquera les actions définies aussi bien aux objets suspects qu'aux objets infectés si cela est possible. Ainsi, si vous sélectionnez **Réparer** en guise de première action et **Quarantaine** en guise de deuxième, Kaspersky Anti-Virus mettra l'objet infecté en quarantaine uniquement s'il ne parvient pas à le réparer, mais placera l'objet suspect directement en quarantaine en ignorant l'action **Réparer**, car les objets suspects ne sont pas soumis à la réparation. Si vous sélectionnez **Ignorer** en guise de première action, la deuxième action ne pourra être appliquée. Pour les autres valeurs, il est conseillé de définir deux actions. N'oubliez que les menaces du type Vers de réseau et Vers classiques sont regroupés, dans la liste des catégories de menaces, sous la même appellation **Virus**. Si Kaspersky Anti-Virus ne parvient pas à placer l'objet en sauvegardé ou en quarantaine, il ne réalisera pas l'action sur l'objet (par exemple, la réparation ou la suppression). L'objet est considéré comme ignoré. Vous pouvez voir pourquoi l'objet a été ignoré dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234). Dans la liste des types de menace, la valeur **Non défini** inclut les nouveaux virus qui ne figurent actuellement dans aucun des types connus.
Valeur par défaut	Désactivée

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

EXCLUSION DES OBJETS

Le paramètre de sécurité **Exclusion des objets** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

*Tableau 88. Paramètre **Exclusion des objets***

Paramètre	Exclusion des objets (**Exclure les objets**).
Description	Ce paramètre vous permet d'exclure de l'analyse des fichiers distincts ou plusieurs fichiers à l'aide d'un masque de nom de fichier. En excluant les fichiers de grande taille de l'analyse, vous pouvez augmenter le volume de fichiers et réduire la durée d'exécution de l'analyse à la demande. Les informations relatives à l'exclusion de l'objet de l'analyse sont reprises dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234) (conformément aux paramètres des journaux d'exécution des tâches définis par défaut). Dans les tâches d'analyse à la demande, quand Kaspersky Anti-Virus analyse un processus dans la mémoire, il analyse également le fichier de lancement du processus même si ce fichier figure dans la liste des exclusions.
Valeurs et certaines recommandations quant à leur utilisation	Composez la liste des fichiers. Vous pouvez saisir le nom du fichier en entier ou à l'aide d'un masque. Pour définir les masques, utilisez les caractères * et ?.
Valeur par défaut	La liste est vide.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

EXCLUSION DES MENACES

Le paramètre de sécurité **Exclusion des menaces** concerne la tâche **Protection en temps réel** des fichiers et les tâches d'analyse à la demande.

*Tableau 89. Paramètre **Exclusion des menaces***

Paramètre	Exclusion des menaces (**Exclure les menaces**).
Description	Si Kaspersky Anti-Virus détermine qu'un objet analysé est infecté ou suspect et qu'il exécute des actions sur celui-ci alors que vous estimez que cet objet ne présente aucun danger pour le serveur, vous pouvez exclure la menace découverte dans l'objet de la liste des menaces que Kaspersky Anti-Virus peut traiter. Vous pouvez exclure une menace selon son nom dans un objet particulier ou toute une catégorie de menaces. Si vous excluez une menace, Kaspersky Anti-Virus considère que l'objet qui contient cette menace est sain.
Valeurs et certaines recommandations quant à leur utilisation	Composez la liste des menaces à exclure (la liste est vide par défaut). Séparez les valeurs dans la liste par un point virgule (;). Pour exclure un objet de l'analyse, indiquez le nom complet de la menace découverte dans cet objet ; – ligne de conclusion de Kaspersky Anti-Virus qui indique que l'objet est infecté ou suspect. Le nom complet de la menace est défini dans les résultats de l'analyse de l'objet. Il peut contenir les informations suivantes : **<catégorie de menace>:<type de menace>.<abréviation de la plateforme>.<nom de la menace>.<code de modification de la menace>**. Admettons que vous utilisez l'utilitaire Remote Administrator en guise d'outil d'administration à distance. La majorité des logiciels antivirus classe le code de cet utilitaire dans les menaces du type Riskware. Afin que Kaspersky Anti-Virus ne le bloque pas, ajoutez le nom complet de la menace dans la liste des menaces exclues du nœud de l'arborescence des ressources fichiers du serveur où se trouvent les fichiers de l'utilitaire. Vous pouvez attribuer les valeurs suivantes au paramètre : • Nom complet de la menace : not-a-virus:RemoteAdmin.Win32.RAdmin.20. Kaspersky Anti-Virus n'exécutera pas les actions uniquement sur les modules dans lesquels il trouve la menace baptisée Win32.RAdmin.20. • Masque du nom complet de la menace : not-virus:RemoteAdmin.* Kaspersky Anti-Virus n'exécutera pas les actions sur les programmes Remote Administrator de toute version. • Masque du nom complet de la menace, avec uniquement le type de menace : not-a-virus:* Kaspersky Anti-Virus n'exécutera aucune action sur tous les objets contenant des menaces de ce type. Vous pouvez consulter le nom complet de la menace découverte dans l'application dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations sur la tâche dans le journal" à la page 234) Vous pouvez également trouver le nom complet de la menace découverte dans l'objet sur le site de l'Encyclopédie des virus Securelist.com/fr. Pour trouver le nom de la menace, saisissez le nom du logiciel dans le champ **Rechercher**.

CF. INSTRUCTION DE LA CONFIGURATION

TRAITEMENT DES FICHIERS AUTONOMES

Le paramètre de la protection **Traitement des fichiers autonomes** est appliqué aux tâches d'analyse à la demande.

*Tableau 90. Paramètre **Traitement des fichiers autonomes***

PARAMETRE	TRAITEMENT DES FICHIERS AUTONOMES
Description	Ce paramètre permet de définir les modes de traitement des fichiers qui se trouvent dans les stockages distants.
Valeurs et certaines recommandations quant à leur utilisation	Vous pouvez attribuer les valeurs suivantes au paramètre : • **Ne pas analyser**. Le système n'analyse pas le fichier autonome. • **Analyser seulement la partie résidente du fichier**. Le système analyse la partie du fichier enregistrée sur le disque. La partie du fichier située sur le stockage distant n'est pas sollicitée. • **Analyser le fichier en entier** : **Uniquement si le fichier a été sollicité durant la période indiquée (jours)**. Le système analyse uniquement les fichiers qui ont été sollicités durant la période indiquée. **Ne pas copier le fichier sur le disque dur si possible**. Le système ne restaurera pas le fichier depuis le stockage HSM sur le disque dur mais l'analysera dans le stockage temporaire. Pour que cette option fonctionne correctement, assurez-vous que le système HSM installé prend en charge l'analyse de fichiers sans restauration sur le disque dur.
Valeur par défaut	**Analyser tout le fichier**

ANALYSE UNIQUEMENT DES NOUVEAUX FICHIERS ET DES FICHIERS MODIFIES

Le paramètre de protection **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** est appliqué dans la tâche **Protection en temps réel des fichiers** et dans les tâches d'analyse à la demande.

*Tableau 91. Paramètre **Analyse uniquement des nouveaux fichiers et des fichiers modifiés***

Paramètre	Analyse uniquement des nouveaux fichiers et des fichiers modifiés
Description	Lorsque l'analyse est activée uniquement pour des nouveaux fichiers ou des fichiers modifiés, Kaspersky Anti-Virus analyse tous les objets de la couverture d'analyse désignée sauf ceux déjà analysé une fois, non infectés et non modifiés depuis cette analyse.
Valeurs et certaines recommandations quant à leur utilisation	Activer/Désactiver.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

ANALYSE DES OBJETS COMPOSES

Le paramètre de sécurité **Analyse des objets composés** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

*Tableau 92. Paramètre **Analyse des objets composés***

Paramètre	Analyse des objets composés.
Description	L'analyse des objets composés dure un certain temps. Par défaut, Kaspersky Anti-Virus analyse uniquement les objets composés les plus souvent infectés ou qui représentent le plus grand danger pour le serveur en cas d'infection. Les objets composés des autres types ne sont pas analysés. Ce paramètre vous permet, conformément à vos exigences de sécurité, de sélectionner les types d'objets composés qui seront analysés par Kaspersky Anti-virus.
Valeurs et certaines recommandations quant à leur utilisation	Sélectionnez une ou plusieurs valeurs dans la liste ci-dessous : • **Archives** ; Kaspersky Anti-Virus analyse les archives traditionnelles. N'oubliez pas que Kaspersky Anti-Virus découvre les menaces dans les archives de la majorité des types mais il peut réparer uniquement les archives ZIP, ARJ, RAR et CAB ; • **Archives SFX**. Kaspersky Anti-Virus analyse le module de décompactage des archives SFX (auto-extractibles) ; • **Bases de données de messagerie**. Kaspersky Anti-Virus analyse les fichiers des bases de données de messagerie de Microsoft Office Outlook et Microsoft Outlook Express ; • **Objets compactés**. Kaspersky Anti-Virus analyse les fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack. Les objets composés de ce type contiennent plus souvent que d'autres des menaces ; • **Messages de texte plat**. Kaspersky Anti-Virus analyse les messages de texte plat, par exemple les messages de Microsoft Office Outlook ou Microsoft Outlook Express ; • **Objets OLE incorporés**. Kaspersky Anti-Virus analyse les objets intégrés dans les documents Microsoft Office. Les documents Microsoft Office contiennent souvent des objets exécutables qui peuvent renfermer des menaces. Si pour la zone de sécurité sélectionnée, le paramètre **Analyse uniquement des nouveaux fichiers et des fichiers modifiés** est désactivée, vous pouvez activer ou désactiver l'analyse uniquement des objets neufs et modifiés pour chaque type d'objet composé séparément. Lorsque l'analyse uniquement des nouveaux fichiers et des fichiers modifiés est activée, Kaspersky Anti-Virus analyse tous les objets de la couverture d'analyse désignée sauf ceux qu'il a déjà analysés une fois, qui n'étaient pas infectés et qui n'ont pas été modifiés depuis cette analyse.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

ACTION A EXECUTER SUR LES OBJETS INFECTES

Le paramètre de sécurité **Action à exécuter sur les objets** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

DANS CETTE SECTION DE L'AIDE

ACTION A EXECUTER SUR LES OBJETS INFECTES DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

*Tableau 93. Paramètre **Action à exécuter sur les objets infectés***

Paramètre	Action à exécuter sur les objets infectés.
Description	Quand Kaspersky Anti-Virus identifie un objet infecté, il empêche l'application d'accéder à l'objet et exécute sur celui-ci l'action que vous aurez définie. Avant de modifier (réparer ou supprimer) un objet, Kaspersky Anti-Virus place une copie de celui-ci dans la sauvegarde (cf. rubrique "Présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 211), un dossier spécial dans lequel les objets sont conservés sous forme chiffrée. Kaspersky Anti-Virus ne tentera pas de réparer ou de supprimer un objet s'il ne parvient pas d'abord à placer sa copie en sauvegardé. L'objet n'est pas modifié. Les informations relatives à l'échec de la réparation ou de la suppression de l'objet par Kaspersky Anti-Virus sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).
Valeurs de paramètres et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Interdire l'accès + réparer**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il laisse l'objet inchangé (l'application qui avait sollicité le fichier ne peut y accéder) ; • **Interdire l'accès + réparer, supprimer si la réparation est impossible**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il le supprime. • **Interdire l'accès + supprimer**. Kaspersky Anti-Virus supprime l'objet infecté. • **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute automatiquement les actions sur l'objet en fonction des données sur le danger que représentent les menaces identifiées et des possibilités de réparation ; par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie, car ils ne s'intègrent pas à d'autres fichiers et ne les infectent pas et, par conséquent, ne peuvent pas être réparés. • **Interdire l'accès**. Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Il se contente d'en interdire l'accès.

•

CF. INSTRUCTION DE LA CONFIGURATION

ACTION A EXECUTER SUR LES OBJETS INFECTES DANS LES TACHES D'ANALYSE A LA DEMANDE

*Tableau 94. Paramètre **Action à exécuter sur les objets infectés lors de l'analyse à la demande***

Paramètre	Action à exécuter sur les objets infectés.
Description	Quand Kaspersky Anti-Virus identifie un objet comme infecté, il exécute l'action que vous avez définie. Avant de modifier (réparer ou supprimer) un objet, Kaspersky Anti-Virus place une copie de celui-ci dans la sauvegarde (cf. rubrique "Présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 211), un dossier spécial dans lequel les objets sont conservés sous forme chiffrée. Kaspersky Anti-Virus ne tentera pas de réparer ou de supprimer un objet s'il ne parvient pas d'abord à placer sa copie en sauvegardé. L'objet n'est pas modifié. Les informations relatives à l'échec de la réparation ou de la suppression de l'objet par Kaspersky Anti-Virus sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).
Valeurs de paramètres et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Réparer**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, l'objet n'est pas modifié ; • **Réparer, supprimer si la réparation est impossible**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il le supprime ; • **Supprimer**. Kaspersky Anti-Virus supprime directement l'objet sans tenter de le réparer ; • **Exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute automatiquement les actions sur l'objet en fonction des données sur le danger que représentent les menaces identifiées et des possibilités de réparation ; par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie, car ils ne s'intègrent pas à d'autres fichiers et ne les infectent pas et, par conséquent, ne peuvent pas être réparés ; • **Ignorer**. L'objet n'est pas modifié. Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Les informations relatives à l'objet infecté détecté sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

•

CF. INSTRUCTION DE LA CONFIGURATION

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

ACTION A EXECUTER SUR LES OBJETS SUSPECTS.

Le paramètre de sécurité **Action à exécuter sur les objets suspects** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

DANS CETTE SECTION DE L'AIDE

ACTION A EXECUTER SUR LES OBJETS INFECTES DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

*Tableau 95. Paramètre **Action à exécuter sur les objets suspectés***

Paramètre	Action à exécuter sur les objets suspects.
Description	Quand Kaspersky Anti-Virus identifie un objet suspect, il empêche l'application d'accéder à l'objet et exécute sur celui-ci l'action que vous aurez définie. Avant de supprimer l'objet, Kaspersky Anti-Virus place une copie de celui-ci dans un répertoire spécial dans lequel l'objet est conservé sous forme chiffrée. Ce répertoire est la sauvegarde (cf. rubrique "Présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 211).
Valeurs et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Interdire l'accès + quarantaine**. Kaspersky Anti-Virus place l'objet suspect en quarantaine (cf. rubrique "Isolement des objets suspects" à la page. 191) : l'objet est déplacé dans un dossier spécial où il est conservé sous forme cryptée. • **Interdire l'accès + supprimer**. Kaspersky Anti-Virus supprime l'objet suspect du disque. Kaspersky Anti-Virus ne supprime pas objet s'il ne parvient pas d'abord à placer sa copie en quarantaine. L'objet n'est pas modifié. Les informations relatives à l'échec de la suppression de l'objet par Kaspersky Anti-Virus sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234). • **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute les actions sur l'objet en fonction des données sur le danger que représente la menace identifiée dans l'objet. • **Interdire l'accès**. Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Il se contente d'en interdire l'accès.

•

CF. INSTRUCTION DE LA CONFIGURATION

ACTION A EXECUTER SUR LES OBJETS SUSPECTS DANS LES TACHES D'ANALYSE A LA DEMANDE

*Tableau 96. Paramètre **Action à exécuter sur les objets suspects lors de l'analyse à la demande***

Paramètre	Action à exécuter sur les objets suspects.
Description	Quand Kaspersky Anti-Virus identifie un objet suspect, il exécute l'action que vous avez définie. Avant de supprimer l'objet, Kaspersky Anti-Virus place une copie de celui-ci dans un répertoire spécial dans lequel l'objet est conservé sous forme chiffrée. Ce répertoire est la sauvegarde (cf. rubrique "Présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 211).
Valeurs et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Quarantaine**. Kaspersky Anti-Virus place l'objet suspect en quarantaine (cf. rubrique "Isolement des objets suspects" à la page. 191) : l'objet est déplacé dans un dossier spécial où il est conservé sous forme cryptée. • **Supprimer**. Kaspersky Anti-Virus supprime l'objet suspect du disque. Kaspersky Anti-Virus ne supprime pas objet s'il ne parvient pas d'abord à placer sa copie en quarantaine. L'objet n'est pas modifié. Les informations relatives à l'échec de la suppression de l'objet par Kaspersky Anti-Virus sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234). • **Exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute les actions sur l'objet en fonction des données sur le danger que représente la menace identifiée dans l'objet. • **Ignorer**. L'objet n'est pas modifié. Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Les informations relatives à l'objet suspect détecté sont conservées dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

•

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

DUREE MAXIMALE DE L'ANALYSE D'UN OBJET

Le paramètre de sécurité **Durée maximale de l'analyse d'un objet** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

*Tableau 97. Paramètre **Durée maximale de l'analyse d'un objet***

Paramètre	Durée maximale de l'analyse d'un objet, s. (**Arrêter si l'analyse dure plus de... sec**).
Description	Kaspersky Anti-Virus arrête l'analyse si celle-ci dure plus longtemps que la valeur définie (en secondes) pour le paramètre. Les informations relatives à l'exclusion de l'objet de l'analyse sont reprises dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234) (conformément aux paramètres des journaux d'exécution des tâches définis par défaut).
Valeurs	Saisissez la durée maximale, en secondes, de l'analyse d'un objet.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

TAILLE MAXIMALE DE L'OBJET COMPOSE ANALYSE

Le paramètre de sécurité **Taille maximale de l'objet composé à analyser** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

*Tableau 98. Paramètre **Taille maximale de l'objet composé à analyser***

Paramètre	Taille maximale de l'objet composé à analyser, Mo (**Ne pas analyser les objets composés de plus de... Mo**).
Description	Si la taille de l'objet composé à analyser dépasse la valeur définie, Kaspersky Anti-Virus l'ignorera. Les informations relatives au fait que l'objet a été ignoré sont reprises dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234) (conformément aux paramètres des journaux d'exécution des tâches définis par défaut).
Valeurs	Définissez la taille maximale de l'objet composé en mégaoctets.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

APPLICATION DE LA TECHNOLOGIE ICHECKER

Le paramètre de sécurité **Application de la technologie iChecker** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande (cf. le tableau ci-dessous).

*Tableau 99. Paramètre **Application de la technologie iChecker***

Paramètre	Application de la technologie iChecker (**Utiliser la technologie iChecker**).
Description	Ce paramètre active ou désactive l'application de la technologie iChecker développée par Kaspersky Lab. La technologie iChecker s'applique uniquement aux objets de type et de format pouvant être infectés. La technologie iChecker permet de ne pas analyser une nouvelle fois les objets du serveur considérés comme non infectés par Kaspersky Anti-Virus à l'issue des analyses antérieures. Le recours à la technologie iChecker diminue la charge du processeur et des systèmes du disque et accélère la vitesse de l'analyse ainsi que l'échange de données. N'oubliez pas que Kaspersky Anti-Virus analyse à nouveau un objet si ce dernier a été modifié depuis la dernière analyse, si le niveau de protection a été augmenté. Kaspersky Anti-Virus conserve les informations sur la non-analyse de l'objet suite à l'application de la technologie iChecker dans le journal d'exécution de la tâche (cf. rubrique "présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 234) (conformément aux paramètres des journaux d'exécution des tâches définis par défaut).
Valeurs	Activée / désactivée.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

APPLICATION DE LA TECHNOLOGIE ISWIFT

Le paramètre de sécurité Application de la technologie iSwift concerne la tâche Protection en temps réel des fichiers et les tâches d'analyse à la demande (cf. le tableau ci-dessous).

*Tableau 100. Paramètre **Application de la technologie iSwift***

Paramètre	Application de la technologie iSwift (**Utiliser la technologie iSwift**).
Description	Ce paramètre active ou désactive l'application de la technologie iSwift développée par Kaspersky Lab. La technologie iSwift concerne tous les objets du système de fichiers NTFS. La technologie iSwift permet de ne pas analyser à nouveau les objets qui, à l'issue des analyses précédentes, ont été reconnus comme sains par Kaspersky Anti-Virus, ainsi que les objets analysés par d'autres applications antivirus de Kaspersky Lab de la version 8.0. Le recours à la technologie iSwift diminue la charge du processeur et des systèmes du disque et accélère la vitesse de l'analyse ainsi que l'échange de données. N'oubliez pas que Kaspersky Anti-Virus analyse à nouveau un objet si ce dernier a été modifié depuis la dernière analyse, si le niveau de protection a été augmenté. Kaspersky Anti-Virus conserve les informations sur la non-analyse de l'objet suite à l'application de la technologie iSwift dans le journal d'exécution de la tâche (cf. rubrique "présentation de la sauvegarde des objets avant la réparation ou la suppression" à la page 234) (conformément aux paramètres des journaux d'exécution des tâches définis par défaut).
Valeurs	Activée / désactivée.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

VERIFICATION DE LA SIGNATURE MICROSOFT DES FICHIERS

Le paramètre de sécurité **Vérification de la signature Microsoft des fichiers** est appliqué dans les tâches d'analyse à la demande. (voir le tableau ci-dessous).

*Tableau 101. Paramètre **Vérification de la signature Microsoft des fichiers***

Paramètre	Vérification de la signature Microsoft des fichiers.
Description	Étant donné que le serveur protégé fonctionne avec le système d'exploitation Microsoft Windows, les fichiers système et fichiers applicatifs sont signés par la société Microsoft. Si ce paramètre est actif dans la tâche, Kaspersky Anti-Virus considère ces fichiers sains, vérifie lors de l'exécution de la tâche que les fichiers sont ou non signés par la société Microsoft. Il conserve des informations à propos des fichiers possédant ce type de signature. Lors des analyses ultérieures, Kaspersky Anti-Virus ne vérifie plus ces fichiers de confiance. Même si la toute première analyse est susceptible de prendre un certain temps, les analyses suivantes, en temps réel ou sur demande, s'effectuent beaucoup plus rapidement.
Valeurs	Activé/désactivé

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES DE L'ANALYSEUR HEURISTIQUE

Les paramètres de l'analyseur heuristique sont utilisés dans les tâches **Protection en temps réel des fichiers** et **Analyse des scripts** ainsi que dans les tâches d'analyse à la demande.

DANS CETTE SECTION DE L'AIDE

Utilisation de l'analyseur heuristique 393

Niveau d'analyse 394

UTILISATION DE L'ANALYSEUR HEURISTIQUE

*Tableau 102. Paramètre **Application de l'utilisateur heuristique***

Paramètre	Application de l'analyseur heuristique (**utiliser l'analyseur heuristique**).
Description	Ce paramètres active l'utilisation du composant d'analyse heuristique (Heuristic Analyzer) de Kaspersky Anti-Virus. L'analyseur heuristique intervient dans la tâche **Protection en temps réel des fichiers**, dans la tâche **Analyse des scripts** et dans les tâches d'analyse à la demande. Kaspersky Anti-Virus utilise l'analyseur heuristique dans l'analyse des fichiers exécutable qu'il a considéré comme sains à l'issue de l'analyse à l'aide des bases. L'analyseur heuristique étudie le comportement des objets à analyser. Il exécute, dans un environnement spécial protégé, des instructions qui contiennent l'objet analysé et émule les appels des fonctions système. Si l'analyseur heuristique découvre dans l'objet des séquences d'instructions propres aux objets malveillants, Kaspersky Anti-Virus attribue à cet objet l'état *suspect*. Grâce à l'analyseur heuristique, Kaspersky Anti-Virus peut découvrir des programmes malveillants de divers types. Vous pouvez lire le nom du programme malveillant que l'analyseur heuristique a attribué à l'objet dans le journal d'exécution de la tâche. Il peut reprendre le nom de la catégorie de programmes malveillants ou le type de menace selon la classification de Kaspersky Lab. Kaspersky Anti-Virus exécute sur l'objet les actions que vous avez définies pour les objets suspects. La recherche de menaces à l'aide de l'analyseur heuristique prend plus de temps, mais elle permet de protéger l'ordinateur non seulement contre les menaces que Kaspersky Anti-Virus connaît, mais également contre les menaces les plus récentes dont les définitions n'ont pas encore été ajoutées aux bases. Vous pouvez activer l'application de l'analyseur heuristique pour l'analyse de tous les objets dans la tâche sélectionnée d'analyse à la demande ou dans la tâche de protection en temps réel. Par défaut, l'analyseur heuristique fonctionne de la manière suivante dans les tâches : • **Protection en temps réel des fichiers** – appliqué au niveau d'analyse **Moyen**; • **Analyse des scripts** : intervient au niveau d'analyse **Moyen** ; • **Analyse des secteurs critiques** : intervient au niveau d'analyse **Moyen** ; • **Analyse des objets en quarantaine** : intervient au niveau d'analyse **Profonde** ; • **Analyse au démarrage du système** – appliqué au niveau d'analyse **Moyen**; • Nouvelle tâche d'analyse à la demande : intervient au niveau d'analyse **Moyen**.
Valeurs	Activée / désactivée.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

NIVEAU D'ANALYSE

*Tableau 103. Paramètre **Niveau d'analyse***

Paramètre	Niveau d'analyse
Description	La recherche de menaces à l'aide de l'analyseur heuristique prend plus de temps. Le paramètre **Niveau d'analyse** permet de régler la durée d'analyse des objets par l'analyseur heuristique et la probabilité de découvrir des menaces dans les objets analysés.
Valeurs	Peut prendre les valeurs suivantes : **Profonde** – **moyenne** – **superficielle**. Si vous choisissez le niveau d'analyse profonde, l'analyseur heuristique exécutera plus d'instructions contenues dans l'objet afin de définir la probabilité de la présence de menaces dans celui-ci L'analyse dans ce cas prend plus de temps. Dans le cadre de l'analyse superficielle, l'analyseur heuristique exécute un nombre restreint d'exécutions dans l'objet, ce qui accélère l'analyse. Réglez le niveau d'analyse à l'aide du curseur en fonction de vos besoins en matière de sécurité et de vitesse d'échange de fichiers sur le serveur.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration manuelle des paramètres de sécurité des tâches d'analyse à la demande 147

Configuration des paramètres de protection de la tâche Protection en temps réel des fichiers 97

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES DES TACHES LIEES A LA MISE A JOUR

La rubrique "Paramètres de toutes les tâches de mise à jour" décrit les paramètres des tâches de mise à jour de n'importe quel type tels que la source des mises à jour, l'utilisation et la configuration du serveur proxy et les paramètres régionaux. Les paramètres propres à des tâches d'un certain type uniquement sont décrites dans des sections distinctes.

DANS CETTE SECTION DE L'AIDE

Paramètres de toutes les tâches de mise à jour 395

Paramètres de la tâche Mise à jour des modules de l'application 401

Paramètres de la tâche Copie des mises à jour 403

PARAMETRES DE TOUTES LES TACHES DE MISE A JOUR

DANS CETTE SECTION DE L'AIDE

SOURCE DES MISES A JOUR

*Tableau 104. Paramètre **Source des mises à jour***

Paramètre	Source des mises à jour.
Description	Vous pouvez sélectionner la source depuis laquelle Kaspersky Anti-Virus téléchargera les mises à jour des bases ou des modules de l'application en fonction du plan de mise à jour utilisé par votre entreprise (des exemples de schémas sont repris au point. Les exemples de schémas de mise à jour se trouvent dans la section "Schémas de mise à jour des bases et des modules des applications antivirus dans l'entreprise" (cf. page 60).
Valeurs possibles	Les serveurs suivants peuvent être utilisés en guise de source des mises à jour : • **Serveurs de mises à jour de Kaspersky Lab**. Kaspersky Anti-Virus télécharge les mises à jour depuis un des serveurs de mise à jour de Kaspersky Lab situés dans divers pays. Les mises à jour sont téléchargées selon le protocole HTTP ou FTP. • **Serveur d'Administration Kaspersky**. Vous pouvez sélectionner cette source si vous utilisez l'application Kaspersky Administration Kit pour l'administration centralisée de la protection antivirus des ordinateurs de votre entreprise. Kaspersky Anti-Virus copiera la mise à jour sur le serveur protégé depuis le serveur d'administration Kaspersky Administration Kit installé dans le réseau local. • **Serveurs HTTP, FTP ou dossiers réseau personnalisés**. Kaspersky Anti-Virus copiera la mise à jour depuis la source que vous aurez définie : dossier FTP, serveur HTTP ou un ordinateur quelconque du réseau local. Vous pouvez définir une ou plusieurs sources de mises à jour. Kaspersky Anti-Virus contactera chaque source indiquée dans l'ordre si la source précédente n'est pas disponible. Vous pouvez définir l'ordre dans lequel Kaspersky Anti-Virus va contacter les sources, activer ou désactiver l'utilisation de sources distinctes. Vous pouvez configurer l'organisation des requêtes de Kaspersky Anti-Virus aux serveurs de mise à jour de Kaspersky Lab au cas où les sources définies par l'utilisateur ne seraient pas accessibles. Vous pouvez utiliser des variables dans le chemin. Si vous utilisez des variables pour l'utilisateur, indiquez le compte utilisateur de celui-ci pour lancer la tâche. Vous ne pouvez pas sélectionner des dossiers sur des disques de réseaux connectés en guise de sources de mise à jour ni des dossiers partagés Novell.
Valeur par défaut	Vous pouvez consulter la liste des serveurs de mises à jour de Kaspersky Lab dans le fichier %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\updcfg.xml.

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

MODE DU SERVEUR FTP POUR LA CONNEXION AU SERVEUR PROTEGE

*Tableau 105. Paramètre **Mode du serveur FTP pour la connexion au serveur protégé***

Paramètre	Mode du serveur FTP pour la connexion au serveur protégé (**Utiliser le FTP en mode passif si possible**).
Description	La connexion aux serveurs de mises à jour selon le protocole FTP s'opère selon le mode FTP passif : on suppose que le réseau local de l'entreprise utilise un pare-feu. Quand le mode passif du serveur FTP ne fonctionne pas, le mode actif est enclenché automatiquement.
Valeurs possibles	Sélectionnez le mode du serveur FTP : activez ou désactivez l'utilisation du mode passif du FTP.
Valeur par défaut	Mode FTP passif, si possible.

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

DELAI D'ATTENTE LORS DE LA CONNEXION A LA SOURCE DES MISES A JOUR

*Tableau 106. Paramètre **Délai d'attente lors de la connexion à la source des mises à jour***

Paramètre	Délai d'attente lors de la connexion (**Délai d'attente**).
Description	Ce paramètre définit le délai d'attente lors de la connexion à la source des mises à jour.
Valeurs possibles	Définissez le délai d'attente en secondes.
Valeur par défaut	10 sec

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

UTILISATION ET PARAMETRES DU SERVEUR PROXY

DANS CETTE SECTION DE L'AIDE

REQUETE ADRESSEE AU SERVEUR PROXY LORS DE LA CONNEXION AUX SOURCES DES MISES A JOUR

*Tableau 107. Paramètre **Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour***

Paramètre	Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour.
Description	Par défaut, lors de la connexion aux serveurs de mise à jour de Kaspersky Lab, Kaspersky Anti-Virus contacte le serveur proxy du réseau et lors de la connexion aux sources de mise à jour définies par l'utilisateur (serveurs HTTP ou FTP ou ordinateurs définis), il contourne le serveur proxy : il suppose que ces sources se trouvent dans le réseau local. N'oubliez pas que les extensions des fichiers des mises à jour des bases sont aléatoires. Si le serveur proxy de votre réseau possède une règle d'interdiction pour le téléchargement de fichiers possédant une certaine extension, il est alors conseillé d'autoriser le téléchargement de fichier de n'importe quelle extension depuis les serveurs de mises à jour de Kaspersky Lab. Vous pouvez consulter la liste des serveurs de mises à jour de Kaspersky Lab dans le fichier %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\updcfg.xml.
Valeurs possibles	Si vous avez désigné un serveur de mises à jour de Kaspersky Lab en tant que source des mises à jour, assurez-vous que la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour** de Kaspersky Lab est cochée. Si la connexion à un des serveurs FTP ou HTTP défini par l'utilisateur requiert un accès au serveur proxy, cochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs personnalisés**. Après avoir coché cette case, vous pouvez désactiver l'envoi de requête au serveur proxy pour accéder aux autres sources de mise à jour pour lesquelles ces requêtes ne sont pas nécessaires (par exemple, s'il s'agit d'ordinateurs du réseau local) : cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.
Valeur par défaut	Kaspersky Anti-Virus contacte le serveur proxy uniquement lors de la connexion aux serveurs de mises à jour HTTP ou FTP de Kaspersky Lab.

CF. INSTRUCTION DE LA CONFIGURATION

PARAMETRES DU SERVEUR PROXY

*Tableau 108. Paramètre **Paramètres du serveur proxy***

Paramètre	Paramètres du serveur proxy.
Description	Lors de la connexion aux serveurs de mise à jour FTP ou HTTP, Kaspersky Anti-Virus identifie par défaut les paramètres du serveur proxy utilisé sur le réseau local grâce au protocole Web Proxy Auto-Discovery Protocol (WPAD). Vous pouvez indiquer manuellement les paramètres du serveur proxy, par exemple si le protocole WPAD n'est pas configuré dans votre réseau local.
Valeurs possibles	Indiquez l'adresse IP ou le nom DNS du serveur (par exemple, proxy.mycompany.com) et son port. Désactivez l'utilisation du serveur proxy si le serveur FTP ou HTTP défini par l'utilisateur se trouve dans votre réseau local.
Valeur par défaut	Identifier automatiquement les paramètres du serveur proxy.

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

METHODE DE VERIFICATION DE L'AUTHENTICITE LORS DE L'ACCES AU SERVEUR PROXY

*Tableau 109. Paramètre **Méthode de vérification de l'authenticité lors de l'accès au serveur proxy***

Paramètre	Méthode de vérification de l'authenticité lors de l'accès au serveur proxy.
Description	Ce paramètre définit la méthode de vérification de l'authenticité de l'utilisateur lors de l'accès au serveur proxy utilisé lors de la connexion aux serveurs FTP ou HTTP de mises à jour.
Valeurs possibles	Choisissez une des valeurs suivantes : • **Aucune authentification requise**. Sélectionnez cette option si l'accès au serveur proxy ne requiert pas la vérification de l'authenticité. • **Utiliser l'authentification NTLM**. Kaspersky Anti-Virus utilisera le compte utilisateur indiqué dans la tâche pour accéder au serveur proxy. (Si le paramètre **Exécuter en tant que** ne définit aucun autre compte utilisateur, la tâche sera exécutée sous le compte **Système local** (**SYSTEM**). Vous pouvez sélectionner cette méthode si le serveur proxy est compatible avec la fonction intégrée de vérification de l'authenticité de Microsoft Windows (NTLM authentication). • **Utiliser l'authentification NTLM avec utilisateur et mot de passe**. Kaspersky Anti-Virus utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy. Vous pouvez sélectionner cette méthode si le serveur proxy est compatible avec la fonction intégrée de vérification de l'authenticité de Microsoft Windows. Saisissez le nom d'utilisateur et le mot de passe ou sélectionnez un utilisateur dans la liste. • **Utiliser le nom d'utilisateur et le mot de passe**. Vous pouvez sélectionner la vérification traditionnelle de l'authenticité (Basic authentification). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste. Vous pouvez sélectionner cette méthode si, par exemple, le compte utilisateur avec les privilèges duquel la tâche de mise à jour sera exécutée ne jouit pas des privilèges d'accès au serveur proxy et que vous souhaitez utiliser un autre compte utilisateur. Si la vérification traditionnelle de l'authenticité en fonction du nom et du mot de passe de l'utilisateur échoue, Kaspersky Anti-Virus utilisera la vérification intégrée de l'authenticité de Microsoft Windows selon le compte utilisateur utilisé dans la tâche.
Valeur par défaut	La vérification de l'authenticité lors de l'accès au serveur proxy n'est pas réalisée.

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES REGIONAUX POUR L'OPTIMALISATION DE LA RECEPTION DES MISES A JOUR (EMPLACEMENT)

*Tableau 110. Paramètre **Paramètres de la tâche de Mise à jour des modules de l'application***

Paramètre	Paramètres régionaux pour l'optimalisation de la réception des mises à jour (**Emplacement**).
Description	Les serveurs de mises à jour de Kaspersky Lab se trouvent dans divers pays. Grâce à ce paramètre, vous pouvez indiquer le pays où se trouve le serveur à protéger. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur depuis les serveurs de mises à jour de Kaspersky Lab en sélectionnant le plus proche.
Valeurs possibles	Vous pouvez sélectionner le pays où se trouve le serveur à protéger.
Valeur par défaut	Kaspersky Anti-Virus identifie par défaut le pays où se trouve le serveur à protéger sur la base des paramètres régionaux définis dans Microsoft Windows, pour Microsoft Windows Server 2003, selon la valeur de la variable Location, définie pour l'utilisateur par défaut (Default User Account Settings). Kaspersky Anti-Virus identifie par défaut le pays où se trouve le serveur à protéger sur la base des paramètres régionaux définis dans Microsoft Windows, pour Microsoft Windows Server 2003, selon la valeur de la variable **Location**, définie pour l'utilisateur par défaut (Default User). Par exemple, si dans les paramètres régionaux de Microsoft Windows vous (pour l'utilisateur courant) attribuez la valeur **Russie** à la variable Location, alors elle demeurera pour l'utilisateur par défaut. Pour optimiser la récupération des mises à jour, vous pouvez exécuter une des actions suivantes : • dans les paramètres régionaux de Microsoft Windows, spécifiez la location de la variable **Emplacement**, définie pour l'utilisateur par défaut ; • dans Kaspersky Anti-Virus, exécuter la tâche de mises à jour pour le compte utilisateur courant ; • sélectionner le pays où se trouve le serveur à l'aide du paramètre de mise à jour **Emplacement du serveur protégé** décrit dans ce tableau.

•

CF. INSTRUCTION DE LA CONFIGURATION

Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 65

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES DE LA TACHE MISE A JOUR DES MODULES DE L'APPLICATION

DANS CETTE SECTION DE L'AIDE

Copie et installation des mises à jour critique ou simple vérification de leur présence 402

Obtention d'informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus 403

COPIE ET INSTALLATION DES MISES A JOUR CRITIQUE OU SIMPLE VERIFICATION DE LEUR PRESENCE

*Tableau 111. Paramètre **Paramètres de la tâche de Mise à jour des modules de l'application***

Paramètre	Copie et installation des mises à jour critique ou simple vérification de leur présence.
Description	A l'aide des paramètres de la tâche **Mise à jour des modules de l'application**, vous pouvez décider de télécharger et d'installer immédiatement les mises à jour critiques des modules de l'application ou de vérifier uniquement si elles sont disponibles.
Valeurs possibles	Choisissez une des valeurs suivantes : • **Rechercher uniquement la présence des mises à jour critiques des modules de l'application**. Vous pouvez choisir cette option, par exemple, pour savoir si des mises à jour urgentes des modules de Kaspersky Anti-Virus ont été diffusées. • **Copier et installer les mises à jour critiques des modules de l'application**.
Valeur par défaut	Rechercher uniquement la présence des mises à jour critiques des modules de l'application.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la tâche Mise à jour des modules 71

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

OBTENTION D'INFORMATIONS SUR LA DIFFUSION DES MISES A JOUR PREVUES DES MODULES DE KASPERSKY ANTI-VIRUS

*Tableau 112. Paramètre **Obtention d'informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus***

Paramètre	Obtention d'informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus
Description	Vous pouvez obtenir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus. Pour recevoir les notifications sur la sortie des mises à jour prévues, sélectionnez **Recevoir des informations sur les mises à jour des modules de l'application prévues** et configurez la notification sur l'événement de Kaspersky Anti-Virus *De nouvelles mises à jour des modules d'application sont disponibles*, qui contiendra l'adresse de la page de notre site Web. Vous pourrez télécharger les mises à jour prévues à partir de cette page (pour plus d'informations sur la configuration des notifications, consultez la section "Configuration des notifications" (cf. page 264)).
Valeurs possibles	Recevoir/ne pas recevoir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus.
Valeur par défaut	Recevoir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la tâche Mise à jour des modules 71

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES DE LA TACHE "COPIE DES MISES A JOUR"

DANS CETTE SECTION DE L'AIDE

Composition des mises à jour 404

Dossier pour l'enregistrement des mises à jour..... 405

COMPOSITION DES MISES A JOUR

*Tableau 113. Paramètre **Composition des mises à jour***

Paramètre	Composition des mises à jour.
Description	Ce paramètre vous permet de définir la composition des mises à jour copiées. Vous pouvez copier uniquement les mises à jour des bases de Kaspersky Anti-Virus, uniquement les mises à jour urgentes des modules ou toutes les mises à jour disponibles. Ou vous pouvez copier les mises à jour des bases et des modules non seulement pour Kaspersky Anti-Virus mais également pour les autres applications des versions 6.0 et 8.0 des solutions de Kaspersky Lab pour entreprise puis, répartir ces mises à jour vers d'autres ordinateurs du réseau local où les logiciels antivirus de Kaspersky Lab de cette version sont installés. Kaspersky Anti-Virus enregistre par défaut les fichiers des mises à jour dans le répertoire %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\UpdateDistribution\.
Valeurs possibles	Choisissez une des valeurs suivantes : • **Copier les mises à jour des bases de l'application**. Choisissez cette option pour télécharger et enregistrer uniquement les mises à jour des bases de Kaspersky Anti-Virus dans le répertoire indiqué. • **Copier les mises à jour critiques des modules de l'application**. Choisissez cette option pour télécharger et enregistrer uniquement les mises à jour critiques des modules logiciels de Kaspersky Anti-Virus dans le répertoire indiqué. • **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application**. Choisissez cette option pour télécharger et enregistrer les mises à jour des bases et les mises à jour critiques des modules logiciels de Kaspersky Anti-Virus dans le répertoire indiqué. • **Copier les mises à jour des bases et des modules pour les applications de Kaspersky Lab des versions 6.0 et 8.0**. Choisissez cette option pour récupérer les mises à jour des bases et les mises à jour critiques des modules non seulement pour Kaspersky Anti-Virus mais aussi des autres applications de Kaspersky Lab des versions 6.0, 8.0 et suivantes.
Valeur par défaut	Kaspersky Anti-Virus copie uniquement les mises à jour des bases.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la tâche Copie des mises à jour 70

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

DOSSIER POUR L'ENREGISTREMENT DES MISES A JOUR.

*Tableau 114. Paramètre **Dossier pour l'enregistrement des mises à jour***

Paramètre	Dossier pour l'enregistrement des mises à jour.
Description	Ce paramètre vous permet d'indiquer le répertoire dans lequel les fichiers des mises à jour seront enregistrés.
Valeurs possibles	Indiquez le répertoire local ou de réseau dans lequel Kaspersky Anti-Virus enregistrera les mises à jour copiées. Pour définir un répertoire de réseau, saisissez son chemin d'accès au format UNC (Universal Naming Convention). Vous ne pouvez pas désigner des répertoires sur des disques de réseau connectés, ni sur des disques créés à l'aide de la commande SUBST. Vous pouvez utiliser des variables dans le chemin. Si vous utilisez une variable d'environnement, désignez le compte utilisateur de cet utilisateur pour l'exécution de la tâche (cf. rubrique "Utilisation de comptes utilisateur pour l'exécution des tâches" à la page 54). Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la tâche Copie des mises à jour 70

Création d'une tâche dans Kaspersky Administration Kit 341

Création d'une stratégie dans Kaspersky Administration Kit 332

PARAMETRES DE QUARANTAINE PAR DEFAUT

DANS CETTE SECTION DE L'AIDE

Répertoire de quarantaine..... 406

Taille maximale de la quarantaine..... 406

Seuil d'espace libre dans la quarantaine..... 407

Dossier de la restauration : quarantaine 408

REPERTOIRE DE QUARANTAINE

*Tableau 115. Paramètre **Dossier de quarantaine***

Paramètre	Répertoire de quarantaine.
Description	Vous pouvez utiliser un répertoire de quarantaine différent du répertoire de quarantaine désigné par défaut.
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Kaspersky Anti-Virus commencera à placer les objets dans le répertoire indiqué par le paramètre dès que vous aurez enregistré la nouvelle valeur du paramètre. Si le répertoire indiqué n'existe pas ou est inaccessible, Kaspersky Anti-Virus utilisera le répertoire défini par défaut. Pour indiquer le chemin d'accès au répertoire de quarantaine, vous pouvez utiliser des variables prédéfinies ; vous ne pouvez pas par contre utiliser des variables définies par l'utilisateur. Dans le cluster, les répertoires de disque de quorum ou de cluster ne peuvent être des répertoires de quarantaine.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\ Quarantine\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres de la quarantaine en MMC 202

Configuration de paramètres de Quarantaine dans Kaspersky Administration Kit 307

TAILLE MAXIMALE DE LA QUARANTAINE.

*Tableau 116. Paramètre **Taille maximale de la quarantaine***

Paramètre	Taille maximale de la quarantaine.
Description	Ce paramètre définit la taille maximale de la quarantaine, à savoir le volume total de données dans le dossier de quarantaine. Le paramètre **Taille maximale de la quarantaine** est informatif. Il ne limite pas la taille du dossier de la quarantaine mais permet à l'administrateur de surveiller l'état de la quarantaine. Une fois que la taille maximale a été atteinte, Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine. Vous pouvez configurer la notification sur le dépassement de la taille maximale de la quarantaine. Kaspersky Anti-Virus envoie une notification dès que le volume total des données dans la quarantaine atteint la valeur indiquée. Pour en savoir plus, lisez la rubrique "Configuration des notifications de l'administrateur et de l'utilisateur" (cf. page 264). La valeur recommandée est égale à 200 Mo.
Valeurs possibles	1 à 999 Mo
Valeur par défaut	Non définie.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres de la quarantaine en MMC 202

Configuration de paramètres de Quarantaine dans Kaspersky Administration Kit 307

SEUIL D'ESPACE LIBRE DANS LA QUARANTAINE.

*Tableau 117. Paramètres **Seuil d'espace libre dans la quarantaine***

Paramètre	Seuil d'espace libre dans la quarantaine.
Description	Ce paramètre est utilisé conjointement au paramètre **Taille maximale de la quarantaine**. Le paramètre **Seuil d'espace libre** dans la quarantaine est informative. Il ne limite pas la taille du dossier de quarantaine mais permet d'obtenir des informations sur la proximité du remplissage de la quarantaine. Si le volume d'espace disponible dans la quarantaine est inférieur à la valeur du seuil, Kaspersky Anti-Virus enregistre l'événement **Dépassement du seuil d'espace libre** pour la quarantaine et continue à isoler les objets suspects. Vous pouvez configurer des notifications pour l'événement Le seuil d'espace disponible dans la quarantaine est dépassé. **Pour en savoir plus sur la configuration des notifications**, lisez la rubrique "Configuration des notifications de l'administrateur et des utilisateurs" (cf. page 264).
Valeurs possibles	Indiquez le volume de la quarantaine en Mo ; il doit être inférieur à la valeur définie par le paramètre **Taille maximale de la quarantaine**. La valeur recommandée est de 50 Mo.
Valeur par défaut	Non définie.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres de la quarantaine en MMC 202

Configuration de paramètres de Quarantaine dans Kaspersky Administration Kit 307

DOSSIER DE LA RESTAURATION : QUARANTAINE

*Tableau 118. Paramètre **Restaurer dans le dossier***

Paramètre	Restaurer dans le dossier.
Description	Le paramètre définit le répertoire spécial utilisé pour les objets restaurés sur le serveur protégé. Lors de la restauration d'un objet, vous pouvez sélectionner l'emplacement où l'objet restauré sera conservé : dans le répertoire d'origine, dans un dossier spécial pour les objets restaurés sur le serveur protégé ou dans un dossier autre indiqué (sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou dans un répertoire de réseau).
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Pour indiquer le chemin d'accès au répertoire de restauration, vous pouvez utiliser des variables prédéfinies ; vous ne pouvez pas utiliser des variables d'utilisateur. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration de paramètres de la quarantaine en MMC 202

Configuration de paramètres de Quarantaine dans Kaspersky Administration Kit 307

PARAMETRES DE SAUVEGARDE

DANS CETTE SECTION DE L'AIDE

Dossier de sauvegarde 409

Taille maximale du dossier de sauvegarde 410

Seuil d'espace libre de la sauvegarde 410

Dossier pour la restauration : Sauvegarde 411

DOSSIER DE SAUVEGARDE.

*Tableau 119. Paramètre **Dossier de sauvegarde***

Paramètre	Dossier de sauvegarde.
Description	Vous pouvez utiliser un répertoire de sauvegarde différent du répertoire de sauvegarde désigné par défaut
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Kaspersky Anti-Virus utilise directement le répertoire indiqué dès que la nouvelle valeur du paramètre a été enregistrée. Si le répertoire indiqué n'existe pas ou est inaccessible, Kaspersky Anti-Virus utilisera le répertoire défini par défaut. Pour indiquer le chemin d'accès au répertoire de sauvegarde, vous pouvez utiliser des variables ; vous ne pouvez pas utiliser des variables définies par l'utilisateur. Dans un cluster, les répertoires de disque de quorum ou des clusters ne peuvent être des dossiers de sauvegarde. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Backup\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la sauvegarde en MMC 218

Configuration de la sauvegarde dans Kaspersky Administration Kit 310

TAILLE MAXIMALE DU DOSSIER DE SAUVEGARDE

*Tableau 120. Paramètre **Taille maximale du dossier de sauvegarde***

Paramètre	Taille maximale du dossier de sauvegarde.
Description	Ce paramètre définit la taille maximale de la sauvegarde, à savoir le volume total de données dans le dossier de sauvegarde. Le paramètre **Taille maximale de la sauvegarde** est informatif. Il ne limite pas la taille du dossier de sauvegarde mais permet à l'administrateur de surveiller l'état de la sauvegarde. Une fois que la taille maximale a été atteinte, Kaspersky Anti-Virus continue à placer des copies des objets infectés dans la sauvegarde. Vous pouvez configurer la notification de l'administrateur sur le dépassement de la taille maximale de la sauvegarde. Kaspersky Anti-Virus envoie une notification dès que le volume total des données dans la sauvegarde atteint la valeur indiquée. Pour en savoir plus, lisez la rubrique "Configuration des notifications de l'administrateur et de l'utilisateur" (cf. page 264). La valeur recommandée est égale à 200 Mo.
Valeurs possibles	1 à 999 Mo
Valeur par défaut	Non définie.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la sauvegarde en MMC 218

Configuration de la sauvegarde dans Kaspersky Administration Kit 310

SEUIL D'ESPACE LIBRE DE LA SAUVEGARDE

*Tableau 121. Paramètres **Seuil d'espace libre de la sauvegarde***

Paramètre	Seuil d'espace libre de la sauvegarde
Description	Ce paramètre est utilisé conjointement au paramètre **Taille maximale du dossier**. Ce paramètre est informatif. Il ne limite pas la taille du dossier de sauvegarde mais permet d'obtenir des informations sur la proximité de son remplissage. Si le volume d'espace disponible dans la sauvegarde est inférieur à la valeur du seuil, Kaspersky Anti-Virus enregistre l'événement **Dépassement du seuil d'espace libre** pour la sauvegarde et continue à isoler les objets suspects. Vous pouvez configurer les notifications sur les événements de ce type. Pour en savoir plus, lisez la rubrique "Configuration des notifications de l'administrateur et de l'utilisateur" (cf. page 264).
Valeurs possibles	Indiquez le volume en Mo ; il doit être inférieur à la valeur définie par le paramètre **Taille maximale de la sauvegarde**. La valeur recommandée est égale à 50 Mo.
Valeur par défaut	Non définie.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la sauvegarde en MMC 218

Configuration de la sauvegarde dans Kaspersky Administration Kit 310

DOSSIER POUR LA RESTAURATION : SAUVEGARDE

*Tableau 122. Paramètre **Restaurer dans le dossier***

Paramètre	Restaurer dans le dossier.
Description	Le paramètre définit le répertoire spécial utilisé pour les objets restaurés sur le disque local du serveur protégé. Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où le fichier restauré sera enregistré : dans le répertoire d'origine, dans un dossier spécial pour les objets restaurés sur le serveur protégé ou dans un autre dossier sélectionné (sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou dans un répertoire de réseau). Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via la console installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Pour indiquer le chemin d'accès au répertoire de restauration, vous pouvez utiliser des variables prédéfinies ; vous ne pouvez pas utiliser des variables d'utilisateur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

CF. INSTRUCTION DE LA CONFIGURATION

Configuration des paramètres de la sauvegarde en MMC 218

Configuration de la sauvegarde dans Kaspersky Administration Kit 310

COMPTEURS DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

COMPTEURS DE PERFORMANCES POUR L'APPLICATION SYSTEM MONITOR

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES COMPTEURS DE PERFORMANCES DE KASPERSKY ANTI-VIRUS

Si le composant **Compteurs de performances** est repris dans les composants installés de Kaspersky Anti-Virus, celui-ci enregistre ses compteurs de performance pendant l'installation pour l'application "System Monitor" de Microsoft Windows.

Grâce aux compteurs de Kaspersky Anti-Virus, vous pouvez contrôler les performances de Kaspersky Anti-Virus durant l'exécution des tâches de protection en temps réel. Vous pouvez identifier les goulots d'étranglement en cas d'utilisation avec d'autres applications et les manques de ressources. Vous pouvez diagnostiquer une mauvaise configuration de Kaspersky Anti-Virus et les échecs de fonctionnement.

Pour consulter les compteurs de performances de Kaspersky Anti-Virus, ouvrez la console **Optimisation** dans l'élément **Administration** du panneau de configuration.

Les points suivants abordent la définition des compteurs, les intervalles de calcul des relevés recommandés, les valeurs limites et les recommandations pour la configuration de Kaspersky Anti-Virus lorsque les compteurs dépassent ces valeurs.

TOTAL DE REQUETES REJETEES

Tableau 123. Total de requêtes rejetées

Nom	Total de requêtes rejetées (Number of requests denied)
Description	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de Kaspersky Anti-Virus, le calcul est réalisé depuis la dernière exécution de Kaspersky Anti-Virus. Kaspersky Anti-Virus ignore les objets dont les requêtes de traitement sont rejetées par les processus de travail de Kaspersky Anti-Virus.
Fonction	Ce compteur permet d'identifier : • La réduction de la qualité de la protection en temps réel en raison d'une charge complète des processus de Kaspersky Anti-Virus ; • L'interruption de la protection en temps réel en raison d'un refus du gestionnaire d'intercepteurs de fichiers.
Valeur normale / limite	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés. Les situations suivantes sont envisageables en fonction du "comportement" du compteur : • le compteur indique certains processus rejetés durant une longue période : tous les processus de Kaspersky Anti-Virus étaient totalement occupés, si bien que Kaspersky Anti-Virus n'a pas pu analyser les objets. • Pour éviter que des objets soient ignorés, augmentez le nombre de processus de Kaspersky Anti-Virus pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres Nombre maximum de processus actifs (cf. page 356) et Nombre de processus pour la protection en temps réel (cf. page 357) ; • Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : le gestionnaire d'intercepteurs de fichiers ne fonctionne plus. Kaspersky Anti-Virus n'analyse plus les objets. Relancez Kaspersky Anti-Virus.

TOTAL DE REQUETES IGNOREES

Tableau 124. Total de requêtes ignorées

Nom	Total de requêtes ignorées (Number of requests skipped)
Description	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par les processus du pilote mais qui n'ont pas donné d'événement sur la fin du traitement , le calcul est réalisé depuis la dernière exécution de Kaspersky Anti-Virus. Si la requête de traitement d'un objet reçue par un des processus de travail n'a pas envoyé d'événement sur la fin du traitement, le pilote transmet cette requête à un autre processus et la valeur du compteur **Total des requêtes ignorées** augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a accepté la requête de traitement (ils étaient occupés) ou n'a pas envoyé d'événement sur la fin du traitement, Kaspersky Anti-Virus ignore cet objet et la valeur du compteur **Total des requêtes rejetées** augmente d'une unité.
Fonction	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
Valeur normale / limite	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur diffère de zéro, cela signifie qu'un ou plusieurs flux du gestionnaire d'intercepteurs de fichiers sont gelés. La valeur du compteur correspond au nombre de flux gelés en ce moment. Si la vitesse d'analyse n'est pas satisfaisante, relancez Kaspersky Anti-Virus afin de rétablir les flux gelés.

NOMBRE DE REQUETES NON TRAITEES EN RAISON D'UN MANQUE DE RESSOURCES SYSTEME

Tableau 125. Nombre de requêtes non traitées en raison d'un manque de ressources système

Nom	Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)
Description	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Anti-Virus. Kaspersky Anti-Virus ignore les objets dont les requêtes de traitement ne sont pas traitées par le pilote d'interception de fichiers.
Fonction	Le compteur permet de repérer et de résoudre une éventuelle baisse de la qualité de la protection en temps réel provoquée par un manque de ressources.
Valeur normale / limite	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si le compteur affiche une valeur différente de zéro, les processus de travail de Kaspersky Anti-Virus ont besoin de plus de mémoire vive pour traiter les requêtes. Il se peut que les processus actifs d'autres applications utilisent toute la mémoire vive disponible.

NOMBRE DE REQUETES ENVOYEES POUR TRAITEMENT

Tableau 126. Nombre de requêtes envoyées pour traitement

Nom	Nombre de requêtes envoyées pour traitement (Number of requests sent to be processed)
Description	Nombre d'objets attendant d'être traités par les processus actifs de Kaspersky Anti-Virus en ce moment
Fonction	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Anti-Virus et le niveau général de l'activité de fichiers sur le serveur.
Valeur normale / limite	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur le serveur
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	non

NOMBRE MOYEN DE FLUX DU GESTIONNAIRE D'INTERCEPTEURS DE FICHIERS

Tableau 127. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers (Average number of file interception dispatcher streams).
Description	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (moyenne pour tous les processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une éventuelle détérioration de la qualité de la protection en temps réel en raison de la charge des processus de Kaspersky Anti-Virus et d'y remédier
Valeur normale / limite	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Chaque processus actif peut accepter un maximum de 60 flux du gestionnaire d'intercepteurs de fichiers. Si la valeur du compteur approche de 60, il se peut qu'aucun des processus actifs ne puisse accepter une nouvelle requête de traitement du pilote d'intercepteurs de fichiers et Kaspersky Anti-Virus ignorera l'objet. Augmentez le nombre de processus de Kaspersky Anti-Virus pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres Nombre maximum de processus actifs (cf. page 356) et Nombre de processus pour la protection en temps réel ;

NOMBRE MAXIMUM DE FLUX DU GESTIONNAIRE D'INTERCEPTEURS DE FICHIERS

Tableau 128. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers (Maximum number of file interception dispatcher streams)
Description	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (nombre le plus élevé de processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une réduction des performances en raison d'une répartition inégale de la charge dans les processus actifs exécutés et d'y remédier
Valeur normale / limite	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur de ce compteur dépasse en permanence et de beaucoup la valeur du compte **Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers**, Kaspersky Anti-Virus répartit de manière inégale la charge sur les processus exécutés. Relancez Kaspersky Anti-Virus.

NOMBRE D'OBJETS INFECTES DANS LA FILE DE TRAITEMENT

Tableau 129. Nombre d'objets infectés dans la file de traitement

Nom	Nombre d'objets infectés dans la file de traitement (Number of items in the infecte object queue)
Description	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment.
Fonction	Le compteur permet d'identifier les situations suivantes : • l'interruption de la protection en temps réel en raison d'un éventuel refus du gestionnaire d'intercepteurs de fichiers ; • la surcharge du processus suite à une répartition inégale du temps de processus entre Kaspersky Anti-Virus et les autres applications exécutées ; • les épidémies de virus.
Valeur normale / limite	La valeur du compteur peut être différente de zéro tandis que Kaspersky Anti-Virus traite les objets suspects ou infectés découverts mais elle revient sur zéro peu de temps après la fin du traitement / la valeur du compteur est différente de zéro pendant une longe période
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur n'est pas égale à zéro pendant une longue période : • Kaspersky Anti-Virus ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Relancez Kaspersky Anti-Virus. • Manque de temps de processus pour le traitement des objets ; Accordez à Kaspersky Anti-Virus plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur. • Une épidémie de virus s'est déclenchée. L'émergence d'une épidémie de virus est également indiquée par le nombre élevé d'objets infectés ou suspects découverts dans la tâche **Protection en temps réel des fichiers**. Vous pouvez consulter les informations relatives au nombre d'objets découverts dans les statistiques de la tâche (cf. page 107) ou dans le journal d'exécution de la tâche (cf. rubrique "Consultation des informations relatives à la tâche dans le journal" à la page 234).

NOMBRE D'OBJETS TRAITES PAR SECONDE

Tableau 130. Nombre d'objets traités par seconde

Nom	Nombre d'objets traités par seconde (Number of objects processed per second)
Description	Nombre d'objets traités par unité de temps pendant laquelle ces objets ont été traités ; le décompte s'opère sur des intervalles de temps égaux
Fonction	Ce compteur affiche la vitesse de traitement des objets ; il permet d'identifier une baisse des performances du serveur en raison d'un manque de temps de processus actif pour les processus de Kaspersky Anti-Virus ou d'un échec de Kaspersky Anti-Virus et d'y remédier.
Valeur normale / limite	Varie / non.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Les valeurs du compteur dépendent des paramètres de Kaspersky Anti-Virus et de la charge des processus des autres applications sur le serveur. Observez le niveau moyen du compteur au cours d'une longue période. Si le niveau du compteur a diminué, c'est peut-être à cause d'une des situations suivantes : • Les processus de travail de Kaspersky Anti-Virus ne disposent pas des ressources de processus suffisantes pour traiter les objets ; Accordez à Kaspersky Anti-Virus plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur. • Un échec s'est produit dans le fonctionnement de Kaspersky Anti-Virus (plusieurs flux sont gelés). Relancez Kaspersky Anti-Virus.

COMPTEURS ET INTERRUPTIONS SNMP DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

PRESENTATION DES COMPTEURS ET PIEGES SNMP DE KASPERSKY ANTI-VIRUS

Si vous avez inclus le composant **Compteurs et pièges SNMP** dans les composants de Kaspersky Anti-Virus à installer, vous pouvez consulter les compteurs et les pièges de Kaspersky Anti-Virus selon les protocoles Simple Network Management Protocol (SNMP) et HP Open View.

Pour consulter les compteurs et les pièges de Kaspersky Anti-Virus depuis l'ordinateur-poste de travail de l'administrateur, lancez sur le serveur protégé le service SNMP (SNMP Service) et le service de pièges SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

COMPTEURS SNMP DE KASPERSKY ANTI-VIRUS

DANS CETTE SECTION DE L'AIDE

COMPTEURS DE PERFORMANCES

Tableau 131. Compteurs de performances

COMPTEUR	DESCRIPTION
currentRequestsAmount	Nombre de requêtes envoyées pour traitement (cf. page 415)
currentInfectedQueueLength	Nombre d'objets infectés dans la file d'attente de traitement (cf. page 417)
currentObjectProcessingRate	Nombre d'objets traités par seconde (cf. page 418)
currentWorkProcessesAmount	Nombre de processus de travail de Kaspersky Anti-Virus en ce moment

COMPTEURS GENERAUX

Tableau 132. Compteurs généraux

COMPTEUR	DESCRIPTION
currentApplicationUptime	Durée de fonctionnement de Kaspersky Anti-Virus depuis sa dernière exécution (en centièmes de secondes)
currentFileMonitorTaskStatus	**Etat de la tâche Protection en temps réel des fichiers : On – en exécution; Off – arrêtée ou suspendue**
currentScriptCheckerTaskStatus	**Etat de la tâche Analyse des scripts : On – en exécution; Off – arrêtée ou suspendue**
lastCriticalAreasScanAge	"Age" de la dernière analyse des zones critiques du serveur (intervalle de temps en secondes entre la date de fin de la tâche portant le statut "Tâche d'analyse des zones critiques" et le moment actuel)
licenseExpirationDate	Date de fin de validité de la licence(Si une licence et une licence de réserve sont installées, cette donnée indique la fin de validité de synthèse des licences active et de synthèse)

COMPTEUR DE MISE A JOUR

Tableau 133. Compteur de mises à jour

COMPTEUR	DESCRIPTION
avBasesAge	"Age" des bases (intervalle de temps en centièmes de seconde entre la date de création des dernières mises à jour installées et l'heure actuelle).

COMPTEURS DE PROTECTION EN TEMPS REEL

Tableau 134. Compteurs de protection en temps réel

COMPTEUR	DESCRIPTION
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalInfectedObjectsFound	Nombre d'objets infectés découverts depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalSuspiciousObjectsFound	Nombre d'objets infectés découverts depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalVirusesFound	Nombre d'objets infectés découverts depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsQuarantined	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotQuarantined	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsDisinfected	Nombre total d'objets infectés réparés par Kaspersky Anti-Virus ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotDisinfected	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de réparer en vain ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsDeleted	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotDeleted	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsBackedUp	Nombre total d'objets infectés réparés par Kaspersky Anti-Virus ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotBackedUp	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de réparer en vain ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**

COMPTEURS DE QUARANTAINE

Tableau 135. Compteurs de quarantaine

COMPTEUR	DESCRIPTION
totalObjects	Nombre d'objets présents actuellement en quarantaine
totalSuspiciousObjects	Nombre d'objets suspects présents actuellement en quarantaine
currentStorageSize	Volume de données en quarantaine (Mo)

COMPTEURS DE SAUVEGARDE

Tableau 136. Compteurs de sauvegarde

COMPTEUR	DESCRIPTION
currentBackupStorageSize	Volume de données en sauvegarde (Mo)

COMPTEURS D'ANALYSE DES SCRIPTS

Tableau 137. Compteurs d'analyse des scripts

COMPTEUR	DESCRIPTION
totalScriptsProcessed	Total de scripts analysés
totalInfectedIDangerousScriptsFound	Total des scripts infectés découverts
totalSuspiciousScriptsFound	Total des scripts suspects découverts
totalScriptsBlocked	Total des scripts dont l'accès a été bloqué

PIEGES SNMP

Les paramètres des pièges SNMP de Kaspersky Anti-Virus sont décrits dans le tableau ci-dessous.

Tableau 138. Pièges SNMP de Kaspersky Anti-Virus

PIEGE	DESCRIPTION	PARAMETRES
eventThreatDetected	Menace détectée.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Dépassement de la taille maximale de la sauvegarde. Le volume total de données de la sauvegarde dépasse la valeur du paramètre **Taille max. du dossier de sauvegarde**. Kaspersky Anti-Virus continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Le seuil d'espace libre pour la sauvegarde est atteint. La quantité d'espace libre dans la sauvegarde, définie par le paramètre **Seuil d'espace libre de la sauvegarde**, est revenue à la valeur indiquée. Kaspersky Anti-Virus continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Dépassement de la taille maximale de la quarantaine. Le volume total de données de la quarantaine dépasse la valeur du paramètre **Taille maximale de la quarantaine**. Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Le seuil d'espace libre pour la quarantaine est atteint. La quantité d'espace libre dans la quarantaine, définie par le paramètre Seuil d'espace libre de la quarantaine, est revenue à la valeur indiquée. Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine.	eventDateAndTime eventSeverity eventSource

PIEGE	DESCRIPTION	PARAMETRES
eventObjectNotQuarantined	Erreur de placement de l'objet en quarantaine	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Erreur de conservation d'une copie de l'objet en sauvegarde	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Une erreur de quarantaine s'est produite	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Une erreur de sauvegarde s'est produite	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Les bases de donnée ne sont plus à jour. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Les bases de données sont périmées. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Anti-Virus est lancé.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Anti-Virus est arrêté.	eventSeverity eventDateAndTime eventSource

PIEGE	DESCRIPTION	PARAMETRES
eventCriticalAreasScanWasntPerformForALongTime	L'analyse des zones critiques n'a pas été réalisée depuis longtemps. Le nombre de jours écoulés depuis la dernière tâche dont le statut est "Tâche d'analyse complète de l'ordinateur" est compté	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	La durée de validité de la clé est écoulée.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	La clé de licence arrive bientôt à échéance. Le nombre de jour restant avant la fin de la validité de la licence est compté	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Erreur d'exécution de la tâche	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Erreur d'exécution de la tâche de mise à jour	eventSeverity eventDateAndTime taskName updaterErrorEventReason

Le tableau suivant décrit les paramètres des pièges et leurs valeurs possibles.

Tableau 139. Valeurs des paramètres des pièges SNMP

PARAMETRE	DESCRIPTION ET VALEURS POSSIBLES
eventDateAndTime	Heure à laquelle l'événement est survenu
eventSeverity	Degré d'importance de l'événement. Le paramètre peut prendre les valeurs suivantes : • critical (1) – critique, • warning (2) – avertissement, • info (3) – informations.
UserName	Nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté)
computerName	Nom de l'ordinateur (par exemple, nom de l'ordinateur dont l'utilisateur a tenté d'accéder à un fichier infecté)
eventSource	Source de l'événement : composant fonctionnel pendant le fonctionnement duquel l'événement s'est produit. Le paramètre peut prendre les valeurs suivantes : • unknown (0) – composant fonctionnel non identifié ; • quarantine (1) – Quarantaine ; • backup (2) – Sauvegarde ; • reporting (3) – Journaux d'exécution des tâches ; • updates (4) – Mise à jour ; • realTimeProtection (5) –Protection en temps réel ; • onDemandScanning (6) – Analyse à la demande ; • product (7) – événement lié non pas au fonctionnement d'un composant particulier mais au fonctionnement de Kaspersky Anti-Virus dans son ensemble ; • systemAudit (8) – Journal d'audit système.
eventReason	Cause de l'événement. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown (0) – cause indéterminée, • reasonInvalidSettings (1) – uniquement pour les événements de la sauvegarde et de la quarantaine, s'affiche si le dossier de sauvegarde ou de quarantaine est inaccessible (privilèges d'accès insuffisants ou le chemin de réseau indiqué dans les paramètres de la quarantaine est incorrect). Dans ce cas, Kaspersky Anti-Virus utilisera le dossier de sauvegarde ou de quarantaine indiqué par défaut.
objectName	Nom de l'objet (par exemple, nom du fichier contenant la menace)
threatName	Nom de menace

PARAMETRE	DESCRIPTION ET VALEURS POSSIBLES
detectType	Type de menace. Le paramètre peut prendre les valeurs suivantes : • undefined (0) – indéterminée ; • virware – virus et vers de réseau traditionnels ; • trojware – chevaux de Troie ; • malware – autres programmes malveillants ; • adware – logiciels publicitaires ; • pornware – programmes au contenu pornographique ; • riskware – applications présentant un risque potentiel.
detectCertainty	Coefficient de certitude de la découverte d'une menace. Le paramètre peut prendre les valeurs suivantes : • Suspicion (suspect) : l'objet est considéré comme étant suspect : il existe une équivalence partielle entre une partie du code de l'objet et une partie du code d'une menace connue ; • Sure (infecté) : l'objet est infecté : il existe une équivalence parfaite entre une partie du code de l'objet et une partie du code d'une menace connue.
days	Nombre de jours (par exemple, nombre de jours d'ici la fin de la validité de la licence)
errorCode	Code erreur
knowledgeBaseId	Adresse de l'article dans la banque de solutions (par exemple, adresse de l'article décrivant une erreur quelconque)
taskName	Nom de la tâche

PARAMETRE	DESCRIPTION ET VALEURS POSSIBLES
updaterErrorEventReason	Cause de la non-application de la mise à jour. Le paramètre accepte les valeurs suivantes. Cause de la non-application de la mise à jour. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown(0) – raison inconnue ; • reasonAccessDenied – accès interdit ; • reasonUrlsExhausted – fin de la liste des sources de mise à jour ; • reasonInvalidConfig – fichier de configuration incorrect ; • reasonInvalidSignature – signature invalide ; • reasonCantCreateFolder – création du répertoire impossible ; • reasonFileOperError – erreur de fichier ; • reasonDataCorrupted – objet corrompu ; • reasonConnectionReset – arrêt de la connexion ; • reasonTimeOut – délai d'attente pour la connexion expiré ; • reasonProxyAuthError – erreur de vérification de l'authenticité sur le serveur proxy ; • reasonServerAuthError – erreur de vérification de l'authenticité sur le serveur ; • reasonHostNotFound – ordinateur introuvable ; • reasonServerBusy – serveur inaccessible ; • reasonConnectionError – erreur de connexion ; • reasonModuleNotFound – objet introuvable ; • reasonBlstCheckFailed(16) – erreur de vérification de la liste des licences rappelées. Il se peut qu'une actualisation ait été diffusée au moment de la mise à jour des bases. Essayez à nouveau de réaliser la mise à jour dans quelques minutes. Consultez la description de ces causes et les actions que l'administrateur du site peut entreprendre sur le site de service d'assistance technique (http://support.kaspersky.com/fr/error).

PARAMETRE	DESCRIPTION ET VALEURS POSSIBLES
storageObjectNotAddedEventReason	Cause du non placement de l'objet en sauvegarde ou en quarantaine. Le paramètre peut prendre les valeurs suivantes : • reasonUnknown(0) – raison inconnue. • reasonStorageInternalError – erreur dans les bases de données ; restaurez Kaspersky Anti-Virus. • reasonStorageReadOnly – la base de données est uniquement accessible en lecture ; restaurez Kaspersky Anti-Virus. • reasonStorageIOError – erreur d'entrée/de sortie : a) Kaspersky Anti-Virus est corrompu, restaurez-le ; b) le disque sur lequel les fichiers de Kaspersky Anti-Virus sont sauvegardés est abîmé. • reasonStorageCorrupted – le référentiel est abîmé ; restaurez Kaspersky Anti-Virus. • reasonStorageFull – la base de données est remplie ; faites de la place sur le disque. • reasonStorageOpenError – échec de l'ouverture du fichier de base de données ; restaurez Kaspersky Anti-Virus. • reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigences de Kaspersky Anti-Virus. • reasonObjectNotFound – l'objet placé dans le référenciel n'existe pas sur le disque. • reasonObjectAccessError – privilèges insuffisants pour l'utilisation de Backup API : le compte utilisateur sous les privilèges duquel l'opération est réalisée ne jouit pas des privilèges Backup Operator. • reasonDiskOutOfSpace – espace insuffisant sur le disque. Les paramètres des pièges SNMP de Kaspersky Anti-Virus sont décrits dans le tableau ci-dessous.

UTILISATION DU CODE ETRANGER

Cette rubrique présente les informations relatives aux éditeurs tiers qui ont développés des codes logiciels qui ont été utilisés dans le développement de Kaspersky Anti-Virus.

DANS CETTE SECTION DE L'AIDE

CODE DE PROGRAMME

Lors de l'élaboration de Kaspersky Anti-Virus, le code de programme de sociétés tierces a été utilisé.

DANS CETTE SECTION DE L'AIDE

BOOST 1.33

CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

Disclaimer This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt. Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

DRIVER INSTALLATION TOOLS (DIFX) 2.1.1 (FILE DIFXAPP.WIXLIB)

Copyright (C) Microsoft Corporation.

GSOAP 2.7.0D

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

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Copyright (C) 1991-1992, L. Peter Deutsch, RSA Data Security, Inc.

RSA's MD5 disclaimer Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

LZMA SDK 4.40

Copyright (C) 1999-2010 Igor Pavlov.

MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Copyright (C) Colin Plumb.

MICROSOFT ACTIVE TEMPLATE LIBRARY 8.0

Copyright (C) 2009 Microsoft Corporation.

MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT 2.0

Copyright (C) Microsoft Corporation.

MICROSOFT DEBUGGING TOOLS FOR WINDOWS 6.12.2.633 (FILE DBGHELP.DLL)

Scope of License. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not publish the software for others to copy.

MICROSOFT DRIVER DEVELOPMENT KIT 6000 SOURCE CODE

Copyright (C) Microsoft Corporation.

MICROSOFT EXCHANGE SERVER 2003 SDK

Copyright (C) Microsoft Corporation.

MICROSOFT INTERNET CLIENT SDK 4.0

Copyright (C) 1997, Microsoft Corporation.

MICROSOFT VISUAL STUDIO 6.0 (COMMON RUNTIME SOURCES AND TOOLS)

Copyright (C) Microsoft Corporation.

MICROSOFT WINDOWS SERVER 2003 SP1 SDK

Copyright (C) Microsoft Corporation.

MICROSOFT WINDOWS SOFTWARE DEVELOPMENT KIT 6.0

Copyright (C) Microsoft Corporation.

SHA-1-1.2

Copyright (C) 2001, The Internet Society.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process

must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

SQLITE 3.7.2 (DBLITE.DLL)

STDSTRING 27.04.2001

Copyright (C) 2002, Joseph M. O'Leary.

WIX 2.0

Copyright (c) 2009 Microsoft Corporation.

WINDOWS TEMPLATE LIBRARY (WTL) 7.5

Copyright (C) 2005 Microsoft Corporation.

Microsoft Permissive License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction" and "distribution" have the same meaning here as under U.S. copyright law.

"You" means the licensee of the software.

"Licensed patents" means any Microsoft patent claims which read directly on the software as distributed by Microsoft under this license.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce the software, prepare derivative works of the software and distribute the software or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free patent license under licensed patents to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the software or derivative works of the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you any rights to use Microsoft's name, logo, or trademarks.

(B) If you begin patent litigation against Microsoft over patents that you think may apply to the software (including a cross-claim or counterclaim in a lawsuit), your license to the software ends automatically.

(C) If you distribute copies of the software or derivative works, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute the software or derivative works in source code form you may do so only under this license (i.e., you must include a complete copy of this license with your distribution), and if you distribute the software or derivative works in compiled or object code form you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

ZLIB 1.0.8, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler.

AUTRES INFORMATIONS

La composition et l'analyse de l'analyse numérique électronique repose sur la bibliothèque logicielle de protection de l'information (PBZI) "Crypto-Si" développée par OOO "CryptoEx".

DANS CETTE SECTION DE L'AIDE

NSIS 2.46

Copyright (C) 1995-2009, Contributors

APPLICABLE LICENSES

All NSIS source code, plug-ins, documentation, examples, header files and graphics, with the exception of the compression modules and where otherwise noted, are licensed under the zlib/libpng license.

The zlib compression module for NSIS is licensed under the zlib/libpng license.

The bzip2 compression module for NSIS is licensed under the bzip2 license.

The LZMA compression module for NSIS is licensed under the Common Public License version 1.0.

ZLIB/LIBPNG LICENSE

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BZIP2 LICENSE

This program, "bzip2" and associated library "libbzip2", are copyright (C) 1996-2000 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

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

Julian Seward, Cambridge, UK.

jseward@acm.org

COMMON PUBLIC LICENSE VERSION 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the

Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

SPECIAL EXCEPTION FOR LZMA COMPRESSION MODULE

Igor Pavlov and Amir Szekely, the authors of the LZMA compression module for NSIS, expressly permit you to statically or dynamically link your code (or bind by name) to the files from the LZMA compression module for NSIS without subjecting your linked code to the terms of the Common Public license version 1.0. Any modifications or additions to files from the LZMA compression module for NSIS, however, are subject to the terms of the Common Public License version 1.0.

KASPERSKY LAB ZAO

Kaspersky Lab a été fondé en 1997. Il s'agit à l'heure actuelle de l'éditeur russe de logiciels de sécurité polyvalents le plus connu : protection contre les virus, le courrier indésirable et les hackers.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Produit phare de la société, Kaspersky Anti-Virus offre une protection efficace pour tous les éléments qui pourraient être la cible d'un virus : postes de travail, serveurs de fichiers, systèmes de messagerie, pare-feu, passerelles Internet et ordinateurs de poches. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en oeuvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab Ltd. Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Site de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)

INDEX

A

B

C

D

E

I

J

K

L

M

N

P

Q

R

S

T

V

Z