# Kaspersky Anti-Virus 8.0 for Lotus Domino


## Guide de l'administrateur

APPLICATION VERSION: 8.0 MAINTENANCE PACK 2

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 de vos questions.



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



Date d'édition : 18/04/2014



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

# TABLE DES MATIERES

# PRESENTATION DU MANUEL

Ce document représente le Manuel de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus® Domino® (ci-après Kaspersky Anti-Virus).

Ce Manuel est un outil dédié aux spécialistes techniques qui doivent installer et administrer Kaspersky Anti-Virus, ainsi qu'assurer le support pour les entreprises qui utilisent Kaspersky Anti-Virus.

Le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino détaille l'installation de Kaspersky Anti-Virus.

Ce guide est conçu dans les buts suivants :

- Aider à configurer et à utiliser Kaspersky Anti-Virus.
- Offrir un accès rapide aux informations pour répondre aux questions liées à Kaspersky Anti-Virus.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes d'obtention du support technique.

### DANS CETTE SECTION



# DANS CE DOCUMENT

Le Manuel de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino comporte les sections suivantes :

### Sources d'informations sur l'application (cf. page 10)

Cette section décrit les sources d'informations sur l'application.

### Kaspersky Anti-Virus 8.0 for Lotus Domino (cf. page 12)

Cette section détaille les fonctions principales de Kaspersky Anti-Virus 8.0 for Lotus Domino et la différence entre Kaspersky Anti-Virus 8.0 for Lotus Domino et ses versions précédentes. Cette section répertorie les spécifications matérielles et logicielles minimales pour l'ordinateur : elles sont en effet indispensables à l'installation et au bon fonctionnement de Kaspersky Anti-Virus, et à l'obtention d'informations sur la distribution et sur les services proposés aux utilisateurs enregistrés de l'application.

### Architecture de l'application (cf. page 17)

Cette section présente le modèle et l'algorithme de fonctionnement de l'application et fournit également des informations sur l'administration des paramètres de Kaspersky Anti-Virus.

### Administration des privilèges des utilisateurs (cf. page 25)

Cette section détaille les modalités d'administration des privilèges utilisateur.

### Licence de l'application (cf. page 29)

Cette section décrit la mise sous licence et l'activation de l'application, ainsi que l'installation et la suppression des fichiers clés de Kaspersky Anti-Virus.

### Interface de l'application (cf. page 33)

Cette section décrit les principaux éléments de l'interface graphique de l'application dans le cadre de l'utilisation via le client Lotus Notes et le navigateur Internet.

### Lancement et arrêt de l'application (cf. page 40)

Cette section explique comment lancer et arrêter l'application sur le serveur, et décrit la procédure de connexion au serveur pour en configurer les paramètres.

### Etat de la protection du serveur (cf. page 41)

Cette section explique comment définir l'état de la protection du serveur et comment activer ou désactiver chaque composant de la protection antivirus.

### Protection par défaut du serveur (cf. page 42)

Cette section décrit le mode de fonctionnement de Kaspersky Anti-Virus en cas d'utilisation des valeurs par défaut des paramètres.

### Mise à jour des bases (cf. page 44)

Cette section explique comment configurer les paramètres de la mise à jour des bases antivirus, aussi bien pour un serveur que pour un groupe de serveurs. Elle détaille également les sources de mise à jour qui peuvent être utilisées et le lancement de la mise à jour des bases antivirus ; manuellement et selon une programmation. Cette section offre également des informations sur le modèle de mise à jour de Kaspersky Anti-Virus dans le contexte d'une installation sur un ou plusieurs serveurs.

### Protection du courrier (cf. page 50)

Cette section explique comment activer ou désactiver la protection de la messagerie pour le serveur Lotus Domino, comment sélectionner les objets des messages à analyser, comment configurer le filtrage des pièces jointes et comment configurer le traitement des objets des messages en fonction des résultats de l'analyse.

### Protection des réplications (cf. page 56)

Cette section explique comment activer ou désactiver la protection des réplications, comment choisir les objets des réplications à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des réplications en fonction des résultats de l'analyse.

### Analyse des bases de données (cf. page 61)

Cette section explique comment activer ou désactiver l'analyse des bases de données, comment sélectionner les objets de la base de données à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des bases de données en fonction des résultats de l'analyse et comment configurer les paramètres de l'analyse.

### Configuration des paramètres de performances (cf. page 69)

Cette section décrit les paramètres qui définissent les performances de l'application et comment les configurer.

**Index**

Cette section vous permet de rechercher rapidement les informations contenues dans le présent document.

# CONVENTIONS

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

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

*Tableau 1. Conventions*

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| N'oubliez pas que... | Les avertissements apparaissent en rouge et sont encadrés.<br>Les avertissements contiennent des informations sur les actions indésirables qui peuvent amener à la perte d'informations ou à des échecs dans le fonctionnement du matériel ou du système d'exploitation. |
| Il est conseillé d'utiliser... | Les remarques sont encadrées.<br>Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes de paramètres ou des cas particuliers importants dans le fonctionnement de l'application. |
| **Exemple :**<br>... | Les exemples sont présentés sur un fond jaune sous le titre "Exemple". |
| La *Mise à jour* est...<br>L'événement *Bases dépassées* survient. | Les éléments de sens suivants sont en italique :<br>• nouveaux termes ;<br>• noms des états et des événements de l'application. |
| Appuyez sur la touche **ENTER**.<br>Appuyez sur la combinaison des touches **ALT**+F4. | Les noms des touches du clavier sont en caractères gras et en lettres majuscules.<br>Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il est nécessaire d'appuyer simultanément sur ces touches. |
| Cliquez sur le bouton **ACTIVER**. | Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras. |
| *Pour planifier une tâche, procédez comme suit :* | Les phrases d'introduction des instructions sont en italique et présentent l'icône "flèche". |
| Dans la ligne de commande, saisissez le texte `help`<br>Les informations suivantes s'affichent :<br>`Indiquez la date au format JJ:MM:AA.` | Les types suivants du texte apparaissent dans un style spécial :<br>• texte de la ligne de commande ;<br>• texte des messages affichés à l'écran par l'application ;<br>• données à saisir par l'utilisateur. |
| <Nom d'utilisateur> | Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les chevrons sont omis. |

# SOURCES D'INFORMATIONS SUR L'APPLICATION

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

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

### DANS CETTE SECTION



## SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez vous servir des sources suivantes pour rechercher vous-même des informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du Service de Support Technique (banque de solutions) ;
- aide électronique ;
- documentation.

Si vous n'avez pas trouvé la solution à votre problème, nous vous conseillons de contacter le Support Technique de Kaspersky Lab (cf. section "Support Technique par téléphone" à la page 98).

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

### Page du site de Kaspersky Lab

Le site Internet de Kaspersky Lab propose une page dédiée à chaque application.

La page (http://www.kaspersky.com/fr/business-security/lotus-notes-domino-antivirus) fournit des informations générales sur l'application, ses possibilités et ses particularités.

La page http://www.kaspersky.com/fr contient un lien vers la boutique en ligne. Ce lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

### Page sur le site Internet du Service de support technique (base de connaissances)

La Base de connaissances est une section du site Internet du Service de Support Technique contenant des recommandations relatives à l'utilisation des applications de " Kaspersky Lab ". La Base de connaissances est composée d'articles d'aide regroupés par thèmes.

La page de l'application dans la Base des connaissances (http://support.kaspersky.fr/domino8) permet de trouver les articles qui proposent des informations utiles, des recommandations et une foire aux questions sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions concernant non seulement Kaspersky Anti-Virus, mais également d'autres applications de Kaspersky Lab, ainsi que les actualités du Service de Support technique.

### Aide électronique

L'aide électronique reprend des informations sur l'administration de la protection du serveur : comment consulter les informations sur l'état de la protection, comment configurer les paramètres de la protection, comment activer et désactiver les composants de la protection, comment lancer manuellement l'analyse des bases de données du serveur et la mise à jour des bases antivirus.

Pour ouvrir l'aide électronique, choisissez l'onglet **Aide** dans la fenêtre de la base de données Centre d'administration.

### Documentation

La distribution de l'application contient des documents qui vous aideront à installer et à activer l'application sur les postes du réseau de l'entreprise, à configurer ses paramètres de fonctionnement et à obtenir des informations sur les principaux modes d'utilisation de l'application.

- Le **Manuel de mise en œuvre** permet à l'administrateur de planifier le déploiement de l'application sur le réseau. Il contient des recommandations pratiques sur l'installation et la préparation de l'application en vue de son utilisation, et explique comment supprimer l'application d'un serveur ou de tous les serveurs protégés du réseau.

- Le **Manuel de l'administrateur** comporte des informations sur l'utilisation de l'application et sur la configuration de ses paramètres. Il décrit également comment administrer la protection d'un serveur ou d'un groupe de serveurs via le client Lotus Notes®, l'interface Internet de l'application et la console de serveur Lotus Domino.

## CONTACTER LE SERVICE COMMERCIAL

Si vous souhaitez poser des questions sur la sélection, sur l'achat ou sur le renouvellement de la licence, vous pouvez contacter nos experts du Service commercial par l'un des moyens suivants :

- En contactant notre siège social à Moscou (http://www.kaspersky.fr/contacts).

- En envoyant un message avec votre question à l'adresse électronique sales@kaspersky.com.

Ce service est offert en russe et en anglais.

## CONTACTER LE SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Pour contacter le Groupe de rédaction de la documentation, il est nécessaire d'envoyer un message par courrier électronique. L'objet du message doit indiquer "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Lotus Domino".

# KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO

Kaspersky Anti-Virus 8.0 for Lotus Domino a été développé pour garantir une protection antivirus totale des serveurs Lotus Domino. L'application assure la protection du trafic de messagerie et des réplications, et analyse les bases de données conservées sur le serveur protégé.

Kaspersky Anti-Virus doit être installé sur des serveurs fonctionnant sous des systèmes d'exploitation de la gamme Microsoft® Windows® ou Linux®. L'application remplit les fonctions suivantes :

- Analyse de tous les messages arrivant sur le serveur Lotus Domino du trafic entrant, sortant ou en transit. Les objets suivants sont analysés à la recherche de menaces :
  - les textes des messages ;
  - les fichiers joints aux messages ;
  - les objets OLE mis en œuvre dans les messages.

  Kaspersky Anti-Virus détecte les objets malveillants dans les archives jointes ainsi que dans les fichiers .exe compactés, à l'exception des archives protégées par un mot de passe.
- Analyse des documents placés sur le serveur protégé et modifiés suite à une réplication. Les réplications sortantes ne sont pas analysées. Les objets suivants sont analysés à la recherche de menaces :
  - le contenu des champs au format Rich Text ;
  - le contenu des champs au format MIME ;
  - les fichiers joints aux documents ;
  - les objets OLE mis en œuvre dans le document.
- Analyse programmée ou à la demande des bases de données du serveur Lotus Domino protégé. Les objets suivants sont analysés à la recherche de menaces :
  - le contenu des champs au format Rich Text ;
  - le contenu des champs au format MIME ;
  - les fichiers joints aux documents ;
  - les objets OLE mis en œuvre dans le document.
- Filtrage des objets selon la taille ou le masque de nom lors de l'analyse des messages électroniques, des réplications et des bases de données. Les objets filtrés sont soumis aux règles de traitement définies par l'administrateur.
- Traitement des objets infectés, potentiellement infectés, protégés et non analysés découverts lors de l'analyse des messages électroniques, des documents répliqués et des documents des bases de données. En fonction des valeurs des paramètres de la protection/de l'analyse, Kaspersky Anti-Virus répare, supprime ou ignore l'objet, avertit l'administrateur de la découverte d'une menace et des résultats du traitement de l'objet, et conserve les données statistiques.
- Notification des expéditeurs, des destinataires et des administrateurs sur les objets infectés, potentiellement infectés, protégés et non analysés découverts dans les messages, ainsi que sur les actions auxquelles ils sont soumis.

- Notification des administrateurs sur les objets dangereux découverts lors de l'analyse des documents répliqués et des documents des bases de données, ainsi que sur les actions auxquelles ils sont soumis.
- Enregistrement des objets analysés dans la base de données Quarantaine. Cette action permet de classer par type (messagerie / réplication / analyse des bases de données) les messages et les documents enregistrés qui ont été découverts lors de l'analyse des réplications, ainsi que les documents découverts lors de l'analyse des bases de données.
- Enregistrement des informations sur les objets infectés, potentiellement infectés, protégés et non analysés, ainsi que sur les actions auxquelles ils sont soumis. Ces informations sont enregistrées dans la base de données Journal des événements et statistiques, et s'affichent dans la console du serveur Lotus Domino. Elles peuvent également être enregistrées dans un fichier texte (option désactivée par défaut).
- Mise à jour des bases antivirus via Internet, en mode automatique ou manuel. Les sources de mise à jour des bases peuvent être les serveurs HTTP ou FTP de mise à jour de Kaspersky Lab sur Internet, des serveurs HTTP ou FTP contenant l'ensemble des mises à jour ou des répertoires de réseau.
- Administration des paramètres de fonctionnement de Kaspersky Anti-Virus installé sur plusieurs serveurs grâce aux profils.
- Restriction de l'accès à la configuration des paramètres et à l'administration de Kaspersky Anti-Virus au niveau des serveurs et au niveau des profils.
- Administration du fonctionnement de Kaspersky Anti-Virus via le client Lotus Notes, la console du serveur Lotus Domino et le navigateur.
- Installation et suppression de l'application via le client Lotus Notes ou via le navigateur Internet.

### DANS CETTE SECTION



# NOUVEAUTES

Kaspersky Anti-Virus 8.0 for Lotus Domino prend en charge les plateformes Lotus Domino 9.0 et Lotus Domino 9.01.

# DISTRIBUTION

Vous pouvez acheter l'application de l'une des manières suivantes :

- Dans une boîte. Le produit est distribué via notre réseau de partenaires.
- Via la boutique en ligne. L'application peut être achetée dans la boutique en ligne de Kaspersky Lab (par exemple http://www.kaspersky.com/fr, section Boutique en ligne) ou du site d'un partenaire.

Si vous achetez le produit en boîte, vous recevez les éléments suivants :

- pochette cachetée contenant le cédérom d'installation où sont enregistrés les fichiers de l'application et la documentation de l'application ;
- manuel résumé de l'utilisateur contenant le code d'activation de l'application ;
- contrat de licence reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction du pays où l'application est diffusée.

Si vous achetez Kaspersky Anti-Virus via la boutique en ligne, vous devrez télécharger l'application depuis le site Internet. Les informations indispensables à l'activation de l'application, dont le code d'activation, sont envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre Service Commercial à l'adresse sales@kaspersky.com.

# CONFIGURATIONS LOGICIELLE ET MATERIELLE

Pour le bon fonctionnement de Kaspersky Anti-Virus, l'ordinateur doit se conformer à des spécifications matérielles et logicielles minimales.

### Configurations matérielles :

- Intel® Pentium® 32 bits ou 64 bits ou suivant (ou équivalent).
- 512 Mo de mémoire vive (1 Go ou plus recommandé).
- 1 Go disponible sur le disque dur (3 Go ou plus recommandés).
- Taille recommandée du fichier de spool : double du volume global de mémoire physique.

### Configurations logicielles :

### Systèmes d'exploitation compatibles :

Plateformes 32 bits :

- Microsoft Windows Server® 2003 Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2003 Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows 2003 R2 Server Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows 2003 R2 Server Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2008 Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2008 Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2012 Standard Edition.
- Microsoft Windows Server 2012 Datacenter Edition.
- Microsoft Windows Server 2012 R2 Standard Edition.
- Microsoft Windows Server 2012 R2 Datacenter Edition.
- Novell® SuSE Linux Enterprise Server 10 (Service Pack 2).
- Novell SuSE Linux Enterprise Server 11.
- Red Hat® Enterprise Linux® 5.5.

- Red Hat Enterprise Linux 5.6.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 6.1.

Plateformes 64 bits :

- Microsoft Windows 2003 Server Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows 2003 Server Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows 2003 R2 Server Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows 2003 R2 Server Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2008 Standard Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2008 Enterprise Edition (Service Pack 2 et suivant).
- Microsoft Windows Server 2008 R2 Standard Edition (Service Pack 1 et suivant).
- Microsoft Windows Server 2008 R2 Enterprise Edition (Service Pack 1 et suivant).
- Microsoft Windows Server 2012 Standard Edition.
- Microsoft Windows Server 2012 Datacenter Edition.
- Microsoft Windows Server 2012 R2 Standard Edition.
- Microsoft Windows Server 2012 R2 Datacenter Edition.
- Novell SuSE Linux Enterprise Server 10 (Service Pack 2).
- Novell SuSE Linux Enterprise Server 11.
- Novell SuSE Linux Enterprise Server 11 (Service Pack 3).
- Red Hat Enterprise Linux 5.5.
- Red Hat Enterprise Linux 5.6.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 6.1.
- Red Hat Enterprise Linux 6.5.

**Versions prises en charge de serveurs Lotus :**

Plateformes 32 bits (pour les systèmes d'exploitation Linux et Windows) :

- Lotus Notes/Domino version 8.0.2 (et les mises à jour Fix Pack 6).
- Lotus Notes/Domino version 8.5.0 (et les mises à jour Fix Pack 1).
- Lotus Notes/Domino version 8.5.1 (et les mises à jour Fix Pack 5).
- Lotus Notes/Domino version 8.5.2 (et les mises à jour Fix Pack 4).

- Lotus Notes/Domino version 8.5.3 (et les mises à jour Fix Pack 6).
- Lotus Notes/Domino version 9.0.
- Lotus Notes/Domino version 9.01.

Plateformes 64 bits (uniquement pour les systèmes d'exploitation Windows) :

- Lotus Notes/Domino version 8.0.2 (et les mises à jour Fix Pack 6).
- Lotus Notes/Domino version 8.5.0 (et les mises à jour Fix Pack 1).
- Lotus Notes/Domino version 8.5.1 (et les mises à jour Fix Pack 5).
- Lotus Notes/Domino version 8.5.2 (et les mises à jour Fix Pack 4).
- Lotus Notes/Domino version 8.5.3 (et les mises à jour Fix Pack 6).
- Lotus Notes/Domino version 9.0.
- Lotus Notes/Domino version 9.01.

**Navigateurs compatibles :**

- Internet Explorer® 7.
- Internet Explorer 9.
- Mozilla™ Firefox™ 3X.
- Google Chrome™ 3X.

# ARCHITECTURE DE L'APPLICATION

Cette section décrit le modèle et l'algorithme de fonctionnement de l'application et fournit également des informations sur l'administration des paramètres de Kaspersky Anti-Virus.

### DANS CETTE SECTION



# PRESENTATION DES MODULES FONCTIONNELS DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus comprend trois modules fonctionnels : module d'administration, module d'analyse de la messagerie et des réplications et module d'analyse des bases de données.

### Module d'administration

Ce module permet à Kaspersky Anti-Virus de remplir les fonctions suivantes :

- Administration du logiciel. Ce module initialise l'analyse du courrier et des réplications, et lance l'analyse des bases de données et la mise jour programmée des bases antivirus.
- Administration des paramètres de fonctionnement de l'application. Ce module reçoit et applique les nouvelles valeurs de paramètres.
- Enregistrement et analyse des informations statistiques. Ce module consigne les données statistiques et les informations relatives aux événements survenus pendant l'utilisation de l'application dans la base de données Journal des événements et statistiques, et envoie des notifications aux administrateurs.
- Notifications. Ce module envoie des notifications électroniques sur les objets infectés, potentiellement infectés et endommagés découverts pendant l'analyse.
- Licence de l'application. Ce module est en charge de l'activation de l'application, de l'analyse des informations de la licence et de l'installation et de la suppression du fichier clé.

### Module d'analyse de la messagerie et des copies

Ce module exécute l'analyse antivirus sur les messages et les copies.

### Module d'analyse des bases de données

Ce module exécute l'analyse antivirus sur les bases de données du serveur Lotus Domino.

Tous les modules se lancent automatiquement au démarrage du serveur Lotus Domino. Les informations relatives au fonctionnement du module sont enregistrées dans la base de données Journal des événements et statistiques, consignées dans le fichier du journal et affichées dans la console du serveur Lotus Domino.

# PRESENTATION DES BASES DE DONNEES DE KASPERSKY ANTI-VIRUS

L'application contient les bases de données suivantes :

- base de données Centre d'administration (kavcontrolcenter.nsf.) : elle sert à administrer les paramètres de Kaspersky Anti-Virus et à les conserver (cf. section "Administration des paramètres de Kaspersky Anti-Virus" à la page 21) ;
- base de données Quarantaine (kavquarantine.nsf) : elle sert à conserver les objets placés en quarantaine et à les manipuler (cf. section "Quarantaine" à la page 71);
- base de données Journal des événements et statistiques (kaveventslog.nsf) : elle sert à conserver les enregistrements sur les événements survenus pendant l'utilisation de Kaspersky Anti-Virus, ainsi que les données statistiques sur les résultats de l'analyse des objets et sur les actions auxquelles ils ont été soumis (cf. section "Journal des événements et statistiques" à la page 76) ;
- base de données Aide (kavhelp.nsf) : contient l'aide sur l'utilisation de Kaspersky Anti-Virus.

Les bases citées sont accessibles via l'interface utilisateur de la base de données Centre d'administration (cf. section "Interface de l'application" à la page 33).

Toutes les bases de données de l'application sont conservées dans le répertoire des bases de données de Kaspersky Anti-Virus (par défaut, il s'agit du répertoire kavdatabases).

# SCHEMA DE LA PROTECTION ANTIVIRUS DU SERVEUR

Kaspersky Anti-Virus assure la protection de la messagerie et des réplications, et analyse les bases de données conservées sur le serveur. La protection du serveur comprend les modules suivants : protection de la messagerie (à la page 50), protection des réplications (à la page 56) et analyse des bases de données (à la page 61) (cf. ill. ci-dessous).

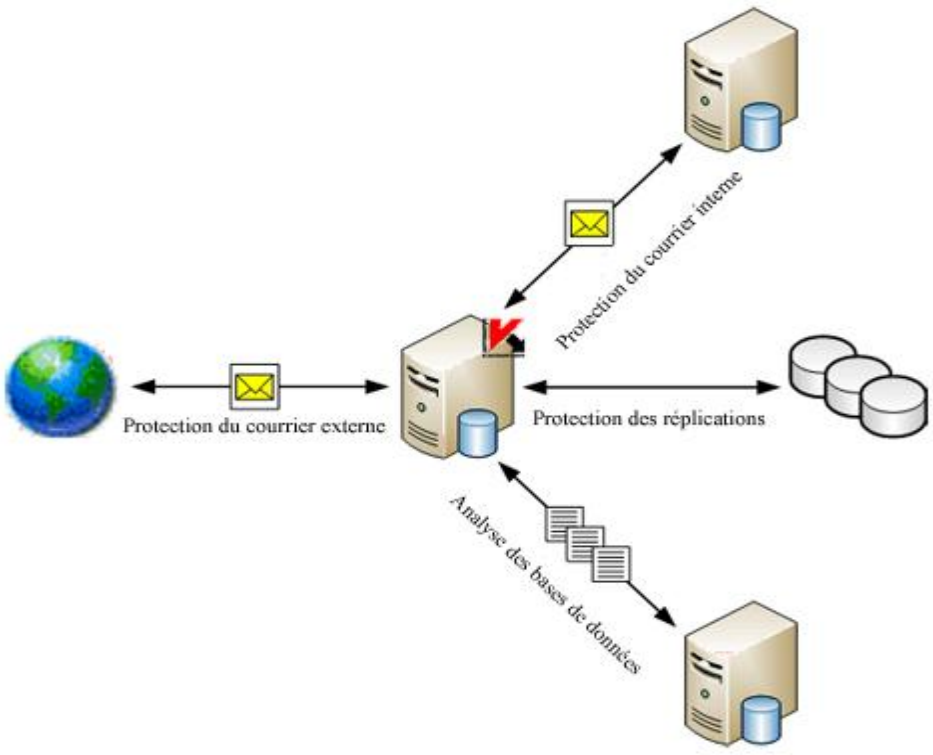


*Illustration 1. Schéma de la protection antivirus du serveur Lotus Domino*

**DANS CETTE SECTION**



# SCHEMA DE FONCTIONNEMENT DE L'APPLICATION

Le schéma de fonctionnement suivant est prévu pour l'application :

1. Le **Module d'administration** reçoit du serveur Lotus Domino des informations concernant le message électronique qui arrive dans la base de données mail.box sur le serveur protégé ou à propos de la tentative de réplication sur le serveur protégé. Le **Module d'administration** transmet le message ou le document modifié suite à la réplication au **Module d'analyse du courrier et des réplications**.

2. Le **Module d'analyse du courrier et des réplications** analyse le message/le document et le traite selon les paramètres de la protection du courrier ou des réplications. Les actions suivantes sont alors exécutées :

   a. Les objets à analyser sont scindés. Les messages électroniques sont scindés entre corps du message, pièces jointes et objets OLE. Dans le document, les champs au format Rich Text et MIME, les pièces jointes et les objets OLE sont séparés.

   b. Le filtrage des objets joints (cf. section "Algorithme de filtrage des pièces jointes" à la page 19) selon la taille et (ou) le nom est réalisé.

   c. L'analyse antivirus des objets (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 20) est exécutée.

   d. Les objets sains sont ignorés sans modification tandis que les autres sont traités conformément aux paramètres de la protection (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21). Avant de passer au traitement, il est possible de conserver une copie de l'objet dans la base de données Quarantaine.

   e. Les messages traités sont transmis au système de messagerie du serveur Lotus Domino pour envoi. Les documents traités sont conservés dans les bases de données du serveur Lotus Domino.

3. Conformément à la programmation de l'analyse des bases ou suite au lancement manuel de l'exécution de l'analyse, le **Module d'administration** transmet l'instruction de démarrage de l'analyse au **Module d'analyse des bases de données**. **Le module d'analyse des bases de données** établit la liste des documents à vérifier conformément aux paramètres d'analyse, puis analyse les documents en fonction de cette liste. L'algorithme d'analyse d'un document par le **Module d'analyse des bases de données** correspond en tout point à l'algorithme d'analyse d'un document par le **Module d'analyse du courrier et des réplications**.

# ALGORITHME DE FILTRAGE DES PIECES JOINTES

Kaspersky Anti-Virus filtre les objets joints aux messages et aux documents. Le filtrage permet d'exclure de l'analyse antivirus les objets conformes aux conditions du filtre.

L'application propose les types de filtres suivants pour les pièces jointes :

- **Filtre selon la taille**. Kaspersky Anti-Virus vérifie la taille des objets joints. Si la taille de l'objet est supérieure à la valeur maximale autorisée, l'objet recevra l'état indiqué dans les paramètres du filtre et l'analyse antivirus de l'objet n'aura pas lieu. L'objet dont la taille est inférieure à la valeur définie sera transféré à l'analyse antivirus.

- **Filtre selon le nom**. Kaspersky Anti-Virus vérifie le nom des objets joints au message. Si le nom de l'objet correspond au masque défini dans les paramètres du filtre, l'objet recevra l'état défini dans les paramètres du filtre et l'analyse antivirus n'aura pas lieu. Si le nom de l'objet ne correspond à aucun des masques définis dans les paramètres du filtre, l'objet sera soumis à l'analyse antivirus.

Si les deux types de filtres des pièces jointes sont définis dans les paramètres de la protection, Kaspersky Anti-Virus analyse d'abord la taille de l'objet. Ensuite, si la taille de l'objet est inférieure à la valeur définie dans les paramètres du filtre selon la taille, Kaspersky Anti-Virus analyse le nom de l'objet. Si la taille de l'objet est supérieure à la valeur définie dans les paramètres du filtre de taille, Kaspersky Anti-Virus ne vérifie pas le nom de l'objet.

À l'issue du filtrage, chaque objet peut se voir attribuer l'un des états suivants :

- *sain* : l'objet ne contient pas de menace ;
- *infecté* : l'objet comporte une menace décrite dans les bases antivirus de Kaspersky Lab. Ces objets seront soumis à une opération de réparation ;
- *non analysé* : Kaspersky Anti-Virus n'a pas réussi à vérifier l'objet. Il est possible qu'une erreur soit survenue au moment de l'analyse de l'objet ou que le temps accordé à l'analyse se soit écoulé ;
- *potentiellement infecté* : le code de l'objet contient soit le code modifié d'un virus connu, soit du code qui évoque un virus mais qui n'a pas encore été identifié et dont la définition ne figure pas encore dans les bases antivirus de Kaspersky Lab.
- *protégé* : l'objet présente des archives protégées par un mot de passe.

Les paramètres de filtrage des pièces jointes sont définis dans les paramètres de la protection du courrier, de la protection des réplications et de l'analyse des bases de données pour chaque composant de la protection séparément.

Suite au filtrage, l'objet est traité conformément à l'état attribué par le filtre : l'objet est soumis aux actions (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21) définies pour les objets de cet état dans les paramètres de la protection du courrier, de la protection des réplications et de l'analyse des bases de données.

# ALGORITHME DE LA RECHERCHE D'EVENTUELLES MENACES DANS LES OBJETS

Kaspersky Anti-Virus analyse l'objet à la recherche de virus selon l'algorithme suivant :

1. L'objet est analysé sur la base des entrées des bases antivirus. Kaspersky Anti-Virus compare l'objet aux entrées des bases. Il détermine ensuite si l'objet analysé est malveillant, à quelle catégorie d'applications dangereuses il appartient et les modes de réparation qui peuvent lui être appliqués.

   Les bases antivirus comportent des descriptions de toutes les applications malveillantes connues sur le moment et des moyens de les neutraliser. Il en est de même pour les applications qui ne sont pas malveillantes mais qui pourraient être utilisées pour l'élaboration d'applications malveillantes.

   Suite à l'analyse, l'objet se voit attribuer l'un des états suivants :

   - *sain* : l'objet ne contient pas de menace ;
   - *infecté* : l'objet comporte une menace décrite dans les bases antivirus de Kaspersky Lab. Ces objets seront soumis à une opération de réparation ;
   - *non analysé* : Kaspersky Anti-Virus n'a pas réussi à vérifier l'objet. Il est possible qu'une erreur soit survenue au moment de l'analyse de l'objet ou que le temps accordé à l'analyse se soit écoulé ;
   - *potentiellement infecté* : le code de l'objet contient soit le code modifié d'un virus connu, soit du code qui évoque un virus mais qui n'a pas encore été identifié et dont la définition ne figure pas encore dans les bases antivirus de Kaspersky Lab.
   - *protégé* : l'objet présente des archives protégées par un mot de passe.

2. L'objet considéré comme sain à l'issue de l'analyse appuyée par bases antivirus est passé dans l'analyseur heuristique. Kaspersky Anti-Virus utilise l'analyseur heuristique pour analyser l'activité de l'objet dans le système. Si cette activité est typique de l'activité des objets malveillants, l'objet est classé comme potentiellement infecté.

## TRAITEMENT DES OBJETS ET ACTIONS EXECUTEES SUR CEUX-CI

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite au filtrage des pièces jointes (cf. section "Algorithme de filtrage des pièces jointes" à la page 19) et suite à l'analyse antivirus (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 20). Les objets sains sont transmis sans aucune modification aux bases de données du serveur Lotus Domino (modules de protection des réplications et analyse des bases de données) ou au système de messagerie du serveur Lotus Domino (module de protection du courrier). Les actions suivantes peuvent être exécutées sur les objets restants :

- **Réparer**. Kaspersky Anti-Virus répare l'objet sur la base des informations contenues dans les bases antivirus à propos de la menace détectée. À l'issue de la réparation, la menace contenue dans l'objet est neutralisée, l'objet est considéré comme sain et enregistré dans la base de données selon l'adresse d'origine ou transmis au système de messagerie. Cette action est réservée aux objets infectés.

  La réparation des objets OLE est impossible. Kaspersky Anti-Virus supprime les objets OLE infectés.

- **Ignorer**. Kaspersky Anti-Virus transfère l'objet à la base de données du serveur Lotus Domino ou au système de messagerie du serveur sans aucune modification.

- **Supprimer**. Kaspersky Anti-Virus supprime l'objet du document ou du message.

Les actions qui seront réalisées par l'application sont définies pour chaque état d'objet dans les paramètres de la protection de la messagerie, de la protection des réplications et de l'analyse des bases de données.

Avant de passer au traitement, il est possible de conserver une copie de l'objet d'origine dans la base de données Quarantaine. Les informations relatives aux actions exécutées sont enregistrées dans la base de données Journal des événements et statistiques.

Kaspersky Anti-Virus peut prévenir les administrateurs, ainsi que l'expéditeur et les destinataires du message (protection du courrier) de la découverte d'objets et des actions exécutées en conséquence (cf. section "Notifications" à la page 85).

# ADMINISTRATION DES PARAMETRES DE FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

L'administration du fonctionnement de Kaspersky Anti-Virus s'opère via les paramètres du profil et les paramètres du serveur.

Le *profil* est un ensemble de paramètres de Kaspersky Anti-Virus qui définit le fonctionnement de l'application pour un serveur ou un groupe de serveurs inclus dans ce profil. Le recours aux profils permet de réaliser une gestion centralisée des paramètres de Kaspersky Anti-Virus.

Les profils permettent de définir des paramètres uniques de Kaspersky Anti-Virus pour un groupe de serveurs, par exemple sur la base de l'emplacement, des fonctions exécutées ou d'autres facteurs. Cette fonctionnalité simplifie considérablement l'administration de l'application quand elle est installée sur plusieurs serveurs et permet de contrôler de manière centralisée l'état de la protection antivirus sur tous les ordinateurs.

Le profil peut contenir un ou plusieurs serveurs. En cas d'utilisation d'un schéma de déploiement particulier de Kaspersky Anti-Virus, le profil contient un seul serveur. En cas d'utilisation d'un schéma de déploiement défini, le profil contient plusieurs serveurs (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino).

Un profil peut définir tous les paramètres de l'application, à l'exception de la licence utilisée par le serveur et de la durée de conservation des objets en quarantaine. Ces deux paramètres sont définis uniquement pour un serveur en particulier, dans les paramètres du serveur (cf. section "Définition de valeurs individuelles pour les paramètres du serveur" à la page 90). De plus, il est possible de redéfinir certains paramètres du profil dans les paramètres du serveur. Cette possibilité permet de définir, pour chaque serveur, des paramètres qui correspondent au rôle du serveur dans le système de la protection antivirus et qui diffèrent des valeurs définies dans le profil. Ces paramètres reprennent par exemple les paramètres de mise à jour, les paramètres d'enregistrement des informations sur les événements survenus pendant l'utilisation de Kaspersky Anti-Virus et les informations statistiques.

Les serveurs sont ajoutés automatiquement au profil après l'installation sur ceux-ci de Kaspersky Anti-Virus. Si l'application est supprimée, le serveur est automatiquement supprimé du profil. Le profil reprend uniquement les serveurs protégés par Kaspersky Anti-Virus.

Vous pouvez créer et supprimer des profils (cf. section "Création et suppression de profils" à la page 87). Le serveur sur lequel Kaspersky Anti-Virus est installé peut être déplacé d'un profil à un autre (cf. section "Déplacement du serveur vers un autre profil" à la page 90).

Les profils peuvent également servir à créer un système de protection à différents niveaux, par exemple pour les serveurs de messagerie ou les serveurs de bases de données. Pour ce faire, vous pouvez créer plusieurs profils avec des valeurs de paramètres différentes. Pour définir un niveau de protection particulier pour un serveur ou un groupe de serveur, il suffit de déplacer le serveur dans le profil dont les paramètres vous conviennent.

Les paramètres du serveur permettent de définir des valeurs individuelles qui correspondent aux fonctions de ce serveur dans le réseau de l'entreprise (cf. section "Définition de valeurs individuelles pour les paramètres du serveur" à la page 90). Ainsi, les paramètres du serveur peuvent intervenir dans la configuration du modèle de mise à jour centralisé des bases antivirus (cf. section "Schémas de mise à jour" à la page 45).

Toutes les informations relatives aux paramètres de Kaspersky Anti-Virus sont conservées dans la base de données Centre d'administration kavcontrolcenter.nsf. La base de données Centre d'administration est créée lors de l'installation de l'application dans le répertoire des bases de données de Kaspersky Anti-Virus (ce répertoire est kavdatabases par défaut). En outre, un profil est créé dans la base de données : le serveur protégé y est ajouté. Les paramètres du profil et les paramètres du serveur reçoivent les valeurs par défaut.

Le mot de passe d'accès au serveur proxy est enregistré dans la base de données kavcontrolcenter.nsf. Il est connu de l'utilisateur disposant d'un accès à cette base. Ainsi, il n'est recommandé d'accorder un accès à la base de données kavcontrolcenter.nsf aux utilisateurs qu'en cas de besoin, et de surveiller cet accès. Il est conseillé de modifier le mot de passe d'accès au serveur proxy lorsqu'un utilisateur disposant d'un accès à la base de données kavcontrolcenter.nsf quitte l'entreprise.

En cas d'utilisation d'un déploiement distribué de Kaspersky Anti-Virus (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino), la base de données kavcontrolcenter.nsf contient des informations concernant les paramètres de fonctionnement de Kaspersky Anti-Virus sur chacun des serveurs protégés. La base de données est créée pendant l'installation sur l'un de ces serveurs, puis une réplique de la base de données Centre d'administration existante est créée sur chacun des autres serveurs. La base de données de l'un des serveurs (choisi par l'administrateur) déjà équipé de Kaspersky Anti-Virus sert de base. Tout nouveau serveur protégé est ajouté au même profil que le serveur à partir duquel la réplique de la base kavcontrolcenter.nsf a été créée. Les paramètres du serveur reçoivent les valeurs par défaut. En cas de suppression de Kaspersky Anti-Virus sur l'un des serveurs, les informations relatives à ce serveur sont supprimées du profil dans la base de données Centre d'administration.

En cas d'utilisation d'un schéma de déploiement isolé, la base de données kavcontrolcenter.nsf est placée sur un serveur et contient uniquement les données relatives à la configuration de ce serveur.

Pour configurer les paramètres de Kaspersky Anti-Virus et pour administrer son fonctionnement, il est nécessaire d'ouvrir la base de données kavcontrolcenter.nsf.

Les autorisations d'ouverture de la base de données kavcontrolcenter.nsf, de configuration des paramètres et d'administration de Kaspersky Anti-Virus sont octroyées uniquement aux utilisateurs possédant les privilèges de l'un des trois groupes fonctionnels suivants : Administrateurs de la sécurité, Administrateurs du Centre d'administration et Administrateurs avec privilèges restreints (cf. section " Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus" à la page 25). Avant d'ouvrir la base de données, assurez-vous que le compte utilisateur possède les autorisations nécessaires pour l'exécution des opérations requises (création ou suppression de profils, configuration des paramètres du profil et configuration des paramètres du serveur, etc.).

La base de données kavcontrolcenter.nsf peut être ouverte sur n'importe quel serveur protégé via le client Lotus Notes ou via l'interface Web (cf. section "Interface de l'application" à la page 33).

Par défaut, les modifications des paramètres des profils et des serveurs sont introduites dans la réplique de la base de données situées sur le même serveur que celui auquel la connexion a été réalisée. Pendant la réplication, les modifications sont propagées à tous les autres serveurs protégés. Un certain délai peut survenir entre la définition des valeurs des paramètres et leur application. Par conséquent, au moment de choisir le serveur sur lequel les paramètres seront configurés, il convient de tenir compte de la topologie des réplications.

Si vous utilisez Kaspersky Anti-Virus via un client Lotus Notes, les modifications des paramètres du serveur pourront être introduites dans la réplique de la base de données du Centre d'administration située sur le serveur dont vous modifiez les paramètres, quel que soit le serveur auquel vous êtes connecté. Dans ce cas, les nouvelles valeurs des paramètres du serveur sont appliquées bien plus rapidement. En cas d'utilisation via le navigateur Internet, cette possibilité n'est pas prise en charge et les modifications des paramètres du serveur sont toujours introduites dans la réplique ouverte.

L'utilisation de la base de données Centre d'administration peut avoir lieu simultanément depuis plusieurs postes de travail ou parallèlement via le navigateur Internet ou le client Lotus Notes. Sachez toutefois que la modification simultanée des paramètres du même profil ou serveur par deux utilisateurs ou plus peut entraîner un conflit de réplications. De plus, il est déconseillé de modifier simultanément les paramètres du serveur et les paramètres du profil auquel appartient ce serveur. Suite à l'application des nouveaux paramètres du profil, les paramètres du serveur peuvent être redéfinis automatiquement.

# CONFIGURATION DES PARAMETRES DE KASPERSKY ANTI-VIRUS VIA LE FICHIER DE CONFIGURATION .INI

L'administration des paramètres de Kaspersky Anti-Virus peut être réalisée via l'interface de l'application ou à l'aide de modifications dans le fichier de configuration notes.ini. L'administration des paramètres de l'application via le fichier de configuration vous permet de définir les valeurs des paramètres inaccessibles via l'interface (par exemple, activer le balayage progressif des objets) et d'administrer certaines fonctions spécifiques de Kaspersky Anti-Virus via la ligne de commande de la console du serveur Lotus Domino.

*Pour modifier les paramètres du fichier de configuration, procédez comme suit :*

1. Ouvrez le fichier de configuration du serveur Lotus Domino notes.ini situé à l'adresse suivante :
   - pour les systèmes d'exploitation Microsoft Windows : dans le répertoire des fichiers binaires du serveur Lotus Domino;
   - pour les systèmes d'exploitation Linux : dans le répertoire de données du serveur Lotus Domino.
2. Modifiez les paramètres (cf. tableau ci-dessous) et enregistrez les modifications.
3. Relancez le serveur Lotus Domino.

Les paramètres définis dans le fichier notes.ini ne se synchronisent pas avec les paramètres définis dans l'interface de Kaspersky Anti-Virus. Les paramètres du fichier de configuration sont prioritaires sur les paramètres de l'interface.

*Tableau 2. Liste des paramètres modifiables*

| PARAMETRES | VALEUR | DESCRIPTION |
|---|---|---|
| KAVCustomUpdUrlOnly | 1 | Le serveur reçoit les mises à jour uniquement depuis la source de mises à jour que vous aurez indiquée. Vous pouvez indiquer la source des mises à jour dans les paramètres du profil ou dans les paramètres du serveur. |
| | 2 / absence de paramètres<br>Par défaut | Si la mise à jour depuis la source que vous aurez désignée échoue, Kaspersky Anti-Virus tentera d'établir une connexion à une autre source de mises à jour, à savoir la ressource à partir de laquelle la dernière mise à jour réussie a été réalisée, ou au serveur de mises à jour de Kaspersky Lab. |
| KAVLicenseNotifyDays | Ce paramètre est ignoré par défaut | 14 jours avant l'expiration de la validité du fichier clé, Kaspersky Anti-Virus en avertit l'administrateur. |

| PARAMETRES | VALEUR | DESCRIPTION |
|---|---|---|
| KAVProcExclude | Les valeurs updall, nupdate, ldap, event, statlog, fixup, compact sont utilisées par défaut | Processus exclus de l'analyse de Kaspersky Anti-Virus L'application ne contrôle pas ces processus. |
| KAVDatabasesPath | Chemin d'accès au répertoire d'installation de l'application<br>La valeur par défaut est kavdatabases | Kaspersky Anti-Virus est installé<br>La valeur du paramètre définit le chemin vers les bases de données de Kaspersky Anti-Virus en fonction du répertoire de données Domino. |
| KAVArchDepthLevel | 32 | Niveau d'imbrication autorisé pour les archives analysées. |
| | 0 / absence de paramètres | Le niveau d'imbrication des archives analysées n'est pas défini. |
| KAVNonIncrementalScan | 0 / absence de paramètres | L'analyse incrémentale est activée. |
| | 1<br>Par défaut | L'analyse incrémentale est désactivée. |

# ADMINISTRATION DES PRIVILEGES DES UTILISATEURS

Cette section détaille les modalités d'administration des privilèges utilisateur.

L'administration des privilèges des utilisateurs s'opère au niveau de la LCA des bases de données de Kaspersky Anti-Virus et au niveau de chaque document (paramètres du profil et paramètres du serveur). Les privilèges au niveau de la LCA sont octroyés à l'aide du mécanisme des *groupes fonctionnels*. Les privilèges au niveau des documents sont octroyés à l'aide des *rôles fonctionnels* (cf. section "*Administration des privilèges au niveau des paramètres du profil/serveur*" à la page 27).

### DANS CETTE SECTION



# ADMINISTRATION DES PRIVILEGES AU NIVEAU DE LA LCA DES BASES DE DONNEES DE KASPERSKY ANTI-VIRUS

L'application prévoit trois groupes fonctionnels pour octroyer des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus : **Administrateurs de la sécurité**, **Administrateur du Centre d'administration** et **Administrateurs avec des privilèges restreints**.

La composition de chaque groupe est définie lors de l'installation de l'application. L'administrateur qui réalise l'installation compose les groupes fonctionnels en choisissant les utilisateurs et (ou) les groupes d'utilisateurs dans le carnet d'adresses du serveur Lotus Domino. Lors de l'installation de l'application, des éléments de chaque groupe fonctionnel sont inclus automatiquement dans la LCA des bases de données Lotus Notes de Kaspersky Anti-Virus.

La LCA des bases de données de Kaspersky Anti-Virus reprend également l'entrée Default (par défaut) et Anonymous (anonyme), ainsi que les serveurs sur lesquels l'application est installée. L'administrateur désigne les serveurs à inclure dans la LCA pendant l'installation de l'application (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino). Les serveurs obtiennent le niveau d'accès Manager (gestionnaire) auquel sont associées les autorisations de création et de suppression de documents ainsi que la réplication ou la copie de documents. Les enregistrements Default (par défaut) et Anonymous (anonymes) dans la LCA des bases de données de Kaspersky Anti-Virus obtiennent le niveau d'accès No access (pas d'accès).

### DANS CETTE SECTION



## PRIVILEGES DES GROUPES FONCTIONNELS

Le tableau ci-après reprend les privilèges des groupes fonctionnels dans la LCA des bases de données de Kaspersky Anti-Virus.

*Tableau 3. Privilèges des groupes fonctionnels*

| GROUPES FONCTIONNELS | BASE DE DONNEES CENTRE D'ADMINISTRATION | BASE DE DONNEES JOURNAL DES EVENEMENTS ET STATISTIQUES | BASE DE DONNEES QUARANTAINE | BASE DE DONNEES AIDE |
|---|---|---|---|---|
| **ADMINISTRATEURS DE LA SECURITE** | Niveau d'accès Manager (gestionnaire) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents.<br>Rôle AppAdmin. | Niveau d'accès Manager (gestionnaire) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents. | Niveau d'accès Manager (gestionnaire) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents. | Niveau d'accès Manager (gestionnaire). |
| **ADMINISTRATEURS DU CENTRE D'ADMINISTRATION** | Niveau d'accès Author (auteur) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents.<br>Rôle AppAdmin. | Niveau d'accès Author (auteur) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents. | Niveau d'accès Author (auteur) auquel sont associées les autorisations de création et de suppression de documents, ainsi que la réplication ou la copie de documents. | Niveau d'accès Reader (lecteur). |
| **ADMINISTRATEURS AVEC DES PRIVILEGES RESTREINTS** | Niveau d'accès Author (auteur) auquel est associée l'autorisation de réplication ou de copie de documents. | Niveau d'accès Author (auteur) auquel est associée l'autorisation de réplication ou de copie de documents. | Niveau d'accès Author (auteur) auquel est associée l'autorisation de réplication ou de copie de documents. | Niveau d'accès Reader (lecteur). |

Une fois Kaspersky Anti-Virus installé, les utilisateurs et les groupes d'utilisateurs inclus dans les groupes fonctionnels reçoivent les privilèges indispensables à l'utilisation de l'application.

Les utilisateurs repris dans le groupe **Administrateurs de la sécurité** bénéficient des privilèges les plus étendus pendant l'utilisation de Kaspersky Anti-Virus et peuvent exécuter les opérations suivantes :

- Administration des privilèges des utilisateurs au niveau de la LCA des bases de données de Kaspersky Anti-Virus.
- Création et suppression de profils.
- Modification des paramètres de tous les profils et des paramètres de tous les serveurs.
- Suppression des entrées des bases de données Quarantaine et Journal des événements et statistiques.

Les utilisateurs repris dans le groupe **Administrateurs du Centre d'administration**, peuvent réaliser les opérations suivantes pendant l'utilisation de Kaspersky Anti-Virus :

- Création et suppression de profils.
- Modification des paramètres de tous les profils et des paramètres de tous les serveurs.
- Suppression des entrées des bases de données Quarantaine et Journal des événements et statistiques.

Les utilisateurs repris dans le groupe **Administrateurs avec des privilèges restreints** ne possèdent pas, par défaut, les privilèges de modification des paramètres des profils/des serveurs, ni les privilèges de suppression des entrées des bases de données Quarantaine et Journal des événements et statistiques. Les privilèges requis pour l'utilisation de l'application sont octroyés aux utilisateurs de ce groupe à l'aide des rôles fonctionnels (cf. section "Administration des privilèges au niveau des paramètres du profil/du serveur" à la page 27).

Les utilisateurs des trois groupes fonctionnels disposent de privilèges pour la consultation des bases Quarantaine, Journal des événements et statistiques et Aide.

# OCTROI DE PRIVILEGES DES GROUPES FONCTIONNELS AUX UTILISATEURS

Lors de l'installation de Kaspersky Anti-Virus, l'administrateur peut activer les utilisateurs de Lotus Domino séparément, ainsi que les groupes d'utilisateurs des trois groupes fonctionnels.

Pour simplifier la procédure d'octroi des privilèges, il est conseillé de ne pas inclure d'utilisateurs individuels dans les groupes fonctionnels, mais bien les groupes composés dans le carnet d'adresses du serveur Lotus Domino (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino). Pendant l'installation, ces groupes sont inclus dans la LCA des bases de données de Kaspersky Anti-Virus et ils reçoivent les privilèges des groupes fonctionnels (cf. section "Privilèges des groupes fonctionnels" à la page 25). Plus tard, l'administrateur du serveur Lotus Domino pourra octroyer aux utilisateurs des privilèges ou les restreindre en modifiant la composition des groupes dans le carnet d'adresses (exclusion ou inclusion d'utilisateurs).

Si des utilisateurs individuels et non des groupes d'utilisateurs ont été inclus dans les groupes fonctionnels lors de l'installation de l'application, l'administration ultérieure des privilèges requière la modification manuelle de la LCA de toutes les bases de données de Kaspersky Anti-Virus. Pour retirer les privilèges d'un groupe fonctionnel à un utilisateur, il est nécessaire de supprimer son compte utilisateur de la LCA de toutes les bases de données de Kaspersky Anti-Virus. Pour octroyer les privilèges de tel ou tel groupe fonctionnel à un utilisateur, il est nécessaire d'inclure son compte à la LCA de toutes les bases de données.

Seuls les utilisateurs qui possèdent les privilèges du groupe fonctionnel **Administrateurs de la sécurité** peuvent modifier les LCA des bases de données de Kaspersky Anti-Virus.

Il est recommandé d'inclure le compte utilisateur dans la LCA des bases de données de Kaspersky Anti-Virus dans la composition du groupe.

*Pour octroyer les privilèges d'un groupe fonctionnel à l'utilisateur, procédez comme suit :*

1. Créez, dans le carnet d'adresses du serveur Lotus Domino, un groupe portant un nom unique, par exemple ControlCenterAdmins.

2. Ajoutez l'utilisateur qui recevra les privilèges de tel ou tel groupe fonctionnel, par exemple du groupe **Administrateurs du centre d'administration**, au groupe ControlCenterAdmins.

3. Ouvrez une session dans le système sous le compte de l'utilisateur possédant les privilèges du groupe fonctionnel **Administrateur de la sécurité**.

4. Ajoutez le groupe ControlCenterAdmins à la LCA des bases de données de Kaspersky Anti-Virus (Centre d'administration, Journal des événements et statistiques, Quarantaine et Aide) et définissez pour le groupe ControlCenterAdmins les privilèges qui correspondent aux privilèges du groupe fonctionnel **Administrateur du Centre d'administration** (cf. section "**Privilèges des groupes fonctionnels**" à la page 25).

# ADMINISTRATION DES PRIVILEGES AU NIVEAU DES PARAMETRES DU PROFIL/SERVEUR

Pour limiter l'accès à l'application au niveau de documents en particulier (paramètres des profils et paramètres des serveurs), les rôles fonctionnels suivants sont prévus :

- L'administrateur de profil dispose des privilèges pour exécuter les actions suivantes :
  - Modification des paramètres du profil et des paramètres de tous les serveurs inclus dans le profil.
  - Suppression des enregistrements des bases de données Quarantaine et Journal des événements et statistiques pour les serveurs repris dans le profil.

- L'administrateur de serveur dispose des privilèges pour exécuter les actions suivantes :
  - Modification des paramètres du serveur, y compris le transfert du serveur dans un autre profil.
  - Suppression des entrées de la base de données Quarantaine et Journal des événements et statistiques pour le serveur.

Les administrateurs de profil et les administrateurs de serveur sont désignés après l'installation de l'application. La désignation a lieu pour chaque serveur (cf. section "Désignation de l'administrateur de serveur" à la page 89) et chaque profil séparément (cf. section "Désignation de l'administrateur de profil" à la page 89).

Seul un utilisateur possédant les privilèges de l'un des trois groupes fonctionnels peut être désigné comme administrateur de profil ou administrateur de serveur (cf. section "Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus." à la page 25).

Par défaut, les paramètres des profils et des serveurs proposent en tant qu'administrateurs les utilisateurs et (ou) les groupes inclus dans le groupe fonctionnel **Administrateurs du centre d'administration** pendant l'installation de l'application.

Quel que soit leur rôle fonctionnel, les utilisateurs des groupes **Administrateurs de la sécurité** et **Administrateurs du Centre d'administration** peuvent modifier les paramètres de tous les serveurs et les paramètres de tous les profils. Pour limiter les privilèges, par exemple autoriser la modification d'un seul profil ou serveur, il est nécessaire de désigner en tant qu'administrateur de profil ou de serveur un utilisateur appartenant au groupe fonctionnel **Administrateurs avec des privilèges restreints**. Les utilisateurs de ce groupe peuvent uniquement modifier les paramètres des profils/des serveurs dont ils sont administrateurs. Si un utilisateur de ce groupe est désigné comme administrateur de profil, il pourra également modifier les paramètres de tous les serveurs repris dans ce profil.

# LICENCE DE L'APPLICATION

Cette section décrit la mise sous licence et l'activation de l'application, ainsi que l'installation et la suppression des fichiers clés de Kaspersky Anti-Virus.

### DANS CETTE SECTION



## PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions selon lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement le Contrat de licence avant de commencer à utiliser l'application.

Il est considéré que vous acceptez les conditions du contrat de licence lorsque vous confirmez votre accord avec le texte du contrat de licence au moment de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application.

## A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence. Un code unique d'activation de votre copie de Kaspersky Anti-Virus est associé à la licence.

La licence donne droit aux services suivants :

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

  Le nombre de périphériques sur lesquels vous pouvez utiliser l'application est défini dans les conditions du Contrat de licence.

- Contacter le Support Technique de Kaspersky Lab.
- Accès aux services complémentaires fournis par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence.

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

Il existe différents types de licence :

- *Evaluation* : licence gratuite, conçue pour découvrir l'application.

  En général, une licence d'évaluation possède une courte durée de validité. A la fin de la durée de validité de la licence d'évaluation, Kaspersky Anti-Virus arrête l'exécution de toutes les fonctions. Pour pouvoir continuer à utiliser l'application, il est nécessaire d'acheter une licence commerciale.

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

  Une fois que la durée de validité de la licence commerciale est écoulée, l'application reste fonctionnelle, mais ses fonctionnalités sont limitées (par exemple, il n'est plus possible de mettre l'application à jour ou d'utiliser le service Kaspersky Security Network). Vous pouvez continuer à utiliser tous les modules de l'application et rechercher la présence éventuelle de virus et d'autres programmes dangereux, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour pouvoir continuer à profiter de toutes les fonctionnalités de Kaspersky Anti-Virus, il est nécessaire de renouveler la licence commerciale.

  Il est conseillé de renouveler la licence avant sa date d'expiration afin de s'assurer une protection maximale contre toutes les menaces informatiques.

# PRESENTATION DU FICHIER CLE

*Le fichier clé* est un fichier de type xxxxxxx.key. L'application charge le fichier clé depuis le serveur d'activation à l'aide du code d'activation. Le fichier clé est indispensable à l'utilisation de l'application.

En cas de suppression accidentelle du fichier clé, vous devez procéder comme suit pour le restaurer :

- envoyer une demande au Support Technique (cf. section "Contacter le Support Technique" à la page 98);
- obtenir le fichier clé sur le site à l'aide du code d'activation fourni.

Le fichier clé contient les informations suivantes :

- Une clé sous forme de séquence unique de lettres et de chiffres. Cette clé permet, par exemple, d'obtenir l'aide du Support technique de Kaspersky Lab.
- Restriction sur le nombre d'ordinateurs : nombre maximal d'ordinateurs sur lesquels vous pouvez activer l'application à l'aide de ce fichier clé.
- La date de création du fichier clé est celle de création du fichier clé sur le serveur d'activation.
- La durée de validité de la licence est la durée d'utilisation de l'application prévue par le Contrat de licence à partir de la date de la première activation de l'application à l'aide du fichier clé en question. Par exemple, 1 an.

  La durée de validité de la licence expire avant ou en même temps que la durée de validité du fichier clé utilisé pour activer l'application.

- Le délai de validité du fichier clé est un délai défini à compter de la création du fichier clé. Ce délai peut s'étendre sur plusieurs années. Toute activation de l'application à l'aide du fichier clé en question après la fin du délai de validité est impossible.

  Le délai de validité du fichier clé est considéré comme échu après la fin de validité de la licence d'utilisation de l'application activée à l'aide de ce fichier clé.

# APPLICATION DU FICHIER CLE

L'installation du fichier clé de Kaspersky Anti-Virus doit avoir lieu sur chaque serveur séparément. Vous pouvez télécharger deux fichiers clés : un fichier clé actif et un fichier de clé complémentaire. Le fichier clé actif entre en vigueur dès son installation. L'application ne peut pas compter plus d'une licence active. La clé complémentaire est utilisée automatiquement à l'expiration de la licence associée à la clé active. Les fichiers clés peuvent être téléchargés au cours du processus d'installation de Kaspersky Anti-Virus (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino).

Vous pouvez télécharger le fichier clé via l'interface de la console du serveur Lotus Domino, via le client Lotus Notes ou via le navigateur Internet.

La suppression du fichier clé actif ou complémentaire est uniquement possible via la console du serveur Lotus Domino, à l'aide de la ligne de commande (cf. section "Utilisation via la console du serveur" à la page 96).

# TELECHARGEMENT DU FICHIER CLE VIA LE CLIENT LOTUS NOTES OU LE NAVIGATEUR INTERNET

Avant l'installation du fichier clé via le client Lotus Notes ou via le navigateur Internet, assurez-vous qu'il est accessible sur le système de fichiers du poste client où la base de données Centre d'administration a été ouverte.

*Pour télécharger le fichier clé via le client Lotus Notes ou le navigateur Internet, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez installer le fichier clé (cf. section "Consultation et modification des paramètres du serveur à la page 39).
2. Dans la zone d'administration, sélectionnez l'onglet **Licence**.
3. Cliquez sur le lien **Ajouter une clé**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier clé portant l'extension key, puis cliquez sur le bouton **Ouvrir**.

   Le fichier clé indiqué se télécharge sur le serveur.

L'onglet **Licence** reprend les informations suivantes sur la licence active :

- **Fonctionnalité**. Les restrictions suivantes sont prévues au niveau de la fonctionnalité :
  - **Complète** : clé ajoutée.
  - **Uniquement l'administration** : la clé n'est pas installée ou la durée de validité de la licence d'évaluation est écoulée.
  - **Uniquement la mise à jour** : une erreur s'est produite lors de la mise à jour des bases antivirus, les bases antivirus sont endommagées ou la clé figure dans la liste noire.
  - **Fonctionnalité complète sans la mise à jour** : la durée de validité de la licence commerciale est écoulée.
- **Type**. Type de licence : évaluation ou commerciale.
- **Date d'expiration**. Date de fin de validité de la licence.
- **Jours restants**. Nombre de jours avant la date de fin de validité de la licence.
- **Clé**. Séquence unique de chiffres et de lettres.
- **Détenteur**. Informations sur le détenteur de la licence : organisation, nom du détenteur, pays, courrier électronique, etc.

# TELECHARGEMENT DU FICHIER CLE VIA LA CONSOLE DU SERVEUR LOTUS NOTES

Avant le téléchargement du fichier clé via l'interface de la console du serveur Lotus Domino, placez le fichier clé dans un répertoire aléatoire du système de fichiers du serveur protégé pour lequel il sera utilisé.

*Si l'ordinateur fonctionne sous le système d'exploitation Linux, procédez comme suit avant de télécharger le fichier clé via l'interface de la console du serveur Lotus Domino :*

1. Définissez le compte utilisateur disposant des privilèges de lancement du serveur Lotus Domino comme propriétaire du fichier clé.
2. Installez les modes d'accès suivants au fichier clé :
   - pour le propriétaire du fichier : lecture, écriture, exécution ;
   - pour le groupe du propriétaire du fichier : lecture, exécution ;
   - pour les autres comptes utilisateurs : lecture, exécution.

*Pour télécharger le fichier clé via l'interface de la console du serveur Lotus Domino, procédez comme suit :*

1. Lancez la console du serveur Lotus Domino.
2. Dans la ligne de commande, saisissez :

   ```
   tell kavcontrol AddKey <chemin_vers_le_fichier_clé>
   ```

   où `<chemin_vers_le_fichier_clé>` est le chemin complet vers le fichier clé sur le serveur Lotus Domino.

# INTERFACE DE L'APPLICATION

Cette section décrit les principaux éléments de l'interface graphique de l'application dans le cadre de l'utilisation via le client Lotus Notes et le navigateur Internet.

### DANS CETTE SECTION



# ACCES A LA BASE DE DONNEES CENTRE D'ADMINISTRATION

Toutes les opérations de configuration et d'administration de Kaspersky Anti-Virus sont réalisées via l'interface utilisateur de la base de données Centre d'administration. L'utilisation des bases de données Quarantaine, Journal des événements et statistiques et Aide passe également par l'interface des bases de données Centre d'administration.

La base de données Centre d'administration est accessible via le client Lotus Notes ou via le navigateur Internet. L'interface Internet permet d'administrer l'application à partir des ordinateurs sur lesquels le client Lotus Notes n'est pas installé (cf. section "Administration à distance de Kaspersky Anti-Virus via le navigateur Internet" à la page 92).

Il existe également une série d'instructions pour l'administration de Kaspersky Anti-Virus via la console du serveur Domino (cf. section "Utilisation via la console du serveur" à la page 96).

Les autorisations d'ouverture de la base de données Centre d'administration, de configuration des paramètres et d'administration de Kaspersky Anti-Virus sont octroyées uniquement aux utilisateurs possédant les privilèges de l'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité** , **Administrateurs du centre d'administration** et **Administrateurs avec privilèges restreints** (cf. section " **Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus** " à la page 25). Avant d'ouvrir la base de données, assurez-vous que le compte utilisateur possède les autorisations nécessaires pour l'exécution des opérations requises.

La structure de la fenêtre de la base de données Centre d'administration et les actions lors de l'exécution d'une opération sont identiques, aussi bien en cas d'utilisation du client Lotus Notes qu'en cas d'utilisation du navigateur Internet. Par conséquent, dans la suite de ce guide, seule l'utilisation de Kaspersky Anti-Virus via le client Lotus Notes sera présentée.

- *Pour ouvrir la fenêtre de la base de données Centre d'administration via le client Lotus Notes, procédez comme suit :*

  1. Lancez le client Lotus Notes.

  2. Ouvrez la base de données kavcontrolcenter.nsf située dans le répertoire de cartographie des bases de données de Kaspersky Anti-Virus.

*Pour ouvrir la fenêtre de la base de données Centre d'administration via le navigateur Internet, procédez comme suit :*

1. Ouvrez le navigateur Internet.

2. Saisissez, dans la ligne d'adresse :

   ```
   http://<nom_du_serveur>/<chemin_d'accès_au
   fichier_kavcontrolcenter.nsf>?OpenDatabase&Login
   ```

   où :

   - `<nom_du_serveur>` est le nom ou l'adresse IP du serveur où Kaspersky Anti-Virus est installé ;
   - `<chemin_d'accès_au fichier_kavcontrolcenter.nsf>` est le chemin d'accès au fichier kavcontrolcenter.nsf du répertoire de données du serveur Lotus Domino.

Cette action entraîne l'ouverture de la fenêtre de la base de données Centre d'administration (cf. ill. ci-après).

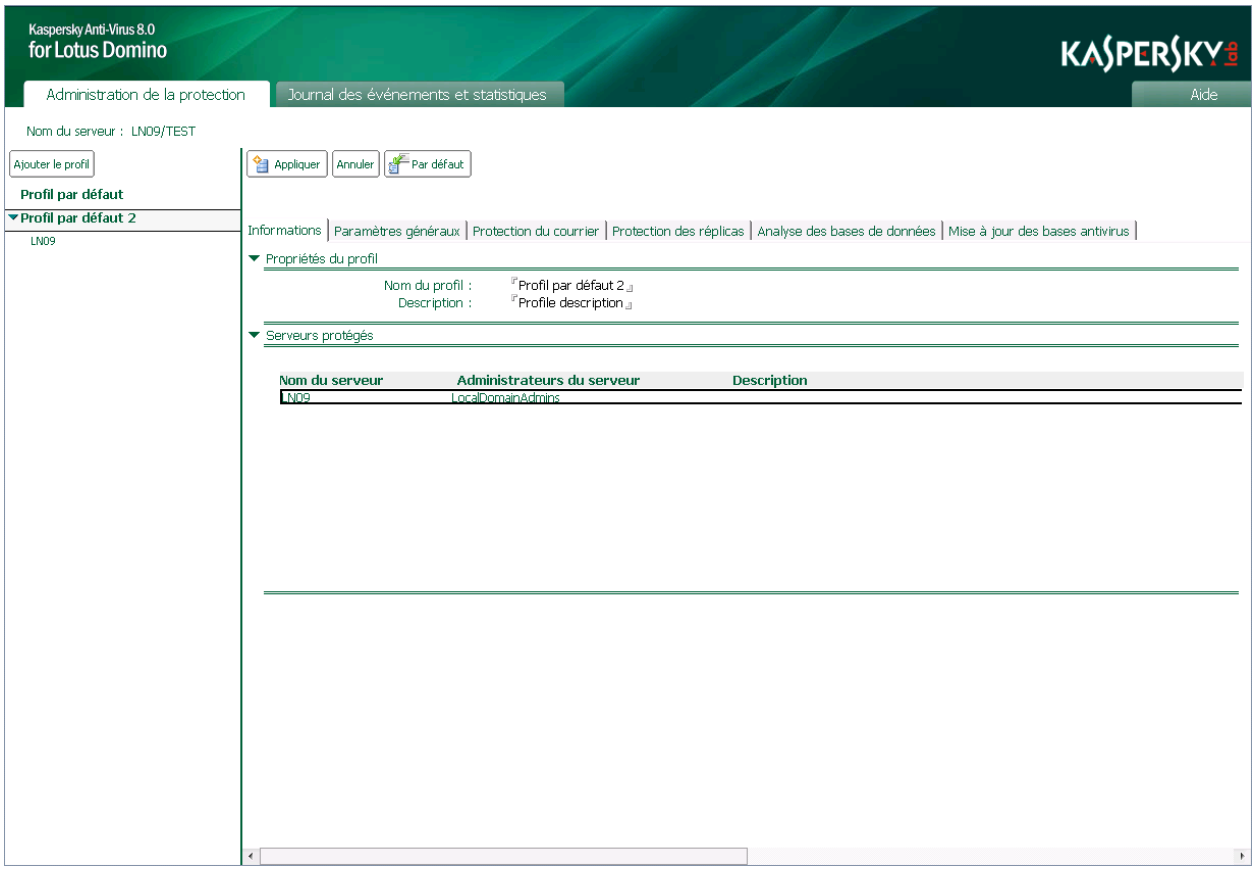


*Illustration 2. Fenêtre de la base de données Centre d'administration*

Ici, et dans la suite du texte, les illustrations représentent la fenêtre de la base Centre d'administration ouverte à l'aide du client Lotus Notes.

Lors de la première ouverture de la base de données Centre d'administration dans la zone de travail, Lotus Notes crée automatiquement un raccourci pour y accéder. Le raccourci pourra être utilisé à l'avenir pour ouvrir la fenêtre de la base de données Centre d'administration.

En cas d'utilisation de Kaspersky Anti-Virus via le navigateur Internet, le chemin d'accès à la base kavcontrolcenter.nsf peut être enregistré sous la forme d'un lien et utilisé à l'avenir pour ouvrir la fenêtre de la base de données Centre d'administration.

# STRUCTURE DE LA FENETRE DE LA BASE DE DONNEES CENTRE D'ADMINISTRATION

La fenêtre de la base de données Centre d'administration est composée des éléments suivants (cf. ill. ci-après):

- *Volet de transfert* : situé dans la partie supérieure de la fenêtre, ce volet contient les onglets qui permettent de naviguer entre les bases de données Centre d'administration, Journal des événements et statistiques et Aide.
- *Volet d'état* : situé dans la partie supérieure de la fenêtre, ce volet contient le nom du serveur auquel la connexion est réalisée et le nom du serveur sur lequel le document est modifié.

  En cas d'utilisation via le client Lotus Notes, le serveur sur lequel la réplique de la base de données Centre d'administration est modifiée peut être différent du serveur auquel la connexion est réalisée.

- *Volet des actions* : situé dans la partie supérieure du volet d'administration, ce volet comporte des boutons permettant de modifier les paramètres du profil ou du serveur.
- *Volet de navigation* : situé dans la partie gauche de la fenêtre, ce volet contient les éléments suivants en fonction de l'onglet sélectionné dans le volet de transfert :
  - liste des profils et des serveurs qu'ils contiennent ;
  - liste des rubriques et des sections du Journal des événements et statistiques.
- *Volet d'administration* : situé dans la partie droite de la fenêtre, ce volet est destiné à l'utilisation des paramètres des profils / serveurs et des enregistrements des bases de données de Kaspersky Anti-Virus.
- *Volet de consultation* : situé dans la partie inférieure de la fenêtre, ce volet est destiné à la consultation des enregistrements du Journal des événements.

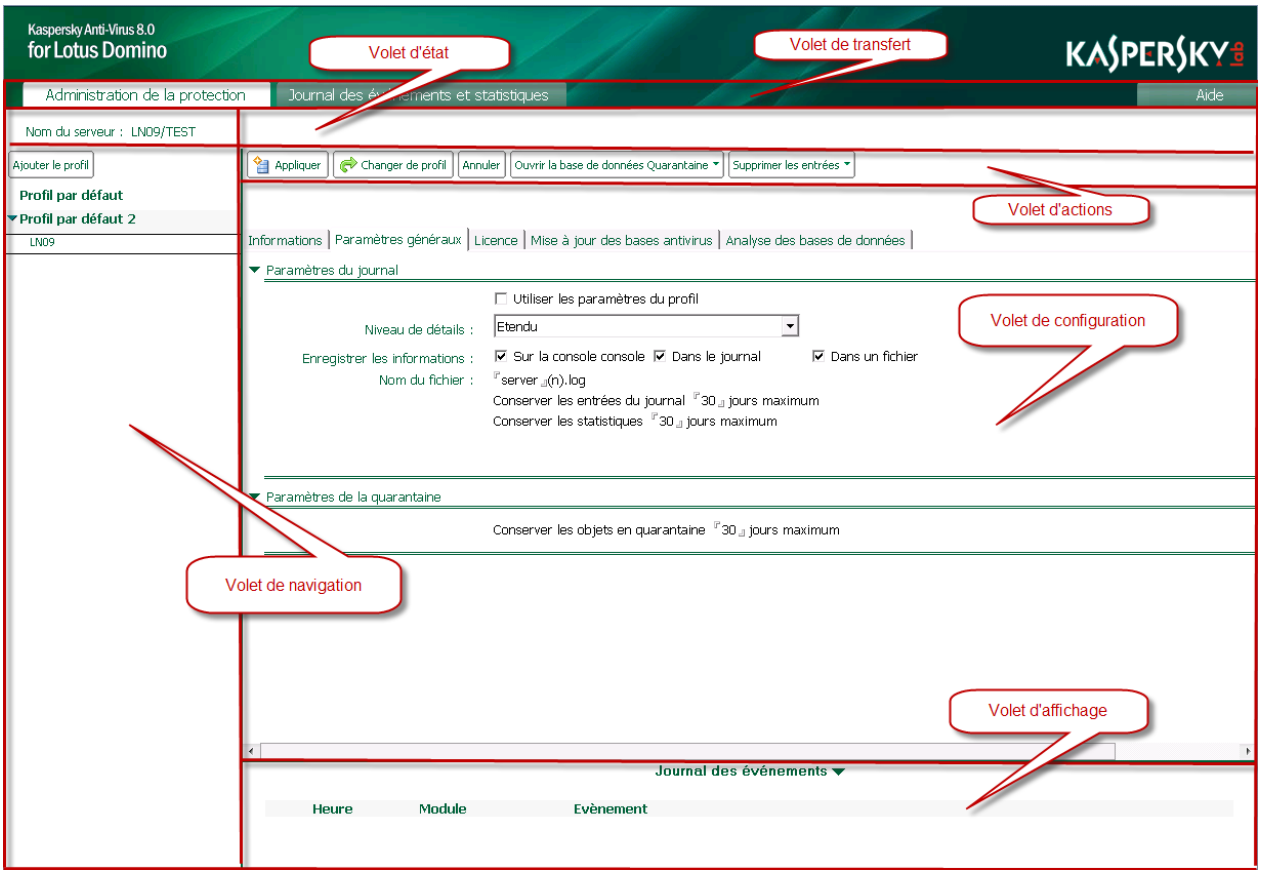


*Illustration 3. Structure de la fenêtre de la base de données Centre d'administration*

Le contenu du volet de navigation, du volet d'administration et du volet de consultation dépend de l'onglet sélectionné dans le volet de transfert.

L'accès aux éléments de l'interface utilisateur et aux champs de saisie dans la fenêtre de la base de données Centre d'administration dépend des privilèges de l'utilisateur.

# ONGLET ADMINISTRATION DE LA PROTECTION

L'onglet **Administration de la protection** du volet de transfert est destiné à une utilisation avec la base de données Centre d'administration :

- configuration des paramètres d'utilisation de Kaspersky Anti-Virus sur les serveurs protégés ;
- configuration des paramètres de la protection antivirus (protection de la messagerie, protection des réplications, analyse des bases de données, mise à jour des bases antivirus, etc.).

Sous l'onglet **Administration de la protection**, le volet de navigation contient la liste des profils et de leurs serveurs.

Dans le volet de navigation, la liste des serveurs repris dans un profil peut être réduite. Pour déployer la liste des serveurs, cliquez ▸ sur l'icône située à gauche du nom du profil.

Le bouton **Ajouter un profil**, prévu pour la création d'un profil (cf. section "Création et suppression de profils" à la page 87) apparaît dans la partie supérieure du volet de navigation.

Quand un profil a été sélectionné dans le volet de navigation, les onglets suivants contenant les paramètres du profil (cf. ill. ci-après) apparaissent dans le volet d'administration :

- **Informations**. L'onglet contient le nom du profil et la liste des serveurs repris dans le profil.
- **Paramètres généraux**. L'onglet reprend le nom de l'administrateur/du groupe d'administrateurs du profil, les paramètres de performances de l'application (cf. section "Configuration des paramètres de performances" à la page 69) et les paramètres du Journal des événements et statistiques pour les serveurs appartenant au profil (cf. section "Configuration des paramètres du journal des événements" à la page 77).
- **Protection du courrier**. L'onglet permet de configurer la protection de la messagerie pour les serveurs qui figurent dans le profil (cf. section "Protection de la messagerie" à la page 50).
- **Protection des réplications**. L'onglet permet de configurer la protection des réplications pour les serveurs qui figurent dans le profil (cf. section "Protection des réplications" à la page 56).
- **Analyse des bases de données**. L'onglet permet de configurer les paramètres de l'analyse des bases de données pour les serveurs qui figurent dans le profil (cf. section "Analyse des bases de données" à la page 61).

- **Mise à jour des bases antivirus**. L'onglet permet de configurer les paramètres de la mise à jour des bases antivirus pour les serveurs qui figurent dans le profil (cf. section "Sélection de la source des mises à jour" à la page 47).

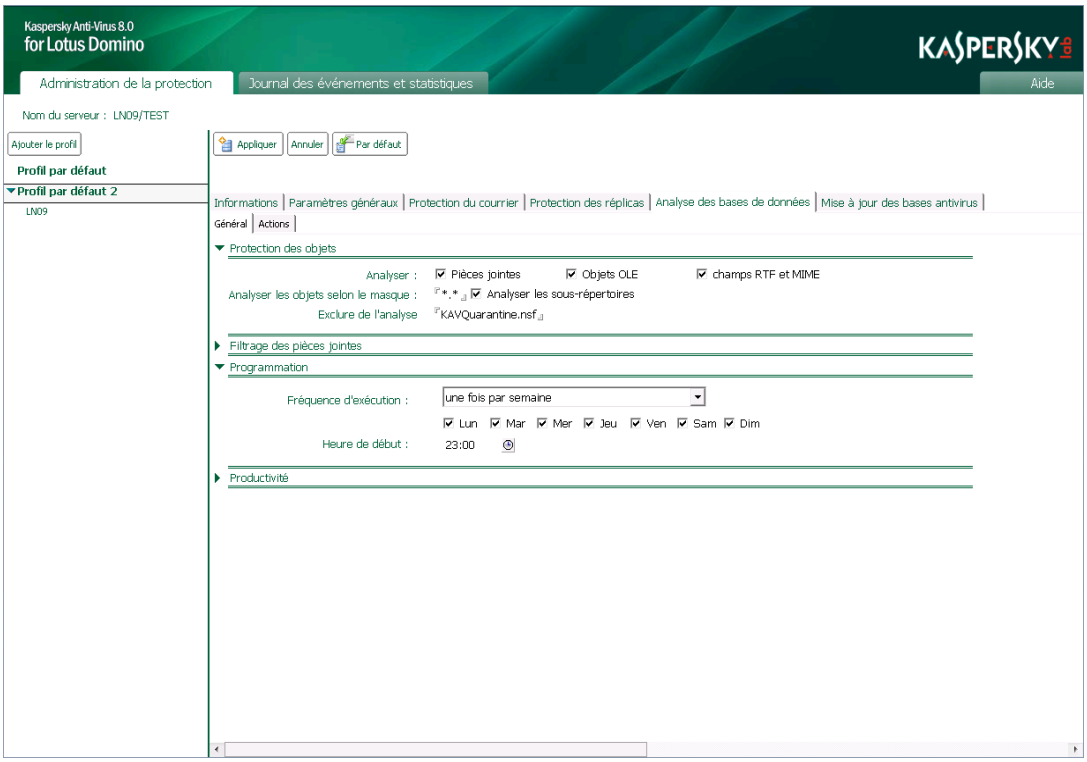


*Illustration 4. Fenêtre de la base de données Centre d'administration en mode de consultation des paramètres du profil*

Si un serveur a été sélectionné dans le volet de navigation, le volet d'administration affiche les onglets qui contiennent les paramètres du serveur, tandis que le volet de consultation affiche les entrées du Journal des événements pour ce serveur (cf. ill. ci-après).

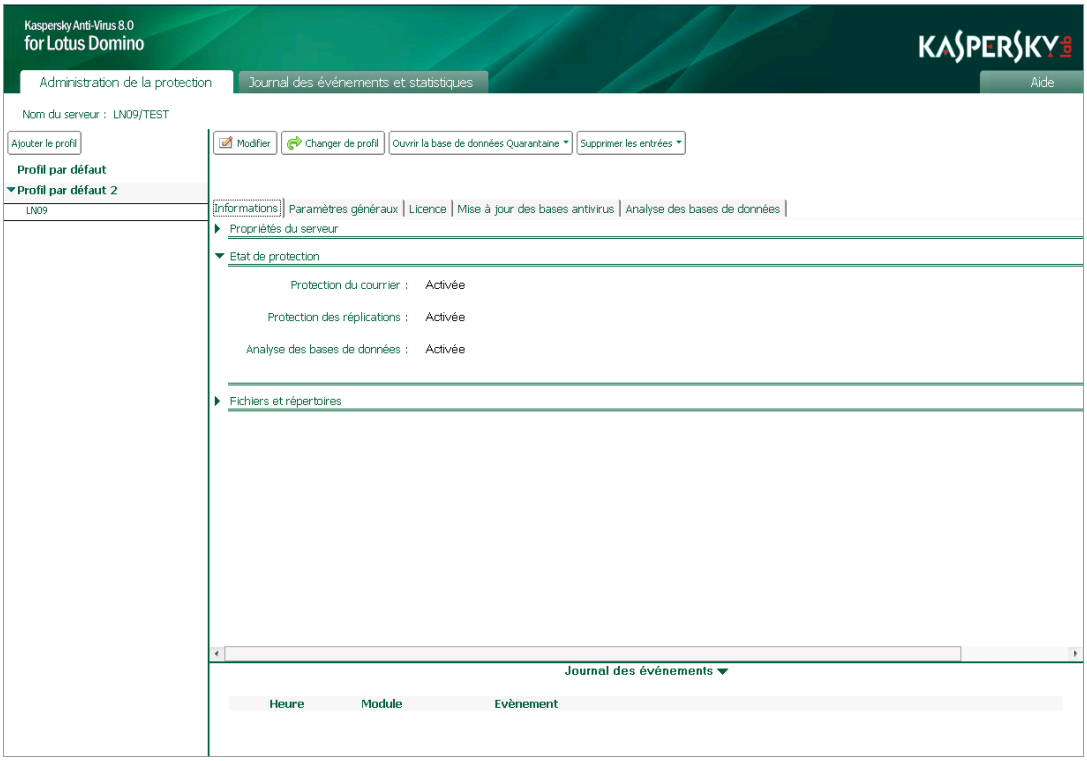


*Illustration 5. Fenêtre de la base de données Centre d'administration en mode de consultation des informations sur l'état de la protection antivirus.*

Les paramètres du serveur sont présentés dans les onglets suivants (cf. ill. ci-dessus):

- **Informations**. L'onglet affiche le nom du serveur, le nom de l'administrateur/du groupe d'administrateurs du serveur, l'état des modules de la protection (cf. section "Etat de la protection du serveur" à la page 41).
- **Paramètres généraux**. L'onglet est destiné à la configuration des paramètres de la quarantaine (cf. section "Configuration des paramètres de la quarantaine" à la page 74) ainsi que les paramètres individuels du Journal des événements et statistiques pour le serveur (cf. section "Configuration des paramètres du journal des événements" à la page 77).
- **Licence**. L'onglet permet d'administrer les clés (cf. section "Administration des licences" à la page 29).
- **Mise à jour des bases antivirus**. L'onglet permet de configurer les paramètres de la mise à jour des bases antivirus pour le serveur (cf. section "Sources des mises à jour des bases antivirus" à la page 44) et du lancement de la mise à jour (cf. section "Mise à jour manuelle" à la page 49).
- **Analyse des bases de données**. L'onglet permet de lancer l'analyse des bases de données manuellement pour le serveur (cf. section "Analyse manuelle" à la page 68).

La partie supérieure du volet d'administration contient le volet des actions où figurent les boutons. Pour modifier les paramètres du profil ou les paramètres du serveur, il est nécessaire de passer du mode de consultation des paramètres au mode de modification en cliquant sur le bouton **Modifier** dans le volet des actions. La sélection des boutons en mode de modification est différente de celle du mode de consultation.

Le tableau ci-dessous reprend les fonctions des boutons nécessaires lors de l'utilisation des paramètres du profil.

*Tableau 4. Boutons du volet des actions pour l'utilisation des paramètres du profil*

| BOUTON | FONCTION |
|---|---|
| **Modifier** | Passer au mode de modification des paramètres du profil. |
| **Appliquer** | Conserver les modifications des paramètres du profil. |
| **Annuler** | Annuler les modifications introduites. |
| **Supprimer** | Supprimer le profil. |
| **Par défaut** | Rétablir les valeurs par défaut des paramètres du profil. |

Le tableau ci-dessous reprend les fonctions des boutons nécessaires à l'utilisation des paramètres du serveur.

*Tableau 5. Boutons du volet des actions pour l'utilisation des paramètres du serveur*

| BOUTON | FONCTION |
|---|---|
| **Modifier** | Passer au mode de modification des paramètres du serveur. |
| **Appliquer** | Enregistrer les modifications des paramètres du serveur. |
| **Changer de profil** | Déplacer le serveur dans un autre profil. |
| **Annuler** | Annuler les modifications introduites. |
| **Ouvrir la base de données de la quarantaine** | Ouvrir la liste des objets placés en quarantaine suite à l'analyse des messages électroniques, des réplications ou des bases de données (cf. "section Quarantaine" à la page 71). |
| **Supprimer les entrées** | Supprimer les entrées de la quarantaine (cf. section "Actions à exécuter sur les objets placés en quarantaine" à la page 73) ou du journal des événements et statistiques pour ce serveur (cf. section "Suppression des informations de la base de données Journal des événements et statistiques" à la page 84). |

## CONSULTATION ET MODIFICATION DES PARAMETRES DU PROFIL

*Pour consulter les paramètres d'un profil, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez le profil dont vous souhaitez consulter les paramètres.

Pour passer du mode de consultation des paramètres du profil au mode de modification, cliquez sur le bouton **Modifier** situé dans le volet des actions.

## CONSULTATION ET MODIFICATION DES PARAMETRES DU SERVEUR

*Pour consulter les paramètres d'un serveur, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez le profil comportant le serveur dont vous souhaitez consulter les paramètres.
3. Sélectionnez le serveur.

La liste des serveurs repris dans un profil peut être réduite. Pour déployer la liste des serveurs, cliquez sur l'icône située à gauche du nom du profil.

Pour passer du mode de consultation des paramètres du serveur au mode de modification, cliquez sur le bouton **Modifier** situé dans le volet des actions.

# ONGLET JOURNAL DES EVENEMENTS ET STATISTIQUES

L'onglet **Journal des événements et statistiques** du volet de transfert est dédié à l'utilisation de la base de données Journal des événements et statistiques, et à la consultation des entrées suivantes :

- informations sur les événements enregistrés lors du fonctionnement de l'application sur l'ensemble des serveurs protégés ;
- statistiques sur les menaces détectées lors de l'analyse antivirus et sur les actions auxquelles elles ont été soumises (cf. section "Consultation de la base de données Journal des événements et statistiques" à la page 81).

L'onglet **Journal des événements et statistiques** du volet de navigation répertorie les sections du Journal des événements et statistiques. Les entrées du Journal des événements et statistiques s'affichent dans la partie droite de la fenêtre du volet d'administration.

# ONGLET AIDE

L'onglet **Aide** permet de consulter la base de données Aide qui comporte le système d'aide de Kaspersky Anti-Virus. Si vous choisissez l'onglet **Aide** dans le volet de transfert, un raccourci vers la base de données Aide se crée dans la zone de travail de Lotus Notes.

# LANCEMENT ET ARRET DE L'APPLICATION

Kaspersky Anti-Virus démarre automatiquement au lancement du serveur Lotus Domino. La protection antivirus est active après l'installation de Kaspersky Anti-Virus et le redémarrage du serveur.

Vous pouvez lancer ou arrêter Kaspersky Anti-Virus manuellement à partir de la console du serveur Lotus Domino, à l'aide des instructions de la ligne de commande (cf. section "Utilisation via la console du serveur" à la page 96).

# ETAT DE LA PROTECTION DU SERVEUR

La protection antivirus du serveur est assurée par les modules suivants : protection de la messagerie, protection des réplications et analyse des bases de données. Tous les composants de la protection sont activés par défaut et sont lancés automatiquement au démarrage du serveur Lotus Domino. L'analyse des bases de données est programmée par défaut une fois par mois à 00 h 00, à partir du jour d'installation.

*Pour voir quel composant est activé ou désactivé, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez consulter l'état de la protection (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet d'administration, sélectionnez l'onglet **Informations**. L'état des modules de la protection apparaît dans le groupe **Etat de la protection** (cf. ill. ci-après).

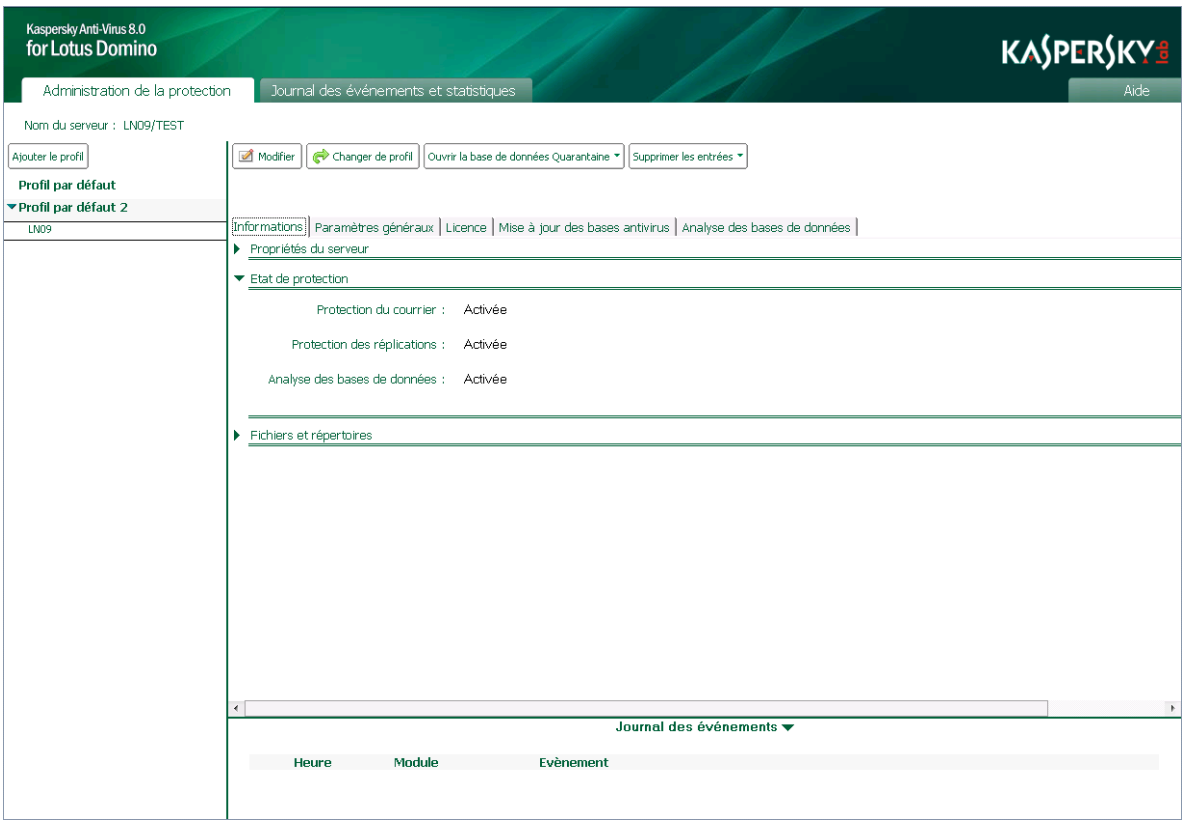


*Illustration 6. Fenêtre de la base de données Centre d'administration en mode de consultation des informations sur l'état de la protection antivirus.*

Vous pouvez activer ou désactiver n'importe quel composant de la protection.

*Pour activer ou désactiver un module de la protection, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez activer ou désactiver le module de protection (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Informations** (cf. ill. ci-dessus).

3. Dans le groupe **Etat de la protection**, sur la ligne correspondant au module souhaité, choisissez l'une des options proposées : **Activer** ou **Désactiver**.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# PROTECTION DU SERVEUR PAR DEFAUT

La protection antivirus est active après l'installation de Kaspersky Anti-Virus et le redémarrage du serveur Lotus Domino. Tous les modules de l'application et les composants de la protection sont lancés automatiquement au démarrage du serveur. Par défaut, Kaspersky Anti-Virus réalise les opérations suivantes :

- Analyse du trafic de messagerie. Les valeurs suivantes sont attribuées aux paramètres de protection de la messagerie pour l'analyse :
  - analyser le corps du message, les pièces jointes et les objets OLE ;
  - réparer les objets infectés, supprimer les objets potentiellement infectés, ignorer les objets protégés et non analysés ;
  - analyser un objet pendant 120 s maximum ;
  - analyser les objets d'une taille maximale de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
  - placer une copie de l'objet infecté ou potentiellement infecté dans la quarantaine ;
  - consigner les informations sur l'objet détecté et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
  - ajouter un message au corps du texte du courrier envoyé (cf. section "Notifications" à la page 85).
- Analyse de tous les nouveaux documents et des documents modifiés suite à la réplication. Les valeurs suivantes sont attribuées aux paramètres de protection des réplications pour l'analyse :
  - analyser les champs du document au format RTF et MIME, les fichiers joints et les objets OLE ;
  - réparer les objets infectés, supprimer les objets potentiellement infectés, ignorer les objets protégés et non analysés ;
  - analyser un objet pendant 120 s maximum ;
  - analyser les objets d'une taille maximale de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
  - placer une copie de l'objet infecté ou potentiellement infecté dans la quarantaine ;
  - consigner les informations sur l'objet détecté et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
  - envoyer un message sur les actions exécutées aux administrateurs (cf. section "Notifications" à la page 85).
- Enregistre les informations sur les événements consignés par Kaspersky Anti-Virus dans la base de données Journal des événements et statistiques et sur la console du serveur Lotus Domino (niveau de détail des informations enregistrées : standard). Les informations sur les événements et les données statistiques relatives aux résultats de l'analyse des objets sont conservés dans la base de données Journal des événements et statistiques pendant 30 jours.
- Lance la mise à jour des bases antivirus chaque jour, à chaque heure. Les serveurs de Kaspersky Lab constituent la source des mises à jour.

L'analyse des bases de données est désactivée par défaut. L'administrateur peut lancer l'analyse manuellement ou configurer son lancement programmé. Par défaut, Kaspersky Anti-Virus utilise les valeurs de paramètres suivantes pour l'analyse des bases de données :

- analyser les champs du document au format RTF et MIME, les fichiers joints et les objets OLE ;
- analyser les bases de données dans la racine du répertoire data (répertoire des données du serveur Lotus Domino) et dans tous les sous-répertoires ;
- exclure de l'analyse la base de données Quarantaine ;
- réparer les objets infectés, supprimer les objets potentiellement infectés, ignorer les objets protégés et non analysés ;
- analyser un objet pendant 120 s maximum ;
- analyser les objets d'une taille maximale de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
- placer une copie de l'objet infecté ou potentiellement infecté dans la quarantaine ;
- consigner les informations sur l'objet détecté et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
- envoyer un message sur les actions exécutées aux administrateurs (cf. section "Notifications" à la page 85).

# MISE A JOUR DES BASES

Cette section explique comment configurer les paramètres de la mise à jour des bases antivirus, aussi bien pour un serveur que pour un groupe de serveurs. Elle détaille également les sources de mise à jour qui peuvent être utilisées et le lancement de la mise à jour des bases antivirus ; manuellement et selon une programmation. Cette section offre également des informations sur le modèle de mise à jour de Kaspersky Anti-Virus dans le contexte d'une installation sur un ou plusieurs serveurs.

### DANS CETTE SECTION



## INFORMATIONS SUR LES BASES ANTIVIRUS

Kaspersky Anti-Virus recherche les programmes malveillants et répare les objets infectés à l'aide des entrées des bases antivirus. Il est nécessaire de maintenir l'actualité des bases antivirus car chaque jour voit apparaître de nouveaux virus, chevaux de Troie et autres programmes malveillants. Il est conseillé d'actualiser les bases antivirus directement après l'installation de l'application car les bases du paquet d'installation ne sont déjà plus d'actualité au moment de l'installation. Le lancement de la mise à jour des bases antivirus est réalisé séparément pour chaque serveur.

Les bases antivirus sont actualisées toutes les heures sur les serveurs de mises à jour de Kaspersky Lab. Les paramètres du serveur, sous l'onglet **Mise à jour des bases antivirus**, contiennent des informations sur l'actualité des bases antivirus.

*Pour obtenir des informations sur les bases antivirus utilisées par Kaspersky Anti-Virus, procédez comme suit :*

1. sélectionnez le serveur pour lequel vous souhaitez consulter des informations (cf. section "Consultation et modification des paramètres du serveur" à la page 39).
2. Dans le volet d'administration, choisissez l'onglet **Mise à jour des bases antivirus**.

Les informations relatives aux bases antivirus utilisées sont reprises dans la partie supérieure de l'onglet.

## SOURCE DE LA MISE A JOUR DES BASES ANTIVIRUS

*La source des mises à jour* est une ressource qui contient les mises à jour des bases antivirus de Kaspersky Anti-Virus. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Kaspersky Anti-Virus copie les mises à jour des bases antivirus via Internet depuis les serveurs de mise à jour de Kaspersky Lab, depuis un serveur HTTP ou FTP, ou depuis une ressource de réseau définie par l'administrateur. Les mises à jour récupérées sont placées sur le serveur dans le répertoire de service kavcommon\updater (kavcommon/updater pour Linux). Ce répertoire est créé à l'installation de l'application et se trouve à l'adresse suivante :

- pour les systèmes d'exploitation Microsoft Windows : dans le répertoire des fichiers binaires Lotus Domino (chemin d'accès par défaut : C:\Program Files\IBM\Lotus\Domino) ;
- pour les systèmes d'exploitation Linux : dans le répertoire des données du serveur Lotus Domino (chemin d'accès par défaut : /local/notesdata).

Les mises à jour récupérées par l'un des serveurs peuvent être utilisées pour la mise à jour de la version de Kaspersky Anti-Virus sur d'autres serveurs Domino. Pour ce faire, il est nécessaire d'indiquer un répertoire de service kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux) situé sur le serveur source de mises à jour en tant que source de mises à jour, ceci à l'adresse suivante :

- pour les systèmes d'exploitation Microsoft Windows : dans le répertoire des fichiers binaires Lotus Domino (chemin d'accès par défaut : C:\Program Files\IBM\Lotus\Domino) ;
- pour les systèmes d'exploitation Linux : dans le répertoire des données du serveur Lotus Domino (chemin d'accès par défaut : /local/notesdata).

Si Kaspersky Anti-Virus est installé sur plusieurs serveurs, l'un d'entre eux peut télécharger les mises à jour via Internet, tandis que les autres peuvent contacter la ressource de réseau sur laquelle ce serveur aura copié les mises à jour récupérées (cf. section "Modèles de mise à jour des bases antivirus" à la page 45).

Lors de la mise à jour, Kaspersky Anti-Virus compare les mises à jour sur le serveur et celles sur la source de mises à jour. En cas de différences au niveau de la composition des bases, la partie manquante est copiée depuis la source des mises à jour. La copie complète des bases n'a pas lieu, ce qui permet d'augmenter la vitesse de la mise à jour et de réduire le volume du trafic réseau.

Le téléchargement des mises à jour peut être soit programmé, soit réalisé manuellement. Les informations relatives aux événements enregistrés durant l'utilisation de Kaspersky Anti-Virus lors de la mise à jour sont consignées dans la base de données Journal des événements et statistiques (cf. section "Journal des événements et statistiques" à la page 76).

Vous pouvez configurer les paramètres de la mise à jour pour quelques serveurs en utilisant un profil ou définir les paramètres pour chaque serveur séparément (cf. section "Administration des paramètres d'utilisation de Kaspersky Anti-Virus" à la page 21).

Si les serveurs de mises à jour de Kaspersky Lab vous sont inaccessibles (par exemple, en cas d'absence de connexion à Internet), contactez le Service de Support Technique de Kaspersky Lab (cf. section "Modes d'obtention du Support Technique" à la page 98, "Contacter le Support Technique" à la page 98) pour recevoir les mises à jour au format ZIP. Les mises à jour obtenues peuvent être par la suite placées sur un site FTP ou HTPP, ou dans un répertoire local ou de réseau.

# MODELES DE MISE A JOUR DES BASES ANTIVIRUS

Si Kaspersky Anti-Virus est installé uniquement sur un serveur, vous pouvez télécharger les mises à jour depuis les serveurs de mises à jour de Kaspersky Lab ou à partir d'une autre source contenant les mises à jour des bases antivirus : serveur FTP/HTTP, répertoire local ou de réseau (cf. ill. ci-dessous).

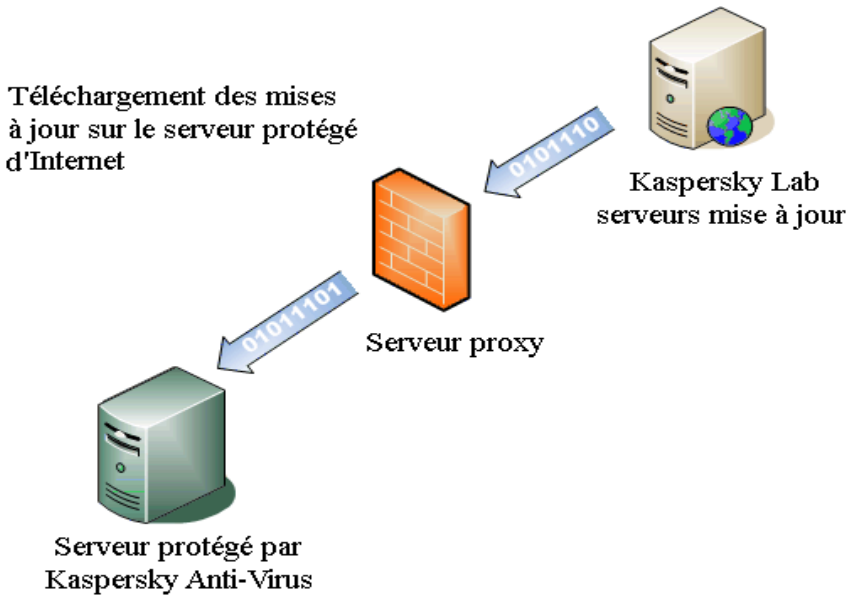


*Illustration 7. Modèle distribué de mise à jour de Kaspersky Lab*

Si Kaspersky Anti-Virus est installé sur plusieurs serveurs, vous pouvez utiliser les schémas de mise à jour suivants :

- mise à jour distribuée : les mises à jour sont téléchargées directement depuis Internet sur chaque serveur protégé (cf. ill. ci-dessus) ;
- mise à jour centralisée : les mises à jour sont téléchargées via Internet sur l'un des serveurs tandis que les autres serveurs contactent un répertoire sur le serveur où Kaspersky Anti-Virus a placé les mises à jour récupérées (cf. ill. ci-après).

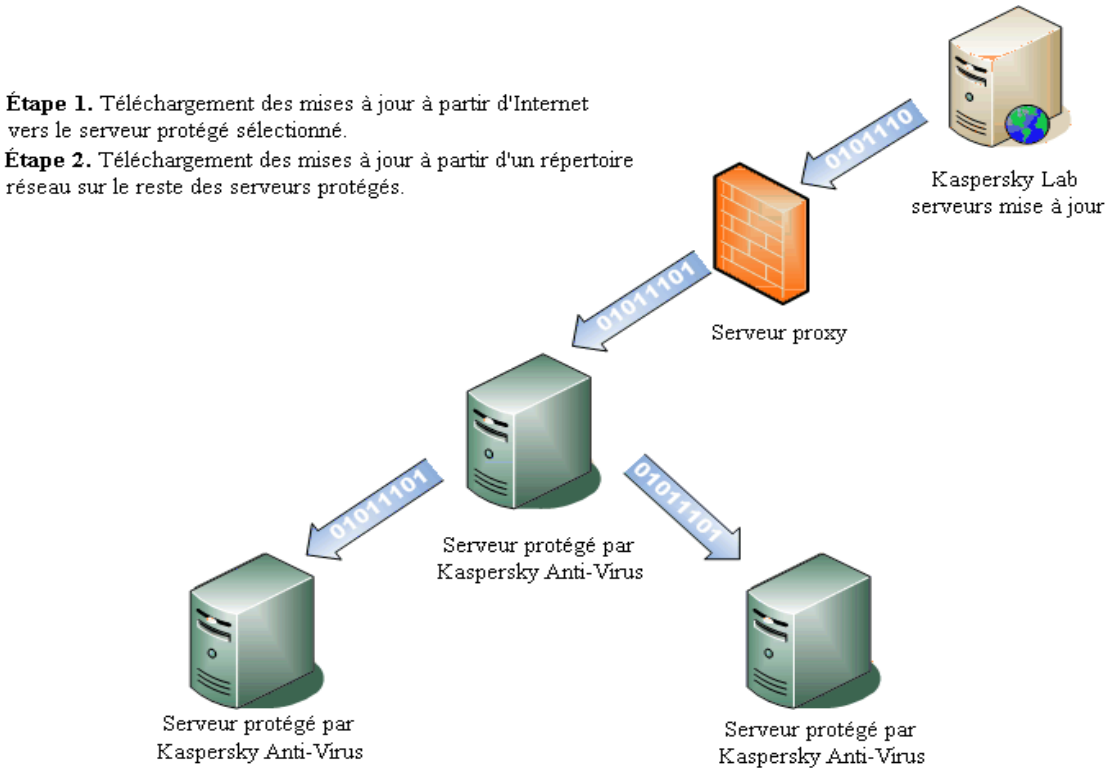


*Illustration 8. Modèle centralisé de mise à jour de Kaspersky Lab*

*Pour créer un schéma de mise à jour centralisée, procédez comme suit :*

1. Sélectionnez le serveur qui recevra les mises à jour via Internet et qui servira de source des mises à jour pour les autres serveurs. Dans les paramètres de la mise à jour pour ce serveur, désignez les serveurs de mise à jour de Kaspersky Lab en guise de source des mises à jour (cf. section "Sélection de la source des mises à jour" à la page 47).

2. Tous les serveurs qui recevront les mises à jour à partir du serveur sélectionné doivent pouvoir accéder en lecture au répertoire kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux) sur ce serveur.

3. Désignez le répertoire kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux) du serveur sélectionné en tant que source de mises à jour pour tous les serveurs qui récupèreront les mises à jour depuis ce serveur.

Pour l'utilisation d'un modèle centralisé de mise à jour, il est conseillé de définir la valeur de paramètre KAVCustomUpdUrlOnly=1 dans le fichier notes.ini (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration notes.ini" à la page 23) pour les serveurs qui recevront les mises à jour à partir du serveur sélectionné.

# SELECTION DE LA SOURCE DES MISES A JOUR

Les paramètres de la mise à jour peuvent être configurés pour un groupe de serveurs ou pour un serveur en particulier. Pour définir une source des mises à jour unique dédiée à un groupe de serveurs, utilisez les paramètres du profil. Pour définir une source des mises à jour pour un serveur distinct, utilisez les paramètres du serveur.

*Pour définir la source de mises à jour, procédez comme suit :*

1. Pour la configuration des paramètres de mise à jour, sélectionnez l'une des options suivantes :

   - Si vous configurez les paramètres de mise à jour pour un groupe de serveurs, sélectionnez le profil (cf. section "Consultation et modification des paramètres du profil" à la page 39).

   - Si vous configurez les paramètres pour un serveur en particulier, sélectionnez le serveur (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** pour passer au mode de modification des paramètres.

3. Dans le volet d'administration, choisissez l'onglet **Mise à jour des bases antivirus**.

   Si vous configurez les paramètres de la mise à jour pour un serveur, décochez la case **Utiliser les paramètres du profil** dans le groupe **Paramètres de la mise à jour**. Si la case est cochée, les paramètres de la mise à jour ne peuvent être modifiés. Si vous souhaitez utiliser les valeurs des paramètres de mises à jour définis par le profil, cochez la case **Utiliser les paramètres du profil**.

4. Désignez la source des mises à jour. Pour ce faire, sélectionnez l'un des éléments suivants dans la liste déroulante **Source des mises à jour** du groupe **Paramètres de la mise à jour** :

   - **Serveurs de mises à jour de Kaspersky Lab** : les sites de Kaspersky Lab qui hébergent les mises à jour pour toutes les applications de la société servent de source pour les mises à jour. Cette source des mises à jour est sélectionnée par défaut.

   - **Autres serveurs HTTP-FTP ou ressources de réseau** : la source des mises à jour est la ressource désignée dans le champ **Adresse URL** (dans les paramètres du profil)/ou **Adresse de la source des mises à jour** (dans les paramètres du serveur). Désignez un serveur FTP ou HTTP, ou un répertoire local ou de réseau. Le chemin d'accès à la ressource doit être conforme au format UNC (Universal Naming Convention).

     Des serveurs FTP soumis à autorisation peuvent être utilisés en tant que sources de mises à jour. Les serveurs HTTP soumis à autorisation ne peuvent en aucun cas servir de sources de mises à jour.

     Si vous souhaitez que les mises à jour soient copiées à partir d'un répertoire de services de Kaspersky Anti-Virus situé sur un autre serveur protégé, indiquez dans le champ **Adresse URL** (dans les paramètres du profil) ou dans le champ **Adresse de la source des mises à jour** (dans les paramètres du serveur) le chemin vers le répertoire kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux). Pour les systèmes d'exploitation de Windows, le chemin d'accès est relatif au répertoire des fichiers binaires du serveur Lotus Domino (par défaut : C:\Program Files\IBM\Lotus\Domino). Pour les systèmes d'exploitation Linux, le chemin d'accès au répertoire est relatif au répertoire des données du serveur Lotus Domino (/local/notesdata).

Si la mise à jour depuis la source que vous aurez désignée échoue, Kaspersky Anti-Virus se connecte à une autre source de mises à jour, à savoir la ressource à partir de laquelle la dernière mise à jour réussie a été réalisée ou le serveur de mises à jour de Kaspersky Lab. Pour que le serveur reçoive les mises à jour uniquement à partir de la source de mises à jour que vous avez indiquée, il est nécessaire de définir la valeur du paramètre KAVCustomUpdUrlOnly=1 dans le fichier de configuration notes.ini (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration notes.ini" à la page 23).

5. Configurez les paramètres du serveur proxy si la connexion à la source des mises à jour est réalisée via le serveur proxy. Pour ce faire, exécutez les actions suivantes:

   - Cochez la case **Utiliser le serveur proxy**, saisissez, dans le champ **Adresse**, l'adresse IP ou le nom symbolique du serveur proxy et dans le champ **Port**, le numéro de port du serveur proxy via lequel la connexion aura lieu.

   - Cochez la case **Utiliser l'authentification sur le serveur proxy** si la connexion au serveur proxy indiqué requiert l'authentification de l'utilisateur. Saisissez les données du compte utilisateur dans les champs **Utilisateur** et **Mot de passe**.

   Le mot de passe d'accès au serveur proxy est enregistré dans la base de données kavcontrolcenter.nsf. Il est connu de l'utilisateur disposant d'un accès à cette base. Ainsi, il n'est recommandé d'accorder un accès à la base de données kavcontrolcenter.nsf aux utilisateurs qu'en cas de besoin, et de surveiller cet accès. Il est conseillé de modifier le mot de passe d'accès au serveur proxy lorsqu'un utilisateur disposant d'un accès à la base de données kavcontrolcenter.nsf quitte l'entreprise.

6. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Si vous configurez les paramètres de mises à jour pour un groupe de serveurs, vous pouvez rétablir les valeurs de paramètres par défaut (cf. section "Protection du serveur par défaut" à la page 42). Pour ce faire, cliquez sur **Par défaut**.

# MISE A JOUR PROGRAMMEE

Kaspersky Anti-Virus exécute la mise à jour des bases antivirus selon une programmation. Vous pouvez configurer la programmation de la même manière pour un groupe de serveurs via le profil ou utiliser les paramètres du serveur afin de définir des valeurs individuelles pour chaque serveur.

*Pour configurer la programmation de la mise à jour pour un serveur ou un groupe de serveurs, procédez comme suit :*

1. Pour la configuration des paramètres de mise à jour, sélectionnez l'une des options suivantes :

   - Si vous configurez les paramètres de mise à jour pour un groupe de serveurs, sélectionnez le profil (cf. section "Consultation et modification des paramètres du profil" à la page 39).

   - Si vous configurez les paramètres pour un serveur en particulier, sélectionnez le serveur (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** pour passer au mode de modification des paramètres.

3. Dans le volet d'administration, choisissez l'onglet **Mise à jour des bases antivirus**.

   Si vous configurez les paramètres de la mise à jour pour un serveur, décochez la case **Utiliser les paramètres du profil** dans le groupe **Paramètres de la mise à jour**. Si la case est cochée, les paramètres de la mise à jour ne peuvent être modifiés. Si vous souhaitez utiliser les valeurs des paramètres de mises à jour définis par le profil, cochez la case **Utiliser les paramètres du profil**.

4. Dans le groupe **Programmation** (cf. ill. ci-dessus) choisissez l'un des éléments suivants dans la liste déroulante **Fréquence d'exécution** :

   - **Tous les jours** : la mise à jour a lieu tous les jours à l'heure définie. La première exécution a lieu par défaut à 00 h 00.

   - **Une fois par mois** : la mise à jour a lieu une fois par mois, le jour indiqué et à l'heure indiquée dans le champ **Heure de lancement**. Pour définir l'heure de lancement de la mise à jour, saisissez la valeur souhaitée dans le champ **Heure de lancement** au format `HH:MM`.

     Si le nombre de jours dans le mois est inférieur à la valeur définie, la mise jour a lieu le dernier jour du mois.

- **Une fois par semaine** : la mise à jour a lieu chaque semaine, au jour défini et à l'heure indiquée dans le champ **Heure de lancement**. Pour programmer le lancement de la mise à jour, cochez les cases en regard des jours où la mise à jour sera lancée et saisissez la valeur souhaitée dans le champ **Heure de lancement** au format `HH:MM`.

- **Manuellement** : la mise à jour programmée n'aura pas lieu. Vous pouvez lancer la mise à jour pour un serveur en particulier en cliquant sur le lien **Lancer la mise à jour** (cf. section "**Mise à jour manuelle**" à la page 49) ou via la ligne de commande de la console du serveur Lotus Domino (cf. section "Utilisation via la console du serveur" à la page 96). Le lancement manuel des mises à jour n'est pas prévu pour un groupe de serveurs.

5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Si vous configurez les paramètres de la mise à jour pour un groupe de serveur, vous pouvez restaurer la valeur des paramètres par défaut. Pour ce faire, cliquez sur **Par défaut**.

# MISE A JOUR MANUELLE

Il est possible de lancer manuellement la mise à jour pour un serveur uniquement. Ce mode de mise à jour n'est pas prévu pour un groupe de serveurs.

*Pour lancer la mise à jour manuelle des bases antivirus, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez lancer la mise à jour des bases antivirus (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet d'administration, choisissez l'onglet **Mise à jour des bases antivirus**. L'onglet reprend les informations sur la date et l'heure de la mise à jour précédente et de la mise à jour suivante, conformément à la programmation. La console Lotus Domino permet de suivre la progression de la mise à jour.

3. Cliquez sur le lien **Lancer la mise à jour** pour lancer la mise à jour des bases antivirus du serveur.

La mise à jour des bases antivirus peut également être lancée manuellement depuis la ligne de commande de la console du serveur Lotus Domino (cf. section "Utilisation via la console du serveur" à la page 96).

# PROTECTION DU COURRIER

Cette section explique comment activer ou désactiver la protection de la messagerie pour le serveur Lotus Domino, comment sélectionner les objets des messages à analyser, comment configurer le filtrage des pièces jointes et comment configurer le traitement des objets des messages en fonction des résultats de l'analyse.

### DANS CETTE SECTION



# ALGORITHME DE PROTECTION DU COURRIER

Si la protection antivirus du courrier est activée (cf. section "Activation et désactivation de la protection du courrier" à la page 51), Kaspersky Anti-Virus analyse et traite tous les messages du courrier entrant, sortant ou en transit qui arrivent sur le serveur Lotus Domino.

La remise des messages est ralentie par l'analyse et le traitement. Les messages sont scindés entre leurs parties constitutives : corps du message, pièces jointes et objets OLE. Ensuite, les pièces jointes sont filtrées selon la taille et (ou) selon le nom des fichiers (cf. section "Algorithme de filtrage des pièces jointes" à la page 19) et l'analyse antivirus des objets (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 20) a lieu.

Dans le cadre de l'analyse des messages électroniques du serveur Lotus Domino, Kaspersky Anti-Virus utilise la tâche kavmonitor. Si la tâche kavmonitor est arrêtée (n'est pas lancée), l'analyse antivirus de la messagerie n'a pas lieu. Les messages électroniques non analysés ne sont pas remis aux utilisateurs. Ces messages s'accumulent dans la base de données mail.box. Pour que le courrier soit remis aux destinataires, le lancement de la tâche kavmonitor est requis.

Les messages infectés, potentiellement infectés et non analysés à cause d'un échec ou en raison de dégâts découverts suite à l'analyse sont traités conformément aux paramètres de la protection du courrier (cf. section "Actions à exécuter sur les objets du courrier" à la page 52). Un traitement particulier peut être réservé aux pièces jointes dont la taille dépasse la valeur définie et/ou dont le nom correspond au masque de nom de fichier défini (cf. section "Filtrage des pièces jointes du courrier" à la page 54).

Après l'installation de l'application, ce sont les valeurs de protection de la messagerie par défaut qui sont utilisées (cf. section "Protection du serveur par défaut" à la page 42). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Lotus Domino protégé. Une partie des paramètres cités ici est désactivée par défaut ou peut être désactivée par l'administrateur.

Avant le traitement du message, une copie est placée par défaut en quarantaine (cf. page 71).

La confirmation de l'analyse par Kaspersky Anti-Virus et la description des actions exécutées sont ajoutées à l'objet et au corps du message. Les notifications relatives aux actions exécutées pendant le traitement du courrier sont envoyées à l'expéditeur et aux destinataires du message, ainsi qu'aux administrateurs (cf. section "Notifications" à la page 85). Les informations relatives aux résultats de l'analyse et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques (cf. section "Journal des événements et statistiques" à la page 76).

Après l'analyse et le traitement des objets, le message est transmis au système Lotus Domino pour la remise.

Vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et des corps de texte (cf. section "Sélection des objets pour la protection du courrier" à la page 52). Vous pouvez limiter la durée d'analyse d'un objet afin d'accélérer la vitesse globale d'analyse des messages (cf. section "Configuration des paramètres de performances" à la page 69).

Les objets dont la taille ne dépasse pas la valeur définie peuvent être analysés dans la mémoire vive du serveur, sans enregistrement sur le disque dur (cf. section "Configuration des paramètres de performances" à la page 69).

Les paramètres de la protection du courrier sont définis par le profil auquel appartient le serveur protégé. La configuration de paramètres individuels de la protection du courrier pour chaque serveur n'est pas prévue. Toutefois, la protection du courrier peut être désactivée (activée) uniquement pour chaque serveur pris séparément (cf. section "Activation et désactivation de la protection du courrier" à la page 51).

N'oubliez pas les restrictions suivantes dans l'utilisation de la protection du courrier :

- Il est impossible de détecter les menaces dans les messages chiffrés par une clé ouverte du destinataire.
- Dans les messages signés par l'expéditeur, l'intégrité de la signature électronique est violée par l'ajout de messages du rapport d'analyse ou lors du remplacement des fichiers joints comportant des menaces par des fichiers réparés.

# ACTIVATION ET DESACTIVATION DE LA PROTECTION DU COURRIER

La protection du courrier est activée par défaut et elle est lancée au démarrage du serveur Lotus Domino. Les informations relatives au lancement des modules chargés de la protection du courrier sont consignées dans le journal des événements de Kaspersky Anti-Virus.

*Pour activer ou désactiver la protection du courrier, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez activer ou désactiver le module de protection du courrier (cf. section "Consultation et modification des paramètres du serveur" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Informations** (cf. ill. ci-dessous).

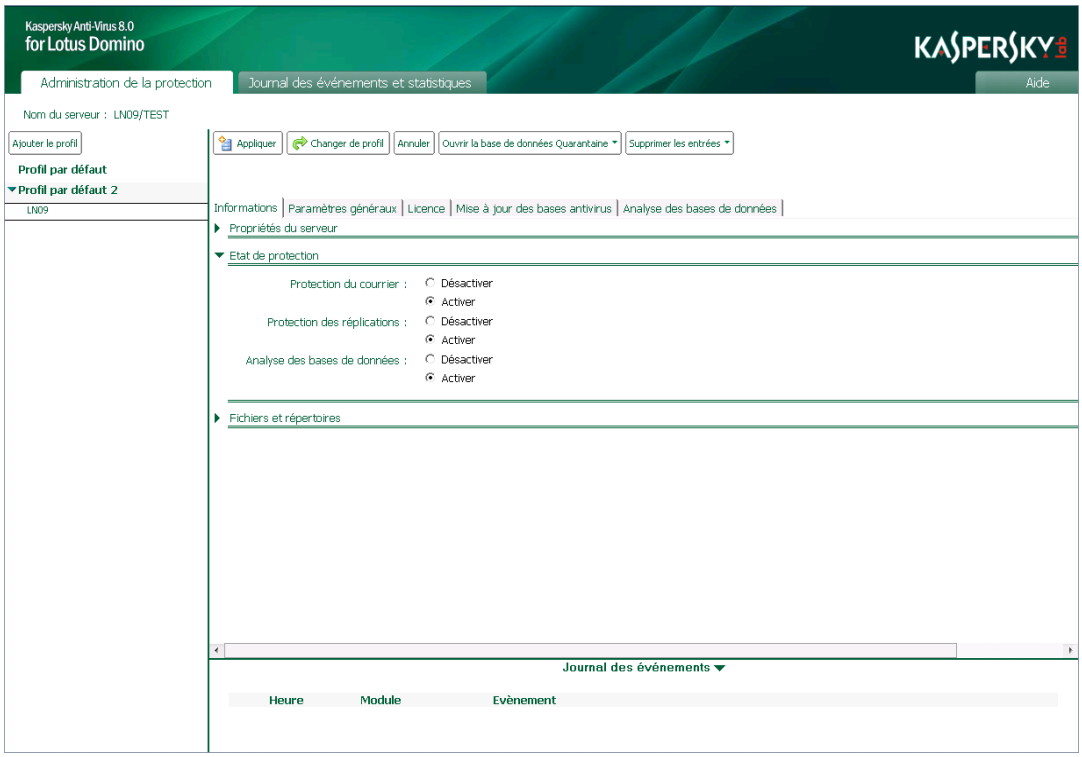


*Illustration 9. Activation/désactivation de la protection du courrier*

3. Dans le groupe **Etat de la protection**, sur la ligne **Protection du courrier** (cf. ill. ci-dessus), choisissez l'option : **Activer** ou **Désactiver**.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# SELECTION DES OBJETS POUR LA PROTECTION DU COURRIER

Par défaut, si la protection antivirus du courrier est activée, Kaspersky Anti-Virus analyse le corps du message, tous les fichiers joints de n'importe quel format et les objets OLE intégrés. Le cas échéant, vous pouvez désactiver l'analyse des objets cités.

Lors de l'analyse d'archives multi-volumes, chaque volume est traité par Kaspersky Anti-Virus comme un objet séparé. Le code malveillant sera découvert uniquement s'il est contenu entièrement dans l'un des volumes. Si le code est scindé en plusieurs parties sur différents volumes, il ne sera pas découvert pendant l'analyse. C'est la raison pour laquelle il est conseillé d'analyser les archives multi-volumes après l'enregistrement sur le disque à l'aide de l'antivirus de fichiers installé sur l'ordinateur.

*Pour sélectionner les objets de la protection du courrier, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection du courrier** → **Général**.

3. Dans le groupe **Protection des objets**, sélectionnez les objets à analyser. Pour ce faire, cochez les cases suivantes :

   - **Pièces jointes**. Kaspersky Anti-Virus analyse tout fichier joint au message.
   - **Objets OLE**. Kaspersky Anti-Virus analyse tous les objets OLE intégrés au message.
   - **Texte du message**. Kaspersky Anti-Virus analyse le corps du texte du message.

   Si la case n'est pas cochée, l'analyse des objets correspondants n'a pas lieu.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ACTIONS A EXECUTER SUR LES OBJETS DU COURRIER

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus et suite au filtrage des pièces jointes (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21). Les objets sains sont transmis sans aucune modification au système de messagerie. L'administrateur peut configurer les actions sur les objets infectés, potentiellement infectés, non analysés et protégés. Les actions qui seront exécutées par l'application sont définies pour chaque état d'objet.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme infecté, Kaspersky Anti-Virus le répare et le transmet au système de messagerie.
- Si l'objet est considéré comme potentiellement infecté, Kaspersky Anti-Virus le supprime du message.
- Si l'analyse de l'objet a échoué (par exemple, le temps dédié à l'analyse s'est écoulé) ou que l'objet est une archive protégée par un mot de passe, Kaspersky Anti-Virus ignore cet objet.

Par défaut, une copie de l'objet est placée dans la base de données Quarantaine avant la réparation ou la suppression. Les informations relatives aux objets détectés et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques (à la page 76).

Après l'analyse antivirus de chaque objet du courrier et l'exécution des actions nécessaires, l'une ou plusieurs des actions suivantes peut/peuvent être exécutée(s) sur l'ensemble du courrier :

- ajout d'informations complémentaires à l'objet ou au corps du message ;
- rédaction et remise d'une notification à l'expéditeur, aux destinataires et à l'administrateur (option désactivée par défaut) ;
- placement de l'ensemble du courrier sortant dans la base de données Quarantaine si un objet infecté ou potentiellement infecté y a été détecté.

# CONFIGURATION DES ACTIONS A EXECUTER SUR LES OBJETS DU COURRIER

*Pour configurer les actions à exécuter sur les objets du courrier, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection du courrier** → **Actions**.
3. Sous l'onglet **Actions**, sélectionnez le groupe de paramètres correspondant à l'état de l'objet dont vous souhaitez configurer le traitement. Vous pouvez choisir parmi les groupes de paramètres suivants :
   - **Objet infecté** : configuration des paramètres de traitement des objets infectés.
   - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
   - **Objet protégé** : configuration des paramètres de traitement des objets protégés.
   - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.
4. Sélectionnez l'action à exécuter sur les objets détectés. Vous pouvez ainsi sélectionner l'option **Réparer**, **Ignorer** ou **Supprimer** et cocher les cases suivantes :
   - **Placer en quarantaine** : avant le traitement, une copie de l'objet est placée dans la base de données Quarantaine.
   - **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées aux emplacements définis dans le groupe **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs emplacements de consignation des données sont sélectionnés, l'enregistrement s'exécute en une seule fois à tous les emplacements indiqués :
     - **Sur la console** (journal système Domino log.nsf) ;
     - **Dans le journal** ;
     - **Dans le fichier** (nom du fichier par défaut : server(N).log, où N est le numéro de séquence du fichier journal).
5. Configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. section "Notifications" à la page 85).
6. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

*Pour configurer les actions qui seront exécutées par Kaspersky Anti-Virus après l'analyse du message et de tous ses composants, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection du courrier** → **Avancé**.

3. L'onglet **Avancé** vous permet de sélectionner l'action que Kaspersky Anti-Virus exécutera après l'analyse du message et de tous ses objets. Pour ce faire, cochez la case **Ajouter un tag à l'objet du message**.

   Kaspersky Anti-Virus ajoute le texte indiqué dans le champ **Tag du message** à l'objet du courrier analysé. Par défaut, le champ **Note du message** contient la valeur **Analysé par Kaspersky Anti-Virus for Lotus Domino**.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# CONFIGURATION DU FILTRAGE DES PIECES JOINTES DANS LE COURRIER

Kaspersky Anti-Virus peut filtrer les objets joints aux messages (cf. section "Algorithme de filtrage des pièces jointes" à la page 19). Le filtrage permet d'exclure de l'analyse antivirus les objets qui répondent aux critères du filtre et de définir pour eux un traitement spécial. Le filtrage des pièces jointes est désactivé par défaut.

*Pour configurer les paramètres du filtrage des pièces jointes, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection du courrier** → **Général**.

3. Dans le groupe **Filtrage des pièces jointes** (cf. ill. ci-dessus), vous pouvez configurer les paramètres de filtrage des objets joints au courrier. Pour ce faire, cochez les cases suivantes et définissez les valeurs des paramètres correspondants :

   - **Filtre selon la taille**. Cochez cette case afin que Kaspersky Anti-Virus vérifie la taille des objets joints au message. Dans le champ **Ne pas analyser les objets dont la taille dépasse**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera filtré et exclu de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour l'objet est *non analysé*.

   - **Filtre selon le nom**. Cochez cette case afin que Kaspersky Anti-Virus vérifie le nom des objets joints au message. Dans le champ **Ne pas analyser les objets selon le masque**, définissez les masques de nom de fichiers qui seront filtrés et exclus de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour l'objet est *non analysé*.

   Le filtrage selon le nom tient compte de la casse dans le nom du fichier.

Vous pouvez désigner plusieurs masques de noms de fichiers et les séparer par "**;**". Utilisez les caractères suivants dans les masques :

- * : n'importe quelle séquence de caractères. Par exemple, si vous saisissez le masque abc*, aucun fichier dont le nom commence par abc, par exemple abc.exe, abc1.com ou abc2.rar, n'est analysé.

- ? : n'importe quel caractère unique. Par exemple, si vous saisissez le masque abc?.exe, aucun fichier dont le nom commence par abc suivi de n'importe quel caractère, par exemple abc1.exe, n'est analysé. Par contre, le fichier abc12345.exe sera analysé.

Si les cases **Filtre selon la taille** et **Filtre selon le nom** ne sont pas cochées, le filtrage des objets correspondants ne s'exécute pas.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# PROTECTION DES REPLICATIONS

Cette section explique comment activer ou désactiver la protection des réplications, comment choisir les objets des réplications à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des réplications en fonction des résultats de l'analyse.

### DANS CETTE SECTION



# ALGORITHME DE PROTECTION DES REPLICATIONS

Si la protection antivirus des réplications est activée (cf. section "Activation et désactivation de la protection des réplications" à la page 57), Kaspersky Anti-Virus analyse les documents modifiés au moment de la réplication. Le contenu des champs du document au format Rich Texte et MIME, les fichiers inclus dans le document et les objets OLE intégrés sont soumis à la recherche d'éventuelles menaces. Les réplications sortantes ne sont pas analysées.

Les objets infectés, potentiellement infectés, protégés et non analysés à cause d'un échec ou en raison de dommages suite à l'analyse sont traités conformément aux paramètres de la protection des réplications (cf. section "Actions à exécuter sur les objets en mode de protection des réplications" à la page 58).

Après l'installation de l'application, ce sont les valeurs de protection des réplications par défaut qui sont utilisées (cf. section "Protection du serveur par défaut" à la page 42). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Lotus Domino protégé.

Un traitement particulier peut être réservé aux pièces jointes dont la taille dépasse la valeur définie et/ou dont le nom correspond au masque de nom de fichier indiqué (cf. section "Configuration du filtrage des pièces jointes en mode de protection des réplications" à la page 60).

Avant le traitement de l'objet, une copie est placée par défaut en quarantaine (cf. page 71). Le document auquel appartient l'objet dangereux n'est pas mis en quarantaine.

La notification sur l'analyse du document par Kaspersky Anti-Virus et la description des actions exécutées sont envoyées aux administrateurs (cf. section "Notifications" à la page 85). Les informations relatives aux résultats de l'analyse et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques (cf. section "Journal des événements et statistiques" à la page 76).

Vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et du contenu des champs RTF et MIME (cf. section "Sélection des objets pour la protection des réplications" à la page 58). Pour augmenter la vitesse globale de l'analyse des réplications, vous pouvez limiter le temps d'analyse par objet (cf. section "Configuration des paramètres de performances" à la page 69). Si la taille de l'objet ne dépasse pas la valeur définie, il est analysé dans la mémoire vive du serveur, sans enregistrement sur le disque dur.

Les paramètres de la protection des réplications sont définis par le profil auquel appartient le serveur protégé. La configuration de paramètres individuels de la protection des réplications pour chaque serveur n'est pas prévue. Toutefois, la protection des réplications peut être désactivée (activée) uniquement pour chaque serveur pris séparément (cf. section "Activation et désactivation de la protection des réplications" à la page 57). L'activation et la désactivation de la protection des réplications pour les groupes de serveurs ne sont pas prévues.

# ACTIVATION/DESACTIVATION DE LA PROTECTION DES REPLICATIONS

La protection des réplications est activée par défaut et elle est lancée au démarrage du serveur Lotus Domino. Les informations relatives au lancement des modules chargés de la protection des réplications sont consignées dans le journal des événements de Kaspersky Anti-Virus.

Le cas échéant, vous pouvez activer et désactiver la protection des réplications. Cette opération est réalisée séparément pour chaque serveur.

*Pour activer ou désactiver la protection des réplications, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez activer ou désactiver le module de protection des réplications (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Informations** (cf. ill. ci-dessous).

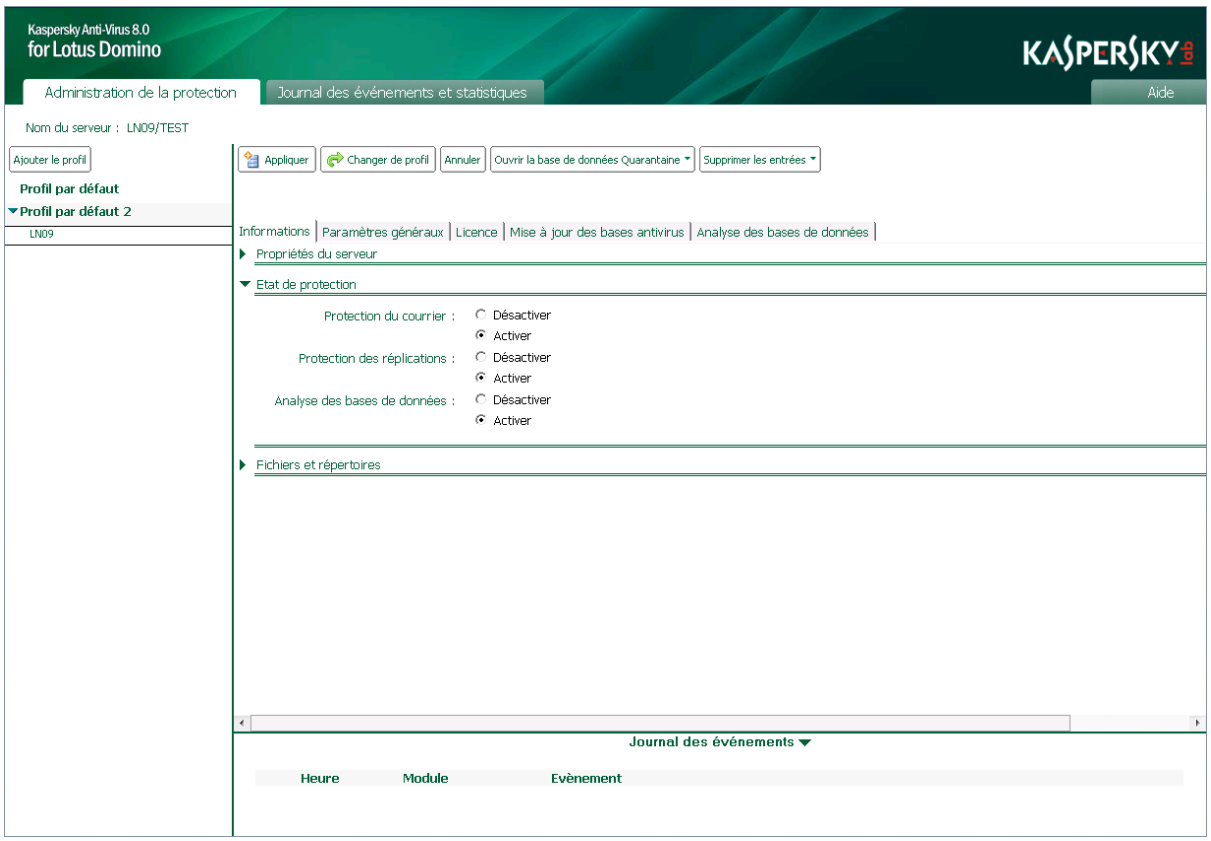


*Illustration 10. Activation/désactivation de la protection des réplications*

3. Dans le groupe **Etat de la protection**, sur la ligne **Protection des réplications** (cf. ill. ci-dessus), choisissez l'option **Activer** ou **Désactiver**.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# SELECTION DES OBJETS DE LA PROTECTION DES REPLICATIONS

Par défaut, si la protection antivirus des réplications est activée, Kaspersky Anti-Virus analyse le contenu des champs du document modifié au format Rich Text et MIME, tous les fichiers joints de n'importe quel format et les objets OLE intégrés. Le cas échéant, vous pouvez désactiver l'analyse des objets cités.

Lors de l'analyse d'archives multi-volumes, chaque volume est traité par Kaspersky Anti-Virus comme un objet séparé. Le code malveillant sera découvert uniquement s'il est contenu entièrement dans l'un des volumes. Si le code est scindé en plusieurs parties sur différents volumes, il ne sera pas découvert pendant l'analyse. C'est la raison pour laquelle il est conseillé d'analyser les archives multi-volumes après l'enregistrement sur le disque à l'aide de l'antivirus de fichiers installé sur l'ordinateur.

*Pour sélectionner les objets de la protection des réplications, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection des réplications** → **Général**.

3. Dans le groupe **Protection des objets**, sélectionnez les objets à analyser. Pour ce faire, cochez les cases suivantes :

   - **Pièces jointes**. Kaspersky Anti-Virus analyse tout fichier joint au document.
   - **Objets OLE**. Kaspersky Anti-Virus analyse tous les objets OLE intégrés au document.
   - **Champs RTF et MIME**. Kaspersky Anti-Virus analyse les champs du document aux formats Rich Text et MIME.

   Si la case n'est pas cochée, l'analyse des objets correspondants n'a pas lieu.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ACTIONS A EXECUTER SUR LES OBJETS LORS DU FONCTIONNEMENT DE LA PROTECTION DES REPLICATIONS

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus et suite au filtrage des pièces jointes (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21). Les objets sains restent dans le document sans aucune modification. L'administrateur peut configurer les actions sur les objets infectés, potentiellement infectés, non analysés et protégés. Les actions qui seront exécutées par l'application sont définies pour chaque état d'objet.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme infecté, Kaspersky Anti-Virus le répare. L'objet réparé est conservé dans le document à l'adresse d'origine.
- Si l'objet est considéré comme potentiellement infecté, Kaspersky Anti-Virus le supprime du document.
- Si l'analyse de l'objet a échoué (par exemple, le temps dédié à l'analyse s'est écoulé) ou que l'objet est une archive protégée par un mot de passe, Kaspersky Anti-Virus ignore cet objet.

Par défaut, une copie de l'objet est placée dans la base de données Quarantaine avant la réparation ou la suppression (cf. page 71). Les informations sur les objets découverts et les actions exécutées peuvent être envoyées aux administrateurs (cf. section "Notifications" à la page 85) et conservées dans la base de données Journal des événements et statistiques (à la page 76).

# CONFIGURATION DES ACTIONS A EXECUTER SUR LES OBJETS LORS DU FONCTIONNEMENT DE LA PROTECTION DES REPLICATIONS

*Pour configurer les actions à exécuter sur les objets en mode de protection des réplications, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection des réplications** → **Actions**.

3. Sous l'onglet **Actions**, sélectionnez le groupe de paramètres correspondant à l'état de l'objet dont vous souhaitez configurer le traitement. Vous pouvez choisir parmi les groupes de paramètres suivants :

   - **Objet infecté** : configuration des paramètres de traitement des objets infectés.
   - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
   - Objet **protégé** : configuration des paramètres de traitement des objets protégés.
   - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.

4. Sélectionnez l'action à exécuter sur les objets détectés. Vous pouvez ainsi sélectionner l'option **Réparer**, **Ignorer** ou **Supprimer** et cocher les cases suivantes :

   - **Placer en quarantaine** : avant le traitement, une copie de l'objet est placée dans la base de données Quarantaine.
   - **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées aux emplacements définis dans le champ **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs emplacements de consignation des données sont sélectionnés en même temps, l'enregistrement s'exécute en une seule fois à tous les emplacements indiqués :
     - **Sur la console** (journal système Domino log.nsf) ;
     - **Dans le journal** ;
     - **Dans le fichier** (nom du fichier par défaut : server(N).log, où N est le numéro de séquence du fichier journal).

5. Configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. section "Notifications" à la page 85).

6. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# CONFIGURATION DU FILTRAGE DES PIECES JOINTES LORS DU FONCTIONNEMENT DE LA PROTECTION DES REPLICATIONS

Kaspersky Anti-Virus peut filtrer les objets joints aux documents (cf. section "Algorithme de filtrage des pièces jointes" à la page 19). Le filtrage permet d'exclure de l'analyse antivirus les objets qui répondent aux critères du filtre et de définir pour eux un traitement spécial. Le filtrage des pièces jointes est désactivé par défaut.

*Pour configurer les paramètres de filtrage des pièces jointes en mode de protection des réplications, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Protection des réplications** → **Général**.

3. Dans le groupe **Filtrage des pièces jointes**, vous pouvez configurer les paramètres de filtrage des objets joints au document. Pour ce faire, cochez les cases suivantes et définissez les valeurs des paramètres correspondants :

   - **Filtre selon la taille**. Cochez cette case afin que Kaspersky Anti-Virus vérifie la taille des objets joints au document. Dans le champ **Ne pas analyser les objets dont la taille dépasse**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera exclu de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour cet objet est *non analysé*.

   - **Filtre selon le nom**. Cochez cette case afin que Kaspersky Anti-Virus vérifie le nom des objets joints au document. Dans le champ **Ne pas analyser les objets selon le masque**, définissez les masques de nom de fichiers qui seront exclus de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour cet objet est *non analysé*.

     Le filtrage selon le nom tient compte de la casse dans le nom du fichier.

     Vous pouvez désigner plusieurs masques de noms de fichiers et les séparer par "**;**". Utilisez les caractères suivants dans les masques :

     - * : n'importe quelle séquence de caractères. Par exemple, si vous saisissez le masque abc*, aucun fichier dont le nom commence par abc, par exemple abc.exe, abc1.com ou abc2.rar, n'est analysé.

     - ? : n'importe quel caractère unique. Par exemple, si vous saisissez le masque abc?.exe, aucun fichier dont le nom commence par abc suivi de n'importe quel caractère, par exemple abc1.exe, n'est analysé. Par contre, le fichier abc12345.exe sera analysé.

   Si les cases **Filtre selon la taille** et **Filtre selon le nom** ne sont pas cochées, le filtrage des objets ne s'exécute pas.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ANALYSE DES BASES DE DONNEES

Cette section explique comment activer ou désactiver l'analyse des bases de données, comment sélectionner les objets de la base de données à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des bases de données en fonction des résultats de l'analyse et comment configurer les paramètres de l'analyse.

### DANS CETTE SECTION



# ALGORITHME D'ANALYSE DES BASES DE DONNEES

L'analyse des bases de données est lancée selon la programmation ou à la demande de l'utilisateur. Les paramètres de l'analyse des bases de données sont définis via un profil ; il n'est pas possible de définir des paramètres spécifiques à un serveur. L'activation ou la désactivation de l'analyse des bases de données (cf. section "Activation et désactivation de l'analyse des bases de données" à la page 62) est possible uniquement pour chaque serveur séparément. L'analyse des bases de données est désactivée par défaut.

Lorsque l'analyse est lancée (à la demande de l'utilisateur ou selon une programmation), l'application recherche par défaut des menaces dans les éléments suivants : champs des documents des bases de données au format Rich Text, objets joints aux documents et objets OLE intégrés.

Par défaut, si l'analyse antivirus des bases de données est activée, Kaspersky Anti-Virus analyse les bases de données situées dans le répertoire racine data (répertoire de stockage des données du serveur Lotus Domino), dans tous ses sous-répertoires et dans les répertoires externes accessibles via les liens. Vous pouvez activer ou désactiver l'analyse des bases de données situées dans les sous-répertoires du répertoire data et des répertoires externes jusqu'au niveau le plus bas de la hiérarchie.

Les objets infectés, potentiellement infectés et non analysés à cause d'un échec ou en raison de dégâts découverts suite à l'analyse sont traités conformément aux paramètres d'analyse des bases de données (cf. section "Actions à exécuter sur les objets lors de l'analyse des bases de données" à la page 64).

Après l'installation de l'application, ce sont les valeurs des paramètres d'analyse des bases de données par défaut qui sont utilisées (cf. section "Protection du serveur par défaut" à la page 42). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Lotus Domino protégé. Une partie des paramètres cités ici est désactivée par défaut ou peut être désactivée par l'administrateur.

Vous pouvez définir les masques des noms des fichiers de bases de données à analyser (cf. section "Sélection des objets des bases de données à analyser" à la page 63). Dans ce cas, Kaspersky Anti-Virus analysera uniquement les fichiers des bases de données définis à l'aide des masques.

Avant le traitement, une copie de l'objet sortant est placée par défaut en quarantaine (cf. page 71).

La notification sur l'analyse du document par Kaspersky Anti-Virus et la description des actions exécutées sont envoyées aux administrateurs (cf. section "Notifications" à la page 85). Les informations relatives aux résultats de l'analyse et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques (cf. section "Journal des événements et statistiques" à la page 76).

Kaspersky Anti-Virus permet d'exclure de l'analyse des bases de données en particulier (cf. section "Sélection des objets des bases de données à analyser" à la page 63). La base de données Quarantaine est exclue de l'analyse par défaut (kavquarantine.nsf).

Vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et du contenu des champs RTF et MIME (cf. section "Sélection des objets des bases de données à analyser" à la page 63). Pour augmenter la vitesse globale de l'analyse des bases de données, vous pouvez limiter le temps d'analyse par objet (cf. section "Configuration des paramètres de performances" à la page 69).

# ACTIVATION ET DESACTIVATION DE L'ANALYSE DES BASES DE DONNEES

Par défaut, l'analyse des bases de données est désactivée. Elle peut être lancée selon une programmation ou à la demande de l'utilisateur. Les informations relatives au lancement des modules chargés de l'analyse des bases de données sont consignées dans le journal des événements de Kaspersky Anti-Virus.

Le cas échéant, vous pouvez activer et désactiver l'analyse des bases de données. Cette opération est réalisée séparément pour chaque serveur.

➧ *Pour activer ou désactiver l'analyse des bases de données, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez activer ou désactiver l'analyse des bases de données (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Informations** (cf. ill. ci-dessous).

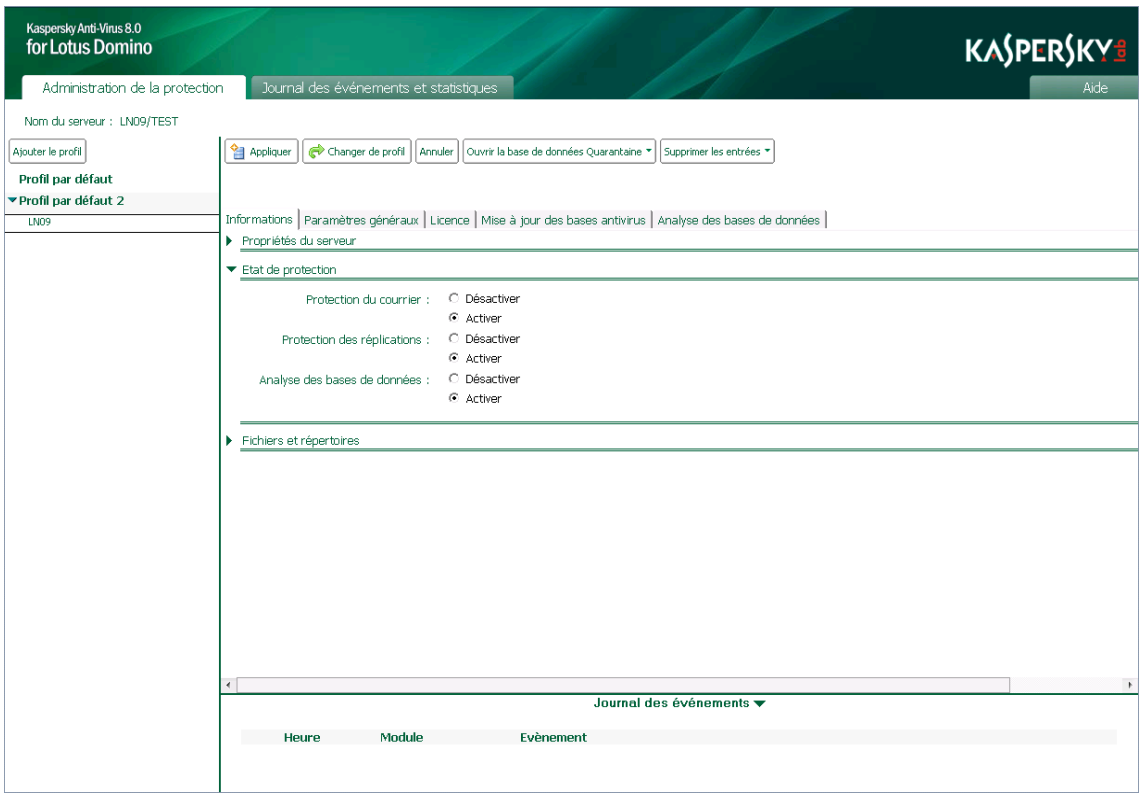


*Illustration 11. Activation/désactivation de l'analyse des bases de données*

3. Dans le groupe **Etat de la protection**, sur la ligne **Analyse des bases de données** (cf. ill. ci-dessus), choisissez l'option **Activer** ou **Désactiver**.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# SELECTION DES OBJETS A ANALYSER DES BASES DE DONNEES

Par défaut, pendant l'analyse des bases antivirus, Kaspersky Anti-Virus analyse les bases de données situées dans le répertoire data (y compris les sous-répertoires). Conformément aux paramètres de l'analyse, Kaspersky Anti-Virus dresse une liste des objets à analyser, puis analyse le contenu des champs au format Rich Text et MIME de chaque document, tous les objets joints, y compris les archives, et les objets OLE intégrés. Le cas échéant, vous pouvez désactiver l'analyse des objets cités.

Lors de l'analyse d'archives multi-volumes, chaque volume est traité par Kaspersky Anti-Virus comme un objet séparé. Le code malveillant sera découvert uniquement s'il est contenu entièrement dans l'un des volumes. Si le code est scindé en plusieurs parties sur différents volumes, il ne sera pas découvert pendant l'analyse. C'est la raison pour laquelle il est conseillé d'analyser les archives multi-volumes après l'enregistrement sur le disque à l'aide de l'antivirus de fichiers installé sur l'ordinateur.

*Pour sélectionner les objets soumis à l'analyse antivirus des bases de données, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Analyse des bases de données** → **Général**.

3. Dans le groupe **Protection des objets**, sélectionnez les objets à analyser. Pour ce faire, cochez les cases suivantes :

   - **Pièces jointes**. Kaspersky Anti-Virus analyse tout fichier joint au document.
   - **Objets OLE**. Kaspersky Anti-Virus analyse tous les objets OLE intégrés au document.
   - **Champs RTF et MIME**. Kaspersky Anti-Virus analyse les champs du document aux formats Rich Text et MIME.

   Si la case n'est pas cochée, l'analyse des objets correspondants n'a pas lieu.

4. Dans le champ **Analyser les objets selon le masque**, définissez les masques des fichiers des bases de données qui seront analysés par Kaspersky Anti-Virus.

   Vous pouvez désigner plusieurs masques de noms de fichiers et les séparer par ";". Utilisez les caractères suivants dans les masques :

   - * : n'importe quelle séquence de caractères. Par exemple, si vous saisissez le masque abc*, tous les fichiers dont le nom commence par abc, par exemple abc.exe, abc1.com ou abc2.rar, sont analysés.
   - ? : n'importe quel caractère unique. Par exemple, si vous saisissez le masque abc?.exe, tous les fichiers dont le nom commence par abc suivi de n'importe quel caractère, par exemple abc1.exe, sont analysés. Par contre, le fichier abc12345.exe ne sera pas analysé.

   La valeur * ou *.* est indiquée par défaut, ce qui signifie que les bases de données présentant n'importe quel nom sont analysées.

5. Cochez la case **Analyser les sous-répertoires** pour que Kaspersky Anti-Virus analyse les fichiers de la base de données situés dans les sous-répertoires du répertoire data jusqu'au niveau le plus bas de la hiérarchie.

Si vous souhaitez que Kaspersky Anti-Virus analyse uniquement les fichiers de la base de données situés dans le répertoire racine data, décochez la case **Analyser les sous-répertoires**.

Vous pouvez également indiquer un masque pour l'analyse des répertoires dotés d'un compte avec la cartographie des bases de données :

- Si le masque n'indique aucun chemin, toutes les bases de données dont le nom correspond au masque sont analysées ; ceci dans tous les répertoires. Par exemple, lors de la saisie du masque m*.nsf, toutes les bases de données dont le nom commence par m sont analysées.

- Si un chemin est indiqué dans le masque ou que la case **Analyser les sous-répertoires** est cochée, les bases de données du répertoire indiqué et de ses sous-répertoires sont analysées conformément au masque. Par exemple, si le masque DATA/Acme/m*.nsf est saisi et que la case **Analyser les sous-répertoires** est cochée, toutes les bases de données dont le nom commence par m et qui se trouvent dans le répertoire Acme ou dans ses sous-répertoires seront analysées.

- Si le chemin est indiqué dans le masque et que la case **Analyser les sous-répertoires** est décochée, seules les bases de données du répertoire indiqué sont analysées. Par exemple, si le masque DATA/Acme/m*.nsf est saisi et que la case **Analyser les sous-répertoires** est décochée, toutes les bases de données dont le nom commence par m et qui se trouvent dans le répertoire Acme seront analysées. Les bases de données des sous-répertoires du répertoire Acme ne seront pas analysées.

6. Dans le champ **Exclure de l'analyse**, indiquez le nom des bases de données que vous souhaitez exclure de l'analyse. Vous pouvez définir plusieurs valeurs en les séparant par ";". La base de données Quarantaine (kavquarantine.nsf) est exclue de l'analyse par défaut.

7. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ACTIONS A EXECUTER SUR LES OBJETS LORS DE L'ANALYSE DES BASES DE DONNEES

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus et suite au filtrage des pièces jointes (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21). Les objets sains sont ignorés sans aucune modification. L'administrateur peut configurer les actions sur les objets infectés, potentiellement infectés, non analysés et protégés. Les actions qui seront exécutées par l'application sont définies pour chaque état d'objet.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme infecté, Kaspersky Anti-Virus le répare. L'objet réparé est conservé dans le document à l'adresse d'origine.

  La réparation des objets OLE est impossible. Kaspersky Anti-Virus supprime les objets OLE infectés.

- Si l'objet est considéré comme potentiellement infecté, Kaspersky Anti-Virus le supprime du document.

- Si l'analyse de l'objet a échoué (par exemple, le temps dédié à l'analyse s'est écoulé) ou que l'objet est une archive protégée par un mot de passe, Kaspersky Anti-Virus ignore cet objet.

Par défaut, une copie de l'objet est conservée dans la base de données Quarantaine (cf. page 71) avant le traitement. Les informations sur les objets découverts et les actions exécutées peuvent être envoyées aux administrateurs (cf. section "Notifications" à la page 85) et conservées dans la base de données Journal des événements et statistiques (cf. section "Journal des événements et statistiques" à la page 76).

# CONFIGURATION DES ACTIONS A EXECUTER SUR LES OBJETS LORS DE L'ANALYSE DES BASES DE DONNEES

*Pour configurer les actions à exécuter sur les objets lors de l'analyse des bases de données, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Analyse des bases de données** → **Actions**.

3. Sous l'onglet **Actions**, sélectionnez le groupe de paramètres correspondant à l'état de l'objet dont vous souhaitez configurer le traitement. Vous pouvez choisir parmi les groupes de paramètres suivants :

   - **Objet infecté** : configuration des paramètres de traitement des objets infectés.
   - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
   - **Objet protégé** : configuration des paramètres de traitement des objets protégés.
   - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.

4. Sélectionnez l'action à exécuter sur les objets détectés. Vous pouvez ainsi sélectionner l'option **Réparer**, **Ignorer** ou **Supprimer** et cocher les cases suivantes :

   - **Placer en quarantaine** : avant le traitement, une copie de l'objet est placée dans la base de données Quarantaine.
   - **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées aux emplacements définis dans le champ **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs emplacements de consignation des données sont sélectionnés en même temps, l'enregistrement s'exécute en une seule fois à tous les emplacements indiqués :
     - **Sur la console** (journal système Domino log.nsf) ;
     - **Dans le journal** ;
     - **Dans le fichier** (nom du fichier par défaut : server(N).log, où N est le numéro de séquence du fichier journal).

5. Configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. section "Notifications" à la page 85).

6. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# CONFIGURATION DU FILTRAGE DES PIECES JOINTES LORS DE L'ANALYSE DES BASES DE DONNEES

Lors de l'analyse des bases de données, Kaspersky Anti-Virus permet d'exclure de l'analyse antivirus les pièces jointes des documents qui correspondent aux paramètres du filtre, et de définir l'ordre de leur traitement. Lors de l'analyse des bases de données, le principe de filtrage des pièces jointes utilisé est le même que celui qui intervient dans le filtrage des pièces jointes du courrier. Le filtrage des pièces jointes est désactivé par défaut.

*Pour configurer les paramètres de filtrage des pièces jointes lors de l'analyse des bases de données, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, **Analyse des bases de données** → **Général** (cf. ill. ci-dessous).

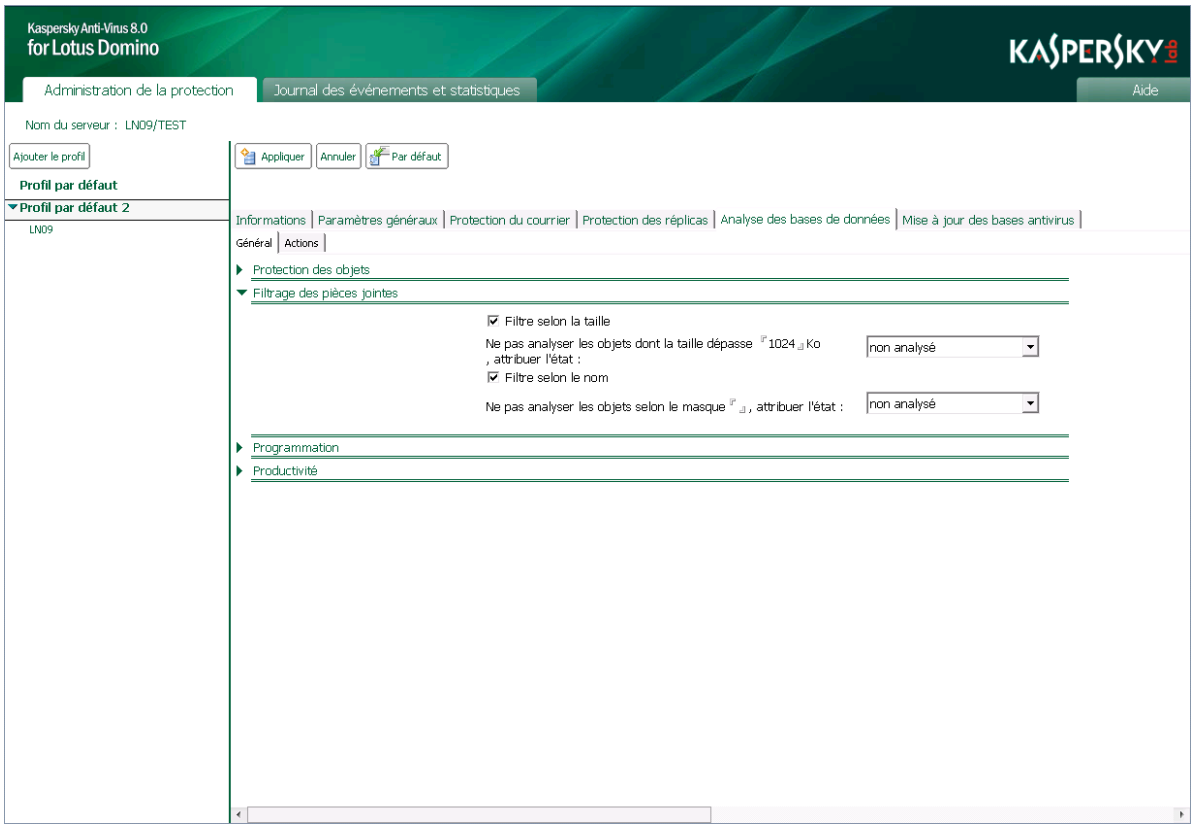


*Illustration 12. Configuration des paramètres du filtrage des pièces jointes lors de l'analyse des bases de données.*

3. Dans le groupe **Filtrage des pièces jointes**, vous pouvez configurer les paramètres de filtrage des objets joints au document. Pour ce faire, cochez les cases suivantes et définissez les valeurs des paramètres correspondants :

   - **Filtre selon la taille**. Cochez cette case afin que Kaspersky Anti-Virus vérifie la taille des objets joints au document. Dans le champ **Ne pas analyser les objets dont la taille dépasse**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera exclu de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour cet objet est *non analysé*.

   - **Filtre selon le nom**. Cochez cette case afin que Kaspersky Anti-Virus vérifie le nom des objets joints au document. Dans le champ **Ne pas analyser les objets selon le masque**, définissez les masques de nom de fichiers qui seront exclus de l'analyse antivirus. Dans la liste déroulante, sélectionnez l'élément qui, en fonction de l'état, recevra cet objet via Kaspersky Anti-Virus. La valeur sélectionnée par défaut pour cet objet est *non analysé*.

   Le filtrage selon le nom tient compte de la casse dans le nom du fichier.

Vous pouvez désigner plusieurs masques de noms de fichiers et les séparer par "**;**". Utilisez les caractères suivants dans les masques :

- * : n'importe quelle séquence de caractères. Par exemple, si vous saisissez le masque abc*, aucun fichier dont le nom commence par abc, par exemple abc.exe, abc1.com ou abc2.rar, n'est analysé.
- ? : n'importe quel caractère unique. Par exemple, si vous saisissez le masque abc?.exe, aucun fichier dont le nom commence par abc suivi de n'importe quel caractère, par exemple abc1.exe, n'est analysé. Par contre, le fichier abc12345.exe sera analysé.

Si les cases **Filtre selon la taille** et **Filtre selon le nom** ne sont pas cochées, le filtrage des objets ne s'exécute pas.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ANALYSE PROGRAMMEE DES BASES DE DONNEES

Vous pouvez configurer le lancement de l'analyse des bases de données selon une programmation. Les paramètres de la programmation de l'analyse des bases de données peuvent être indiqués uniquement pour les groupes de serveurs utilisant les paramètres du profil.

*Pour configurer les paramètres d'analyse des bases de données selon une programmation, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et, dans le volet d'administration, sélectionnez l'onglet **Analyse des bases de données** (cf. ill. ci-après).

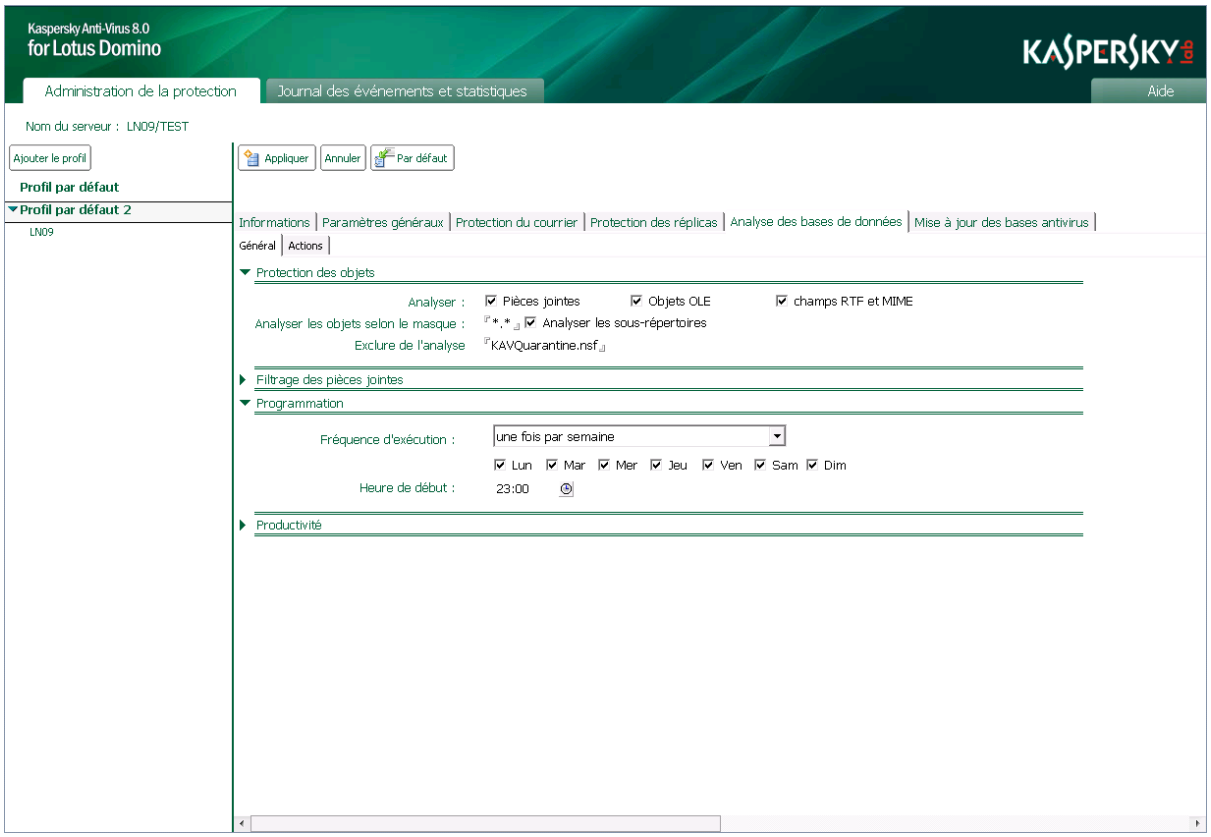


*Illustration 13. Configuration des paramètres de lancement des bases de données selon une programmation.*

3. Dans le groupe **Programmation** (cf. ill. ci-dessus) choisissez l'un des éléments suivants dans la liste déroulante **Fréquence d'exécution** :

   - **Une fois par semaine**. Kaspersky Anti-Virus analyse les bases de données chaque semaine, le jour défini et à l'heure indiquée dans le champ **Heure de lancement**. Pour programmer le lancement de l'analyse des bases de données, cochez les cases en regard des jours où l'analyse sera lancée et saisissez la valeur souhaitée dans le champ **Heure de lancement** au format `HH:MM`.

   - **Une fois par mois**. Kaspersky Anti-Virus analyse les bases de données chaque mois, à la date et à l'heure indiquées dans le champ **Heure de lancement**. Pour définir l'heure de lancement de l'analyse des bases de données, saisissez la valeur souhaitée dans le champ **Heure de lancement** au format `HH:MM`.

     Si le nombre de jours dans le mois est inférieur à la valeur définie, l'analyse des bases de données a lieu le dernier jour du mois.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ANALYSE MANUELLE DES BASES DE DONNEES

Vous pouvez lancer l'analyse manuelle des bases de données pour chaque serveur. Ce mode d'analyse n'est pas prévu pour un groupe de serveurs.

*Pour lancer l'analyse manuelle des bases de données, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez lancer l'analyse des bases de données (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet d'administration, choisissez l'onglet **Analyse des bases de données**. L'onglet reprend les informations sur la date et l'heure de l'analyse précédente des bases de données et de l'analyse suivante, conformément à la programmation.

3. Cliquez sur le lien **Lancer l'analyse** afin de lancer l'analyse des bases de données.

L'analyse des bases de données peut également être lancée manuellement depuis la ligne de commande de la console du serveur Lotus Domino (cf. section "Utilisation via la console du serveur" à la page 96).

# CONFIGURATION DES PARAMETRES DE PERFORMANCES

Vous pouvez réguler les performances de Kaspersky Anti-Virus lors de l'analyse des objets à l'aide des paramètres suivants :

- *Durée d'analyse d'un objet.* Si le temps prévu pour l'analyse est écoulé, l'analyse de l'objet s'interrompt. Kaspersky Anti-Virus attribue l'état *non analysé* à l'objet et passe à l'analyse de l'objet suivant.

- *Analyse d'un objet dans la mémoire de l'ordinateur.* Si la taille de l'objet ne dépasse pas la valeur définie, il est analysé dans la mémoire vive du serveur, sans enregistrement sur le disque dur.

Les paramètres de performances de Kaspersky Anti-Virus peuvent être configurés séparément pour chaque module de la protection.

➧ *Pour configurer les paramètres de performances de Kaspersky Anti-Virus, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** pour passer au mode de modification des paramètres.

3. Dans le volet des actions, sous l'onglet **Protection du courrier** ou **Protection des réplications** ou **Analyse des bases de données**, sélectionnez l'onglet **Général** (cf.ill.ci-dessous).

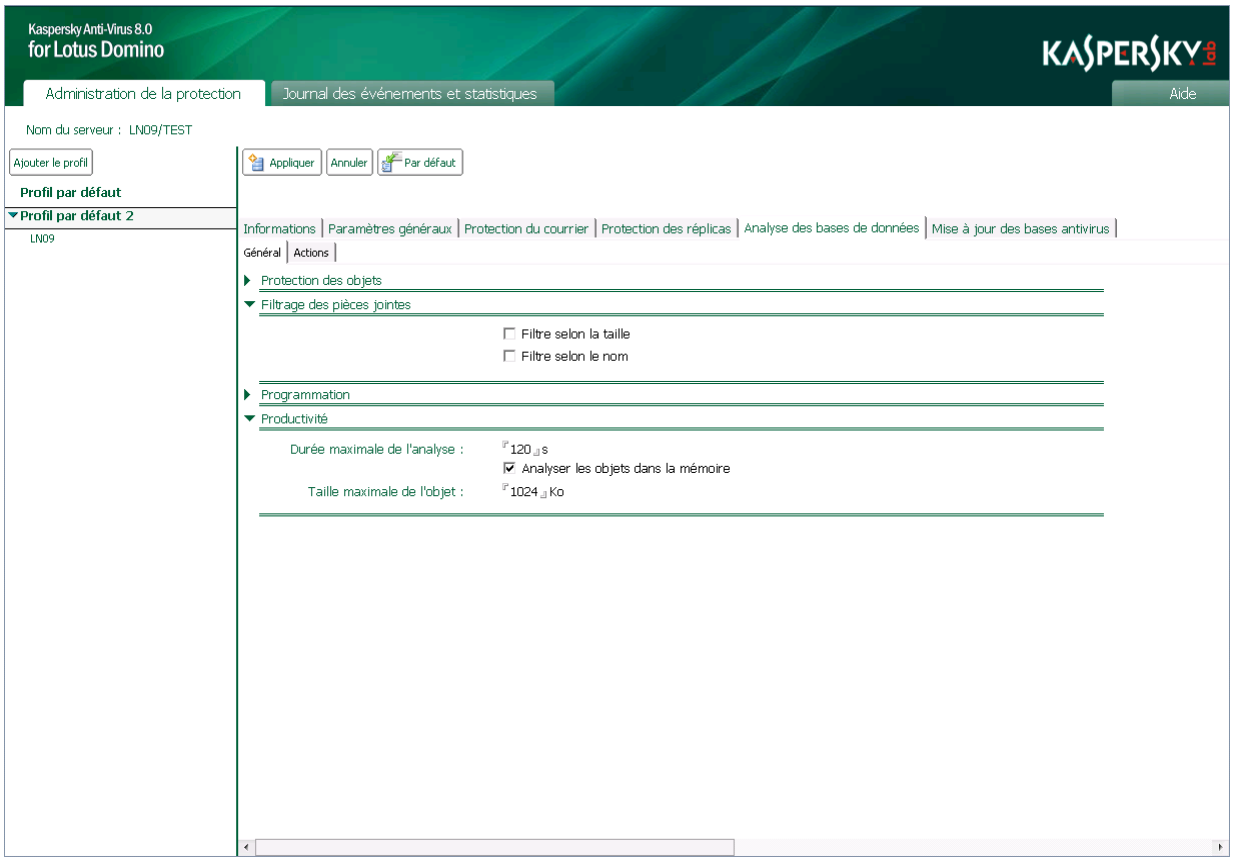


*Illustration 14. Configuration des paramètres de performances de Kaspersky Security lors de l'analyse des bases de données.*

4. Dans le groupe **Productivité**, configurez les paramètres de performances de l'application. Pour ce faire, exécutez les actions suivantes:

   - Dans le champ **Durée maximale de l'analyse**, définissez la durée maximale de l'analyse d'un objet en millisecondes. Par défaut, la durée maximale de l'analyse est de 120 s.

   - Cochez la case **Analyser les objets dans la mémoire**, puis dans le champ **Taille maximale de l'objet**, indiquez la taille maximale d'un objet à vérifier en kilooctets. Par défaut, la taille maximale de l'objet est de 1 024 Ko.

5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# QUARANTAINE

Cette section explique comment consulter les objets placés en quarantaine, comment configurer le traitement des objets placés en quarantaine et comment configurer les paramètres de la quarantaine.

### DANS CETTE SECTION



# PRESENTATION DE LA BASE DE DONNEES QUARANTAINE

En mode de protection du courrier, de protection des réplications et d'analyse des bases de données, Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus et suite au filtrage des pièces jointes (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 21). Par défaut, avant toute réparation ou suppression, Kaspersky Anti-Virus crée une copie de l'objet et la consigne dans la base de données Quarantaine : kavquarantine.nsf.

La base de données Quarantaine sert à conserver les objets placés en quarantaine et à les manipuler. Une base de données Quarantaine se trouve sur chacun des serveurs protégés sous la forme d'une copie et contient les objets originaux mis en quarantaine par les tâches Protection du courrier, Protection des réplications et Analyse des bases de données de ce serveur. Lors de l'installation de l'application, vous pouvez choisir si vous souhaitez conserver les objets de la quarantaine sous toutes leurs répliques ou si la base de données Quarantaine contiendra uniquement les objets de son propre serveur (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino).

Par défaut, avant toute réparation ou suppression, les objets considérés comme *infectés* et *potentiellement infectés* par l'analyse antivirus sont placés dans la quarantaine. Dans les paramètres de protection du courrier, de protection des réplications et d'analyse des bases de données, vous pouvez configurer les critères de placement des objets dans la quarantaine pour chaque statut d'objet.

Il n'est pas possible de mettre des objets manuellement en quarantaine.

La base de données kavquarantine.nsf est créée lors de l'installation de l'application dans le répertoire des bases de données de Kaspersky Anti-Virus (ce répertoire est kavdatabases par défaut). L'accès aux objets placés dans la base de données Quarantaine est possible via l'interface utilisateur de la base de données Centre d'administration (cf. section "Interface de l'application" à la page 33).

Pour une recherche et un affichage plus convivial des informations dans la base de données, les objets mis en quarantaine suite à l'analyse des messages électroniques, des réplications et des bases de données, sont divisés en plusieurs sections (cf. section "Consultation des objets placés en quarantaine" à la page 72).

Par défaut, la durée maximale de conservation des objets dans la base de données Quarantaine est de 30 jours. Vous pouvez modifier la durée de conservation des objets en quarantaine dans les paramètres du serveur. Si une limite de la durée de conservation des objets (cf. section "Configuration de la quarantaine" page 74) est définie, les objets conservés jusqu'à l'échéance du délai sont supprimés de la base de données Quarantaine une fois que ce dernier est dépassé. Le cas échéant, vous pouvez supprimer manuellement les objets de la quarantaine.

Le volume total des objets conservés en quarantaine est limité par la taille physique de la base de données. La base de données Quarantaine peut présenter une taille maximale de 64 Go. Quand cette valeur est atteinte, plus aucun objet ne pourra être mis en quarantaine. Dans ce cas, il est recommandé de supprimer manuellement les objets les plus anciens de la quarantaine (cf. section "Actions à exécuter sur les objets placés en quarantaine" à la page 73) ou de modifier les paramètres de conservation des objets mis en quarantaine.

# CONSULTATION DES OBJETS PLACES EN QUARANTAINE

La consultation des objets placés dans la base de données Quarantaine s'opère via l'interface utilisateur de la base de données Centre d'administration. Pour une recherche et un affichage plus convivial des informations dans la base de données, les objets mis en quarantaine suite à l'analyse des messages électroniques, des réplications et des bases de données sont divisés en plusieurs sections.

Vous pouvez consulter les objets de types suivants placés dans la quarantaine : courrier, bases de données, réplications. Chaque type d'objet apparaît dans une nouvelle fenêtre. Vous pouvez ouvrir les entrées de la quarantaine pour tous les serveurs protégés ; ceci en une seule fois.

*Pour consulter les objets placés dans la base de données Quarantaine et les informations à leur sujet, procédez comme suit :*

1. Sélectionnez un serveur au hasard dans n'importe quel profil (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

   Si, lors de l'installation de l'application, la case **Enregistrer les objets en quarantaine dans toutes les répliques** n'a pas été cochée dans les paramètres de déploiement, alors chaque réplique ne contient l'enregistrement que d'un seul serveur (en cours d'utilisation) (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino).

2. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données Quarantaine** et, dans la liste déroulante qui s'ouvre, sélectionnez l'un des éléments suivants :

   - **Messages électroniques**.
   - **Bases de données**.
   - **Réplications**.

   Cette action affichera les entrées de la quarantaine pour tous les serveurs protégés dans le volet d'administration. Les entrées relatives aux messages électroniques mis en quarantaine sont regroupées par date de placement des objets dans la quarantaine et par les adresses électroniques des expéditeurs des messages. Les entrées relatives aux objets mis en quarantaine suite à l'analyse des bases de données et des réplications sont regroupées par date de mise en quarantaine des objets et par nom des bases de données auxquelles appartiennent les documents analysés. Pour ouvrir la liste complète des entrées regroupées, cliquez sur l'icône . Pour réduire la liste, cliquez sur l'icône .

Vous pouvez consulter des informations complémentaires sur chacun des objets mis en quarantaine. Le volet d'affichage dans le groupe **Détails** indique les informations suivantes sur l'objet sélectionné :

### Pour les messages électroniques :

- **Date** : date et heure de la mise en quarantaine de l'objet.
- **Nom du serveur** : nom du serveur sur lequel l'analyse a été réalisée.
- **Expéditeur** : adresse électronique de l'expéditeur du message électronique.
- **Destinataires** : adresses électroniques des destinataires du message électronique.
- **Copie** : adresses électroniques des destinataires de la copie du message électronique.
- **Copie cachée :** adresses électroniques des destinataires de la copie cachée du message électronique.
- **Objet du message** : objet du courrier placé en quarantaine.
- Liste des fichiers joints.
- Informations textuelles comportant le nom de l'objet, le motif de son placement en quarantaine et l'énumération des actions exécutées sur cet objet.

**Pour les documents répliqués et les documents des bases de données :**

- **Date** : date et heure de la mise en quarantaine de l'objet.
- **Serveur** : nom du serveur sur lequel l'analyse a eu lieu.
- **Module** : nom du module ayant réalisé l'analyse et mis l'objet en quarantaine.
- **Base de données** : nom de la base de données où se trouve l'objet.
- **Modifié par** : nom de l'utilisateur qui a introduit les dernières modifications dans le document et nom du serveur sur lequel ces modifications ont été introduites, au format : **Nom de l'utilisateur/nom du serveur**.
- **Document** : numéro (nom) du document placé en quarantaine sur le serveur Lotus Domino.
- Liste des fichiers joints.
- Informations textuelles comportant le nom de l'objet, le motif de son placement en quarantaine et l'énumération des actions exécutées sur cet objet.

# ACTIONS A EXECUTER SUR LES OBJETS PLACES EN QUARANTAINE

Avant toute réparation ou suppression d'un objet considéré comme *infecté* ou *potentiellement infecté* suite à l'analyse antivirus, Kaspersky Anti-Virus place une copie de cet objet dans la base de données Quarantaine. Vous pouvez exécuter les actions suivantes sur les objets placés en quarantaine :

- supprimer les objets manuellement ;
- supprimer de la base de données Quarantaine les entrées créées antérieurement à nombre de jours donné ;
- remettre les courriers de la base de données Quarantaine à leurs destinataires.

Kaspersky Anti-Virus supprime automatiquement les objets de la base de données Quarantaine à l'issue de la durée de conservation des objets indiquée dans les paramètres du serveur.

➧ *Pour supprimer manuellement les objets de la base de données Quarantaine, procédez comme suit :*

1. Sélectionnez un serveur au hasard dans n'importe quel profil (cf. section "Consultation et modification des paramètres du serveur" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données Quarantaine** et, dans la liste déroulante qui s'ouvre, sélectionnez l'un des éléments suivants :
   - **Messages électroniques**.
   - **Bases de données**.
   - **Réplications**.

   Cette action affichera les entrées de la quarantaine pour tous les serveurs protégés dans le volet d'administration.

3. Dans le volet d'administration, déployez la liste des entrées regroupées en cliquant sur le bouton .

4. Dans la liste des entrées, sélectionnez avec la souris l'objet que vous voulez supprimer de la quarantaine, puis dans le volet de consultation, cliquez sur le bouton **Supprimer**.

   Vous pouvez sélectionner plusieurs objets à l'aide des touches **Ctrl** et **Shift**.

*Pour transférer un message électronique de la base de données Quarantaine aux destinataires, procédez comme suit :*

1. Sélectionnez un serveur au hasard dans n'importe quel profil (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données Quarantaine** et, dans la liste déroulante qui s'ouvre, sélectionnez l'élément **Messages électroniques**.

   Les entrées des messages mis en quarantaine sur tous les serveurs protégés apparaissent dans le volet d'administration.

3. Dans le volet d'administration, déployez la liste des entrées regroupées en cliquant sur le bouton .

4. Dans la liste des entrées, sélectionnez avec la souris le message électronique que vous voulez transférer aux destinataires, puis dans le volet de consultation, cliquez sur le bouton **Envoyer aux destinataires**.

   Vous pouvez sélectionner plusieurs messages à l'aide des touches **Ctrl** et **Shift**.

*Pour supprimer de la base de données Quarantaine les entrées créées antérieurement à un nombre de jours donné, procédez comme suit :*

1. Sélectionnez un serveur au hasard dans n'importe quel profil (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Supprimer les entrées** et dans la liste déroulante, sélectionnez l'élément **Quarantaine**.

3. Dans la fenêtre qui s'ouvre, saisissez le nombre de jours et cliquez sur le bouton **OK** pour supprimer les entrées de la quarantaine créées avant la période définie.

# CONFIGURATION DES PARAMETRES DE LA QUARANTAINE

Vous pouvez modifier la durée de conservation des objets dans la base de données Quarantaine.

*Pour modifier la durée de conservation des objets dans la base de données Quarantaine, procédez comme suit :*

1. Sélectionnez le serveur dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-dessous).

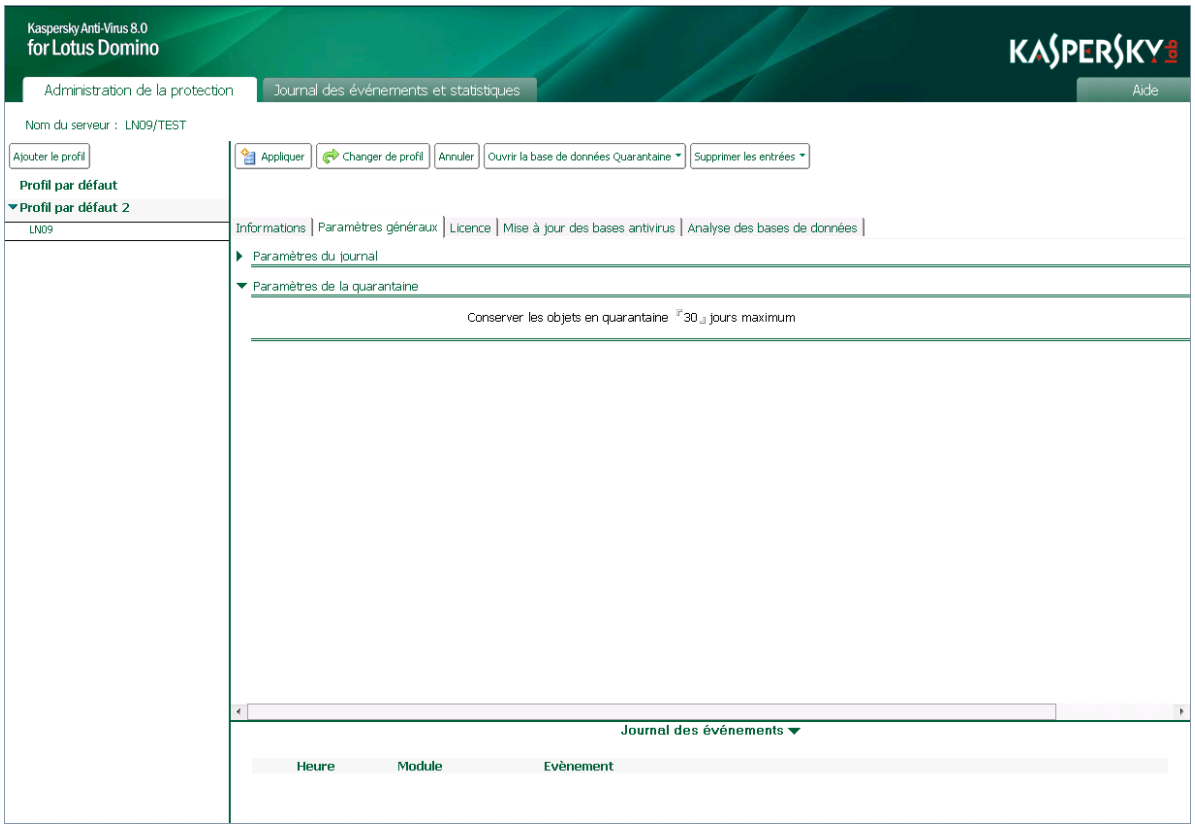


*Illustration 15. Configuration des paramètres de la quarantaine*

3. Dans le groupe **Paramètres de la quarantaine**, indiquez la durée de conservation, en jours, des objets placés dans la base de données Quarantaine. La durée de conservation des objets par défaut est fixée à 30 jours.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# JOURNAL DES EVENEMENTS ET STATISTIQUES

Cette section explique comment configurer le journal des événements et statistiques, et comment consulter la base de données Journal des événements et statistiques (informations pour un serveur ou pour tous les serveurs).

### DANS CETTE SECTION



## PRESENTATION DE LA BASE DE DONNEES JOURNAL DES EVENEMENTS ET STATISTIQUES

Kaspersky Anti-Virus permet de conserver les informations relatives aux événements survenus pendant l'utilisation de l'application ainsi que les statistiques relatives aux menaces découvertes suite à l'analyse antivirus et aux actions exécutées sur celles-ci dans la base de données Journal des événements et statistiques.

La base de données Journal des événements et statistiques est déployée sous forme de réplique et figure sur chaque serveur protégé. Elle contient la synthèse des statistiques de tous les événements survenus sur l'ensemble des serveurs protégés. Toutes les modifications sont propagées via le mécanisme standard de réplication selon la planification et la topologie. Les informations sont enregistrées par défaut dans la base de données Journal des événements et statistiques kaveventslog.nsf.

Dans le cadre de l'utilisation d'un modèle distribué du déploiement de Kaspersky Anti-Virus, la base de données kaveventslog.nsf reprend toutes les informations sur tous les serveurs protégés.

La base de données kaveventslog.nsf est créée au cours du processus d'installation de l'application dans le répertoire des bases de données de Kaspersky Anti-Virus (ce répertoire est kavdatabases par défaut). L'accès aux informations conservées dans la base de données Journal des événements et statistiques est possible uniquement via l'interface utilisateur de la base de données Centre d'administration. Vous pouvez consulter et supprimer les entrées de la base de données Journal des événements et statistiques (cf. section "Consultation de la base de données Journal des événements et statistiques" à la page 81).

Le journal des événements reprend les informations sur l'activité des modules de Kaspersky Anti-Virus au niveau des tâches de serveur Lotus Domino (cf. section "Architecture de l'application" à la page 17). Le niveau de détail des informations du journal des événements peut être définit dans le groupe **Niveau de détail** (cf. section "**Configuration des paramètres du journal des événements**" à la page 77). Par défaut, les informations les plus importantes sur le fonctionnement de tous les modules de Kaspersky Anti-Virus sont conservées : informations sur les événements critiques indiquant des problèmes dans le fonctionnement de l'application ou des vulnérabilités dans la protection du serveur.

Les paramètres du journal des événements (cf. section "Configuration des paramètres du journal des événements" à la page 77) permettent également de définir l'emplacement de l'affichage des informations sur les événements et la durée de conservation des entrées dans la base de données kaveventslog.nsf. Vous pouvez configurer les paramètres du journal des événements aussi bien pour un groupe de serveurs, à l'aide d'un profil, que pour chaque serveur séparément. Le fichier pour l'enregistrement du journal des événements peut être désigné uniquement dans les paramètres du serveur. Il n'est pas possible de modifier ce paramètre via le profil.

Les statistiques reprennent les informations relatives aux résultats de l'analyse antivirus des objets, aux menaces identifiées et aux actions exécutées sur les objets. Les statistiques de chaque composant de la protection sont séparées. Vous pouvez définir les informations qui doivent être conservées dans les statistiques en configurant les paramètres du profil pour les tâches de protection du courrier, de protection des réplications et d'analyse des bases de données. Par défaut, les informations obtenues suite à l'analyse des objets *infectés*, *potentiellement infectés*, *protégés* et *non analysés* sont conservées. Les informations sur les objets non analysés s'accompagnent d'une explication sur les raisons de l'échec de l'analyse.

Les entrées de la base de données Journal des événements et statistiques sont conservées par défaut pendant 30 jours. Vous pouvez modifier la durée de conservation des entrées sur les événements et les statistiques ; ceci aussi bien via les paramètres de profil que via les paramètres du serveur (cf. section "Configuration des paramètres du journal des événements" à la page 77, "Configuration des paramètres des statistiques" à la page 79). Une fois ce délai écoulé, les entrées sont supprimées automatiquement.

Pour chaque serveur protégé, il est également possible de supprimer manuellement les informations relatives à ce serveur (cf. section "Suppression des informations de la base de données Journal des événements et statistiques" à la page 84) de la base de données Journal des événements et statistiques.

Les événements enregistrés sur le serveur protégé au cours de la session active de l'application peuvent également apparaître sur la console du serveur Lotus Domino et être enregistrés dans un fichier texte (cf. section "Configuration des paramètres du journal des événements" à la page 77). Par défaut, le système utilise cinq fichiers de journal écrasés de manière cyclique avec le nom server(N).log, où N est le numéro de séquence du fichier journal. Les fichiers journaux se trouvent sur le serveur protégé dans le répertoire de service logs et contiennent les informations sur ce serveur uniquement.

Vous pouvez modifier le nombre de fichiers journaux utilisés, leur nom et la taille acceptée à l'aide des paramètres du fichier de configuration notes.ini (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration .ini" à la page 23).

# CONFIGURATION DES PARAMETRES DU JOURNAL DES EVENEMENTS

Vous pouvez configurer les paramètres du journal des événements aussi bien pour un groupe de serveurs, via le profil, que pour chaque serveur pris séparément, dans les paramètres du serveur.

Par défaut, les paramètres du journal des événements sont définis par le profil auquel appartient le serveur protégé. Pour que Kaspersky Anti-Virus utilise les valeurs définies dans les paramètres du serveur, dans le groupe **Paramètres du journal** de l'onglet **Paramètres généraux**, décochez la case **Utiliser les paramètres du profil**.

➧ *Pour configurer les paramètres du journal des événements, procédez comme suit :*

1. Choisissez l'une des options suivantes :

   - Si vous configurez les paramètres du journal des événements pour des groupes de serveurs, sélectionnez le profil (cf. section "Consultation et modification des paramètres du profil" à la page 39).

   - Si vous configurez les paramètres du journal des événements pour un serveur en particulier, sélectionnez le serveur (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-dessous).

Si vous configurez les paramètres du journal des événements pour un serveur distinct, décochez la case **Utiliser les paramètres du profil** dans le groupe **Paramètres du journal**. Quand la case est cochée, les paramètres du journal des événements et des statistiques ne sont pas affichés. Si vous souhaitez utiliser les valeurs des paramètres définis par le profil pour le serveur, cochez la case **Utiliser les paramètres du profil**.

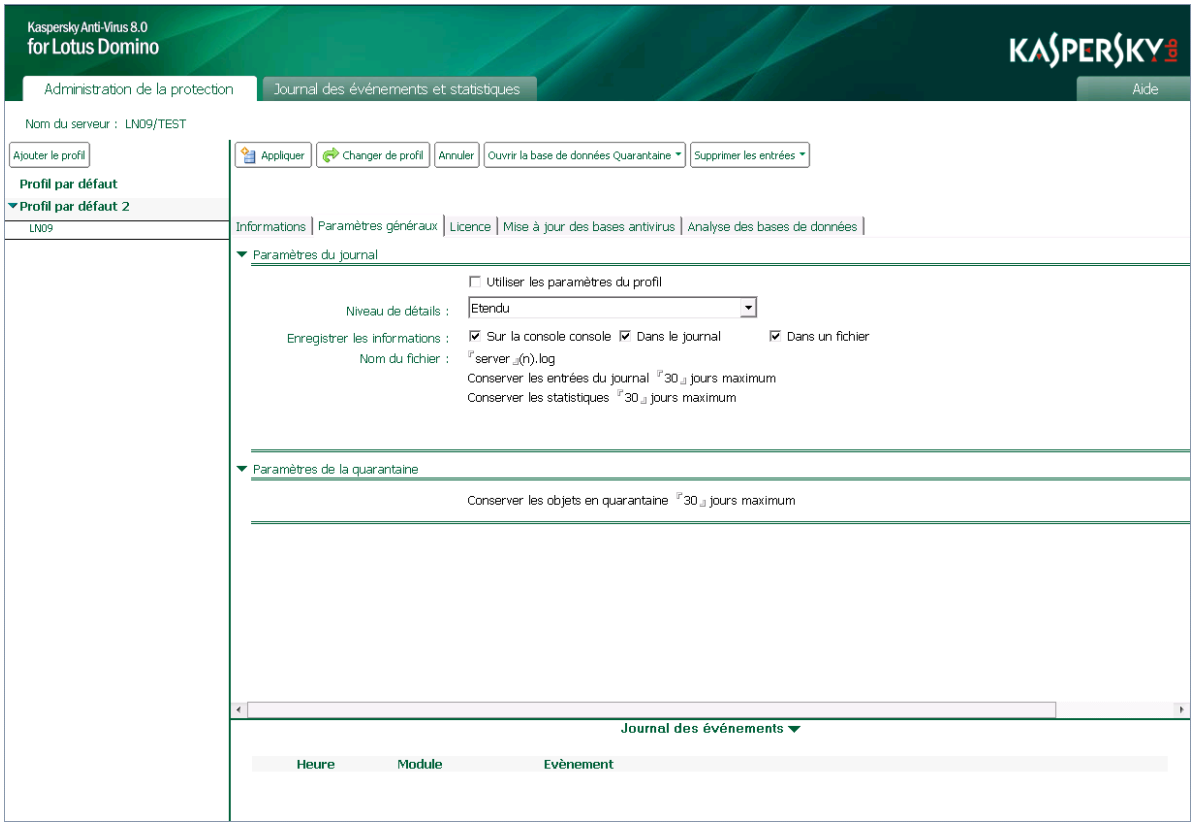


*Illustration 16. Configuration des paramètres du journal des événements pour un serveur*

3. Dans le groupe **Paramètres du journal** (cf. ill. ci-dessus), définissez les valeurs pour les paramètres suivants :

   - Dans le groupe **Niveau de détail**, sélectionnez le niveau de détail des informations consignées dans le journal. Pour ce faire, sélectionnez l'une des options suivantes dans la liste déroulante :

     - **Standard**. Kaspersky Anti-Virus enregistre les *Evénements critiques* et les événements importants qui surviennent au cours du fonctionnement de l'application (par exemple, l'événement *Erreur de connexion avec la source de mises à jour*). Cette option de la liste est sélectionnée par défaut. Dans le fichier notes.ini, valeur du paramètre KAVDefaultLogLevel=0 (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration .ini" à la page 23).

     - **Etendu**. Kaspersky Anti-Virus consigne les événements critiques *Evénements critiques* signalant des vulnérabilités dans la protection du serveur ou des problèmes dans le fonctionnement de l'application. Il consigne également les informations relatives au fonctionnement de tous les modules de Kaspersky Anti-Virus. Dans le fichier notes.ini, valeur du paramètre KAVDefaultLogLevel=1 (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration .ini" à la page 23).

   - Dans le groupe **Enregistrer les informations**, indiquez l'emplacement de l'enregistrement des informations sur les événements consignés. Pour ce faire, cochez les cases suivantes :

     - **Dans le journal**. Kaspersky Anti-Virus enregistre les informations sur les événements dans la base de données Journal des événements et statistiques (kaveventslog.nsf) : Vous pouvez consulter le journal des événements via l'interface utilisateur de la base de données Centre d'administration (cf. section "Consultation de la base de données Journal des événements et statistiques" à la page 81).

La base de données kaveventslog.nsf est créée au cours du processus d'installation de l'application dans le répertoire des bases de données de Kaspersky Anti-Virus (ce répertoire est kavdatabases par défaut).

- **Sur la console**. Kaspersky Anti-Virus affiche les informations sur les événements survenus au cours de son fonctionnement sur la console du serveur Lotus Domino. Les informations fournies concernent la session actuelle d'utilisation de l'application. Le niveau de détail des informations est sélectionné par l'utilisateur.

- **Dans le fichier**. Kaspersky Anti-Virus enregistre les informations sur les événements dans le fichier texte du journal. Par défaut, le système utilise cinq fichiers journal écrasés de manière cyclique avec le nom server(N).log, où N est le numéro de séquence du fichier journal. Les fichiers journaux se trouvent sur le serveur protégé dans le répertoire de service logs et contiennent les informations sur ce serveur uniquement.

Le répertoire logs est créé pendant l'installation de l'application et se trouve à l'adresse suivante : pour les systèmes d'exploitation Microsoft Windows, dans le répertoire des fichiers binaires du serveur Lotus Domino (chemin par défaut : C:\Program Files\IBM\Lotus\Domino\kavcommon) ; pour les systèmes d'exploitation Linux : dans le répertoire de données du serveur Lotus Domino (chemin par défaut : /local/notesdata/kavcommon).

La taille des fichiers du journal peut être définie par le paramètre KAVDefaultLogLevel=1 dans le fichier de configuration notes.ini (cf. section "Configuration des paramètres de Kaspersky Anti-Virus via le fichier de configuration notes.ini" à la page 23). La consultation des fichiers du journal s'opère via les outils standards de consultation des fichiers texte du système d'exploitation Microsoft Windows ou Linux.

Vous pouvez désigner, dans les paramètres du serveur, un autre fichier pour la conservation des informations relatives aux événements survenus pendant l'utilisation de Kaspersky Anti-Virus. Pour ce faire, saisissez le nom du fichier dans lequel vous souhaitez enregistrer les informations relatives aux événements dans le champ **Nom du fichier**. Par conséquent, un fichier au nom défini est créé dans le répertoire de service logs. La modification du nom du fichier via les paramètres du profil n'est pas prévue.

- Dans le champ **Supprimer les entrées dans le journal** indiquez la durée en jours à l'issue de laquelle les entrées relatives aux événements seront supprimées automatiquement de la base de données Journal des événements et statistiques (kaveventslog.nsf). La durée de conservation des informations par défaut est fixée à 30 jours.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Si vous configurez les paramètres de la mise à jour pour un groupe de serveur, vous pouvez restaurer la valeur des paramètres par défaut. Pour ce faire, cliquez sur **Par défaut**.

# CONFIGURATION DES PARAMETRES DES STATISTIQUES

Kaspersky Anti-Virus peut tenir des statistiques séparées sur les menaces découvertes et sur les actions exécutées pour chaque module de la protection. Par défaut, les informations obtenues suite à l'analyse des objets *infectés*, *potentiellement infectés*, *protégés* et *non analysés* sont conservées. Les informations sur les objets non analysés s'accompagnent d'une explication sur les raisons de l'échec de l'analyse.

Dans les paramètres du profil, vous pouvez définir les informations statistiques à conserver pour chaque module de la protection. Le choix des objets pour lesquels des statistiques doivent être enregistrées sur chaque serveur en particulier n'est pas prévu.

La durée de conservation des statistiques dans la base de données Journal des événements et statistiques peut être définie aussi bien pour un groupe de serveurs que pour chaque serveur séparément. Utilisez les paramètres du profil afin de configurer la durée de conservation des informations statistiques pour un groupe de serveurs. Utilisez les paramètres du serveur afin de configurer la durée de conservation des informations statistiques pour chaque serveur séparément. La valeur est limitée à 30 jours par défaut via le profil auquel appartient le serveur protégé. Pour que Kaspersky Anti-Virus utilise les valeurs définies dans les paramètres du serveur, dans le groupe **Paramètres du journal** de l'onglet **Paramètres généraux**, décochez la case **Utiliser les paramètres du profil**.

*Pour configurer la durée de conservation des données statistiques, procédez comme suit :*

1. Choisissez l'une des options suivantes :

   - Si vous configurez les paramètres des statistiques pour un groupe de serveurs, sélectionnez le profil (cf. section "Consultation et modification des paramètres du profil" à la page 39).

   - Si vous configurez les paramètres des statistiques pour un serveur en particulier, sélectionnez le serveur (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-dessous).

Si vous configurez les paramètres des statistiques pour un serveur distinct, décochez la case **Utiliser les paramètres du profil** dans le groupe **Paramètres du journal**. Quand la case est cochée, les paramètres du journal des événements et des statistiques ne sont pas affichés. Si vous souhaitez utiliser les valeurs des paramètres définis par le profil pour le serveur, cochez la case **Utiliser les paramètres du profil**.

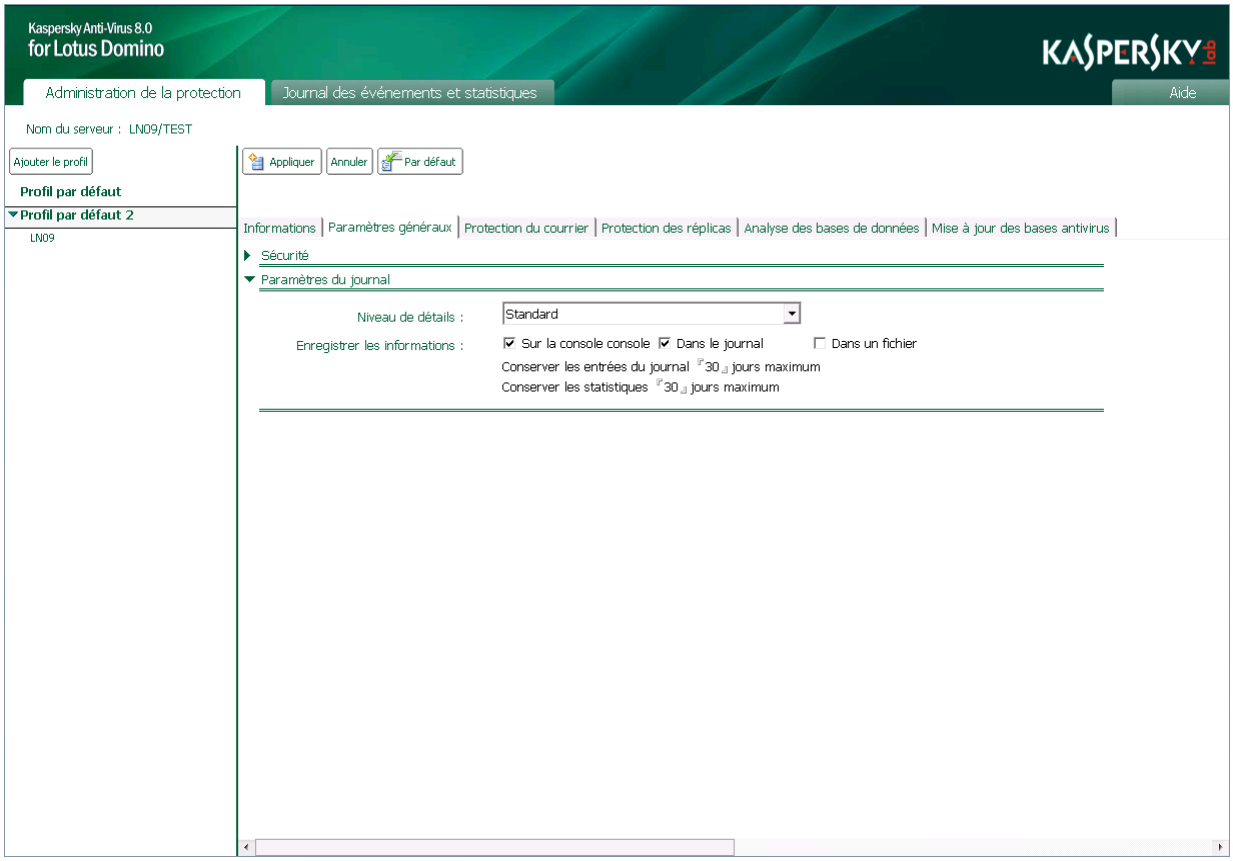


*Illustration 17. Configuration de la durée de conservation des statistiques.*

3. Dans le champ **Supprimer les entrées des statistiques après** du groupe **Paramètres du journal**, indiquez la durée en jours à l'issue de laquelle les entrées seront automatiquement supprimées de la base de données Journal des événements et statistiques (kaveventslog.nsf). La durée de conservation des informations par défaut est fixée à 30 jours.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

Dans les paramètres du profil de chaque module de protection, vous pouvez choisir les objets pour lesquels Kaspersky Anti-Virus conservera les statistiques.

# CONSULTATION DE LA BASE DE DONNEES JOURNAL DES EVENEMENTS ET STATISTIQUES

Vous pouvez consulter et supprimer les entrées de la base de données Journal des événements et statistiques (kaveventslog.nsf) sous l'onglet **Journal des événements et statistiques** des sections suivantes :

- **Journal des événements**.
- **Statistiques de la protection du courrier**.
- **Statistiques de l'analyse des bases de données**.
- **Statistiques de la protection des réplications**.

Vous pouvez consulter les informations pour un seul serveur (cf. section "Consultation du journal des événements pour le serveur" à la page 83) ou les informations globales sur tous les serveurs (cf. section "Consultation du journal global des événements et des statistiques" à la page 81), quel que soit le profil auquel ils appartiennent.

### DANS CETTE SECTION



# CONSULTATION DU JOURNAL GLOBAL DES EVENEMENTS ET DES STATISTIQUES

*Pour consulter le journal global des événements et des statistiques pour tous les serveurs protégés, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Journal des événements et statistiques.**
2. Dans le volet de navigation, sélectionnez la section contenant les informations qui vous intéressent : **Journal des événements**, **Statistiques de la protection du courrier**, **Statistiques de l'analyse des bases de données** ou **Statistiques de la protection des réplications**.
3. Avec la souris, sélectionnez l'une des sections reprises.

   Cette action affichera les entrées de la section sélectionnée pour tous les serveurs protégés dans le volet d'administration. Les sections **Général** reprennent toutes les informations enregistrées dans la base de données kaveventslog.nsf pour la rubrique sélectionnée. Dans les autres sections, les entrées sont regroupées pour faciliter la consultation et la recherche d'informations.

   Pour ouvrir la liste complète des événements regroupés, cliquez sur l'icône . Pour réduire la liste des événements, cliquez sur l'icône .

Vous pouvez trier les entrées du tableau par ordre croissant ou décroissant selon les valeurs reprises dans les colonnes **Date** et **Heure**, ainsi que par ordre alphabétique pour les valeurs des colonnes **Nom du serveur** et **Module**. Pour annuler le tri des entrées, cliquez sur l'icône située à gauche du nom de la colonne.

## JOURNAL DES EVENEMENTS

La section **Journal des événements** contient les sections suivantes :

- **Général** : liste complète des événements, sans aucun regroupement.
- **Selon le nom du serveur** : liste des événements, regroupés selon le nom du serveur sur lequel ils ont eu lieu.

- **Selon la date** : liste des événements regroupés selon la date et l'heure de l'enregistrement.
- **Selon le degré d'importance** : liste des événements regroupés selon le degré d'importance (**Événements critiques**, **Événements importants**, **Événements informatifs**).

Pour ouvrir la liste complète des événements regroupés, cliquez sur l'icône . Pour réduire la liste des événements, cliquez sur l'icône .

Les informations suivantes sont affichées pour chaque événement :

- Icône illustrant le degré d'importance de l'événement :
  - : *événement critique*. Evénement critique signalant un problème dans le fonctionnement de Kaspersky Anti-Virus. Il s'agit par exemple de la découverte d'une menace ou d'un échec de l'application.
  - : *avertissement*. Evénement auquel il faut absolument prêter attention car il signale une situation qui requiert une intervention, par exemple *La durée de validité de la licence expire bientôt*.
  - : *événement d'information*. Evénement informatif, par exemple *Les tâches ont bien été déchargées*.
- **Date** : date d'enregistrement de l'événement.
- **Heure** : heure d'enregistrement de l'événement.
- **Nom du serveur** : nom du serveur sur lequel l'événement a été enregistré.
- **Module** : nom du module pendant l'utilisation duquel l'événement a été enregistré.
- **Evénement** : description de l'événement enregistré, reprend le type d'événement et les informations complémentaires à son sujet.

Les entrées du volet d'administration peuvent être triées par ordre croissant ou décroissant selon les valeurs reprises dans les colonnes **Date** et **Heure**, ainsi que par ordre alphabétique pour les valeurs des colonnes **Nom du serveur** et **Module**. Pour annuler le tri des entrées, cliquez sur l'icône située à gauche du nom de la colonne.

## STATISTIQUES

Les sections des statistiques contiennent les sections suivantes :

- **Général** : statistiques complètes de la section sélectionnée, sans aucun regroupement.
- **Selon le nom du serveur** : statistiques regroupées selon le nom du serveur où les statistiques ont été enregistrées.
- **Selon la date** : statistiques regroupées selon la date et l'heure de l'enregistrement.
- **Selon l'état de l'objet** : statistiques regroupées selon l'état de l'objet (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 20).
- **Selon le nom de l'expéditeur** : statistiques regroupées selon les adresses des expéditeurs des messages infectés (uniquement pour les statistiques de la protection du courrier).
- **Selon le nom de la base de données** : statistiques regroupées selon les noms des bases de données dans lesquelles des documents infectés ont été découverts (uniquement pour les statistiques de la protection des réplications et l'analyse des bases de données).
- **Selon le nom de l'auteur des dernières modifications** : statistiques regroupées selon le nom des auteurs des dernières modifications dans le document (uniquement pour les statistiques de la protection des réplications et de l'analyse des bases de données).

Pour ouvrir la liste complète des entrées regroupées, cliquez sur l'icône . Pour réduire la liste, cliquez sur l'icône .

Les informations suivantes sont affichées pour chaque entrée :

- Icône indiquant l'état de l'objet analysé :
  - : objet supprimé ;
  - : objet réparé ;
  - : objet non analysé ;
  - : objet potentiellement infecté.
- **Date** : date d'analyse de l'objet.
- **Heure** : heure d'analyse de l'objet.
- **Nom du serveur** : nom du serveur sur lequel l'analyse a été réalisée.
- **Expéditeur** : adresse électronique de l'expéditeur du message dans lequel l'objet a été découvert.
- **Destinataires** : adresses électroniques des destinataires du message dans lequel l'objet a été découvert (uniquement pour les statistiques de la protection du courrier).
- **Nom de la base de données** : nom de la base de données dans laquelle se trouve le document analysé (uniquement pour les statistiques de la protection des réplications et de l'analyse des bases de données).
- **Module** : nom du module ayant analysé l'objet.
- **Détectés** : résultat de l'analyse de l'objet.
- **Modifié par** : nom de l'utilisateur qui a introduit les dernières modifications dans le document et nom du serveur sur lequel ces modifications ont été introduites, au format **<Nom de l'utilisateur/nom du serveur>** (uniquement pour les statistiques de protection des réplications et l'analyse des bases de données).

Les entrées du volet d'administration peuvent être triées par ordre croissant ou décroissant selon les valeurs reprises dans les colonnes **Date** et **Heure**, ainsi que par ordre alphabétique pour les valeurs des colonnes **Nom du serveur** et **Module**. Pour annuler le tri des entrées, cliquez sur l'icône située à gauche du nom de la colonne.

## CONSULTATION DU JOURNAL DES EVENEMENTS POUR LE SERVEUR

*Pour consulter le journal des événements d'un serveur en particulier,*

sélectionnez le serveur pour lequel vous souhaitez consulter des informations (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

Les entrées du journal des événements pour le serveur sélectionné s'affichent dans le volet de consultation. Les informations affichées sont les mêmes que celles du journal général des événements (cf. section "Journal des événements" à la page 81) mais seulement pour le serveur que vous avez sélectionné.

Les entrées sont regroupées par date d'enregistrement. Pour ouvrir la liste complète, cliquez sur l'icône . Pour réduire la liste, cliquez sur l'icône .

# SUPPRESSION DES INFORMATIONS DE LA BASE DE DONNEES JOURNAL DES EVENEMENTS ET STATISTIQUES

Les entrées de la base de données Journal des événements et statistiques sont automatiquement supprimées à l'issue de la durée indiquée dans les paramètres du journal des événements et les paramètres des statistiques (cf. section "Configuration des paramètres du journal des événements" à la page 77, "Configuration des paramètres des statistiques" à la page 79). Toutefois, vous pouvez le cas échéant supprimer les entrées manuellement. La suppression des entrées de la base de données s'exécute indépendamment sur chaque serveur.

*Pour supprimer manuellement des entrées de la base de données Journal des événements et statistiques, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez supprimer les entrées de la base de données Journal des événements et statistiques (cf. section "Consultation et modification des paramètres du serveur" à la page 39) (cf. ill. ci-dessous).

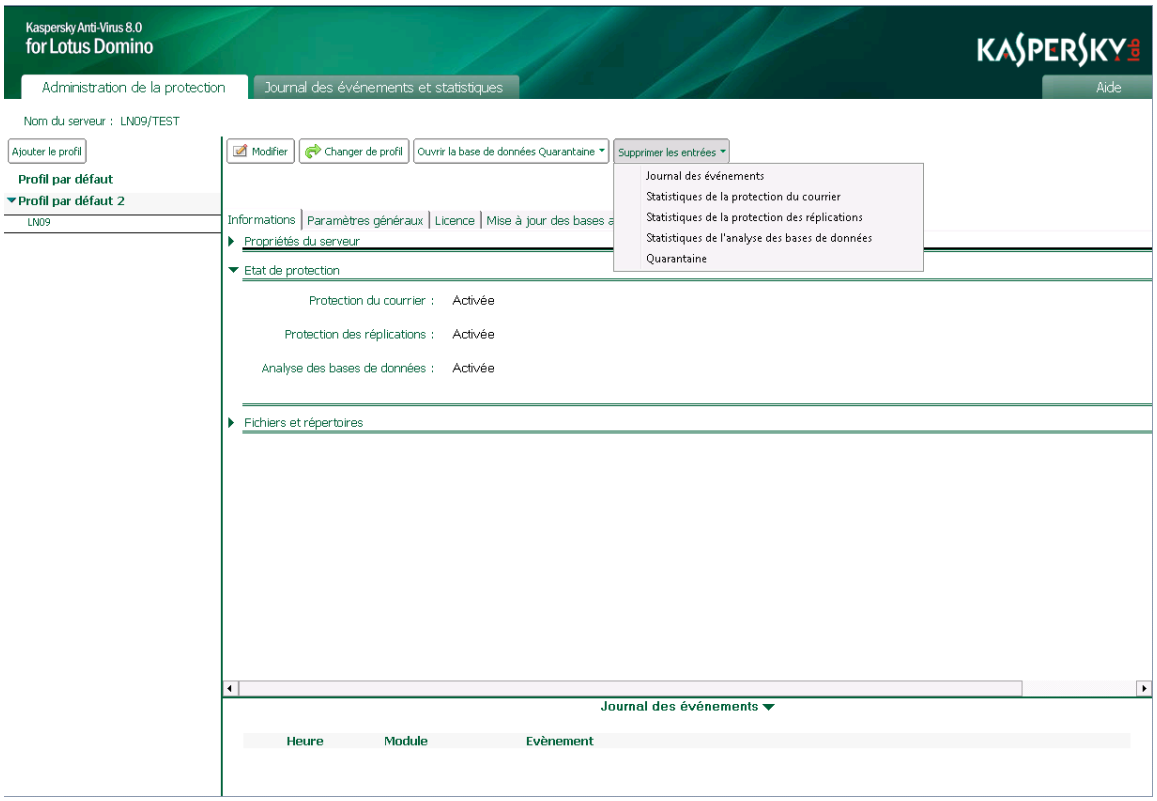


*Illustration 18. Suppression des entrées de la base de données Journal des événements et statistiques*

2. Dans le volet des actions, cliquez sur le bouton **Supprimer les entrées** et, dans la liste déroulante qui s'ouvre, sélectionnez l'un des éléments suivants :

   - **Journal des événements**.
   - **Statistiques de la protection du courrier**.
   - **Statistiques de la protection des réplications**.
   - **Statistiques de l'analyse des bases de données**.

Les informations correspondant à l'élément sélectionné seront supprimées de la base de données kaveventslog.nsf.

# NOTIFICATIONS

Vous pouvez configurer l'envoi de notifications lors de la détection par l'analyse de courriers, de réplications et de bases de données d'objets présentant les états suivants :

- *infecté ;*
- *potentiellement infecté ;*
- *protégé ;*
- *non analysé.*

La notification peut contenir des informations sur les actions exécutées sur les objets et sur les résultats du traitement des objets.

Lors de l'analyse du courrier, des informations peuvent être ajoutées au corps du message ; ceci en fonction du modèle du champ **Texte du message**. L'expéditeur et les destinataires de ce message, ainsi que les administrateurs du serveur et les administrateurs du profil auquel il appartient, peuvent recevoir une notification rédigée selon un modèle défini dans les paramètres de la protection du courrier (cf. section "Actions à exécuter sur les objets du courrier" à la page. 52).

Dans le cadre de l'analyse des réplications et des bases de données, les messages de notification peuvent être envoyés aux administrateurs du serveur et aux administrateurs du profil auquel ce serveur appartient. Les modèles des messages de notification sont définis dans les paramètres de la protection des réplications (cf. section "Actions à exécuter sur les objets lors du fonctionnement de la protection des réplications" à la page 58) et dans les paramètres d'analyse des bases de données (cf. section "Actions à exécuter sur les objets lors de l'analyse des bases de données" à la page 64).

Vous pouvez désigner les administrateurs du serveur (cf. section "Désignation de l'administrateur du serveur" à la page 89) ; ceci sous l'onglet **Informations** des paramètres du serveur, dans le groupe **Propriétés du serveur**. Vous pouvez désigner les administrateurs du profil (cf. section "Désignation de l'administrateur du profil" à la page 89) ; ceci sous l'onglet **Paramètres généraux** des paramètres du profil, dans le groupe **Sécurité**.

Les paramètres de notification sur les objets infectés, potentiellement infectés, protégés et non analysés détectés sont définis pour chaque état d'objet séparément dans les paramètres de la protection du courrier, de la protection des réplications et de l'analyse des bases de données.

Les paramètres de notification sont définis par le profil auquel appartient le serveur protégé. La configuration de paramètres individuels de notification pour chaque serveur n'est pas prévue.

*Pour configurer les paramètres de notification, procédez comme suit :*

1. Sélectionnez le profil dont vous souhaitez modifier les paramètres (cf. section "Consultation et modification des paramètres du profil" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Modifier** pour passer au mode de modification des paramètres.
3. Dans le volet des actions, sous l'onglet **Protection du courrier** ou **Protection des réplications** ou **Analyse des bases de données**, sélectionnez l'onglet **Actions**.
4. Sous l'onglet **Actions**, sélectionnez le groupe de paramètres correspondant à l'état de l'objet dont vous souhaitez configurer les notifications de détection. Vous pouvez choisir parmi les groupes de paramètres suivants :
   - **Objet infecté** : pour la configuration des paramètres de notification sur la détection des objets infectés.
   - **Objet potentiellement infecté** : pour la configuration des paramètres de notification sur la détection des objets potentiellement infectés.

- **Objet protégé** : pour la configuration des paramètres de notification sur la détection des objets protégés.
- **Objet non analysé** : pour la configuration des paramètres de notification sur la détection des objets non analysés pour cause de corruption ou de dysfonctionnement.

5. Configurez les paramètres selon lesquels les notifications relatives à l'objet détecté et aux actions exécutées seront envoyées. Pour ce faire, cochez ou décochez les cases suivantes :

   - **Ajouter une notification au corps du texte du courrier**. Kaspersky Anti-Virus ajoute des informations au corps du message ; ceci en fonction du modèle du champ **Texte du message**.
   - **Signaler à l'expéditeur**. Kaspersky Anti-Virus envoie à l'expéditeur un message électronique contenant le texte défini dans le modèle du champ **Texte du message**.
   - **Signaler aux destinataires**. Kaspersky Anti-Virus envoie un message électronique aux destinataires avec le texte défini dans le modèle du champ **Texte du message**.
   - **Signaler aux administrateurs**. Kaspersky Anti-Virus envoie un message électronique aux administrateurs du serveur et aux administrateurs du profil auquel le serveur appartient. Ce message est rédigé selon le modèle du champ **Texte du message**.

   Vous pouvez désigner les administrateurs du serveur (cf. section "Désignation de l'administrateur du serveur" à la page 89) : sous l'onglet **Informations** des paramètres du serveur, dans le groupe **Propriétés du serveur**. Vous pouvez désigner les administrateurs du profil (cf. section "Désignation de l'administrateur du profil" à la page 89) : sous l'onglet **Paramètres généraux** des paramètres du profil, dans le groupe **Sécurité**.

6. Dans le champ **Texte du message**, saisissez le texte de la notification. Vous pouvez utiliser les macros suivantes dans le texte de la notification :

   - **%v** : nom de la menace découverte dans l'objet ;
   - **%n** : nom de l'objet dans lequel la menace a été découverte ;
   - **%t** : type d'objet dans lequel la menace a été découverte : corps du message, pièce jointe ou objet OLE ;
   - **%q** : informations sur la conservation d'une copie de l'objet dans la base de données Quarantaine : **oui** , objet mis en quarantaine, **non** , objet non mis en quarantaine ;
   - **%a** : informations sur les actions exécutées sur les objets : **supprimé** : objet supprimé, **ignoré** : objet ignoré, **réparé** : objet réparé ;
   - **%S** : nom du serveur ;
   - **%P** : chemin vers la base de données dans laquelle l'objet dangereux a été détecté ;
   - **%T** : nom de la base de données ;
   - **%R** : identificateur de la réplique de la base de données ;
   - **%U** : document UNID ;
   - **%N** : document NOTEID ;
   - **%M** : date de la dernière modification du document ;
   - **%A** : auteur du document ;
   - **%E** : auteur de la dernière modification apportée au document.

7. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

# ADMINISTRATION DE LA CONFIGURATION

L'administration de la configuration de Kaspersky Anti-Virus est réalisée à l'aide des paramètres des profils et des paramètres des serveurs protégés (cf. section "Administration des paramètres de fonctionnement de Kaspersky Anti-Virus" à la page 21).

Le profil permet de définir des paramètres uniques de fonctionnement de Kaspersky Anti-Virus pour un groupe de serveurs et de créer un système de protection à différents niveaux. Les paramètres du serveur permettent de redéfinir une partie des paramètres pour chaque serveur, selon la fonction du serveur dans le réseau.

Il est possible de créer et de supprimer des profils, de déplacer des serveurs d'un profil vers un autre, de modifier les valeurs des paramètres du profil ainsi que les valeurs des paramètres du serveur.

Avant de réaliser les opérations avec les profils et les serveurs (création ou suppression d'un profil, configuration des paramètres du serveur, etc.), assurez-vous que le compte utilisateur sous lequel la base de données Centre d'administration a été ouverte possède les autorisations requises pour exécuter ces opérations.

### DANS CETTE SECTION



## CREATION ET SUPPRESSION DE PROFILS

L'autorisation de créer ou de supprimer les profils est accordée uniquement aux utilisateurs qui possèdent les privilèges des groupes fonctionnels **Administrateurs de la sécurité** et **Administrateurs du Centre d'administration** (cf. section "**Privilèges des groupes fonctionnels**" à la page 25).

*Pour créer un profil, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, cliquez sur le bouton **Ajouter le profil**.

   Les paramètres du nouveau profil s'affichent dans le volet d'administration. Le nouveau profil est créé par défaut avec les valeurs recommandées par les experts de Kaspersky Lab. Vous pouvez modifier les paramètres du profil.

3. Dans le volet d'administration, saisissez le nom du profil sous l'onglet **Informations**, dans le groupe **Propriétés du profil**, dans le champ **Nom du profil**. Le nom saisi doit être différent du nom des autres profils de la base de données Centre d'administration (cf. ill. ci-après).

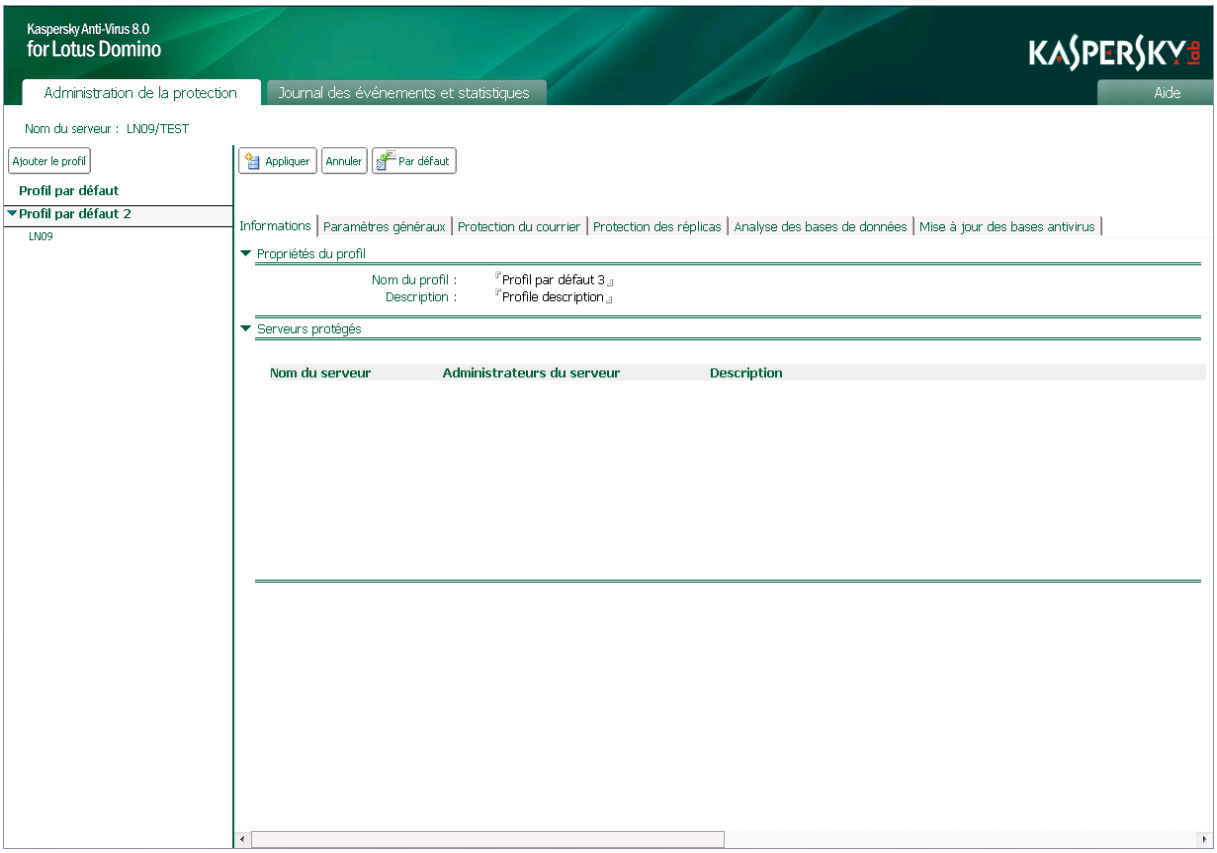


*Illustration 19. Configuration des paramètres du profil*

4. Si nécessaire, dans le champ **Description**, saisissez des informations complémentaires sur le profil.

5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

Les informations relatives au profil créé seront ajoutées à la réplique de la base de données Centre d'administration qui se trouve sur le serveur où la base de données a été ouverte. Lors de la réplication suivante, les modifications seront transmises aux autres serveurs protégés.

*Pour supprimer un profil, procédez comme suit:*

1. Sélectionnez le profil que vous souhaitez supprimer (cf. section "Consultation et modification des paramètres du profil" à la page 39).

   Avant la suppression du profil, tous les serveurs qu'il comporte doivent être déplacés (cf. section "Déplacement des serveurs vers un autre profil" à la page 90).

2. Dans le volet des actions, cliquez sur **Supprimer**.

Les informations relatives au profil créé seront supprimées de la réplique de la base de données Centre d'administration qui se trouve sur le serveur où la base de données a été ouverte. Lors de la réplication suivante, les modifications seront transmises aux autres serveurs protégés.

Il est possible de supprimer un profil à l'aide de l'option **Supprimer** du menu contextuel du profil ou à l'aide de la touche **Delete** du clavier. Dans ce cas, la suppression effective du profil se produit à la fermeture de la base Centre d'administration ou après avoir appuyé sur la touche **F9**.

# DESIGNATION DE L'ADMINISTRATEUR DE PROFIL

*Pour désigner un administrateur de profil, procédez comme suit :*

1. Sélectionnez le profil pour lequel vous souhaitez désigner un administrateur (cf. section "Consultation et modification des paramètres du profil" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Paramètres généraux**.

3. Dans le groupe **Sécurité**, indiquez le nom de l'administrateur de profil ou le nom du groupe d'administrateurs de l'une des manières suivantes :

   - Saisissez manuellement le nom de l'administrateur ou le nom du groupe d'administrateurs. Le format de l'entrée du nom de l'administrateur est hiérarchique (hiérarchie Lotus Notes, hiérarchie de l'organisation).

   - Choisissez le nom de l'administrateur ou du groupe d'administrateurs dans le Carnet d'adresses du serveur Lotus Domino. Pour ce faire, cliquez sur le bouton .

   L'administrateur de profil doit être un utilisateur qui possède les privilèges de l'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité**, **Administrateurs du Centre d'administration** ou **Administrateurs avec des privilèges restreints** (cf. section "**Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus**" à la page 25).

   Par défaut, les administrateurs du profil sont les utilisateurs ajoutés au groupe fonctionnel **Administrateurs du Centre d'administration** (cf. section "**Privilèges des groupes fonctionnels**" à la page 25) lors de l'installation de l'application.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Vous pouvez rétablir les valeurs des paramètres par défaut en cliquant sur le bouton **Par défaut**.

# DESIGNATION DE L'ADMINISTRATEUR DE SERVEUR

*Pour désigner un administrateur de serveur, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez désigner un administrateur (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Informations**.

3. Dans le groupe **Sécurité**, indiquez le nom de l'administrateur de serveur ou le nom du groupe d'administrateurs de l'une des manières suivantes :

   - Saisissez manuellement le nom de l'administrateur ou le nom du groupe d'administrateurs. Le format de l'entrée du nom de l'administrateur est hiérarchique (hiérarchie Lotus Notes, hiérarchie de l'organisation).

   - Choisissez le nom de l'administrateur ou du groupe d'administrateurs dans le Carnet d'adresses du serveur Lotus Domino. Pour ce faire, cliquez sur .

   L'administrateur de serveur doit être un utilisateur qui possède les privilèges de l'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité**, **Administrateurs du Centre d'administration** ou **Administrateurs avec des privilèges restreints** (cf. section "**Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus**" à la page 25).

   Par défaut, les administrateurs du serveur sont les utilisateurs ajoutés au groupe fonctionnel **Administrateurs du Centre d'administration** (cf. section "**Privilèges des groupes fonctionnels**" à la page 25) lors de l'installation de l'application.

4. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# DEPLACEMENT DU SERVEUR VERS UN AUTRE PROFIL

*Pour déplacer un serveur d'un profil vers un autre, procédez comme suit :*

1. Sélectionnez le serveur que vous souhaitez déplacer vers un autre profil (cf. section "Consultation et modification des paramètres du serveur" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Changer de profil**.
3. Dans la fenêtre **Changement de profil** qui s'ouvre, sélectionnez dans la liste le profil vers lequel vous souhaitez déplacer le serveur, puis cliquez sur **OK**.

Le serveur sélectionné sera déplacé dans l'autre profil. Lors de la réplication suivante, les modifications seront transmises aux autres serveurs protégés.

Si la case **Utiliser les paramètres du profil** est cochée dans les paramètres du serveur, alors les valeurs des paramètres du nouveau profil seront utilisées pour le serveur après son déplacement. Si la case **Utiliser les paramètres du profil** n'est pas cochée, les valeurs actuelles des paramètres seront conservées.

# DEFINITION DE VALEURS INDIVIDUELLES POUR LES PARAMETRES DU SERVEUR

Le serveur protégé utilise par défaut les paramètres définis par le profil auquel il appartient. Vous pouvez redéfinir certains des paramètres définis par le profil en modifiant les valeurs individuelles des paramètres du serveur.

Il est possible de redéfinir les paramètres suivants :

- Paramètres de la mise à jour:
  - source des mises à jour des bases antivirus ;
  - paramètres de la connexion à la source de mises à jour ;
  - programmation de la mise à jour ;
- Paramètres du Journal des événements et statistiques :
  - niveau de détail des informations enregistrées dans le journal ;
  - emplacement des informations sur les événements enregistrés ;
  - durée de conservation des entrées du journal des événements ;
  - durée de conservation des statistiques.

*Pour configurer les paramètres individuels de la mise à jour pour le serveur, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez définir des valeurs de paramètres de mise à jour spécifiques (cf. section "Consultation et modification des paramètres du serveur" à la page 39).
2. Dans le volet des actions, cliquez sur le bouton **Modifier** et dans le volet d'administration, sélectionnez l'onglet **Mise à jour des bases antivirus**.
3. Dans le groupe **Paramètres de la mise à jour**, décochez la case **Utiliser les paramètres du profil**.

Si la case est cochée, les paramètres de la mise à jour ne peuvent être modifiés.

4. Pour chaque serveur, configurez les paramètres de la mise à jour des bases antivirus (cf. section "Sélection de la source des mises à jour" à la page 47) ou la programmation de la mise à jour (cf. section "Mise à jour selon la programmation" à la page 48).

5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

*Pour configurer les valeurs individuelles des paramètres du Journal des événements et statistiques pour le serveur, procédez comme suit :*

1. Sélectionnez le serveur pour lequel vous souhaitez définir des valeurs de paramètres spécifiques concernant le Journal des événements et statistiques (cf. section "Consultation et modification des paramètres du serveur" à la page 39).

2. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans le volet d'administration, l'onglet **Paramètres généraux**.

3. Dans le groupe **Paramètres du journal**, décochez la case **Utiliser les paramètres du profil**.

   Quand la case est cochée, les paramètres du Journal des événements et statistiques ne sont pas modifiables.

4. Configurez les paramètres du journal des événements (cf. section "Configuration des paramètres du journal des événements" à la page 77) ou les paramètres de collecte et de conservation des statistiques (cf. section "Configuration des paramètres des statistiques" à la page 79).

5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

# ADMINISTRATION A DISTANCE DE KASPERSKY ANTI-VIRUS VIA LE NAVIGATEUR INTERNET

Lors de l'utilisation d'un déploiement distribué de Kaspersky Anti-Virus sur le réseau d'une entreprise, l'administration des paramètres de protection et des tâches principales de l'application sur l'ensemble des serveurs protégés de Lotus Domino peut être effectuée via le navigateur Internet. L'interface Web permet d'administrer Kaspersky Anti-Virus sur les serveurs protégés depuis des ordinateurs qui ne seraient pas équipés du client Lotus Notes.

Pour l'administration de Kaspersky Anti-Virus via le navigateur Internet, le serveur qui hébergera ce processus doit présenter une tâche HTTP active. Le téléchargement de la tâche HTTP sur les autres serveurs protégés n'est pas nécessaire.

L'utilisation du navigateur Internet vous permet d'exécuter les actions suivantes :

- Installer et supprimer Kaspersky Anti-Virus (informations détaillées dans le Manuel de mise en œuvre de Kaspersky Anti-Virus 8.0 for Lotus Domino).
- Activer l'application (cf. section "Application du fichier clé" à la page 31).
- Se connecter à la base de données Centre d'administration (kavcontrolcenter.nsf) (cf. section "Accès à la base de données Centre d'administration" à la page 33) et exécuter manuellement les opérations suivantes sur les serveurs protégés :
  - lancer la tâche de mise à jour des bases antivirus (cf. section "Mise à jour manuelle" à la page 49) ;
  - lancer la tâche d'analyse des bases de données (cf. section "Analyse manuelle des bases de données" à la page 68) ;
  - supprimer les entrées de la base de données Journal des événements et statistiques (cf. section "Suppression des informations de la base de données Journal des événements et statistiques" à la page 84) ;
  - supprimer les objets de la base de données Quarantaine (cf. section "Actions sur les objets placés en quarantaine" à la page 73).

# VALIDATION DE L'EXACTITUDE DE LA CONFIGURATION DE L'APPLICATION

Cette section décrit l'algorithme de vérification de l'exactitude de la configuration de l'application pour chaque module de la protection à l'aide du fichier d'essai EICAR et de ses modifications.

### DANS CETTE SECTION



## FICHIER D'ESSAI EICAR ET SES MODIFICATIONS

Ce fichier d'essai a été développé par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le fichier d'essai EICAR n'est pas un virus et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

N'utilisez jamais de virus authentiques pour vérifier le fonctionnement de votre antivirus !

Vous pouvez télécharger le fichier d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Avant de lancer le téléchargement, il est absolument nécessaire de désactiver le logiciel antivirus installé sur votre ordinateur car le fichier anti_virus_test_file.htm sera identifié et traité par l'application comme un objet infecté transmis par le protocole HTTP.

N'oubliez pas de réactiver la protection antivirus dès que le téléchargement du fichier d'essai sera terminé.

L'application identifie le fichier téléchargé depuis le site de la société EICAR comme un objet infecté par un virus qui ne peut être réparé et exécute l'action définie pour ce genre d'objet.

Vous pouvez également utiliser une modification du fichier d'essai standard afin de vérifier le bon fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il est nécessaire de modifier le contenu du fichier standard en y ajoutant l'un des préfixes présentés dans le tableau ci-dessous. Il est possible d'utiliser n'importe quel logiciel de traitement de texte ou hypertexte pour modifier le fichier de test.

Vous pouvez vérifier le bon fonctionnement de votre logiciel antivirus à l'aide d'une modification du fichier EICAR uniquement si vous possédez des bases antivirus dont la date de publication est postérieure au 24 octobre 2003 (mise à jour cumulée, octobre 2003).

La première colonne du tableau ci-dessous contient les préfixes qu'il est nécessaire d'ajouter en tête de la ligne du fichier d'essai traditionnel. La deuxième colonne reprend toute les valeurs possibles de l'état attribué par Kaspersky Anti-Virus à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de Kaspersky Anti-Virus.

Après avoir ajouté le préfixe au fichier d'essai, enregistrez le fichier, par exemple sous le nom : eicar_dele.com. Nommez tous les fichiers d'essai modifiés selon le même principe.

*Tableau 6. Modifications du fichier d'essai*

| PREFIXE | ETAT DE L'OBJET | INFORMATIONS RELATIVES AU TRAITEMENT DE L'OBJET |
|---|---|---|
| Pas de préfixe, fichier d'essai standard. | *Irréparable*.<br>L'objet contient le code d'un virus connu. Réparation impossible. | Kaspersky Anti-Virus identifie cet objet comme un virus qui ne peut être réparé et applique l'action prévue pour les objets infectés. |
| CORR- | *Corrompu*. | Kaspersky Anti-Virus a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide). |
| WARN- | *Potentiellement infecté*.<br>L'objet contient le code d'un virus inconnu. Réparation impossible. | L'analyseur heuristique attribue l'état potentiellement infecté à l'objet. Au moment de la découverte, les bases de Kaspersky Anti-Virus ne contenaient pas la description de la réparation de cet objet. L'objet est supprimé. |
| | *Potentiellement infecté*.<br>L'objet contient le code modifié d'un virus connu. Réparation impossible. | Kaspersky Anti-Virus a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'application ne contenaient pas la description de la réparation de cet objet. L'objet est supprimé. |
| ERRO- | *Erreur d'analyse*.<br>Une erreur s'est produite lors de l'analyse de l'objet. | Kaspersky Anti-Virus ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multi-volumes) ou il n'y a pas de lien vers l'objet |
| CURE- | *Réparable*.<br>L'objet contient le code d'un virus connu. | L'objet contient un virus qui peut être réparé. Kaspersky Anti-Virus répare l'objet et le texte du corps du fichier d'essai est remplacé par CURE. |

# TEST DE LA PROTECTION DU COURRIER

Pour tester la détection de virus dans les messages électroniques, vous pouvez utiliser n'importe quel système de messagerie utilisé sur un serveur Lotus Domino protégé. Il est conseillé de tester la détection des virus par Kaspersky Anti-Virus dans le corps du message, dans les fichiers joints et dans les objets OLE intégrés.

➧ *Pour vérifier la découverte de virus dans un message électronique, procédez comme suit :*

1. Créez un message au format **Texte normal**.
2. Placez le texte du fichier standard ou modifié au début du message et joignez au message un fichier ou un objet OLE contenant le fichier d'essai.
3. Envoyez le message à une adresse qui vous convient, par exemple l'adresse de l'administrateur du serveur ou de l'administrateur du profil auquel le serveur appartient.
4. Lisez le contenu du message qui parvient à cette adresse.

Kaspersky Anti-Virus détecte l'objet, l'identifie comme *infecté* et, en cas d'utilisation d'un fichier de test modifié, l'identifie en fonction du préfixe utilisé (cf. section "Fichier d'essai EICAR et ses modifications" à la page 93). Ensuite, l'application exécute l'action sélectionnée dans les paramètres de protection du courrier pour les objets de ce type. Par défaut, les objets infectés et que Kaspersky Security ne peut pas réparer sont supprimés du courrier.

# TEST DE LA PROTECTION DES REPLICATIONS

Il est conseillé de tester la détection des virus par Kaspersky Anti-Virus dans le texte des documents aux formats Rich Text et MIME, dans les fichiers joints à ces documents et dans les objets OLE intégrés.

*Pour vérifier la détection de virus lors de la réplication des bases de données, procédez comme suit :*

1. Sélectionnez le serveur non protégé avec lequel la réplication est configurée sur le serveur protégé.
2. Exécutez l'une des actions suivantes :
   - Sélectionnez, sur le serveur concerné, la base de données dont la réplique se trouve sur le serveur protégé, puis choisissez le document contenant les champs RTF et MIME.
   - Créez sur le serveur non protégé une base de données à partir de l'un des modèles proposés, puis, sur le serveur protégé, créez la réplique de cette base. Enfin, créez dans la base du serveur non protégé un document contenant les champs RTF et MIME.
3. Placez le texte du fichier d'essai standard ou modifié dans les champs RTF et MIME du document sélectionné.
4. Ajoutez au document sélectionné un fichier et un objet OLE contenant le texte du fichier d'essai standard ou modifié.

À la prochaine réplication, Kaspersky Anti-Virus détectera les objets, les identifiera comme *infectés* et, en cas d'utilisation d'un fichier de test modifié, les identifiera en fonction des préfixes utilisés (cf. section "Fichier d'essai EICAR et ses modifications" à la page 93). Ensuite, l'application exécutera les actions sélectionnées dans les paramètres de la protection des réplications pour les objets de ce type. Par défaut, les objets infectés que Kaspersky Anti-Virus ne peut pas réparer sont supprimés, les informations relatives à la détection et à l'action exécutée sont consignées dans la base de données Journal des événements et statistiques et un message d'avertissement est envoyé aux administrateurs du serveur et aux administrateurs du profil auquel ce serveur appartient.

Lisez les statistiques de la protection des réplications et consultez les messages envoyés aux administrateurs.

# TEST DE L'ANALYSE DES BASES DE DONNEES

Il est conseillé de tester la détection des virus par Kaspersky Anti-Virus dans le texte des documents aux formats Rich Text et MIME, dans les fichiers joints à ces documents et dans les objets OLE intégrés.

*Pour vérifier la découverte de virus pendant l'analyse des bases de données, procédez comme suit :*

1. Exécutez l'une des actions suivantes :
   - Sur le serveur protégé, sélectionnez la base de données, puis choisissez un document contenant des champs RTF et MIME.
   - Créez une base de données sur la base de l'un des modèles existants et créez-y un document contenant des champs RTF et MIME.
2. Placez le texte du fichier d'essai standard ou modifié dans les champs RTF et MIME du document sélectionné ou créé.
3. Ajoutez au document sélectionné un fichier et un objet OLE contenant le texte du virus d'essai standard ou modifié.

À la prochaine analyse des bases de données, Kaspersky Anti-Virus détectera les objets, les identifiera comme *infectés* et, en cas d'utilisation d'un fichier de test modifié, les identifiera en fonction des préfixes utilisés (cf. section "Fichier d'essai EICAR et ses modifications" à la page 93). Ensuite, l'application exécutera les actions sélectionnées dans les paramètres de l'analyse des bases de données pour les objets de ce type. Par défaut, les objets infectés que Kaspersky Anti-Virus ne peut pas réparer sont supprimés, les informations relatives à la détection et à l'action exécutée sont consignées dans la base de données Journal des événements et statistiques et un message d'avertissement est envoyé aux administrateurs du serveur et aux administrateurs du profil auquel ce serveur appartient.

Lisez les statistiques de l'analyse des bases et consultez les messages envoyés aux administrateurs.

# UTILISATION VIA LA CONSOLE DU SERVEUR

Vous pouvez administrer certaines fonctions de Kaspersky Anti-Virus via la ligne de commande de la console de serveur Lotus Domino. Cette section reprend les instructions système qui permettent d'administrer les fonctions principales de Kaspersky Anti-Virus.

Les instructions système sont saisies uniquement pour la tâche kavcontrol sur chaque serveur protégé séparément.

L'instruction doit respecter la syntaxe suivante :

```
tell kavcontrol <instructions> [<paramètre>]
```

où :

- `<instruction>` est l'instruction de Kaspersky Anti-Virus ;
- `<paramètre>` désigne le paramètre indispensable à l'exécution de l'instruction (le cas échéant).

S'il est nécessaire de définir pour le paramètre un chemin d'accès à un fichier ou à un répertoire, il convient de respecter les règles de formation des chemins d'accès du système d'exploitation installé sur le serveur. Si le chemin d'accès au fichier contient un espace, le chemin d'accès complet devrait être saisi entre guillemets doubles. Ces guillemets ne doivent pas être séparés du paramètre par un espace. Un espace est nécessaire entre le paramètre et l'instruction.

**Exemple :**

Correct :

```
tell kavcontrol addkey "/home/username/my key"
```

Incorrect :

```
tell kavcontrol addkey " /home/username/my key"
```

Le tableau ci-après reprend la liste des instructions de Kaspersky Anti-Virus.

*Tableau 7. Instructions de Kaspersky Anti-Virus*

| INSTRUCTION | PARAMETRES | ACTION |
|---|---|---|
| Help | | Afficher les commandes disponibles. |
| addkey | <chemin_complet_au_fichier_de_licence_sur_le_serveur> | Ajouter un fichier clé. |
| delkey active | | Supprimer le fichier clé actif. |
| delkey reserve | | Supprimer le fichier clé complémentaire. |
| delkey both | | Supprimer les deux fichiers clés. |
| license | | Afficher les informations sur le fichier clé actif. |
| Start KAVScanner<br>Start KS | | Lancer l'analyse des bases de données. |
| Stop KAVScanner<br>Stop KS | | Arrêter l'analyse des bases de données. |

| INSTRUCTION | PARAMETRES | ACTION |
|---|---|---|
| Pause KAVScanner<br>Pause KS | | Suspendre l'analyse des bases de données. |
| Resume KAVScanner<br>Resume KS | | Reprendre l'analyse des bases de données. |
| Start KAVUpdater<br>Start KU | | Lancer la mise à jour des bases antivirus. |
| Stop KAVUpdater<br>Stop KU | | Arrêter la mise à jour des bases antivirus. |
| Version | | Afficher le numéro de la version de Kaspersky Anti-Virus installée sur le serveur. |
| Status | <nom_du_service>/ absence de paramètre | Permet de consulter les informations sur l'état du service indiqué ou de tous les services. |

# CONTACTER LE SERVICE DE SUPPORT TECHNIQUE

Cette section présente les différentes méthodes d'obtention du Support Technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Service de Support Technique.

### DANS CETTE SECTION



## MODES D'OBTENTION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans l'une des sources d'informations relatives à l'application (cf. section "Sources d'informations sur l'application" à la page 10), contactez le Service de Support Technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le Support Technique, veuillez lire les règles d'octroi du Support Technique (http://support.kaspersky.fr/support/rules).

Vous pouvez contacter les experts du Service de Support Technique de l'une des manières suivantes :

- Par téléphone. Vous pouvez contacter les experts du Service de Support Technique en France.
- En envoyant une demande depuis Kaspersky Company Account sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Service Support Technique via un formulaire.

Le support technique est fourni uniquement aux utilisateurs de l'application ayant acheté une licence. Le support technique n'est pas prévu pour les utilisateurs d'une version d'évaluation.

## ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique français http://support.kaspersky.com/fr/b2b.

Avant de contacter le Service de Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique(http://support.kaspersky.com/fr/support/rules). Nos experts pourront ainsi vous venir en aide plus rapidement.

## OBTENTION DU SUPPORT TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky Company Account (https://companyaccount.kaspersky.com) est un service Web conçu pour l'envoi de demandes à Kaspersky Lab et le suivi de leur traitement par les spécialistes.

Pour accéder à Kaspersky Company Account, il vous est demandé de vous inscrire. Vous pouvez vous inscrire seul sur la page d'inscription (https://support.kaspersky.com/companyaccount/registration?LANG=fr) ou par l'intermédiaire d'un utilisateur enregistré disposant des droits d'administrateur sur le compte utilisateur de votre entreprise dans Kaspersky CompanyAccount.

Dans Kaspersky Company Account, le compte utilisateur de votre entreprise est créé dès le premier enregistrement de la licence Kaspersky Company Account acquise par votre société. Tous les employés enregistrés dans Kaspersky Company Account sont associés à ce compte utilisateur.

Si un nouveau compte utilisateur est créé pour votre entreprise lors de l'inscription à Kaspersky CompanyAccount, les privilèges concernant son administration vous sont attribués par défaut. Il s'agit des privilèges couvrant l'ensemble des actions possibles avec ce compte utilisateur. Si, lors de l'inscription, vous vous ajoutez à un compte utilisateur existant, des privilèges restreints vous sont attribués par défaut.

Pour en savoir plus sur Kaspersky Company Account et sur les actions qu'il vous permet de réaliser, consultez la page du site Internet du Support Technique http://support.kaspersky.com/fr/faq/companyaccount_help.

### Demande adressée par email au Support Technique

Vous pouvez envoyer une demande par email au Service de Support Technique en anglais, en russe et dans d'autres langues.

Lors de la soumission d'une demande, spécifiez les renseignements suivants :

- type de demande ;
- nom et version de l'application ;
- texte de la demande.

Si nécessaire, vous pouvez également joindre des fichiers au formulaire de demande électronique.

Un spécialiste du Service de Support Technique vous répond via le système Kaspersky Company Account à l'adresse électronique que vous avez indiquée lors de l'inscription.

### Demande adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Service de Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivants au laboratoire d'étude des virus :

- si vous suspectez que le fichier ou la ressource Web contient un virus mais que Kaspersky Anti-Virus ne détecte aucune menace. Les experts du laboratoire d'étude des virus analysent le fichier ou l'URL envoyé et, en cas de découverte d'un virus inconnu jusque-là, ils ajoutent les informations le concernant à la base des données accessible lors de la mise à jour des applications antivirus de Kaspersky Lab ;
- si Kaspersky Anti-Virus identifie un fichier ou une ressource Web comme porteur d'un virus mais que vous êtes sûr que ce n'est pas le cas.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus via le formulaire de demande (https://my.kaspersky.com/fr/kpc/newrequest) sans vous enregistrer dans Kaspersky CompanyAccount.

# GLOSSAIRE

## A

### ARCHIVE

Un ou plusieurs fichiers regroupés dans un même fichier compressé. Pour la compression ou la décompression de telles données, une application spécifique appelée compresseur est indispensable.

## B

### BASES ANTIVIRUS

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Ces bases antivirus sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

### BALAYAGE PROGRESSIF

Analyse sélective des fichiers. Lors du balayage progressif, l'application analyse uniquement les fichiers modifiés depuis la dernière analyse.

## D

### DUREE DE VALIDITE DE LA LICENCE

La durée de validité de la licence est la période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. La quantité de fonctions accessibles et de services complémentaires dépend du type de licence.

## M

### MASQUE DE FICHIER

Représentation du nom d'un fichier par des caractères génériques. Les caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quel caractère et ? représente un caractère unique).

### MISE A JOUR DES BASES

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

## O

### OBJET INFECTE

Objet dont un segment de code correspond parfaitement à un segment de code d'une application connue présentant une menace. Les experts de Kaspersky Lab déconseillent l'utilisation de tels objets.

### OBJET OLE

Objet rattaché à un autre fichier ou intégré à un autre fichier à l'aide de la technologie Object Linking and Embedding (OLE). Par exemple, un objet OLE peut être un tableau Microsoft Office Excel®, intégré à un document Microsoft Office Word.

### OBJET POTENTIELLEMENT INFECTE.

Objet dont le code contient un extrait modifié de code d'un programme dangereux connu ou objet dont le comportement évoque un tel programme.

## P

### PAQUET DE MISES A JOUR

Paquet de fichiers pour la mise à jour des modules de l'application. L'application de Kaspersky Lab copie les paquets de mise à jour depuis les serveurs de mises à jour de Kaspersky Lab, puis les installe et les applique automatiquement.

## Q

### QUARANTAINE

Dossier dans lequel l'application de Kaspersky Lab place les objets potentiellement infectés détectés. Les objets en quarantaine sont enregistrés sous forme chiffrée pour éviter toute action de leur part sur l'ordinateur.

## R

### REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Il n'est pas possible de réparer tous les objets infectés.

## S

### SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab à partir desquels les applications de Kaspersky Lab reçoivent les mises à jour des bases et des modules de l'application.

# KASPERSKY LAB ZAO

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

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

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

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

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

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

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

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

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

| | |
|---|---|
| Site de Kaspersky Lab : | http://www.kaspersky.com/fr |
| Encyclopédie des virus : | http://www.securelist.com/fr |
| Laboratoire d'étude des virus : | newvirus@kaspersky.com (uniquement pour l'envoi d'objets potentiellement infectés sous forme d'archive) |
| | https://my.kaspersky.com/fr/kpc/newrequest |
| | (pour les questions aux experts antivirus) |
| Forum de Kaspersky Lab : | http://forum.kaspersky.fr |

# INFORMATIONS SUR LE CODE TIERS

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

# NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Google Chrome est une marque de Google, Inc.

Intel et Pentium sont des marques déposées de Intel Corporation aux Etats-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans d'autres pays.

Lotus, Domino et Lotus Notes sont des marques commerciales d'International Business Machines Corporation enregistrées dans de nombreuses juridictions à travers le monde.

Excel, Internet Explorer, Microsoft, Windows et Windows Server sont des marques déposées de Microsoft Corporation aux Etats-Unis et dans d'autres pays.

Mozilla et Firefox sont des marques de Mozilla Foundation.

Novell est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

Red Hat et Red Hat Enterprise Linux sont des marques commerciales de Red Hat Inc. déposées aux Etats-Unis et dans d'autres pays.

# INDEX

## O



## P



## Q



## S



## V